Message

Cybersecurity is a necessary consideration for individuals and families, as well as businesses, governments, and educational institutions. It’s a 21st century war in which national security, the economy and critical infrastructure are at risk.

No culture can be made secure without understanding human behaviour and motivation. Moreover, people, given the right level of understanding and awareness, can be engaged as a positive force in the quest for improved security. It is inspirational to find that that IITM group of institutions is providing a platform to bring together industry, academia and government to exchange views and enable a joint, assiduous and speedy effort to step up awareness among people in this direction. This is a promising indication that the science of cyber security is gaining momentum in India.

The national conference addresses the dynamics of the current concerns and challenges, upcoming developments in the sphere of cyber security and allied areas, besides the underlying potentials of modern software processes and practices to combat threats in cyber space. It provides a common platform for the research community and academia to exchange ideas on ongoing developments in the realm of cyber security.

I commend the IITM group of institutions for their effort to address the threat to cyber security in its numerous aspects and wish them all success in their future endeavours.

T. N. Chaturvedi
MESSAGE

Cyber Security inevitably assumes an important role to protect the evolving modern information society. The current Cyber Security infrastructure is the thread through which all critical national infrastructures such as banking, finance, energy, communication, commerce to name a few are woven together. Existence of a trustworthy cyber security infrastructure is a precondition for all E-governance and E-commerce initiatives being taken world over.

The failure to meet an expected service level might have a significant impact on the society. An emerging issue is that infrastructures, until now independent, are becoming entangled into network-of-networks. It is this interconnection where the information and communication technologies play a pivotal role. The information technology has changed the way business is transacted, government operates, and national defense is conducted. We must make continuous and consistent efforts to secure information system for emergency preparedness communications, and the physical assets that support such systems.

I appreciate the efforts of the IITM Group of Institutions to have taken initiative and given a serious thought to this issue among others as the cyber threat has taken the dimension of a national threat and it is imperative to spread the awareness and underline the importance of cyber security in the community.

I congratulate IITM Group of Institutions and wish the conference a great success.

President
Mata Leelawati Shikshan Sansthan
# CONTENTS

## Research Papers & Articles

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Enhancement in Wireless Menu Card with Network Attached Storage</td>
<td>Stuti Saxena, Nargish Gupta, Sumit Gupta</td>
<td>3-7</td>
</tr>
<tr>
<td>using DSR Protocol and Ant Colony Optimization Technique: A Review</td>
<td>Hashneet Kaur, Hardeep Kaur</td>
<td></td>
</tr>
<tr>
<td>E-Commerce Frauds Using Parallel Imports</td>
<td>Kartik Durga, Prachi Aggarwal, Anil Kumar</td>
<td>12-15</td>
</tr>
<tr>
<td>Big Data and Cloud Security</td>
<td>Sakshi Dewangan, Rajesh Singh Negi</td>
<td>16-24</td>
</tr>
<tr>
<td>An Effective Approach towards Encryption of Limited Data</td>
<td>Ruchi Kawatra, Sapna Arora Saini</td>
<td>32-36</td>
</tr>
<tr>
<td>Vulnerabilities of Data Storage Security in Big Data</td>
<td>Govind Murari Upadhyay, Harsh Arora</td>
<td>37-41</td>
</tr>
<tr>
<td>Cyber Security and Big Data Analytics</td>
<td>Priya Bhardwaj, Nidhi</td>
<td>42-45</td>
</tr>
<tr>
<td>Comparative Analysis of Visual Cryptography Schemes</td>
<td>Pramod Kumar Soni, Madhu Chauban</td>
<td>46-51</td>
</tr>
<tr>
<td>Securing Database using SQL Injection: A Review</td>
<td>Isha Shingari, Priti Sharma</td>
<td>52-56</td>
</tr>
<tr>
<td>Survey on Cloud Computing Security Issues</td>
<td>Amanpreet Kaur Sara</td>
<td>57-61</td>
</tr>
<tr>
<td>Title</td>
<td>Authors</td>
<td>Pages</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Cyber Crime – A Threat to Mankind</td>
<td>Charul Nigam, Vaishali Singhal</td>
<td>74-78</td>
</tr>
<tr>
<td>Enhancing ATM Security Using Fusion of Biometric Techniques</td>
<td>Sakshi Singh, Simranjeet Kaur</td>
<td>79-82</td>
</tr>
<tr>
<td>Comparative Analysis of IDS Approaches and their Techniques</td>
<td>Osheen, Manpreet Singh, Raj Kumar Singh</td>
<td>83-88</td>
</tr>
<tr>
<td>Big Data Security</td>
<td>Dr. Prerna Mahajan, Geetika Gaba, Nagendra Singh Chauhan</td>
<td>89-94</td>
</tr>
<tr>
<td>Biometrics: Human Body as a Password</td>
<td>Shriya Jain, Ruby Dhaiya, Ashi Chauhan</td>
<td>95-99</td>
</tr>
<tr>
<td>Artificial Intelligence Impact on Cyber Security</td>
<td>Eshita Madhok, Ashutosh Gupta, nidhi Grover</td>
<td>100-107</td>
</tr>
<tr>
<td>A Comprehensive Study of Contemporary Tools and Techniques</td>
<td>Dhananjay, Aishwarya Raman, Sheetal Kaushik</td>
<td>108-120</td>
</tr>
<tr>
<td>Comparative Analysis of Intrusion Detection System Schemes for MANETs</td>
<td>Ruby Dahiya, Manpreet Singh, Mohit Jalan</td>
<td>121-124</td>
</tr>
<tr>
<td>Scientific Research and Development of Mobile Application</td>
<td>Dimple Chawla, Rahul Aggarwal, Akansha Aggarwal</td>
<td>125-131</td>
</tr>
<tr>
<td>Cyber Security: A Brief Encounter</td>
<td>Anil Kumar Pandey</td>
<td>132-133</td>
</tr>
</tbody>
</table>
Security Enhancement in Wireless Menu Card with Network Attached Storage

Stuti Saxena*
Nargish Gupta**
Sumit Gupta***

Abstract

The presence of cellular technology and the development of portable devices provide a transparent yet potential framework for business purpose applications. M-commerce is considered as the new phase of e-commerce. This research work intends to propose a wireless menu card (WMC) for food chains. It refers that order will be placed using personal digital assistants (PDAs) such as Tablets or smart phones. This system will be using Wi-Fi storage device or say Network attached storage (NAS) which is virtually implemented on cloud through which you can store large data. So, through the use of PDAs and Wi-Fi storage device the system can provide increased capability, security, saving time, reduced human errors and hence will be able to provide better quality of service.

Keywords: smart phones, Wi-Fi storage device, mobile application, wireless technology, business application, personal cloud, network attached storage.

I. Introduction

In today's ambitious world, people desire everything to take place at their door steps. The knowledge or material which is saved in the system can be perceived over the mobile by the person anywhere in the world. This encourages more to move towards wireless technology as the peoples are able to obtain information anytime anywhere [1].

Now a day there is an increase in users every day due to the fast growth in Wi-Fi telecommunication and cyberspace [4]. Since mobile devices are becoming smaller, economical, better and more linked, they are modifying the way people using and work with data. The ease and dynamic functionality provided by mobile devices, has lead to the inspiration for many industries to interrogate the benefits of using them. Connectionless and handheld devices are gaining attention as vendors are using the common points of over tone computing, instant delivery and information can be accessed anytime, anywhere [3].

As the wireless menu card system focusing on the food chain, so without any technology, when customer places order the attendant needs to pen down orders. Then this order is taken to the kitchen, receipt is generated, and place the requested menu. Such procedure view simple and easy, but this system leads to human mistakes in communicating order when there is increase in customer’s number in course of peak hours and also increases the work load on attendants [6]. Thus to avoid all this problem the wireless menu card system uses tablets and Wi-Fi storage device.

In today's time, smart phones are proficient of giving connectivity where ever they are located along with supporting ranges of services and applications. They are furnished with any wireless interfaces which can be jointly oppressed to develop advanced enhancement techniques that can increase throughput, improve quality, capability [2]. The combination of mobile and Wi-Fi technologies can promote pervasive platform for developing business purpose applications [6].

Use of Wi-Fi storage device is just for creating your own personal cloud with network attached storage. When we accumulate anything “in the cloud”, such as storing music files, movies, documents and data on
gigantic internet servers around the world. That way you can approach to your files wherever you are, whenever you want, on your laptop or smart phone or even a different computer. This is the basic idea of cloud storage.

A personal cloud is necessarily your very own cloud storage [8]. Instead of using public clouds, a personal cloud helps you to manage all your information in one secure place on your network so that you can share data, multimedia files, and access your content pervasively.

You can build your own personal cloud by either using a Network Attached Storage (NAS) or by granting to an online cloud storage service. There are several benefits of using a NAS as your personal cloud. For example, there is no need of monthly fees or due to growth in data there are no increase costs. Also, you had an exact idea about your data that where it is and how or who can access it.

Use of mobile telecommunication may tend to two kinds of effects on business purpose operations:

- It eases the connection among employee, customer and owner. As a result better communication can increases the capability and profitability.
- Due to changing data access patterns it renovates business processes [5].

II. Related Work

To improve the traditional food ordering system many previous work had been made by using wireless technology, such as iMenu[7], FIWOS [3], and WOS [4]. Many lounges and restaurants had implemented and developed many PDA-based mobile applications for commercial use. Easy-Order is an initial e-commerce approaches developed on pervasive technology designed to combine with mainframe computers. iMenu is an initial wireless web-based approach for ordering system which builds pervasive computing systems using connectionless multi-tiered internet framework [7].

Color by the Bay (CBTB) is another PDA-based connectionless food ordering system which is used at Singapore. In this system the users at CBTB can give order with the help of PDA provided by the restaurant. When the customer is over with his/ her ordering process. These details are sent to the server from the device. Now the PDA used by a user is to be taken by the waiter to be utilized by the other user. Thus CBTB, iMenu, WOS and FIWOS are good solution for the problems of traditional food ordering system. But these systems have some limitations, so to overcome this other system was developed called CWOS-RTF [6]. In this system the problem of the waiter and the administrator is reduced as they had introduced the smart phones. Smart phone converges two portable technologies i.e. Cell phones and PDAs to produce products. CWOS-RTF consists of four modules.

- The application for user's to make order in smart phones.
- The web application for keeping track by the owner.
- The database for owner to maintain the order details, and to update the menu.
- The connectionless framework to support network communications.

Now waiter need not to roam about to take order the customer will themselves place an order using their own smart phones. Thus in this now the customer must possess the smart phones, this leads to its limitation.

Smart phone technologies are implemented to support telemedicine services for different health problems like urinary incontinence, diabetes and blood coagulation. There are powerful smart phone applications refined for healthcare purposes to detect the heart failure, to monitor medicine intake, and to confront the obesity challenges etc [9]. There is a system called Wedjat [10]. This system is developed to issue reminders to patients, record time of medicine in-take informs medicine intake directions, and informs medicine intake directions. Moreover, machine vision can also be combined with smart phones to perceive traffic signage for safety at road [11]. Disaster Alert System is one of the smart phone applications that can provide effective measures in detecting disaster situations [12]. The smart phones also fulfill the graphical demands of the customers.

Concentrating on the discussed limitations, we proposed our work. We had also used smart phones as
tablet. In this the customer’s not having smart phones can also place order as all the tables will have their own tablets provided by the food outlet itself.

III. Proposed Work
As we have already discussed the conventional food ordering system i.e. taking note of customer’s order using paper and pen. These systems are usually prone to manual mistakes. Order can be mislaid or even wrongly noted at the time of rush. Receipts are generated in written form which leads to difficulty in maintaining record for future use. The objective of this proposed system is to overcome such hassle and the limitation of related work. In our Wireless Menu Card (WMC) system we had different modules:

- Use of Wi-Fi storage device as a network attached storage.
- An Application for tablets which can read the content from NAS for customer’s to make order.

- A Desktop Application for owner to make updating in storage device and to see details.

As we have mentioned that we are using Wi-Fi storage device. This device helps us to create our own personal cloud with network attached storage. That way we can approach to our files wherever we are, whenever we want. Instead of using public clouds, a personal cloud helps you to manage all your information in one secure place on your network so that you can share data, multimedia files, and access your content pervasively.

An Application for tablets which can read the content from NAS for customer’s to make order. Thus we will develop an application which can easily read the data from Wi-Fi Storage device. The Application will do the following activities:

- Must display the name of the storage device in range
- Upon selecting the particular storage device the content from the Wi-Fi device will be displayed on the screen on welcome screen.

![Fig. 1: Flow of process at user side](image-url)
Once user taps the welcome screen it should show the list of categories in a drop down list with related food items ex: Starters, Drinks and Main Course etc.

Once the user selects a category (Ex Starter from above example), it should show the list of items from that category – this screen must have a back/home button.

Once user selects an item, the product details should be displayed (ex: an image of the product, more description, etc.) – this screen must have back/home navigation button.

Now the user can place the order through the tablet. The order will be received at the kitchen end. The Desktop Application will be a simple, easy to use application installed in each food outlet so they can easily update the menu on-demand on their own. This application will be cloud enabled and it will update the content in Wi-Fi storage device. However, this application should adhere to the following high level standard requirements:

- Authentication (so that only manager’s can update the menu).
- Once the restaurant owner makes the changes in the desktop application, there should be a button which allows the manager to publish the content to the device.
- This content must be encrypted in a bundle and the file format should be readable by the mobile app and desktop application only.
- Owner should have ability to add any number of categories, items, columns, etc. And the App should be intelligent enough to accommodate these changes.

As this wireless menu card system is basically focusing on the food outlets. Thus, when a customer will come to food outlets there will be a tablet on their table which will show the outlets name. Then the customer will select the respective outlet in which he/she interested to order and will place the order. The device will show all the respective menu details with the resent offers. If there is any changes in the menu any day the respective content will be updated with the help of desktop application.

**IV. Conclusion**

In this paper, we have proposed a wireless menu card system with network attached storage. We have focused on use of smart phones i.e. tablet in place of using PDAs to provide efficient interface for customers to order and view menu. With Wi-Fi storage device we have introduced network attached storage to store data on private cloud. This system also overcomes the limitation that every customer must carry its own smart phone instead in this it will be provided by the food outlet itself. Thus through this system we had tried to improve the service efficiency.
References


Hashneet Kaur*
Hardeep Kaur**

Abstract
Ad Hoc Networks (MANETs) are self-organized network where nodes are free to move in any direction. MANET doesn’t need any centralized system. Due to its dynamicity, Black hole attack is a serious security issue to be resolved. It takes place when a malicious node called as black hole enters into the network. Black hole node shows its fake behaviour during the process of route discovery. Today, many prevention techniques have been proposed for MANET. However, in the presence of fake nodes, the networks are subjected to different kinds of attacks. In this problem, a fake node advertises itself of having a shortest path to another node whose packets the fake node want to drop. In this flooding process, if the reply from the actual node reaches later than the fake node reply as requested by the main node. A forging path is created via a fake node. An ideal path is one in which the packet reach to destination with minimum delay and lesser overhead. In this paper we apply Dynamic Source Routing (DSR) protocol in order to prevent black hole attack using Ant Colony Optimization.

Keywords: Black Hole Attack, Dynamic Source Routing, Ant Colony Optimization.

I. Introduction
Whenever a node requires sending data from source to destination, it runs an appropriate path finding algorithm.

Hence in addition to acting as hosts, each mobile node does the function of routing and forward messages for other mobile nodes [1]. Most important networking operations include routing and network management [2]. There are three types of routing protocols broadly classified as proactive routing protocol, reactive routing protocol, Hybrid routing protocol.

II. Routing Protocols
In order to find out suitable routes between communication nodes routing protocols act as second hand. It is a self-directed collection of mobile users that speak moderately over bandwidth constraint wireless link [3]. THE network topology keeps on changing unpredictably over time and place as nodes are free to move. The network is de-centralized and all the network activities like discover the topology and delivering messages must be execute by the nodes [4]. Routing protocols are broadly classified into two categories mainly [proactive, reactive].
III. Adhoc Routing Protocol

1. Proactive Routing Protocol (mainly table driven):- WRP, DSDV, CGSR.

2. Reactive Routing Protocol (on demand):- DSR, AODV, TORA, ABR.

DSR (Dynamic Source Routing): DSR is an on-demand routing protocol having Route Discovery and Route Maintenance it’s two parts. In DSR, when a node wants to send a packet from the source who does not have a path to reach the destination in its route cache memory, the source node will initiates a Route Discovery in order to find out a route between source and destination and that node is known as the source target, and the destination where the packet is to reach is known as the Destination target. In the route discovery process the source node will generate a route request with unique id and broadcast that packet to all the nearby nodes. Here each node will receive the Route Request and check whether it has recently seen the route request or not. If the node already seen that request it will discards. Otherwise, it will check in its route cache memory whether it has a route to the destination or not. When the Request reaches the destination, the destination node will sends a Route reply back to the source node, and giving a copy of the list of route record from the route Request. The source node will update the new route in its Route Cache memory after having a reply from the destination node.

But when the topology is changing or the link between source and destination is broken. It leads to the failure in the communication between the source node and the destination node and thus route maintenance mechanism is involved in this. In order to transfer the packet, it will find out another relevant path toward the destination and if it fails to find out the path, it will again attempt the new route discovery in order to find out the new path towards the destination.

IV. Black Hole Attack

Black Hole Attack is one of the serious attacks in mobile ad-hoc network. In Black Hole attack, a single or multiple nodes starts dropping the message packets before it reached to the final destination [5]. In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the packets. The
black hole attack is broadly classified into two types (i) single black hole attack in which a single fake node will drop the packets and (ii) gray black hole attack in which more than one node act as a fake node and drop the packet. Black hole attack mainly involved two properties. It will advertise itself to the source node as having a valid route through it toward the destination. Even though the route is fake. The fake node will DROP the obstruct packet.

Black hole attack is also known as sleep deprivation attack and it can be generated internally as well as externally.

In internal black hole attack the fake node is within the network itself and drops the packet.

In external black hole attack the node is outside the network and through external process it will drop the packets.

V. Black Hole Preventative Technique Ant Colony Optimization

ACO is a famous swarm intelligence approach, has taken the inspiration from real ants who are wandering around their nests to forage for search of food. The basic idea of the ant colony optimization meta-heuristic is taken from the food searching behavior of real ants. This behavior of the ants can be used to find the shortest path in networks. Between the nest and the food source. For finding the shortest path, a volatile chemical solution known as pheromone is secreted by ant. It takes place when an ant is returning back to the nest after finding food and leave the trail of pheromone. Ants can also smell pheromone and tend to follow with higher probability those paths characterized by strong pheromone concentrations. The ants are known as the small control packet with unique identity which is used to find the path toward their destination. Because of its robustness, and adaptive nature, ACO can find its applications in routing, assignment & scheduling. It is also widely used in bio-informatics and communication networks.

VI. Conclusion

BLACK hole attack is the major issue in mobile adhoc network. Many different researchers proposed various techniques for the prevention of black hole attack. In
In this paper, the reactive routing algorithm i.e., DSR is used which will eliminate the routing overhead problem because of its on-demand process, along with ant colony optimization. The optimization technique used is iterative in nature. Many different techniques have been proposed in ad-hoc networks that determine the path and transmission of data which leads to the loss in packet. More than 15 years of its studies both the productiveness and conceptual background have been revealed, thus making ACO an effective technique for the transfer of data with less packet loss as well as lower overhead problem.

References
E-Commerce Frauds Using Parallel Imports

Kartik Durga*
Prachi Aggarwal**
Anil Kumar***

Abstract
In this paper, we will discuss about the frauds in e-commerce, which uses the concept of parallel imports. We will discuss how the import duties are being bypassed on an international level, resulting in the loss of millions and billions of dollars to government. This may be regarded as the dark side of E-Commerce. Millions and billions worth of import duties and taxes are being bypassed illegally and no one has any clue about it. Paper is organized in V different Sections.

Keywords: E-Commerce; Fraud; Money; Import Duty; International; Government

I. Introduction
In today’s world, e-commerce is one of the biggest businesses which has grown rapidly. Currently there are more than a million e-commerce websites making billions of dollars but with great success comes even greater risks and frauds. E-Commerce fraud is defined as a method to obtain money or something valuable by deceiving someone. Many people try different methodologies to dupe the ecommerce websites and many of them remain uncaught. Frauds maybe of different types, for example, credit card frauds, phishing etcetera. But there is a new kind of fraud going on under the cover which has not been noticed yet. In this fraud, people order stuff from international e-commerce websites and the goods are delivered using the concept of parallel imports. In this, seller bring goods along them or import them from abroad for the customers via routes which are illegal. And here’s the tricky part. Some goods/items are liable for the government import duties and taxes. For example, when you order an automobile part, you have to pay x% import duty on that but since the order is brought by some agent in his/her check-in luggage, the import duties are bypassed [1]. Government allows people to bring goods along with them for their personal use but if someone uses this freedom for illegal usage then that’s a crime. Due to this fraud, the governments are losing millions and billions of dollars in form of taxes and duties. Also the grey market goods which are imported in India use the parallel imports concept. Parallel imports are illegal in India. People buy the goods at lower prices that they want to import via this method, stuff them in their luggage and bring them to India. These goods can be of any type. These are then sold here at prices lower than the original price in the local market. The tricky part is that these goods are mostly duplicate so are available at cheaper prices. Cheaper rates means less or no import duties. Thus evading the taxes. Also if the custom officer assesses the value of goods more than their actual value is, then you will have to pay import duty according to the assessed value [2].

II. Literature Survey
It was in [3] 1971 that the foundation of E-Commerce was laid. Cannabis was sold to students using ARPANET. In the late 70’s and 80’s, a lot of development was done. In 1995, a person named Jeff Bezos created the first commercial online E-Commerce portal called Amazon.com. Suddenly there was a flood of online market places such as eBay, IndiaMART, AliBaba.com etcetera but then started the frauds in E-Commerce. Every year, many frauds in E-Commerce come into sight. Many people get caught. For example: [4] Recently in India, a website named Timtara.com
IITM Journal of Management and IT

was found out to be a fraud website where the owners duped the customers for 12 lakh rupees [5]. Also some frauds came into light where a delivery guy tried to cheat the customers by replacing the original item with stones. In 2015, Flipkart, an Indian E-Commerce giant lost approximately 50-60 lakh Rupees in a new kind of fraud where people convinced the website that duplicate items were being shipped instead of the original items. In United Kingdom, the losses due to E-Commerce frauds alone counted up to approximately £217.4 million, which accounted for 45% of all card fraud and 66% of total remote purchase fraud. Here are the details of the losses due to E-Commerce frauds from 2004-2014 in United Kingdom [6]. This clearly shows how the E-Commerce frauds have increased in United Kingdom and the same way it is happening in the rest of the world. People around the world are getting motivated by real world to innovate new methods of fraud and the governments are struggling to find methods to stop them. The latest type of fraud which we have researched about is still operating under the hood. In this, the governments are losing huge amounts of money and very less people are aware about it. According to a new study conducted by ACI Worldwide, the increase in E-Commerce activity between Black Friday and December 31 contributed to a the highest fraudulent rates are Indonesia with 35% of its E-Commerce transactions being fraudulent; Venezuela having 33%; South Africa having 25%; Brazil having 11%; and Romania having

Fig. 1: E-Commerce Fraud Types [1].

Fig. 2: Fraud Losses on UK - Issued Cards
10%. On the flip side, the report ranks Denmark, New Zealand, Finland, Norway and Switzerland as the least-fraudulent countries. Other findings show that Europe’s fraud rate is slightly lower than the global average. Asia’s fraud rate is similar to the global average. Africa’s fraud rate is as much as 10 times higher than the global average. South America has a fraud rate three times higher than the world average. So according to the above correlative rise in fraud attempts, peaking on Christmas Eve. Although E-Commerce sales increased by 21 percent, the 2015 holiday shopping season saw 8 percent more fraud attempts, as compared to 2014.

According to a survey conducted for CyberSource by Mindwave Research of 312 online retail companies in the United States and Canada, in 2007, the losses due to E-Commerce frauds was $3.7 billion, $4.0 billion in 2008, $2.7 billion in 2010, $3.4 billion in 2011 and $3.5 billion in 2012 [7]. According to a research by fraud prevention technology provider Forter, which compiled the report, the top 5 countries which have stated facts, we notice that e-commerce frauds using the concept of parallel imports are on a rise now and till now no measures or steps have been taken to reduce this type of fraud. Below we have suggested some measures to stop this kind of fraud.

**III. Proposed Technology**

To prevent this kind of fraud, governments should take steps. The government can make changes in their import duty norms. Whenever an international courier is received, a thorough checking process should be done. Moreover, what we can do is that we can create different categories for different commodities so that any person sending a courier will mention under what category the thing lies. It is described with the help of a diagram.

With the help of this, the governments can gradually start obtaining the import duties and taxes. Also, in the customs department of the airport, people with luggage that looks suspicious, should undergo thorough checking so that those who carry parcels/shipments in their luggage to evade the taxes and import duties can be caught. The people who are caught should be penalised heavily so as to prevent this evading of taxes in the future.

**IV. Advantage**

The advantage of this research is that it will help the countries and their governments to earn the money through taxes and import duties which is their right. Moreover frauds can be stopped in the field of E-Commerce and people and governments will not get cheated again. It will create transparency among the governments, E-Commerce websites and the people who purchase goods from these sites. Whenever a person will purchase goods internationally, he or she will have to pay the amount which will eventually include all the taxes and duties. This way the government, the seller, the buyer and the website all will be safe from fraud.
V. Conclusion

Thus to conclude in the end, we have found a new kind of fraud going on under the covers that needs to be exposed so that everyone can get to know about it. This industry of E-Commerce is growing rapidly and if these kinds of frauds can be stopped then the governments can earn their share. If it is not stopped, then it will become a global issue in the future.

VI. Future Scope

More research can be done on this front such as more techniques can be designed to stop/avoid these kinds of frauds in the coming future. Moreover better import policies and custom policies can be implemented which will not allow the bypassing of the goods or people bringing surplus amounts under the tag of allowed value of goods so that no one can leave customs without paying the import duties.

References

1. Section – XVII, Chapter 87, Import Tariff 2015-2016, Central Board of Excise and Customs, India.
6. Fraud the Facts 2015, Financial Fraud Action UK.
Big Data and Cloud Security

Sakshi Dewangan*
Rajesh Singh Negi**

Abstract

In today’s face paced technologically mingled life, everybody has so much information that they do not know how to properly access it or the fact whether it is even worth keeping. These calls for a proper analytics mechanism that helps to keep all data sorted be it from multiple sources. The heap of information present today is most sitting in raw format as the proper means and tools to analyze and use the information efficiently had been missing. This is where Bigdata comes into action. It helps in data-driven decision making. Big Data are high volume, high velocity and high variety information asset that require new forms of processing to enable enhanced decision making, insight discovery and process optimization. It is an intelligent analyses tool that can process data that exceeds our current capability. Cloud computing on other hand provides services on demand rather than product. Big data integration with cloud is the future of IT sector.

In this paper we will discuss we will discuss Big data its advantages with cloud. Issues related to cloud security and Hadoop. Some possible approaches to reduce the risks that can make these technologies more efficient in terms of practical usage.

Keywords: Bigdata, analysis, file system, database, risk, map reduce, Hadoop, internet, cloud computing, security, privacy, encryption.

I. Introduction

The traditional system of storing data used flat files which are maintained by the file system and regulated by the Operating System. File systems were an attempt to computerize the manual filing system. When a user wants to store some data in the computer, he must place the data in files. Files are further placed in directories that are located in specific areas of the hard disk. A number of directories can be created with provision of a directory contained in another directory. User has a number of options such as renaming, deleting files, etc...Application programs use these files to access the data stored in them. This allowed a user even with little knowledge to perform operations such as deletion, insertion, manipulation and retrieval of data as required. These flat files store data in the form of records. A delimiter is used to separate the records such as a comma, space, pipe or any other special character. A special predefined character is used to mark the end of the file. Despite its ease, file system had various problems such as redundancy, security breaches; high cost of storing the data, data inconsistency, more memory was required due to redundancy of data. Also, data in file systems was scattered around multiple files. This made access and analysis of data a troublesome task. Changing one part of the data meant changing the application to suit the modified file format since applications were specific to the file system. Thus, a need for more systematic and structured arrangement of data aroused.

To solve the problem of unstructured data, the concept of databases emerged. These databases are built on top of the data storage services provided by file systems. A database is a collection of a large number of file systems and other sources of data that stores the data in a structured format for use by the user. A database is a computer database that is an up to date repository of information that can belong to either a specific organization or may be placed on the World Wide Web. The typical definition of a database is that it is an organized collection of data that are modeled in such a way that the data can be used in real aspects of life. For example, a user has data about the number of owners in a specific locality who own a dog, now he wants to find the breed of dog that is preferred by most owners. So he can analyze the data present in the database and retrieve results on the basis of his query.
This query analyses purpose is served by the Database Management System also known as DBMS. The general definition of DBMS holds that Database management systems (DBMSs) are computer software applications that interact with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.[1] Databases are of multiple types out of which relational DBMS are most commonly used. It stored data in the form of tables allowing the user to form various relationships among various tables i.e. a logical connection exists between the tables in the database. It is the collection of schemas, tables, queries, reports, views and other objects. Some of the well known databases include MySQL, PostgreSQL, Microsoft SQL Server, Oracle, Sybase and IBM DB2. Databases eliminate the shortcomings that are faced in the traditional file system. It provides a higher level of service as compared to the traditional file systems. Databases use sophisticated protocols and algorithms to implement reliable data storage on top of unreliable file systems. These algorithms make database storage a little expensive than file system storage, but databases provide far greater security than file systems. Relational database systems are based on Codd's Rules which are a set of thirteen rules beginning from zero that define the basic standard for a relational database. Some of them are logical data independence, physical data independence, data integrity, information rule, etc...

When the amount of data in a database exceeds our current capability of processing data, it is termed as Big Data. As stated, Big Data are high volume, high velocity and high variety information asset that require new forms of processing to enable enhanced decision making, insight discovery and process optimization[2]. The size of big data is measured in terabytes or petabytes or in higher memory units.

II. What is Big Data and Importance

When the data in an organization becomes so large and complex that it cannot be handled by traditional tools we say it as Big data. It basically concerns large-volume of data which is very complex [7]. We can define Big data with its for V’s-

- Velocity
- Volume
- Variety

Volume

Data storage in now days is growing exponentially as data now is not just text data.

We all are familiar with Facebook and other social networking websites where data is not just a text there data is in different formats like videos, music etc. Therefore the data storage of an organization is way
beyond gigabytes and terabytes. Data here not only generated daily but the historical data is also included for analysis. In 2012- 2.5 Exabyte’s of data is created each day. And this is doubling every year.

Velocity
This means how fast the data is coming from different resources. This concept is used for real time data where the data creation is very high speed which includes each click from the button, broadcasting the real time information.

Variety
Data can be stored in different formats. For example we can data in different formats like excel file, word file, text file which are the traditional formats. It is not necessary that data is present in these traditional formats it may also be in the forms like pdf, video, music or on something new formats. As we are in the world of social networks we may have data in the form of events. Now it is necessary for the organization to organize it in a meaningful way.

A. Sources of big data
- Sensor data- It is high velocity data which comes from sensors distributed over a geographical location like geo-location, temperature, noise, pollution, biometrics, red-lights etc.
- Machine log data-Machine data consist of records of all the activity and behavior of the user using the machine. It is used for identifying the third party services.

Figure 2: sectors where Bigdata is used

- Data storage- data from different storage location SQL, NoSQL, file systems.
- Public web-it is external where other people can use it on regular basis. Here we can integrate web applications which can generate lots of data.
- Social web-High velocity and high volume data that can be used to detect trends and analyse those trends for a specific brand. It is also used to target a set of customers to social accounts.
- Business Applications- These are the apps that uses API’s which can pull data from both inside and outside your organization.
- Media- is connected in and out from the organization, connected with API’s.

B. Importance of big data
Data is very important for an organization it serves as a backbone for them. In today’s era there is an explosion in data rate and we are trying to store all of this.

Why there is a need to store this much of data?
After capturing the big data the data is analyzed and processed. Companies after analyzing it gains complete understanding of their business, their customers and their competitors. By analyzing such information the companies can check their strategy and improvement in it or in case if analysis is not so good for a particular product then it may result in a new marketing strategy which eventually helps in near future.
All the analysis results in-

- Efficiency improvements
- Increased sales
- Lower costs
- Better customer service
- Improved products and services.

If we take an example of a Company, who manufactures shoes. The company should know who buys his products and who does not. From where the company could get this sort of data here company can use social media and web log files from the ecommerce sites that can help company in two ways-

1. Revaluation of strategy- case who didn’t buy the product in this case company can make modifications in their product or strategy to attract them.

2. Target customers- case who buy the product in this company will target particular set of customers to increase their sales

III. Hadoop

Hadoop is a processing engine which can handle large volumes of data in any structure. Hadoop provides two things-

1. Distributive storage of data (HDFS)
2. Distributive processing of large data sets (Map Reduce algorithm)

HDFS- Hadoop distributive file system

Distributive storage of data is called Hadoop Distributed File System, or HDFS. It provides cheap storage of data with low fault-tolerance. It also sees the hardware failure and in case of failure tried to use different node to save the data by replicating it therefore if one fails other node can be used. HDFS stores files in different servers, files are divided into blocks and saved to more than one servers. This helps in reduction of disk failures and performance. HDFS keeps an eye on every server and the blocks that they maintains this ensures continuous data availability. If we want to read some data we request for a block checksum of block is checked if it is found damaged then other server is looked for the same block. It lets the organization to spend less money for looking the servers; it’s the software that looks for the servers now.

Map Reduce

Map reduce consist job scheduler a software component. Job of job scheduler to choose the server for user query (job) it also schedules multiple user jobs on cluster of servers. It takes care of distributed computing.

Hadoop map reduce is an open source implementation of Google Map reduce algorithm. Hadoop Map reduce consist of two functions- map and reduce both are user defined. Input to Hadoop Map reduce is a key value pair (key, value) and then a map function is called for each set of pair. The function produces zero or more intermediate values (key’, value’), then these intermediate keys are grouped and reduce functions are called which produces aggregate results. Users have to define only the input and reduce functions rest is on Map Reduce. It uses HDFS to read and write the data. However it an reads the data from other sources like local file system, web and databases.

The advantage of using Hadoop MapReduce is job optimization. It allows an expert user to efficiently use Big data for analysis. The user need not to know

![Diagram of HDFS breaking of files.](image)

Figure 3: HDFS breaking of files.
SQL for queries only some knowledge of java is required [12].

Advantages-
- Scalability - the data is stored and distributed across number of servers which can operate in parallel.
- Flexibility - organizations can introduce new data sources and operations can be done of any type of data structured or unstructured.
- Fast-Hadoop stores data in distributed manner and MapReduce algorithm uses key value pair as an input which enables faster processing to locate the data.

IV. Cloud Computing

If we talk about cloud computing it is a kind of technology that depends on the sharing of computer resources. It basically delivers the services through INTERNET. Primary goal of cloud computing is to reduce the investment cost for hardware and software, to increase the scalability as it provides everything on demand and the resources on cloud are always available and reliable [14]. Cloud computing consist of computers connected to network that handles the load. The main benefit of cloud computing is to eliminate the cost at users end.

User only required having a computer and simple software to access the cloud services rest is handled by the cloud. The user can put any king of data in the cloud and data in the cloud is safe from any damage and the user can access that data any time any place he or she just needs a INTERNET connection.

V. Benefits of Big Data Analytics

The main importance of big data is only in the field of analysis. Analytics is a broad term for data analysis application. Stored data holds no value if not efficiently utilized. Stored data cannot generate business values. Once the data is stored such as in Hadoop, it can be analyzed and that in turn gives it a tremendous value. Diverse analysis technologies exist in the market today that can be used for big data application such as in-memory analytics, in-database analytics, and appliances. Analysis is a broad term that is used with Big Data in different ways. Analytics can mean either getting data in or getting data out. Proper analysis of data helps in decision making [4]. This was commonly used for business intelligence. Business intelligence is a broad category of applications, technologies, and processes for gathering, storing, accessing, and analyzing data to help business users make better decisions. This term was more popular in the 1990's. Today, it has been replaced with analytics since 2010. Analysis can be predictive, explorative or descriptive depending upon the purpose of data analysis.

Following are the features of Bigdata:
- Easy analysis of information from multiple sources that otherwise have no meaning.
- Bigdata is timely that means that workers are working hard to manage the data and make decisions.
- Big data is trust worthy. Data accumulated from multiple sources help in identification of exact patterns. This data is more reliable than the one performed manually by workers.
- Big Data is Secure
- Big Data is Relevant - most of the companies are not happy with the way their filtering applications work. Thus they turn to big data.
- Big Data is Actionable
- Big data provides ample of opportunities for scratch companies to enter into the market.

Some of the benefits of Big data analysis in different sectors are:
- Big data analytics benefits business intelligence, customer relations and many analytic applications. For example, big data is most commonly used to identify the buying patterns of customers. The products that customers view, order or just visit are used by vendors to gain knowledge about the likings of the customer. Based on this, only relevant products or items are shown to the customer.
- The most easy, efficient and fast way to gain review about anything these days is the internet. For example, Starbucks introduced a new coffee with its major concern being that the taste might be too strong for customers. Once the coffee was out, Starbucks monitored all blogs, articles, comments
and post on the internet and discussion forums. Using all this information from the internet and analyzing it, Starbucks discovered that although the new coffee was appreciated by the customers but the price was too high. So by morning, Starbucks lowered the price of the coffee and all negative reviews had disappeared.

- Government uses big data in many of its aspects. For example, police use phone records of criminals to track them or their GPS records to see the places they have been prior to their crime commitment in order to find the guilty. Health ministry uses Bigdata to check infant ratio, percentage of diseases widely spread in a particular area or season.

- Business organizations use Bigdata to analyze their business sales, profit and losses across regions over the year.

- Big data is not just for big companies. Retailers use big data analytics to check current trends among the population. retailers use Bigdata .i.e. collaborating data from web browsing patterns, social media, industry forecasts, existing customer records, etc. and predict trends, prepare for demand, pinpoint customers, optimize pricing and promotions, and monitor real-time analytics and results.

- Role of Social media in big data analysis- social media is one fast growing field. Billions of users from all over the world are active on multiple social sites. Millions of comments on various technologies, software, apps, dressing materials etc are used to analyze the customer likings. Based on this , various vendors make new catalogs of their products.

- Cloud and Bigdata-Big Data stores most of its data in distributed file systems. These files can be accessed from anywhere .i.e. cloud data. Thus extracting and analyzing this data from any part of the world becomes a cake walk.

- Fraud detection- fraud is a billion dollar business that is increasing every year at an unstoppable rate. Traditional mechanisms of detecting fraud have been long used. However, they are complex and time consuming. Big data records the patterns of every customer and their usual ways of depositing, transferring or withdrawing money. Any unusual activity either in the amount withdrawn can indicate the risk of a fraud.

- Data from applications is used by app developers to gain information about the likes and dislikes of the customer. For example, game developers add new features to their games every month. On app purchases that are made by the player helps them earn a lot of money. [3]

- Weather forecasting is solely based on using old data to determine weather patterns. Data from weather sensors, satellite, etc. is collected and used to determine weather conditions for each region.

- Another use of big data is made by Courier companies. The use of big data helps them to map out more efficient trucking routes. The resulting improvements have allowed UPS to save 30 million miles and 3 million gallons of fuel per year from their routes. The more efficient trucking routes have also led to less traffic accidents.

- Science - scientist use large amount of astronomical data collected over the years to determine constellation positions, meteor showers in a region, birth and death of a star, measuring distances between various space objects and on the basis of these patterns , they model their spacecrafts with ample fuel, food, oxygen and other necessities for sustenance.

VI. Need for Security

Big data is now being used by many industries for analysis purpose data which ensures new marketing strategies; such kind of data must be secured. It any security comes it will result in serious legal repercussions and a great damage to reputation. To secure this much of data different mechanisms should be used.

The importance of big data in an organization for fraud detection is quite useful. Detecting threats and malicious intruders should be detected and solved using big data analysis. The main issues with big data is security and privacy.as this concept of big data is increasing day by day different organizations are dealing with the problems with the privacy of data.
VII. Issues and Challenges
Cloud computing delivers the services on demand rather than products but it comes with lots of security issues as it surrounded by different technologies together such as networks, databases, operating systems and memory management therefore the issues related to these technologies are automatically included in cloud computing.

- A network which connects the systems should be secure.
- Mapping between virtual machine – physical machine done carefully.
- Not only encryption should be used appropriate data sharing policies should be enforced.

A. Issues in big data
The amount of data generated every second of the day is unimaginable. Data from multiple sources is flooding devices where its storage lies. Bigdata is data that is greater than terabytes in size. Data from social media, sensors, machines, phones, etc, need to be stored and processed so as to best exploit it. Processing this data is not an easy task. Data that is collected from numerous sources is raw data that is it barely holds any meaning. A series of steps is followed to make this data meaningful and then put it in the warehouse. Fortunately, the technology today has made this painstaking task simpler.

The following steps are followed in the data cleaning process.

1) Data Acquisition - data just does not arise on its own. It is collected, recoded from various sources over time. From the toxins we breath to the number of people dying every day produces terabytes of raw data per day. Data acquisition involves business understanding that means determining business objectives.

2) Information extraction and cleaning- Much of the data collected is useless and can be discarded. This step involves initial data collection (relevant), data description, data exploration, and the verification of data quality. Data exploration includes viewing summary statistics. Various models can be applied to identify patterns such as cluster analysis.

3) Data Integration, Aggregation, and Representation- Once the data resources are identified; they are selected, cleaned and built in to the desired form. Combining the data from multiple sources into a single meaningful format is what this step consists of. For example, we perform multiple scientific experiments but the observations are made on the basis of all those experiments and not just one. Data analysis is considerably more challenging than simply locating, identifying and understanding data. Mathematical techniques are used to identify patterns. On this basis models are assessed and built. Thus data visualization is an important part of the process.

4) Query processing, Data Modeling and Analysis-query analysis in data mining differs from the traditional method. Large volume of data requires efficient algorithms that can analyze data and display desired results. For example, plotting points on a graph for analysis becomes very difficult when extremely large amounts of information or a variety of categories of information is being dealt with. For example, if there are 10 million rows of sales data in 5 years that is to be compared. The user trying to view 10 million plots on the screen will have a hard time seeing so many data points. Thus in such cases, one of the many visualization and analysis technique is used to form a cluster by grouping data together so that it is visible to the user. This technique is called as cluster analysis.

5) Interpretation- The entire purpose of going through all these process is the end purpose of data interpretation. Data interpretation is performed by the user on the basis of the result that is display after Big data analysis is performed by the machine. [13]

Executing these processes is not an easy task. It needs to be performed accurately and timely.

- Timeliness - the larger the data size, the longer it takes to process it. Thus the design of the system must be efficient enough to accommodate a data this vast. A smaller set of data is processed fast and chances of error are also less.
Privacy - Privacy is a major concern in Big data. Since data lies in distributed file systems, data flows freely from one user to another specially in public servers. This is why most companies prefer having a private storage. In case of health records, some records may be sensitive and unauthorized access much not be permitted. Individuals do not realize how their information is used for data mining purpose by the very companies that provide them with that service. The most prominent threat is to that of a person's location at a particular time or at all times.

Cost - with in increasing data every second, the cost of storing this data is also increasing. Since Big data required both historical and present data, discarding old data is out of question.

Skills - the skills required to efficiently use this data in the form of human resource is also less in comparison to the world population.

B. Issues in cloud computing

Issues in cloud computing can be categorized

- Network level- in this level we deals with network that includes network protocols and it security.

- Authentication level- it includes the encryption and decryption techniques also with authenticating services (administrative rights for node, authenticating a node and logging).

- Data level- it deals with data integrity its protection and distribution.

C. Approaches

Cloud is a combination of different technologies the approach to follow should be applicable to is integrated technologies. The recommendations are designed in such a way the they don't lower the efficiency and scalability if cloud computing. Some measures are-

- File encryption- data is stored in a cluster therefore any intruder can steal all critical information. Data must be stored in encrypted form and keys should not be publically disclosed. Even if a hacker is successful to enter still he isn't able to read the data.

- Network encryption- it simply means the network communication should be encrypted such that a hacker won't be able to manipulate the packets that are flowing inside the network.

- Authentication- all the transactions should be authenticated i.e. all those events that include events on data must be logged and the user that is doing such transactions also be logged. This will result in knowing if any user is trying to do any malicious operation.

- Node maintenance- system where the software is running must eliminate the risk of virus.

- Testing of map reduce jobs- map reduce job entered by the user should be properly tested in the distributed environment. [15]

- Nodes authentication- whenever a node joins a cluster it should be authenticated. If in case a node is trying to do some malicious operation it should be disconnected from the cluster. Kerberos can be used to authenticate the node.

VIII. Conclusion

From a historical view point, Big data is a huge evolution in the decision making process that provides computer based decision making. It comprises of all benefits of a data warehouse and an added functionality of analyzing data from distributed file systems. It owns the ability to capture, store and analyze high-volume, high velocity, and high-variety data is allowing decisions to be supported in new ways. It is also creating new data management challenges.

From Big data is a special asset that merits leverage. Statistical information, or data, is a potentially rich and a valuable source of knowledge. the most interesting fact about this is the cost of storing this information is getting cheaper and cheaper thus allowing us to keep much more information than was previously possible. Big data is cost effective. Sophisticated computer algorithms have been designed to make this process even easier by sometimes revealing interesting relationships that would never have been possible previously.

We also need to resolve legal issues around intellectual property rights, data privacy and integrity, cyber security and Big data code of conduct.

Cloud computing is widely used in organization for research purpose and its security is a primary concern and it should be eliminated to minimal in order to provide secure environment for complex operations.
References

1. https://www.google.co.in/search?q=bigdata&oq=BIGDATA&aqs=chrome.0.69i59j0j0i3.1047j0j4&sclient=chrome&sourceid=chrome&es_sm=93&ie=UTF8&q=traditional+systems+of+storing+data

2. Basic Concepts in Big Data ChengXiang (“Cheng”) Zhai Department of Computer Science University of Illinois at Urbana— Champaign Bp://www.cs.uiuc.edu/homes/czhai czhai@illinois.edu


13. Challenges and Opportunities with Big Data: white paper


Cloud Computing: Security Issues and Challenges

Sheetal Mavi*

Abstract

Cloud computing is an architecture which provides computing services over the internet on demands and pay per use access to shared resources namely networks, storages, servers, services and applications, without physically acquireance. So it saves managing cost and time for organizations. Many industries like banking, healthcare sectors and education sectors are moving towards the cloud computing due to the efficiency of services and resources like using processing power, transaction carried out, bandwidth consuming, data transformation, or storage space occupying etc which is provided to users on basis of pay per use pattern. Cloud computing is fully internet dependent technology where client data is stored and maintained in the data center of a cloud provider like Google, Amazon, Salesforce.com and Microsoft etc.

Keywords: Cloud computing, security, privacy, encryption, Security Management Model.

I. Introduction

Cloud Computing has emerged as a scalable services consumption and carriage platform in the area of Services now. The main enabling technology of Cloud Computing includes Virtualizations and Service-Oriented Architecture (SOA) of hardware and software. The aim of Cloud Computing is to provide environment for the collaboration and share the resources among the cloud service consumers, cloud partners, cloud vendors and stakeholders in the cloud value chain. The resources shared at different levels result in various cloud offerings framework as infrastructure cloud (e.g. hardware, IT infrastructure management), Software cloud (SAAS focuses on middleware as a service, or classic Consumer Relationship Management as a service), application cloud (e.g. Application as a Service, UML (Unified Modelling Tools) modelling tools as a service, social network as a service), and business cloud (e.g. business processing as a service). “Cloud computing” is the natural step in the emerging scenario of on-demand technology services and products. To a large extent, cloud computing is based on virtualized envision resources. Cloud computing forerunners have been around for some time now [1, 12, 15, 17, 18, 24, 29, 30, 35, 40], but the term became “favoured” sometime in October 2007 when IBM and Google announced a collaboration in that domain [27, 22]. It was followed by IBM’s announcement of the “Blue Cloud” effort [23]. Since then, everyone is talking about “Cloud Computing”. Of course, there also is an unavoidable Wikipedia entry [45]. VCL has been in production use at NC State University since 2004, and is a suitable vehicle for dynamic implementation of almost any current “cloud” computing solution. This discusses “cloud”-related research and engineering challenges and summarizes and concludes the paper.

Cloud Computing -A key differentiating element of a successful information technology is its ability to become reliable, valuable, economical and true contributor to digital infrastructure [4]. “Cloud” computing embraces digital infrastructure, and builds upon decades of research in virtualization, “grid computing”, utility computing, distributed computing, and, more recently, networking, web and software services. It provides service as oriented architecture, reduced information technology to head for the end-user, greater flexibility, reduced total cost of ownership for users. This paper discusses the concept of security issues and challenges in “cloud” computing, it tries to address, related research challenges, and a “cloud” implementation available today.

II. Issues in Cloud

Security is the important aspect in the field of computing, as it an obvious expectation for users. The security issues are crucial for cloud environment too. As the cloud computing approach can be associated with the user’s sensitive data stored both at client’s end as well as in cloud servers, identity management and
authentication are much prioritized in cloud computing (Kim & Hong, 2012; Emam, 2013; Han, Susilo & Mu, 2013; Yassin, Jin, Ibrahim, Qiang & Zou, 2012). Verification of eligible users’ credentials and protecting such credentials are the part of the main security issues in the cloud – violation. In these, areas could lead to undetected security breach (Kumar, 2012) at least to some extent for some period. We are residing everything as in providers’ premises which makes the information highly unsecured. It is the main barrier in adoption of cloud computing. Some security concerns are mention below

#1: Company has breach the law (risk of data seizure by (foreign) government).
#2: Storage services provided by one cloud seller may be incompatible with another seller’s services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud).
#3: Who controls the encryption/decryption keys? Logically it should be the customer who controls these keys.
#4: Ensuring the integrity of the data like transfer, storage, and retrieval means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist.
#5: Some government regulations have some strict limits on the data for its citizens that can be stored and for how long, and some banking regulators require that customer’s financial data remain in their home country.
#6: Customers may be able to sue cloud service providers if their privacy rights are breach or violated, and in any case the cloud service providers may face harm to their reputation. Concerns arise when it is not clear to the individuals why their personal information is requested or how it will be used or send to other parties.
#7: With the cloud model the control physical security is lost as because of shared computing resources with other companies, No knowledge or control of the resources to run.
#8: The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the audit ability of records.
#9: In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators.

#10: Security concern #10: Users must keep up to date with application improvements to be sure they are protected.

Cloud computing enters with various possibilities and challenges simultaneously. Of the major challenges, security is appraised to be a critical obstacle for cloud computing in its track to success (Khoshed, Ali & Wasimi, 2012). The security challenges for cloud computing approach are somewhat strong and huge. Data location is an important factor in cloud computing security (Teneyuca, 2011). Location transparency is one of the well known workable flexibilities for cloud computing, which is also a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated and could be damaged. Cloud users’ personal data security is thus a crucial concern in a cloud computing environment (Joint, Baker & Eccles, 2009; Ismail, 2011; King & Raja, 2012). In terms of customers’ personal or business data security, the strategic policies of the cloud providers are of the highest significance (Joint & Baker, 2011) as the technical security alone is not adequate to address the problem. Trust is one of the another problem which raises security concerns to use cloud service (Ryan & Falvy, 2012) for the reason that it is directly related to the authority and authenticity of the cloud service providers. Trust establishment might become the key to create a successful cloud computing environment. The provision of trust model is crucial in cloud computing as this is a common interest area for all stakeholders or vendors for any given cloud computing scenario. Trust in cloud can depend on a number of factors among which some are automation management, human factors areas, processes and policies (Abbadi & Martin, 2011). Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent.

III. Some Solution For Security Issues In Cloud Computing

Following given approaches can be helpful to secure the cloud computing...
Investigation Support: Analysis tools are provided to the users to observe how the data gets stored, used and protected, and verify the policy of enforcement. But the investigation of illegal action is very difficult because data for multiple customers may be collocated and it may also be geographically spread across set of hosts and data centers. To solve this audit tools must be contractually committed along with the evidence.

Network Security: A user can contradict the access of any Internet based service by using IP Spoofing which can be a cause of security harm [6]. To solve this problem we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol used for managing security of message transmission on The Internet which also avoids resource hacking problem.

Encryption Algorithm: Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability [6]. To solve this problem the cloud provider must provide evidence or proof that encryption scheme were designed and tested by experienced specialists.

Backup: The physical devices can be damaged by the natural disasters that may cause the loss of data. To avoid this problem, the key of assurance of service is backup of information provided by vendor.

Customer satisfaction: It seems quite hard for the customer to verify the recently implemented security practices and an initiative of a cloud computing provided by the service provider because the customers generally has no access to the provider's facility which can be comprised of multiple facilities spread around the globe [8]. Solution for this Provider should get some standard certificate from some governing or standardized institution that ensures users that provider has established adequate internal control and these control are operating efficiently.

IV. Security Management Model (SMM)
This section contains twenty recommended models of security management and their requirements for cloud computing service providers should definitely consider as they evolve their compliance programs

1) Security management (People): It is very important to develop a formal charter for the security organization and agenda. The charter should be ally with the strategic plan of the organization or company the security team works for. Lack of responsibilities and clear define roles and agreement on expectations, can result in a confusion and loss among the team of security about what is expected of them, how their experience and skills can be edged, and meeting their performance goals.

2) Security governance: A security guiding committee should be evolved whose main aim is to focus on guidance on security initiatives and alignment with business and the IT strategies. This committee should clearly define the roles and responsibilities of the security management team and other groups involved in performing information security functions.

3) Software-as-a-Service (SaaS) security: SaaS is the major cloud service model for the computable future and the area where the most critical need for security practices and oversight will reside. Just as with a managed service provider, corporations or end users will need to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data. The technology analyst and consulting firm Gartner lists [14] seven security risks which one should discuss with a cloud-computing vendor:

   Privileged user access: Get as much information as you can about the people who manage your data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

   Regulatory compliance: Make sure that the vendor is willing to undergo external audits and/or security certifications. Data location: When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not
even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

Data segregation: Make sure that encryption should available at all stages, and that these encryption schemes were tested, designed and maintained by experienced professionals.

Recovery: Even if you don’t know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has “the ability to do a complete restoration, and how long it will take.”

Investigative support: Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a allowable commitment to support specific forms of investigation, along with proof that the vendor has already successfully supported such activities, then only safe assumption is that investigation and discovery requests will be impossible. Long-term viability: Ideally, the cloud computing provider will never go broke or get acquired and tolerated up by a larger company. But you must be sure that your data should remain available even after such an event. Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application. To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.

4) Risk management: Risk management entails identification of technology assets [15]; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls.

5) Risk Evaluation: Security risk assessment is critical to helping the information security organization make informed decisions when balancing the duelling priorities of business utility and protection of assets [16][17]. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as-needed basis. More detailed and technical security risk assessments in the form of threat modelling should also be applied to applications and infrastructure.

6) Data governance: This framework should describe that who can take what actions with what information, and when, under what circumstances, and using what methods.

7) Virtual machine security: In the cloud environment, physical servers are stabilized to multiple virtual machine instances on virtualized servers. Not only data center security teams can replicate typical security controls for the data center at large scale to secure the virtual machines, they can also advise their customers or vendors on how to prepare these machines for migration to a cloud environment when suitable.

8) Disaster recovery: In the SaaS environment, customers can depend heavily on access to their services and any intervention in access can be disastrous. With the help of virtualization software virtual server can be backed up, moved and copied just like a file (live migration). Benefit is quickly reallocating computing resources without any downtime Ability to deliver on service-level agreements and provide high-quality service

9) Third party risk management: Lack of a third-party risk management program may result in
damage to the provider’s reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

10) Vulnerability assessment: Classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading.

11) Security image testing: Virtualization-based cloud computing provides the ability to create “Test image” VM secure builds and to clone multiple copies. Gold image Virtual machines also provide the ability to keep security up to date and reduce exposure by patching offline. Offline virtual machines can be patched off-network, providing an easier, more cost-effective, and less production-threatening way to test the impact of security changes.

12) Security awareness: People are the weakest link for security. Knowledge, culture and awareness are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expose the company.

V. Conclusions

Cloud computing has various prospects, but the security threats embedded in cloud computing approach are directly proportional to its proposed advantages. Cloud computing is a great opportunity and profitable option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The huge possibilities of cloud computing cannot be ignored simply for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer (Dukaric & Juric, 2013). Security for cloud computing environment is a non-compromising requirement. Cloud computing is inevitable to become the ideal (and possibly the ultimate) approach to business computing though the security barriers along with other issues need to be solved for cloud computing to International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 33 make it more viable (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011). Given its total benefits and dynamism provided that it is deployed with in an integrated and secure infrastructural framework, cloud computing can offer virtual ownership and access to ‘super computers’ without achieving them physically. Perhaps this is what inspired the term SCC (Scientific Cloud Computing). Research effort has been contributed to develop faster yet secured SCC tools (Jorissen, Villa & Rehr, 2012) which will greatly inspire the era of research and motivation in various fields of clouding computing itself. The social conclusion of cloud computing approaches can emerge with severe impact if robust security models for cloud computing does not exist. The issues in security for cloud computing are not related to direct security and technical aperture only; a number of social deviation may be resulted even when there is no ‘hard’ security breach taken place. The dispersive processing like transmission and storage features is behind reason. One of the examples is the obtaining of digital clues. The evolution of cloud computing might significantly affect the collection and retention of digital evidence (Mason & George, 2011). The vastness and potentiality of cloud computing cannot be overlooked, subsequently robust security models for cloud computing scenarios is the most prioritized factor for a successful cloud based infrastructure development and deployment. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements that from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users’ and the cloud service providers’ ends. The security issues in cloud computing are somewhat sensitive and crucial on the basis of sociological and technological viewpoints – the technological inconsistency that results in security breach in cloud computing might lead to significant sociological impacts. As a result, when dealing with cloud computing and its security issues, technical as well as epistemological factors are equally important to take into consideration. Based on the fact that the
The impact of cloud computing can include both the technical and social settings; the research on cloud computing and its related concerns are not related only with computing aspects. Service-oriented architecture and other characteristics of cloud computing suggest that the concept of cloud computing would require to analyze the practicality in line with social, business, technical, and legal perspectives—all these facets will incorporate security issues either in technical or strategic form. Even if not considering the nature of security issues, it can be doubtless concluded that the acute unfavorable effects as a result of security in cloud computing, the classification of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems.

References
9. ILKAY ALTINTAS, GEORGE CHIN, DANIEL CRAWL, TERENCE CRITCHLOW, DAVID KOOP, JEFF LIGON, BERTRAM LUDAESCHER, PIERRE MOUALLEM1, MEIYAPPAN NAGAPPAN, NORBERT PODHORSZKI, CLAUDIO SILVA, MLADEN VOUK, “Provenance in Kepler-based Scientific Workflow Systems”, Poster # 41, at Microsoft eScience Workshop Friday Center, University of North Carolina, Chapell Hill, NC, October 13 – 15, 2007, pp. 82.


An Effective Approach towards Encryption of Limited Data

Ruchi Kawatra*
Sapna Arora Saini**

Abstract
Processed information from a network is very difficult to maintain. As the data travels from one point to another, there are different threats / obstacles through which a programmed data has to go through. In the modern world, it is necessary to secure data and maintain its features like confidentiality, integrity, privacy and security. For the same, cryptographic techniques are used. These techniques are the base on which these features sustain. Cryptography is art of writing secret code from a plain code so that the privacy of data gets sustained. Generally, we deal with the type of data algorithms which works with extensible data.

Our approach is towards encryption of limited amount of data.

Keywords: Encryption, Decryption, SDEA (Short Data Encryption Algorithm), Cryptography

I. Introduction
The word cryptography comes from a Greek words means hidden or secret writing. Cryptography is the art of secret writing. Generally, people think of cryptography as the art of managing information into apparent unintelligibility in a manner allowing a secret method of unmasking. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Cryptography provides services such as

- Integrity checking – reassuring the recipient of a message that the message has not been altered since it was generated by legitimate source.
- Authentication - verifying someone’s or something’s identity.

In simple words we can explain that a message in its original form is known as plain text or clear text. The mangled information is known as cipher text. The process for producing cipher text from plain text is known as encryption. The reverse of encryption is called decryption [1].

Cryptographic systems tend to involve both an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you like to start the communication secretly.

Sometimes a cryptographic algorithm has a variable-length key. It can be made more secure by increasing the length of the key.

Sometimes, Steganography and cryptography are used interchangeably assuming that both are used for protecting confidential information. However there is a big difference between the two. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver knows the existence of message, if it exists [2]. Steganography prevents discovery of the very existence of the communication. In cryptography, encryption prevents any unauthorized user from detecting the contents of communication. In Cryptography the structure of the secret message is changed, no such thing in steganography.

II. Type of Cryptography
There are three types of cryptographic techniques:

1. Symmetric Key Cryptography: It is also known as secret key cryptography. In this only a single
key is used. Here same key is shared by both the parties communicating. It is simple and faster. Given a message and the key, encryption produces unintelligible data, also known as cipher text, which is about the same length as the plain text. Decryption is the reverse process of encryption and involves the use of same key as that of encryption. The Captain Midnight code and the mono-alphabetic cipher are both examples of secret key cryptography.

2. Asymmetric Key Cryptography: It is also known as public key cryptography. Unlike secret key cryptography, the keys are not shared. In this two different keys are used. A private key that is not shared with anyone and a public key that is preferably known to the entire world. The users get the keys from an authorized Certificate Authority.\[5\][6]

3. Hash Function: They are also known as message digests or one-way transformations. It is a one way encryption. A cryptographic hash function is a mathematical transformation that takes a message of arbitrary length and computes from it a fixed length number. No key is used for encryption or decryption process.

III. Existing Techniques

A number of image based encryption algorithms is available like Baker’s Transformation, in this Baker’s map is used for image encryption; Magic cube transformation is used to scramble the image pixels etc. But all these have some disadvantages for that purpose new algorithm has been developed in recent years.

As mentioned in Introduction section, there are two main types of cryptography in use today - symmetric or secret key cryptography and asymmetric or public key cryptography. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970’s.

1. Data Encryption Standard (DES): The main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES).\[2][3] However, this has now been replaced by a
A new standard known as the Advanced Encryption Standard (AES) which we will look at later. DES is a 64-bit block cipher which means that it encrypts data 64 bits at a time.

DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team. DES is a 64-bit block cipher under 56-bit key. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. However, DES is widely used algorithm in different domains like Education, military & others, but some of the design considerations are under controversy.

2. **Triple Des (TDES):** As a replacement to DES, TDES was a better solution to make possible changes. However its encryption algorithm status is too strong (i.e difficulty in breaking the cipher text) sue to advances in key searching.\[10\] The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is that it is too time consuming.

3. **Advanced Encryption Standard (AES):** AES was developed by two scientists Joan and Vincent Rijmen in 2000. AES uses the Rijndael block cipher. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length are 128-bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds. But for the case of limited data, it would be quite difficult to work with.

4. **BLOWFISH:** Blowfish \[9\] was one of the fastest & better options for existing encryption algorithm (in case of data on 32 bit microprocessors). It is efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. Blowfish is a cipher based on Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64-bit block cipher and is suggested as a replacement for DES.

### IV. Implementation

A **transposition cipher** \[10\][11] is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters’ positions to encrypt and an inverse function to decrypt.

The proposed algorithm is used to encrypt data by using ASCII values of plain text or data to be encrypted. The secret key is used to make modification in another string and that new modified string is used in the encryption process. The encryption process is illustrated in Fig. 3: Public-key cryptography.

![Public-key cryptography](image_url)
to encrypt or decrypt data. Therefore, it is assumed that it is a type of symmetric key algorithm because it uses same key for encryption and decryption purposes.

The proposed **algorithm** is –

1. The plain text is selected.
2. Fetch a string in order to encrypt it in a secure manner (say medal).
3. Convert it into ASCII code.
4. DECIMAL/ASCII: 77 69 68 65 76
5. 8 BIT BINARY VALUE OF STRING- "MEDAL": 01001101 01000101 01000100 01000001 01001100
6. ADD BINARY VALUE OF 1 IN EACH BYTE: 01001110 01000110 01000101 01000010 01001101
7. Perform Shift left operation 2 times: 00111001 100011001 00010101 00001001 00110101
8. Choose 1 symbol from queue: (say 5)
9. ASCII VALUE OF SYMBOL GENERATED: (5) 00110101
10. 8 BIT BINARY VALUE SYMBOL GENERATED & STORED AS KEY: 01101110 01010011 01101010 01111100 01101110
11. CIPHER TEXT ACHIEVED THROUGH BINARY ADDITION: n s J > j

Decryption is the reverse process and performed in the following manner:

1. The cipher text is selected.
2. Fetch the ASCII value of the data.
3. Convert it into ASCII code.
4. Perform Shift right operation 2 times.
5. Subtract binary value 1 from each byte.
6. Convert the upcoming value into decimal number
7. Now, find out the string associated with decimal number i.e, MEDAL.

Encryption process example for our approach:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>MED</td>
<td>AL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>5</th>
<th>3</th>
<th>1</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>L</td>
<td>D</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
V. Conclusion

Encoding & decoding is not at all much difficult task if suitable & precise algorithms are used but problem arises when we have to work out encryption of less amount of data with current & traditional algorithms which generally doesn't seems to be much cost effective. TO keep the same goal in mind with the integration of CIA (Confidentiality, Integrity & Authenticity), we designed an effective approach.

As a future work, we can merge the concept with
- Different data formats (Audio, Video & MM)
- Analysis of New information in an updated media file
- Working the same algorithm to partial secret key algorithm to make it more secure & confidential.
- Educational concepts.

References

Vulnerabilities of Data Storage Security in Big Data

Govind Murari Upadhyay*
Harsh Arora**

Abstract
In the era of big data, the massive amount of data needs to be managed, organized and secure over the network for all users. Vulnerabilities and threats make the data insecure and unreliable. In order to keep this bulk of data secure and safe, some security mechanism related to same need to be implemented. Confidentiality and privacy in big data must be maintained. Authentication and data integrity are other related parameters of big data security. Various challenges, issues and problems arise when available data gets interrupted by third party intruders. The intruders can be from external and internal environment from an organizational point of view. These individuals access, view, edit the sensitive data by unauthorized means. There should be some counter measures and access control methods, algorithms and the corresponding techniques like Map Reducer, Data Filtrations methods, Various encryption methods and finally we cannot ignore the best technique “Hadoop” which is used to handle, manage, organize and secure the big data specifically. Hence, monitoring and detection of attacks and prevention of threats to be implemented altogether. Although huge amount of data is present yet the available data must be focused according to cyber security point of view. There should be no compromise with big data storage, security, integrity and reliability. Big data available should be valid and secured using security mechanism and data controlled techniques.

Keywords: Big data, vulnerabilities, filtration, data security, Hadoop, Map Reducer, Intruders, Encryption, threats.

I. Introduction
The word “Big Data” is used to describe the increased and massive volumes of structured and unstructured data which is so large that it is very difficult to process this data using traditional databases and software technologies. Big data storage leads to large amount of data storage and managing and securing the big data is equally important and valuable at the same time. Big data requires bigger responsibilities as companies of all sizes and in virtually every industry are struggling to manage exploding amounts of data. In order to analyze complex data and to identify patterns, it is very important to securely store, manage and share large amount of complex data. When it is the matter of “Big data”, we cannot ignore the word or technique “Hadoop” - the term which is used to support the processing of large set of data in distributed computing environment [1]. As both business and IT executives know all too well, managing big data involves far more than just dealing with storage and retrieval challenges- it requires addressing a variety of privacy and security issues as well. So there should some mechanism to protect such a huge amount of data present on the web. For making big data secure, organizations need to employ three key types of security protocols or controls.

(A) Preventive
(B) Detective
(C) Administrative

The techniques such as encryption, logging and honeypot detection must be necessary. In many organizations the deployment of big data for fraud detection is very attractive and useful [1]. As the phenomenon of large data exist almost in every field whether it is physics, biology, ecology, scientific area and others so it is the prime objective to secure the bulk of data present everywhere and big data as an information security problem which has a lot of challenges which have to curbed [2].
II. Data Security in Big Data

(A) Confidentiality and privacy in Big data
Computations and database operations are done on massive amount of data, so it’s highly important to protect data in order to make it reliable, integrated, and confidential and privacy is maintained. In this era, many organizations are using the technology to protect and secure this bulk of data in order to make it integrated. Not only security but also data privacy challenges exists in the industries and federal organizations [1]. Out of this bulk and huge data called big data it is required to make secure data highly confidential among various companies and stakeholders. There should be a balance between data privacy and national security. Big data contains huge data volume and this requires a new generation of encrypted solutions and on the other hand big data techniques can also be used to address and security changes in network system [2]. Security policies need to apply on big data which refer to set of rules and practices that specify or regulate how a system organization provides security services to protect sensitive and critical system resources [3]. Confidentiality covers two related concepts:
1. Data confidentiality assumes that private or confidential information is not made available or disclosed to unauthorized individuals.
2. Privacy assumes that individuals control or influence what information related to them may be collected and stored and by when and to whom that information may be disclosed.

(B) Authentication and data integrity
Big data needs to be authenticated and integrated that gives the assurance that data received are exactly as sent by an unauthorized entity that contains no modification, insertion, deletion or replay [3]. Big data integrity deals with a stream of messages, assumes that messages are received as sent with no duplication, insertion, modification or replays. Integrity service relates to active allocates, the concern is detection as well as prevention.

(C) Security mechanism and access control related to big data
In this era of big data, in order to manage this huge and massive amount of data on the network is a critical issue that must be handled to keep it safe, secure and integrated so all security mechanism need to be implemented. In the context of network security, access control is the ability to limit and control the access to host systems and applications via communication links. Apart from access control, other security mechanisms are required to be protected and integrate the big data over the network. These security mechanisms are authenticated exchange, traffic padding, routing control and notarization.

III. Problems, challenges, issues related to big data security
Encryption of data is the prime objective if it is the concern of data security in big data. Also appropriate policies are required for managing and sharing of data on the web. For this purpose security algorithms need to apply on big data to make it secure. As per the network access security model, there are many internal security controls to protect and secure the data still there are many threats to the available big data. The existence of vulnerabilities in a network system and database makes the big data insecure and there should be some mechanism to exploit these vulnerabilities in the system as these vulnerabilities has great impact on all the system programs such as utility programs and many more. There can be the possibilities of various threats to big data and various factors associated with network and communications are responsible for these threats. These threats basically allow the system open to intruder mean the third party object or role players which can easily access the data available on network. In other words it would be appropriate to say that the valuable data can be extracted by any of the unauthorized person or hacker during the communication of data from source to destination all over the network. So issues related to confidentiality and privacy comes into the limelight that exposes critical corporate data and related personal information to new security threats. The threats can be related with information access threats and service threats. Now the question in this context is how threats have become the challenges and how they are represented. The insight threat acts as security challenge when intruder or individuals misuse the data and sensitive data is extracted by some internal intruders or individuals by authorized access. The threats can be because of
internal or external intruders. The individuals within the organizations have been reliable to same and have authority to access the data and thus possess the necessary authorization to access proprietary or sensitive data. The other types of active intruders are from external environment. These individuals access, view, edit the sensitive data by unauthorized access means, thus act as a big outside threat to the big data in the network. Challenges related to cyber security and of course related with the topic in context “Big data security” can be depicted through various parameters and aspects.

1. **Distributed computation framework challenges**

   When data is accessed in a distributed and parallel fashion than computations need to occur in parallelism and to access and manage the massive amount of data, the distributed computations framework becomes the challenge. Complications regarding this frame need to be resolved by the attacks preventions measures which would describe how to secure the big data in which manner and also at the same time describe how data can be secure in presence of entrusted manner. Untrusted mappers may return wrong results which further generate incorrect aggregate results. Map reduce framework used for secure computations in distributed programming framework where each input file is divided and reduced in the multiple parts or blocks in the first phase of map reducer. Each individual block or chunk is being read by mappers and related calculations are performed and output related to these blocks are combined together later on form of list of key and value pairs [1].

2. **Security for traditional databases challenge**

   Security for traditional databases includes various secure policies that must be evolved with respect to security infrastructure. Here the context is about non relational data storage and its security. In traditional databases where the relativity among data is not so advanced and managing such data in context of big data itself is a big challenge coming on another side nosql database were built to tackle different challenge in analyzing the data as data security was never part of such design at any point [TTBDS]. Hence robustness gets affected such a case which could be processed by clustering aspect of nosql database. Huge volume of data is being handled and processed as a challenged by various companies. Where the criteria is to deal with big bulk of unstructured data sets that originally become the part of traditional relational database but from security and efficiency point of view traditional relational database is being converted into nosql database. For accommodating and accessing big data hence the idea is not to compromised with operational feature of database and traditional database must be handled from the vision of accessing it on the web where the complete data must be secure and companies must review securities policies. For the middleware by enhancing it with addition of security feature to its main counterpart.

3. **Big data storage, Accessing the valuable Transactional Logs Challenges**

   In context of accessing the data and various transactions in available databases, the data has to be travelled through multiple tiers or layers as far as storage media is concern the much tier architecture or framework of database is very helpful whether it is traditional database, relational nosql database management system or big data concern. Multitier storage media helps and allows to move data between tiers and communication of data takes place in effective and efficient manner. But the challenge is how to make data secure rather than any other factor of communication and storage of big data. The vulnerabilities and threats have always been exist as challenges in the network and database security. Also besides normal database storage, the size of datasets has been continuously growing exponentially depending upon the requirements of companies as per their applications and relativity with others. So it has become as necessity to auto apply tiering methodology on scalable and available data in order to make bulk of data secure, manageable, accessible and reliable. But problems and issues lie here also related to auto tiering concept is that it does not keep tract about the place of data storage which definitely...
becomes a new challenge in the context of data storage security.

For big data security data must be integrated and aligned and place of available data must be tracked and defined and to make available the big data 24X7, the effective security mechanisms should exist to beat the security challenges. With autotier storage system, critical information should be properly aligned in different tiers however the lower tier has low percentage of security, so the organizations should study and analyzed these multitier strategies and policies and should track how data is passing, communicating and locating in different locations or places and corresponding tier framework and flow of secure data through multiple paths.

4. Input validation/ Filtering challenges
Validation of data is highly important for an enterprise to make data integrated all together whether it is centralized database or distributed database. In an organizational network, multiple systems devices software applications are connected together and the corresponding data available may be insecure everywhere on the network. Now the question is how can be assure that source of input is valid. Input validation must be recognized. Data in input sources should not be entrusted, malicious and corrupted. So to make data valid and trusted there must be some mechanism of filtering and protecting data during the network transmission and communication of big data in different locations over the web. Validation problems arise while data is input from various sources on net filtering of data is most critical issue and challenge in context of big data security, which completely leads to input data validation. Filtering and validation challenges of data must be analyzed and corrective measures should be taken by following various routing network algorithms and produces along with various firewall mechanisms. But we cannot ignore the concept of filtering data, otherwise it will remain as a big challenge in context of input data validation. There should be no compromise with big data storage, security and reliability so challenges related to validation of data and filtration must be controlled and counter measures are necessary to handle it all.

5. Monitoring and Real time Security Challenges
The problem with big data arises when it is the point of real time security. All devices in a network involved in the communication of amiable data need to have some alert mechanism. The alerts are generated by security devices. This aspect of alerting from connecting devices must be taken into account considerably but normally these things are ignored straightway from enterprise or organization. This monitoring and real time security has become a critical issue and challenge.

IV. Counter measure for big data security
From big data security point of view, the reliable security mechanisms are needed to cope up with the existing threats and challenges. In context of network access security model, access channel is used to maintain the flow control of data. The gatekeepers plays very important role for security control of data on the network. Internal security controls are applied on the data and processes to make data secure and protected. There should some privacy measure algorithms and techniques to cope up with inside threats, intruders’ interference and hacking of data. Various detection systems are used to detect the unusual pattern of data access. Various encryption techniques are used to protect the online data or big data which is available everywhere on network. The question is how to tackle and control such a big data. Many organizations are facing to implement the control measures and techniques as this is a great challenge. In a big data environment, beside storage of data, integrity, consistency, reliability, availability, accuracy and security factors are highly important and required. Some regulatory and control measures are used to maintain these properties. So a technique such as attribute based encryption is used to protect and secure data. To make a big data secure, detection and prevention of predictable threats are required that becomes the part of big data analysis. These techniques are used to give valid input data that leads to make it reliable for transmission all over. As with these techniques, detection can be done at early stages, so it helps to prevent distribution of errors and analyze the patterns of all mutable data resources.
Another technique which can be used to protect data from various threats is “Feature Extraction”. To make data authentic and reliable and when it is all about big data than we should invariably encounter Hadoop. This technology is highly effective to manage are considered problem or challenge which is how to manage and to secure, integrate, authenticate “big data”. So the term finally “big data” should be associated completely with the technology meant to handle this massive data is “Hadoop”. Which organizes the data online all over the world and makes data extraction feasible everywhere in efficient and effective manner. In cyber space quality data should be extracted and available to the use at any location along with the privacy, secured measures to cope up the challenges reconcile the data protection with data user privacy. As we can see from cyber security point of view related to big data access control mechanism for data security are required and all challenges and issues are tackled effectively with use of database software technologies like Hadoop. For better benefits, and for better organized data in secure environment.

V. Conclusion

The significance for cyber security for big data lies in the fact to make complete bulk of data available on network should be integrated and secured. Multiple users all over the world should be able to access big data under the umbrella of network and database security. The purpose is how to beat the challenges and issues available in the existing system. These challenges are coping up by using some counter measures and techniques to handle big data which cover filtration methods, encryption methods like attribute based encryption, feature extraction are used. Finally Hadoop technology has crossed most of the challenges and issues related to big data includes to prevent the predictable security attacks and threats and how to cope up with these threats. Accordingly proper counter measures should be taken into account by considering all security policies and parameters.

References

Cyber Security and Big Data Analytics

Priya Bhardwaj*
Nidhi**

Abstract
This research report examines the differences between the traditional methods of cyber security with the Big Data analytics. Since Internet is growing at a fast pace, the need for cyber security measure is essential in almost every aspect of our lives. This growing network is becoming more of a threat these days than a blessing, because today many people are using it as a safe and secure passage for committing high-profile crimes. This paper tells us the importance of Big Data in the field of cyber security.

Keywords: Cyber Security, Big Data Analytics, MapR, Hadoop

I. Introduction
Cybercrime (computer crime) can be described as a term for any felonious activity by a person whose primary means of communication is a computer. Today more research is needed to secure the cyber from these unauthorized people. Cyberspace has become today’s new battlefield and cyber security continues to be a top priority for every sector.

Cyberspace can be distributed into the following resources: devices, information, networks, and people. Securing these resources is the job of cyber security. Cyber security has transformed very quickly from the technical area to the scientific notion. Globalization and Internet has given organizations, individuals and nation enormous power due to the advancing network technologies. For everyone – students, teachers, entrepreneurs, socialists, soldiers, pioneers, hackers, and even terrorists – collecting and sharing information, communication, everything has been digitized. As a result, all the sectors now have a cyber-drawback, the varsity and influence of which are hard to foretell, and the struggle facing in cyberspace are becoming more crucial than attacks taking place on the ground.

The nature of a civil security threat has not changed, but the Internet has provided a new delivery process that can escalate the speed, scale, and power of an attack. Every sector is introducing better security options to protect their systems and prevent data loss.

The year 2014 which is also known as the “Year of the Data Breach” has recorded an average cost per breach reaching $12.7 million. This has reminded us the need to use better protection and secure gateways to help fortify systems, statistics and individual. Today, the conversation regarding these crimes are less about intercepting these attacks but more about how momentarily you can expose that an attack is happening.

II. Categories of Cyber Crimes
Cybercrimes can be broadly classified into three sectors:
1. Property
2. Government
3. Individual

Each class uses a various techniques and each technique used vary from criminals to criminals.

A. Property
Just as in real word criminals can loot and mug, even in the cyber world they steal and rob. These include intellectual property crime, time theft, credit card fraud, transmission of viruses and unauthorized access to computer systems.

B. Government
The growth of Internet has broadened the horizons for criminals to use cyber space as a medium to terrorize civilians and threaten the government. Internet terrorism is a common example of this category. In this, the criminals attack government websites. The criminals here can be terrorist or unfriendly governments of other nation.
C. Individual
This type is in the form of cyber stalking, email spoofing, spamming, trafficking and cyber stalking. Today, the governments are more concerned about this category and are seeking help from other nations as well in order to arrest the perpetrators.

III. Reasons Behind the Success of Cybercrimes
The traditional method of cyber security is designed in a very sophisticated way to analyze and get rid of these security breaches. Today, IT leaders are losing control of the technology. The modern day infrastructure is growing at a rapid pace.

Traditional methods such as using firewalls and anti-viruses, is putting enterprises in jeopardy. The improvement in today’s attacks are far more complicated for the traditional tools like firewalls and antivirus software. These methods are an obsolete way of securing our computer network and its high time to past them.

One of the main reasons behind these cyber attacks is the use of these software’s for securing the systems. People still use passwords and pin codes to ensure the safety of their accounts in the cyber space. But these passwords and pin codes can be decrypt very easily, leaving them vulnerable against these attacks.

The average security threats are discovered approximately 6 to 9 months after the actual breach is committed. In order to avoid these attacks one should use impenetrable system that uses a unified system of software and hardware to validate any data that is send or received over the cyberspace. What we are seeing is the result that the attacks and threats are far bigger then they appear.

One such method used to identify and prevent these attacks is SIEM i.e. Security Information and Event Management systems and it uses a lot of planning to implement. This technology collects log data from different systems across the world to discover any suspicious activity or behavior of any kind. It is a very time-efficient software for the administrators.

This technology is being used in the industry since 2000 and they had a goal to help enterprises detect cyber frauds and data beaches at an early stage. SIEM programs do not reduce cyber attacks by itself, but help the authorities to detect these threats as early as possible by using functions like correlation of data from multiple devices, known anomaly patterns, etc. from many devices so that necessary steps could be taken. SIEM solutions can be very useful in events such as :

- It can assure that antivirus and Operating Systems Software, are all updated, and are capable of generating logs.
- can monitor doubtful user authentication
- can be used to monitor servers to find out if there has been any unauthorized attack
- can process which systems in the network have been affected by viruses and if the other systems are getting affected or not
- can provide all accessed files, especially the ones with private access

But despite being so efficient it does have some disadvantages. This software often ends up costing more than expected. SIEM technology requires proficiency that can sometimes be outsourced. It can be difficult to tune and it sometimes takes considerable amount to yield results.

Because SIEM technology collects structured data, there is not a very large volume of data that can be processed. This can cause collateral damage to the organization. These tools are not prepared to meet the needs of the modern architecture. We need to build software and enhance security systems that can actually add value. To have new approach and thinking.

This is where the Big Data analytics comes in play. The main aim is to give the next generation the tools and methods they need, in order to detect these attacks without the need of the Hadoop administrators or any other the scientists. The criminals have gained expertise in becoming almost invisible in the activities, it is needed to have something off their charts; hence a combination of Hadoop tools with well-programmed machine learning models.

IV. The Big Data Analytics
Big Data is large-volume, large-velocity and large-volume information assets that demand efficient, innovative forms of information processing for better
decision making. Unlike traditional analysis methods, Big Data Analytics helps expose invisible structures, unknown correlations and other important organizational information. However, big data tools can analyze this data far better than the traditional methods that struggle processing big data within a specific period of time and at an unacceptable cost. As the industry is growing, so is the data within. Today almost every organization is processing terabytes of information every day. Because of this the threat to these organizations has also increased. The term Big Data and Big Data Analytics is majorly used when we are concerned with large amount of structured as well as unstructured data with could previously not be handled. Many industries nowadays are using Big Data Analytics to overcome the security needs, for example the banking sector to detect transactions frauds.

Big Data analytics is developing effective defenses against cyber threats. Better and faster security management tools are reducing the critical time from detection to remediation, making it possible to identify frauds and breaches as soon as it occurs. It also helps us to question from observation, formulate new hypotheses, explore and discover new concepts, and make decisions. The main efforts done by big data analytic is the use of new analytics techniques on either new data or data that has been mixed in new ways.

Big Data Tools is the first step towards the cyber security, using machine learning, text mining and ontology modeling for detecting threats and attacks. One of the main components of the Big Data Analytics is the Hadoop by the Apache Network Foundation. Hadoop is an open source software mainly designed to process large amount of information. It provides a programming model called MapReduce to implement parallel processing. With this, Hadoop also has a distributed file system called HDFS (Hadoop Distributed File System) to store and process manipulate large data sets.

Equipped with these abilities, the scientific researches identify new possibilities to practice new methods and technologies. The Hadoop ecosystem has reached a level of maturity and capability such that more and more organizations can use it for more and more cases. The main purpose of Big Data Analytics is to become more effective in recognizing the pattern that represents network threats by learning more about the organizations’ cyber security defense mechanism.

V. Hadoop

Hadoop is an open-sourced computational software for processing and analyzing large amounts of structured and unstructured data. It is built as a java platform and is designed to execute queries and other operations against large datasets that can be tens of terabytes and even petabytes in size.

Hadoop has multiple concepts like HDFS, MapReduce, HBASE, PIG, HIVE, SQOOP and ZOOKEEPER to perform the easy and fast processing of huge data. In a Hadoop cluster, data is distributed to all the nodes. A MapReduce program has two steps: the Map function analyses input data and the Reduce function collects this result to form the final result. Each cluster node has a local file system and local CPU on which the MapReduce programs runs. Data is broken into small packets, stored on different nodes, and are stored in a three different locations for security issues. There are many nodes in each cluster in the machine. Hadoop is also used for web searches, email spamming, recommending search engines and for analyzing unstructured data.

Today Hadoop is used in almost every aspect of the society. The scientific community uses Hadoop to monitor natural phenomenon. The science and intelligence society needs to analyze large amounts of data generated by servers, email, instant messaging etc. to identify potential terrorist threats. The publishing industry uses Hadoop to index and reformat huge document stores.

A Hadoop based cyber security system can unlock any mystery regarding the cyber attacks. With a variety of processing options and algorithms available, scientists and researchers can now have a real idea about the situation and what can be done. The following list gives an overview of some cyber security projects using Big Data technology (especially Hadoop and MapReduce).

A. DOFUR/DDoS forensics using MapReduce

DDoS or the Distributed Denial of Service attacks has become serious as one of the menace in the Internet society. This attack is an attempt to make the Internet services unavailable to the customers by creating large
amounts of data logs. These attacks can take down a whole website in a very short period of time. A DDoS is not any random attack but well planned and coordinated. With the large data sets generated, the administrator finds it very difficult to know the exact source of the attack before it's too late. The entire process is divided into 4 steps:

- **Data Collection:** Event data, logs are collected from firewall. This collected data is collected in big data appliances.
- **Data Processing:** This step checks whether the collected data satisfies certain requirements. Then it is analyzed and processed using No-SQL, Hadoop and Map reduce methods.
- **Data Analysis:** The data from previous step is again analyzed using prediction and classification to gain insight of the user behavior, system status or any malicious activity in the system.
- **Result:** If attacks are detected, it informs the administrator and terminates. Predicted information of analyzed system is reported to the authority.

### B. APTs

APTs are network attacks where a criminal breaches security firewall of a network to gain access to unauthorized data. The person stays there on the network hidden until he is able to steal data or personal files to cause damage to the organization. Big Data Analytics is a suitable method for APT detection. The main problem in detecting APTs is analyzing large data-sets for any abnormality. This large amount of data makes the analyzing process look like finding for a needle in a haystack.

### VI. Conclusion

The WWW seems to be a massive environment but surprisingly one of its qualities, bringing the world closer is making it a small place to live in for its customers. Cyber attacks are a danger to the organizations. Bad guys have better weapons and the organizations are becoming vulnerable. We need to develop new software’s for securing networks. The problem using large volume of data for identifying a cyber-crime is the skill to quickly process and identify threats before it's too late. Big data analytics are used to identify unusual behaviors, identifying threats and allowing instant action to minimize or prevent losses. It provides real-time security measures to discover threats that are unlikely to discover. By using Big Data technology such as MapR Converged Data Platform, these organizations can fortify the national security; transform teaching, and much more. Big Data Analytics tools provide enterprises a cost-efficient and stable architecture to analyze various unstructured and structured data in no time.

### References

1. AFCEA Cyber Committee- *Security and Cloud Computing*
2. Journal of King Saud University – Computer and Information Sciences (2013) 25, 63–75
3. Georgia Tech Research Institute Cyber Technology and Information Security Laboratory- *Cyber Security:*
4. International Research of Scientific Research - *Cyber security a challenge to developers, is face recognition technique a solution to this problem?* Volume: 2 | Issue: 7 | July 2013 • ISSN No 2277 – 8179
8. Information Systems Group Saarland University - *Efficient Big Data Processing in Hadoop MapReduce*
Compartive Analysis of Visual Cryptography Schemes

Pramod Kumar Soni*
Madhu Chauhan**

Abstract

Visual cryptography is a technique to encrypt images, any handwritten notes or typed text which is in the form of images. Security is a major aspect when transmitting information in modern era of information technology. Cryptography is basically uses the techniques of mathematics to provide the basic aspects of information technology such as confidentiality, data security, and authentication. The VCS is a method that hides a secret image by partitioning it into small parts. A distinguish property of VCS is that one can easily decrypt the encrypted image by superimposing parts without any mathematical computation as we did in cryptography.

In this work we are analyzing the different techniques in Visual Cryptography on parameters of security efficiency and computation techniques.

Keywords: Visual cryptography; Halftoning, Watermarking.

I. Introduction

Visual cryptography is a cryptographic technique that allows us to encrypt text or pictures without any requirement decryption algorithm or technique. To decrypt the data, human eye or analysis is required. This method was developed by Naor and Shamir in 1994. This is one of the methods to securely share our data. In this scheme the image is divided or broken into certain number of shares, say n. the original data or image can only be decrypted if all these n shares are combined. If any of the share is missing, the data cannot be decrypted. This technique is used to broadcast secret message.

The basic model proposed by Naor and Shamir work on binary image, in which a image is divided into m number of parts (shares). Each pixel of image is denoted by n sub pixels in m image parts (shares). The resulting structure of each sub image is described by a unit matrix A where $A = [A_{ij}]$ an [m x n] matrix where $A_{ij} = 1$ if the $j^{th}$ sub-pixel in the $i^{th}$ sub image is black $A_{ij} = 0$. If the $j^{th}$ sub-pixel in the $i^{th}$ parts (share) is white. When the parts (shares) are grouped together in last in first out manner secret image can be obtained but the size of image is increased by n times. The grey levels of each pixels in decrypted image is proportional to the hamming weight $H(V)$ of the OR-ed Vector “V, where vector “V is the grouped sub pixels for each original pixel. A solution of the “n out of “m visual secret sharing consists of two collections of m x n Boolean Matrices M_0 and M_1. To share a white pixel, randomly choose one of the matrices from M_0, and to share a black pixel, randomly choose one of the matrices from M_1. The following conditions are considered for the construction of the matrices:

Advantage of Visual Cryptography

- The major benefit of visual cryptography is that decryption algorithm is not required.
- This Technique is easy to implement.
- Computational cost is low as secret message can be identified by human eyes.
- Cipher text can be send using e-mail and fax.

Disadvantage of Visual Cryptography

- When the message is decoded, there is some change in aspect ratio which may lead to loss of information as there is pixel expansion (to almost double) during decoding
- Sometimes it becomes difficult to align the transparencies in proper manner.
- For colored images some additional processing is required.
Major Application Areas of Visual Cryptography
- Remote Electronic Voting
- Biometric System
- Bank customer Identification
- Watermarking
- Steganography

II. Visual Cryptography Techniques
A. Visual cryptography for gray level image
Earlier efforts in visual cryptography were limited to binary images which is inefficient for real time processing. ChouLin proposed visual cryptography for gray level images by dithering techniques. A dithering technique is used to transform gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to complete the work of creating parts (shares). The effect of this scheme is satisfactory in terms of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

B. (k: n) Scheme of visual cryptography
K by n scheme can be considered as an extension to the basic model which was proposed by Naor and Shamir. In this scheme n shares are generated out of original image. Original image can reconstructed only if k or more shares are stacked together such that 2<k<n. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained i.e. the original image can never be obtained if one has k-1 shares. If k=n, then all participants are required to reconstruct the secret.

C. Halftone visual cryptography scheme
Halftone visual cryptography introduces digital halftoning technique which has broadened the area of visual cryptography. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. These schemes make use of error diffusion as it less complex and provide good quality halftone shares. The text/image to be encrypted is embedded into binary valued shares and these shares are half toned by error diffusion technique.
D. Extended Visual Cryptography

Traditional VCS produces distorted images on decryptions. It suffers the problem of managing pixels on decryptions; because of these readers cannot visual identify the shares. This shortcoming is solved by EVCS (extended Visual cryptography scheme), which alters the working of traditional visual cryptography by adding a meaningful information to each share i.e., a cover page. In EVCS consists of two phases in first phase, a meaningless share is constructed using an OT and traditional Visual Cryptography scheme is used for construction. In later phase additional information in the form cover page by a stamping algorithm. The result shows that the problem of pixel expansion is also resolved.

E. Random Grid Visual Cryptography

A random grid based Visual cryptography scheme used to generate meaningful as well as meaningless shares. First, analyze the distribution of pixels on the share image and stack image. A probability allocation method is introduced which is capable of producing the better visual quality in share image and stack image. With this method, it not only hide the secret image by using different cover images, but also visual quality of images is improve as needed. The important part is improvement of contrast of both secret and stack images to their theoretical maximum. This method is superior to past methods for visual secret sharing.

Pixel expansion and visual quality are major problems in VSS. To solve the pixel expansion problem random grid approach is used, which consider share as big as original secret image. Here, Contrast enhanced VSs [8] and void-and-cluster base post processing [8] methods are introduced to improve contrast of reconstructed image. In VAC algorithm, arrays are constructed which works in terms of majority pixel and minority pixel. If less than half pixels are black then they are minority pixels and majority pixels are white. Cluster and void are used for arrangement of minority pixel in background of majority pixel. In homogeneous distribution, minority pixels are added in center of large void and majority pixels are added in center of tight cluster. So, optimal visual quality is obtained by applying contrast enhanced RGVSS and reconstruction of secret image is obtained by VAC based post processing method.

F. Multiple secret sharing VC

All the earlier research works in visual cryptography were aiming on securing only singe image at a time. Wu and Chen [10] were first researchers, who invented a visual cryptography scheme to share multiple secret images in two shares. In this technique, two secret
binary images can be hidden into two randomly generated shares, namely X and Y, such that the first secret can be seen by stacking the two shares, denoted by X—”Y, and the later secret can be obtained by rotating X by 90 degree anti-clockwise. J Shyu et al [11] proposed a scheme for multiple secrets sharing in visual cryptography, where more than two secret images can be secured at a time in two shares. Later the angle the restriction of rotating angles of 90°, 180° and 270° is removed by Wu and Chen.

G. Progressive Visual Cryptography Technique
In progressive visual cryptography scheme for color images without any pixel expansion based on the halftoning technique. Progressive visual cryptography scheme is a special encryption technique which can be utilized to recover the secret image gradually by stacking more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of shares being stacked, the details of the hidden information can be generated progressively. Firstly, a chromatic image is divided into three monochromatic images in tones of RGB (Red, green and Blue). These three images are transformed into binary images by halftone technique. The secret image shares from binary images are obtained by the unexpanded VC algorithm. To prevent attack from hackers, the secret image shares are watermarked with different cover images (additional information) and are transmitted. At the receiver end the cover images are extracted from the shares and stacked one by one which reveals the secret image progressively. This scheme provides a more efficient way to hide colour images in different meaningful shares without any pixel expansion, providing high security and recovered images with high contrast.

III. Comparison of Different Visual Cryptography Techniques
Factors on which VCS schemes are compared and final summary is presented.
- Improve visual quality
- User Friendly
- Meaningless share
- Improved contrast in share and stack images.
Table No. 1: Comparison of Different Visual Cryptography Techniques

<table>
<thead>
<tr>
<th>Technique used</th>
<th>Number of secret image</th>
<th>Merits</th>
<th>Merits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional VC</td>
<td>1</td>
<td>Provide security for binary image</td>
<td>Not generate meaningful share image</td>
</tr>
<tr>
<td>Extended VC</td>
<td>1</td>
<td>Generate meaningful share</td>
<td>Contrast loss occur</td>
</tr>
<tr>
<td>Multiple secret sharing VC</td>
<td>2</td>
<td>Image can encrypt two secret images between two shares. Rotating angles is 90°</td>
<td>Size of the shares is 4 times the size of the main secret image.</td>
</tr>
<tr>
<td>Progressive VC</td>
<td>1</td>
<td>No pixel expansion</td>
<td>No absolute guarantee on the correct reconstruction of the original pixel</td>
</tr>
<tr>
<td>Halftone VC</td>
<td>1</td>
<td>Provide meaning full share images</td>
<td>Tradeoff between pixel expansion and contrast of original image</td>
</tr>
</tbody>
</table>

- Reduction of restriction for encryption process
- Visual quality analysis
- Security Analysis
- User friendly

IV. Conclusion & Future Scope

In day to day life, it is important to provide security to digital information. Since, Visual Cryptography is one of the techniques used for secret sharing of images. It uses a general access structure (GAS) algorithms and provides an image of high resolution with outstanding visual quality. In this user-friendly secret sharing method not only security is provided but pixel expansion problem is also removed. It also produces meaningful shares which is easy to carry and manage. Encryption is performing on all pixels in the cover image and secret image, which guarantees that visual quality of share and stack image can reach the theoretical maximum.

Also, Encryption method is flexible to use. In this paper we had presented a comparative analysis of different visual cryptography techniques used by programmers and researchers in computer science on different parameters as discussed above.

Visual cryptography is the current area of research where lot of future scope exists. Right now different cryptographic techniques are is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. Visual cryptographic work can be extended with the format of color images, three dimensional Images, better quality color images, more number of shares and multiple secret images.

References


12. mizuho nakajima, yasushi yamaguchi, “extended visual cryptography for natural images”,
Securing Database using SQL Injection: A Review

Isha Shingari*
Priti Sharma**

Abstract
In one way or other we all are connected with internet. All web applications are dependent on the internet. Now a day’s web applications play a vital role in everybody’s life. Exponential growth could be observed in many user friendly web applications. Thousands of transactions are done daily through these applications, 80% out of which are vulnerable to malicious attacks according to the survey by the Open Web Application Security Projects (OWSAP). SQL injections is the highest security threat for web applications. SQL injection is a mechanism for inserting a malicious code in user code. Results in adding or modifying data, leak of confidential information, bypass authentication, performing denial of service, network hacking, table structure, and deleting the database. In this paper we have discussed the various aspects of SQL injection.

Keywords: malicious code, Vulnerabilities, SQL injection, Web applications, Attack, Database component; formatting; style; styling; insert (key words)

I. Introduction
In last decade the user of the internet has rapidly increased so as the web applications. Web applications are the applications that can be accessed over the internet with any browser on any operating system.

To serve numerous users, great volume of data is stored in web applications database [5] all around the world. Security threat in web application is becoming a headache for the developers. Web applications that are not carefully designed (in security terms) are more prone to SQL injection attacks. SQL injection is a kind of code injection in the web application in which attacker add unauthentic code in to the user code to get unlimited and authentic access.

The attackers code is sent in such a way that it is interpreted as a query. SQL injections are very hazardous because it opens the flood gate for various hackers to do what they look for. SQL injections have the capability to affect the SQL query that sends to the backend database [6] such as username, passwords and feedbacks. SQL injection takes advantage of security vulnerabilities in the database. Attackers make use of these flaws to submit malicious code.

According to a survey conducted by OWSAP [11] SQL injections (SQLIA) was measured as top 3rd ranked attack in 2010 but in 2013 it is topped in list of vulnerabilities. The vulnerabilities in website database are outcomes of unsuitable programming due to which an invader can exploit and access the not to be disclosed information.

II. SQL Query Basics
For the better understanding of SQL injection, Lets discuss some basic about SQL query. SQL is (structured query language) textual language interacted with relational database [4]. The query is the collection of statements which a single result set is returned. Database is responsible for storing the information on the servers. The authentic contents of database are marked as rows in the tables [5].

Whenever a query is generated to make a request for an exact set of information from database it initiates the connection with database then performs a query. The query will return only specific row/rows against the request. So the attacker goal is to induce the database query to return the extra rows that were not requested by the user.

So it can be concluded that if an attacker convinces the database or the server to return any row/rows from the users table then they should be able to authenticate illegally.
III. SQL Injection Attacks

Web application consists of many interlinked components and each component plays a significant role in correct working of the web application. Browser sends the request to the web server and returns the desired result. The communication between web server and database is done by means of SQL commands.

With the help of SQL commands attacker can get the access to the user information. SQL injection is an attack on web applications which have vulnerabilities. Actually these vulnerabilities happen due to the weakness in the design of web application due to semantics, logic or syntax. The attackers can put in a crafted query in form of SQL command which is then executed by a web application and bare the back-end database.

The attacks are occurred through user inputs without proper validation. The idea of SQL injection covers following points: SQL injection occurs due to the vulnerabilities in design. The Integrity, Privacy and Security of user are at stack. *SQL manipulation and Code Injection are used for attacks.

* Attacker used special crafted input to attack the system. * SQLIA helps the attacker to get the control over application database.

IV. Basic Principal in SQL Injection SQLIA

It happens where flaws are found in design of the applications. These loopholes can seep out the confidential/sensitive data. For understanding the basic the principal of sql injection, consider the simple example of a login form. The registered user has to submit user name and password.

If an attacker wants to put in malicious code in form of sql injection then the attacker attempts to get the admittance to the database illegally by manipulating the conditions in sql query. This attack generally happens during the processing of the request by providing inputs by the user. For example: Normal

Query: SELECT * from table name WHERE user=''' and password='''

The above SQL statement shows two inputs which user has to provide. Say user name= Ria and password is =steps3 Instead of typing the actual username and password, if the attacker attempts illegally to access the database by adding malicious code (SQLIA). The attacker provides inputs ‘any text’ OR ‘1’=’1’ in user box and ‘——’ in password box.

Query with injection SELECT * from table name WHERE user='abc' OR '1'='1' and password='——';

Now the attacker has the access to system because condition 1=1 is always true and — indicates the comment statement. This shows the loopholes of the application i.e. the input variables are not properly checked during design stage of the application. Consider another example with a normal statement which will return customer information according to customer names. Where Relation name is Customerinfo, Desired Attribute is Name and condition is, Name="Ria"

Input: SQL> select Name from Customerinfo where Name ="Ria"; Output: Name Ria Output will display only desired result i.e. only one Name But when a few SQL injection statements are executed then the results will be according to the attacker's intention

Input: SQL> select name from customerinfo where name ="Ria" or '1'='1'; Output: Name Ria Kartik Mihika It will provide the list of customers under the attribute name. SQLIA will provide the unlimited and unauthorized access to the user database. That's why it is considered as a top threat for the application.

SQL code injection attacks can be executed in two ways- code injection and manipulation of SQL statements. Code injection involves the insertion of new SQL statements or database commands into the SQL statement. SQL manipulation modifies the sql statements through set operations.

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.
V. Process for SQL Injection
In this process the attacker adds SQL statements through user input fields to get the access to the backend resources. Lack of proper sanitization of inputs becomes the cause attacker to be successful. The process of SQLIA involves three steps [9]
Step1: Attackers send malicious code to web application in the form of request
Step2: Creation of SQL statements The above figure shows the client send the request (HTTP request) to the web server and web server send the request to the database.
The database has relational tables containing data. The data could be extracted from these tables by using SQL commands. As processing of queries and result of these queries will be communicated between web server and the database server through DBMS .So we can observe that SQL injection attacks occurs with some modification in Commands.
VI. Ways of Injecting Code
The most frequent techniques [2] used for injecting Malicious SQL statements in an applications are:-
Through user input: In this case, attackers inject SQL Commands by providing rightfully crafted user input. The attacker targets that web application in which user provides information and then request is processed. Like HTTP GET or POST Requests [8] [12] Through cookies: Cookies stores information on client machine generated by web application.
If a Web application uses the cookie’s contents to build SQL queries, an attacker can easily attack by putting [12] it in the cookie. Through server variables: Server variables such as HTTP, network headers etc. are used for knowing the logging usage and identifying browser trends. The attacker can assault using forged header [2] in the server variables when these variables are logged to the database.
Through order: The attacker can just enter a malicious string and manipulate code to be executed instantly (i.e. in a direct manner) or by some other activity (i.e. in an indirect manner). The attacker can also modify the implicit functions by making some changes in the values. Through database: The attacker introduces the attacks by SQL manipulation. The attacker modifies the existing SQL statement [9].
This SQL manipulation attack can be through Inference, Basic Union Queries, and Piggy-Backed Queries &Tautology
VII. Injected Code Storage Areas

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary</td>
<td>Earlier application search criteria and other cached data.</td>
</tr>
<tr>
<td>Short-term</td>
<td>Information put in daily/weekly logs that are reviewed irregularly or over written/purged frequently Storage Type: Long-term Storage Example: Data permanently stored in backend systems that must be physically removed.</td>
</tr>
</tbody>
</table>

VIII. Attacks Performed by SQL Injection
Bypass authentication: Allows an attacker to log on to an application without supplying a genuine user name. For Example: SELECT Emp_id from Employee username=' 'or '1'='1' and password=' '; _where _ _ As the condition 1=1 is always true and —— is used for comments, so comments will be ignored and the attacker can enter the system without proper authentication. Information disclosure: Attacker can directly or indirectly get in touch of sensitive information from a database. In this type, the attacker uses union queries which contain set operators. For example: SELECT Salary_info from Employee where user name=‘abc ‘ and password=’ ‘ ; UNION SELECT Salary _info from Employee where Emp_id= ‘1234’ ; The first part of query gives null values but has the right to the information of employee having id 1234 Unauthorized knowledge of database: In this type the attacker injects a query which causes a syntax or logical error in to the database.
On the basis of the resulting error message the attacker pulls out the information regarding the details of database being used. For example: SELECT Emp_id from Employee where user name="xyz" and password=’@#$%^&*’ The query is incorrect. An error message is displayed due to improper syntax. The attacker uses this message to extract information about the database in being used by user.

Compromised Availability of Data: Attacker deletes or removes information with a harming intention. This can be implemented when an additional query is added with main query. For example: SELECT Salary_info from Employee where user name='abc' and password=''; DROP table user: First query is null so the system executes the second query and will delete the table from the database. Remote command executions: It allows an attacker to host operating system accessible by performing a command execution.

In this the attacker performs remote execution of procedure by injecting queries.[7] For example: SELECT Emp_Salary from Employee where username=’’; SHUTDOWN; and password=’’; In above query only SHUTDOWN operation will be performed which shut down the database.

IX. Why SQL Injection Still Works
After all of these years, SQL injection vulnerabilities still stand as an old reliable for attackers looking for to break into corporate databases. The following are the main reasons [10] Reluctant Behavior: Even after knowing that that SQUIA is a threat, the designers are still reluctant in reducing the attractiveness of database. The data in the SQL database must be encrypted and the encryption key should be somewhere else.

Needs fewer Resources: The resources are required for SQL injection attacks. They are just a computer and rest depends on the capabilities of the attacker. Rest is up to the attacker to which extent the attacker could peep in to our database. Insecure Development Architecture: The biggest reason behind SQL injection is improper development planning and the usage of insecure development architecture.

Protecting yourself from such attacks lies in design and architecture in which a portal is developed, and there are many techniques which can improve the security of a portal against SQL injections. Trusting Input: The shortage of many of techniques comes down to developers and their organizations putting too much trust into user input.

Trust without the verification is one of the key reasons why SQL injection is still so prevalent. Some application developers just don't know any better; they inadvertently write applications that blindly accept any input without validation. If organizations want to reduce the risk of SQUIA then they are required to sanitize input.

Non-belief at All Costs: The Standard Query Language acts as a widespread language that works across database platforms. But that quest to keep application code and application data on a single database server is a double-edged sword because stored procedures or prepared statements are often specific to a database platform.

f) Code Samples Outdated: Most code samples from which programmers take their first SQL programs are susceptible to SQL injection. If organizations use legacy technologies or components that promote construction of ad-hoc queries, then they're likely to boost their risk of SQL injection attacks. g) Budget shortfalls: The monetary constraints are keeping the vulnerabilities active. The cost of writing code and doing new code and ensuring the code is not exploitable.

The cost of running the code repeatedly adds to cost in very competitive market. X CONSEQUENCES OF SQUIA Injection attacks can have sewer effects on database not only they can modify the data but can even hack one’s network. Following are some consequences of SQUIA [9] [10] determining database schema: The attacker can have complete access of the database by knowing database schema.

The attack can be very specific by knowing as table names, column names, and column data types. Extracting data: when the attacker has full access on database the sensitive information can be access which is highly desirable by the attacker. Most of the SQUIA attacks are done for this reason.

Adding or modifying data: Sometimes the objective of attacker is to add or Change information in a
database to mark the presence or to alert the user’s data. Executing the denial of service. When attacker is involved in locking or dropping database tables in the database of web application results in denying service to other user. The attacker can terminate the entire database also.

Bypassing authentications: In this category the objective of the attack is to bypass database and application authentication mechanisms. Bypassing such methods can allow the attacker to presume the privileges and rights associated with another application user.

X. Conclusion

Information is most important asset and achieving the security of the data stored on web is the top priority in this competitive world.

The attacks exploits security vulnerability occurs in DB of an application by injecting some code. Vulnerabilities are becoming the opportunities for the attackers. The absence of good mechanism for accessing the application at design level is exposed. We need a complete methodology for evaluating the performance of the source code in the existing system.

References

1. M. Dornseif - Common Failures in Internet Applications, May 2005
5. Geoffrey Vaughan- Understanding SQL injection attacks inside and out- University of Ontario Institute of Technology, Canada- 2012.
11. www.w3.org/protocols- last access January 2014.
Survey on Cloud Computing Security Issues

Amanpreet Kaur Sara*

Abstract

In today’s reality the most recent pattern in IT is cloud computing. Cloud computing is not another thought but rather has some new features, for example, low expenditure, quick arrangement and trustworthy services. It is a developing innovation in light of grid computing, parallel computing, distributing computing and virtualization. The cloud computing give a chance to IT sector part by opening up another boulevard of giving cloud based services to worldwide associations running from SaaS based application services and remote application facilitating services. The most essential consideration toward any business association is security. Security is exceptionally troublesome assignment to execute at each level in cloud design framework. Hazard distinguishing proof and investigation is vital to organize the usage (degree and time allotment) of governance and controls, and to build up extension for looking into or reviewing cloud computing situations. In view of the noticeable proof and analysis of risk, controls ought to be outlined and executed to guarantee that vital moves are made to control risks and to accomplish business and IT goals. The main objective of this survey paper is on mitigations for cloud computing security challenges as a principal step towards assuring secure cloud computing environment.

Keywords: security challenges; cloud computing; Risks; mitigation.

I. Introduction

The IT world develops from mainframes computers to client servers, the Internet, virtualization and cloud computing. The Cloud Computing is most rising IT business innovation. By “Cloud computing gives a mutual pool of configurable IT services. According to NIST “Cloud computing provides a shared pool of configurable IT resources (e.g. processing, network, software, information and storage) on demand, as a scalable and elastic service, through a networked infrastructure, based upon (pay-per-use or subscription), which require minimal management effort, is mainly based upon service level agreements between the cloud service provider and users, and frequently utilizes virtualization resources”.[1] With the change in time as the IT industry achieve its heights it also captured by many risks these risk acts as main obstacle to an organization to transfer its data/information to cloud. We will discuss these risks and challenges in the coming section.

II. Literature Survey

A. Cloud Computing:

The NIST Definition of Cloud Computing Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1] Cloud computing, also known as a pool of resources, where we can use resources as on demand with the use of internet through some tools without contacting to the server.[2]

B. Essential characteristics of Cloud Computing:

Five important characteristics of Cloud Computing are explained as under:

- On-demand-self-service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

On-demand-self-service:

Client can profit or leave the services as he or she want whenever on the premise of their requests without dealing the service provider.

Broad Network Access:

It has capacity over the n/w and got to through standard mechanism that promote use via heterogeneous slim or thick customer platforms, for example, cellular telephones, tablets and PDAs.
Resource Pooling:
It’s a pool of services of computing resources so that multiple customer can use it with lowest cost or we can say that it reduces the infrastructure cost.

Rapid Elasticity:
Capabilities can be flexibly avail and discharged, now and again naturally, proportional quickly outward and internal similar with interest. To the buyer, the capacities accessible for provisioning regularly have all the earmarks of being boundless and can be appropriated in any amount whenever.[1]

Measured Service:
Cloud computing frameworks consequently control and streamline resource utilization by giving a metering ability to the kind of services (e.g. storage, processing, bandwidth, or active user accounts) (Cloud Security Alliance, 2009, p15).

C. Cloud Computing Services Model :
- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

SaaS (Software as a Service):
Model is referred as on-demand software service. You don’t need to stress over the establishment, setup and execution of the application. Cloud provider will do that for you. You simply need to pay and utilize it through some customer. e.g.: Google Apps, Microsoft Office 365.[2]

PaaS (Platform as a Service):
As the name recommends, gives you platform for computing which ordinarily incorporates operating
IaaS (Infrastructure as a Service):
As the name recommends, gives you the infrastructure, physical or virtual machines (VMS) and many other resources e.g.: Amazon EC2, Windows Azure, Rackspace, and Google Compute Engine.

D. Cloud Computing Deployment Model:
With reference to NSIT the cloud services can be deployed with help of various models which are explained as under:

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

The definitions of the deployment models listed next are taken as it is from the NIST definition, although other researches mention this deployment models with similar definitions.[6]

Private Cloud:
The cloud infrastructure is worked exclusively for an association. It might be overseen by the association or an outsider.

Public Cloud:
The cloud infrastructure is made accessible to the common public or a large industry group and is owned by an organization selling cloud services.

Hybrid Cloud:
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Community Cloud:
The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party.

E. Cloud computing Risks:
Despite the fact that there are numerous drivers for moving to a cloud based arrangement, cloud computing is not without risk or totally secure. The cloud threats connected with every cloud conveyance model change and are reliant on an extensive variety of factors including the sensitivity of resources of information, cloud architectures and security controls included in a specific cloud environment. An intensive comprehension and the change of security risk speak to essential steps towards securing cloud environment and binding the advantages of cloud computing [5]. Taking after is cloud computing recognized security risks:

- Data security risks
- Administration and control security risks
- Logical access security risks
- Network security risks
- Physical access security risks
- Compliance security risks
- Virtualization security risks.

**Data security, Administration and control:**
Information security risk establish the greatest obstacle for cloud computing. Data/information security is a vital viewpoint while information/data in travel/transit, processed and stored. A few organizations are still hesitant to move information/data and applications to the cloud, particularly if basic to the business, because of the danger of information/data spillage prompting privately and security risks, the absence of control over facilitated information/data and applications, accessibility worries of cloud administrations and information, the risk of information/data uprightness hindrance, and ineffectual assurance of information in travel/transit, in rest or in backup because of insufficient encryption.

**Data Privacy:**
*Challenge:* The sharing of cloud structure can prompt information/data security and classification issues [5].
*Solution:* Information that is permitted in the cloud ought to be distinguished and arranged as needs be [5].

**Data control:**
*Challenge:* As the organization does not have any straight control over data being hosted by a cloud service provider so it not easy to protect data and to enforce privacy-identity and cyber-crime security.
*Solution:* External audits should be performed on a regular basis to monitor the cloud service provider’s compliance to contracted terms and the effective execution of security policies, procedures and Standards.

**Availability of data and services:**
*Challenge:* Failure of recovery processes and tested plans are critical in the event of a failure to ensure availability of services and data.
*Solution:* Data must be available and data back-up and recovery schemes for the cloud must be in place and effective to prevent data loss, inadequate data overwrite or destruction.

**Data Integrity:**
*Challenge:* The reliability of networks, applications, databases and system software in a shared, globally accessed cloud environment is threatened by much vulnerability when not adequately and timely patched.
*Solution:* Tasks for efficient patch management should be clearly defined and implemented.

**Data Encryption:**
*Challenge:* A major risk in cloud computing environments is insufficient encryption and key managing of data.
*Solution:* Encryption and key management should be based on industry and government Standards.

**Logical access:** The risks of un approved access to information/data and applications in the cloud. Access by means of an open system and facilitated administrations implies expanded disclosure and thusly more risk. Privileged access rights ought to be allocated suspiciously to approved persons just, and assessment for sufficiency all the time [5]. The execution of security devices and strategies are required to guarantee approved client access to information and applications.

**Network Security:**
Hacking and obstruction risk incorporate attackers accessing information/data and applications through some sort of remote access framework and web application. Assaults like to embed resentful code into standard SQL code with the goal that hackers can increase unapproved access to database or critical information/data [12]. Security risks, for example, man-in-the-center assaults, authentication. [5,12,13] Methods like sifting and proxy based servers which energetically recognize and separate clients for suspected information/data [12].

**Physical Security:**
The cloud administrations brought on by physical access are diverse between tremendous cloud administration suppliers and their clients. These providers ought to be knowledgeable about securing vast server farm offices and have considered flexibility.
among other accessibility methodologies. There is a risk that cloud client framework can be physically upset all the more effortlessly whether by insiders or remotely where less secure office situations or remote working is standard practice. [5]

**Compliance:**
Organizations are at last in charge of guaranteeing the security and integrity of their information, anyhow when it is held by service providers in the cloud. Association further need to demonstrate consistence with security benchmarks separated from the areas of their information/data and applications.

**Virtualization:**
Security risks are normal risk proficient in virtual situations. Full Virtualization and Para Virtualization are two sorts of virtualization in a cloud computing model. In full virtualization, whole hardware architecture is replicated virtually. However, in para virtualization, an operating system is modified so that it can be run concurrently with other operating systems.

Elements affecting security risks incorporate variable workloads, dynamic movement and changes, manager aptitudes, learning and preparing, access controls, antagonistic visitors, the vanishing of “edge security”, multiplication of VMs, setup settings, hypervisor and VM screen layer vulnerabilities, absence of deceivability, absence of procedure administration, and VM server sprawl.

**III. Conclusion**
Concept of Cloud Computing brings many uncertainties to compliance with privacy regulations. So, current privacy regulations are not enough to resolve all privacy concerns related to Cloud computing. Here I gave an overview of risks to security of cloud computing. We also discussed effective mitigations, and introducing elements of security in cloud computing. Security could be one major issue in the adaptation of Cloud computing. Not many organizations are aware of privacy issues in Cloud Computing. Security issues are an active domain of research and experiment at this point in time. Research is on to address concerns related to network security, data protection, segregation of resources and virtualization.

**References**
1. NSIT (The NIST Definition of Cloud Computing, SP800-145.pdf)
Survey Paper on Cyber Crime: A Threat to National Security

Priyanka Khosla *
Praveer Dubey **

Abstract
Cyber security is an activity that facilitates in securing information and information systems (data bases, data centers, networks, computers and applications) with appropriate technological and procedural security measures. This survey report pays attention to the general interest as well as the tension that hinders the privacy and the cyber security. It explores and relates how cyber security challenges are also challenges for maintaining privacy as well as protection of data. It also highlights the way cyber security policy affects privacy and clarifies how cyberspace governance and data security becomes a global issue. Finally, it has given directions to set key policies with a view to generate dialogue on cyber security as an important element of online privacy protection. Firewalls, Antivirus software and other technical solutions that safeguards computer networks and personal data are vital but not sufficient to ensure security. Cyber Security plays a significant role in the overall development of information technology and services provided by internet. "Cyber Security" is the major concern that seeks our attention whenever "Cyber Crimes" is highlighted. Therefore, “National Cyber Security” starts on how fine is our infrastructure to handle “Cyber Crimes”.

Keywords: cyberspace; cyber security; cyber stalking; phishing; bombing

I. Introduction
As “cyberspace” has drawn attention to the global communication and information infrastructure, the safety of cyberspace has now become an urgent and high priority for government and corporations worldwide. Cyberspace is “the realm of electronic world that is created by interconnection of networks of information technology and the information available on those networks. It is a technology available worldwide where 2 billion or more people are connected together to exchange information, services, ideas and friendship.” The term cyber security is commonly understood as any kind of measures or steps undertaken to secure information available throughout the world and to secure the infrastructure on which the information resides. Advent of internet has given a new outlook to the usage of computer in our day-to-day lives and exposed our lives to the complexities of cyber-crime. The ‘borderless’ nature and ‘anonymous’ character of the problem have made cyber security a major concern across the globe. It is being used to carry out multiple forms of cyber-crime viz. identity theft, financial fraud, stealing of corporate information, planting of malicious software (malware)/Trojans, conducting espionage, disrupting critical infrastructures, facilitating terrorist activities, etc.

A. Types of Cyber crime/attack
The internet frauds that are reported in the country are mostly related to money circulation schemes, cyber stalking, E-Mail bombing, spoofing, theft of debit or credit card information, Salami Attack, Web Defacing, pornography, remittance towards participation in lottery etc

- **Cyber Stalking**: Furtively following a person, tracking his internet chats.
- **Intellectual Property Crime**: Source Code Tampering etc.
- **Salami Attack**: (Theft of data or manipulating banking account) Deducting small amounts from an account without coming in to notice, to make big amount.
• **E-Mail Bombing**: Flooding innumerable number of E-mails in the email-box, to make important message unnoticeable at times or to halt the services.

• **Phishing**: It refers to stealing of sensitive data in Electronic Banking i.e. it includes Bank Financial Frauds.

• **Personal Data Theft**: Stealing private data available on web or social networking websites, personal computer systems and email account.

• **Identity Theft**: Stealing Cyberspace identity information of individual, Hacking the personal identity information or employing phishing techniques.

• **Spoofing**: Stealing the Credentials in friendly and familiar GUI’s, Using tools and other manipulative techniques.

• **Data Theft**: Using malicious code like Worms, Trojan Horses, Virus etc to infect computer systems or hacking the computer systems. Employing different methods to install and propagate malicious code.

• **Sabotage of Computer**: Hacking computer with the help of malware.

• **DOS, DDOS Demat of Service**: Flooding a computer with Denial of Service Attacks, DDOS is Distributed DOS attack.

• **Web Defacing**: Infecting the websites by manipulating or adding the spam messages to web pages.

• **Spam and spoofing**: Sending unsolicited emails through manual and automated techniques.

• **Transmitting obscene material**: Transmitting the indecent and nasty content over the social networking websites on web or any kind of electronic media.

• **Pornography**: Publishing pornographic material online on web like on websites, social networking sites etc.

• **Video Voyeurism and privacy violation**: Transmitting personal Video’s on web and mobile phones in the form of MMS.

• **Offensive messages**: Sending or publishing the indecent messages over electronic media like email, websites and social media.

---

**B. Cyber Security Challenges**

A report released in January 2014 from the World Economic Forum examines the emergence for novel and innovative approaches to raise resilience against cyber attacks and recommends that the failure to successfully protect cyberspace could have a consequence of approximately US$ 2.9 trillion by 2020. However, the challenges for privacy and data protection have become a challenge for data security. The consequence is that Cyber security is by no ways a static issue with an everlasting solution. Following are some of the emerging challenges for data protection and cyber security.

- Complexity of the connected environment
- Growing sophistication of the threat
- Threats are moving to the mobile sphere
- The “big data” paradox: is it a bigger risk or a solution?
- For many, breach preparedness is still not a priority

**C. Cyber Security Policy Developments**

Cyber security is an incredibly complex and changing policy issue. No country, organization or individual is ever completely immune to cyber risks, and approaches to protecting against cyber threats can vary greatly depending on the values and decisions that underlie cyber security activities. As the cyber security policy is taken into consideration by the stakeholders, it has become necessary to ensure that the discourse around cyber security includes the acknowledgement of its link to data security on web or on personal systems, faith and privacy.

The following section will consider cyber security policy developments and foreign policy considerations.

**Stewardship vs. securitization**

As cyber security policy has taken a position at a national level, there is possibly a risk that data security at the national level and public safety objectives could take a leading role in formulating responses to cyber thefts or threats, at the expense of privacy protection. In this manifestation, cyber security policy should
promote – “securitization of cyberspace: a transformation of the domain into a matter of national security.” When national security is so often used to rationalize extraordinary intrusions on privacy of individual, it will be imperative to make certain that cyber security approaches and activities do not support building massive surveillance systems for unlimited and endless monitoring and scrutiny of the personal information of individuals. Cyber security efforts should not expand surveillance to the loss of civil liberties, individuals’ privacy or other democratically held values. Governments must build in the necessary checks and controls to reflect the privacy norms we ascribe to as a society. As an alternative, Deibert presents an argument for a stewardship approach to cyber security, where “governments, NGOs, armed forces, law enforcement and intelligence agencies, private sector companies, programmers, technologists, and average users must all play vital and interdependent roles as stewards of cyberspace.” The concept of stewardship in cyber security acknowledges that cyberspace belongs to no one in particular, but that everybody has an influential role to play in shaping its foundation and a stake in its evolution. This alternative approach recognizes that cyber security is a shared responsibility because of the ways in which cyberspace is interconnected and interdependent, and the role all organizations have to play to ensure that their actions do not introduce security risks into cyberspace in general, or fail to uphold privacy principles. A stewardship approach also calls for accountability on all of the stakeholders involved in cyber security: “Securing cyberspace requires reinforcement, rather than a relaxation, of restraint on power, including checks and balances on governments, law enforcement, intelligence agencies, and on the private sector.” As holders of vast amounts of personal information, it is logical to expect that the private sector assume some responsibilities to protect the infrastructure of cyberspace and the personal information that flows through it.

Cyberspace governance and security is a global issue

Given that information flowing through cyberspace is not constrained by national borders, “with whom we share data and where it eventually exists in cyber world is an intrinsic international concern.” As such, citizens of every country face similar risks in the fortification of their privacy rights. Issues of cyber security and privacy protection are global challenges that require a global response.

II. Security Training and Awareness

The human participation is the weakest connection in any information security program. Communicating the impact of information security and promoting safe computing are keys in securing a company from cyber crime.

The best practices used to lessen cyber crimes are explained below:

Use an easy “passphrase” — E@tUrVegg1e$ (Eat your veggies) and make sure to use a combination of lower and upper case alphabets, symbols, and numbers to make it less prone to brute force attacks. Try to avoid simple dictionary words because they are easy target for dictionary attacks – (kind of brute force attack).

Any “passphrases” should not be shared or written anywhere.

Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.

Do not click on links or attachments coming via e-mail from untrusted and unauthenticated sources.

Do not send sensitive business files to personal email addresses.

Suspicious or malicious activities should be immediately reported to security personnel.

Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation.

Educate employees about phishing attacks and how to report fraudulent activity.

III. Recommendations

Utilities should endeavor for real-time situational intelligence data of operational technology (OT) systems’ security posture. Huge damage can easily
be caused due to attacks on utility OT systems that can effect in loss of money and can reduce customers’ confidence in electricity provider. By real time situation data of OT systems, utility can significantly tackle any potential threat in time.

Utilities should recognize that threats can be originated from both either inside or outside of the utility’s systems. For example, anyone within the utility's system can execute an internal attack by using a simple USB thumb drive or a malware can be embedded in new equipment.

Both OT and IT systems are susceptible to cyber attacks due to various networks (and silos) across utility systems. Security gaps are left because of multiple networks often having varying degrees of security and often do not integrate with one common system. These gaps can easily be identified by hackers. Thus, utility cyber security systems are supposed to permit integration of OT and IT networks and scale across multiple service territories and systems.

If utilities work together with vendors using standards based architecture, it will help them to implement scalable security systems that can work in multiple vendors.

Defense in depth is strongly advocated for cyber security by implementing multiple levels of security to achieve

- Prevention
- Detection
- Identification
- Mitigation

Threats will be evolving continuously, but a multifaceted approach to security is a critical defensive strategy.

OT and IT network convergence are driven by new technologies; specialized representative should be established by utilities or office where security liability for all networks is at topmost priority.

IV. Conclusion

The cyber crime threats are ominous and too real to be overlooked. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do something about it. At the very least, every company must conduct a professional analysis of their cyber security and cyber risk; engage in a prophylactic plan to minimize the liability; insure against losses to the greatest extent possible; and implement and promote a well-thought out Cyber policy, including crisis management in the event of a worst case scenario.

References

1. Thilla Rajaretnam Associate Lecturer, School of Law, University of Western Sydney, “The Society of Digital Information and Wireless Communications (SDIWC)”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)
Survey of Cyber Security in Smart Grid

Nidhi Srivastava*
Vivek Vikram Singh**

Abstract
Smart grid is the next generation power system which is an evolutionary regime for existing power system. The smart grids have integrated communication technology with the computing which is in contrast to the traditional power systems. The traditional power systems are not intelligent are used to track power electronics. The big challenge in implementing these smart grids is the susceptibility to cyber attacks. In a smart grid network millions of systems are connected over a communication network so prevention and detection of cyber attacks is a concern. This paper discusses the cyber security issues for smart grid. We focus on reviewing the network vulnerabilities, possible cyber attacks and there countermeasures and architectures in Smart Grid.

Keywords: Cyber Security, Smart Grid, Attacks and Countermeasures.

I. Introduction
In past decades, the power supply demand has increased drastically to which the development of the Smart Grids is not corresponding. According to the statistics the production and consumption of energy in the US has increased approximately two and three times [35]. Apart from handling such increase in demand we also need to manage renewable (e.g. solar, hydro) and traditional resources (e.g. coal, petroleum) efficiently [36]. Therefore, the National Institute of Standards and Technology (NSIT) has addressed the emerging issue by developing next-generation power system, Smart Grid [37].

When compared with the traditional systems, the Smart Grid is seen to be a technology that will integrate power systems to establish two-way communication having very high speed and energy management capabilities. However, such a interconnected network inescapably capitulate to the vulnerabilities of the communication network. Research on Cyber security for the Smart Grid is still in its infant stage, our emphasis is on analyzing the cyber attacks and reviewing the existing solutions. Following concerns are discussed in the paper:

- The objective and requisites of cyber security in the smart grid.
- Possible cyber security threats in the electric power system.
- Countermeasures to the cyber attacks to have attack prevention and defense policy.

II. The objective and requisites of cyber security in smart grid
The Smart Grid network is critical for information exchange. In order to have reliable and secure operation it is required to have thorough understanding of the security objectives and requisites before providing the countermeasures for the same.

The cyber security unit in the NSIT has recently released guidelines for Smart Grid cyber security [14]. We cite three level security objectives for smart grid as shown in fig 1.

- Integrity: Safeguarding against information modification to ensure authenticity and non-repudiation of information. Integrity of information should be preserved as loss of integrity can induce erroneous decision regarding Smart Grid.
- Availability: The information in a Smart Grid network should be delivered reliably and timely. Availability is of utmost importance because loss of it may further pose a challenge in power delivery.
- Confidentiality: Preventing unauthorized access of information to protect personal privacy.
Confidentiality of the smart grid network should be ensured to preserve the information from cyber attacks.

For a smart grid system to be reliable, integrity and availability are the prominent security objectives. Confidentiality is gaining importance in systems that have customer interactions.

III. Architecture of communication Network in the Smart Grid

A. Basic Architecture of a smart grid Network

Electric Power system is complex physical network. There are 2000 power distribution substations and about 5600 distributed energy facilities and more than 130 million customers all over the America [38].

Smart Grid is having 7 logical domains according to NIST’s conceptual model and they are: Bulk Generation, Transmission, Distribution, Customer, Markets, Service Provider and Operations [37]. The concept of two way power in the flow of information is being taken care in the first four domains and working on the collection of information and power management is focused in the other left domains.[5-7] The involvement of all the domains may create the highly circulated and hierarchical model.

The main strength of the network is to establish inter-domain communication where the infrastructure node can start acting as a gateway or as high bandwidth routers to circulate the message across the different domains in the smart grid. In strengthen the network

Fig. 1: Three level security objectives for smart grid

Fig. 2: Basic architecture of a smart grid network
conventional technology is also used to get high speed data and transforming information across the different domains [1-3].

Ad hoc nodes are being used for the intra domain communication which are for sensor meters or intelligent electronic devices (IED’s) configured on the power infrastructure but these are having limited bandwidth and limited computational ability for protection and monitoring purpose [9].

B. Characteristics of smart Grid

- Communication in the power grid is a one way process where electronic devices report their work to the center repository and in the case of smart grid two way communications is followed i.e. up and down and bottom to up[39].
- Smart Grid is not just using IPv6 protocol but also on network functionalities &requirement [10].
- Smart grid is having a feature of millisecond to min in the delay requirement as compare to the IP traffic[12].
- As there is a big issues in the traffic of WWW So we need to have a constant watch on the flow of information and Smart is taken as differ network then this hence could be taken as less traffic area [13].
- In Internet design throughput is the main element among the user whereas high throughput is not provided in the power communication but it provides reliable and more secure system [37].

IV. Classification of Attacks In a Smart Grid Network

Security attacks in communication networks can be categorized into two types: one is selfish misbehaving users and the other one is malicious users. Selfish misbehaving users, try to seize more network resources for their own advantage, by violating network protocols [15-17].

Whereas, malicious users do not have the purpose of their own benefit, they are the disruptive people, who only aim to acquire the access and modify the data and information on the network. Both the malicious and selfish users create challenging security problems to communication networks.

However, malicious users are more problematic to smart grids than selfish users, because so many electronic computing devices are deployed for monitoring and controlling of smart grids. Thus malicious users may create terrible problems to power supplies thought smart grids.

Based on smart grid’s security objectives: availability, integrity and confidentiality, the following three malicious attacks are discussed:

1. Attacks on availability; Denial of Service (DOS): Malicious users attempt to obstruct or delay the communication in the smart grid.
2. Attacks on integrity: Malicious users purposefully modify or disrupt the data of smart grid.
3. Attacks on confidentiality: Malicious users attempt to acquire unauthorized private information from communication network of smart grid.

A. Denial of services attack on smart grids

Basic security objective of smart grid operations is availability. Denial of services attacks can severely interrupt the network communication in smart grid that may cause failure or delay in the operations of electronic devices which is not permissible. DOS
attacks can be explained at different network layers as follows:

- **Physical Layer**: For malicious users attempting DOS attacks at physical layer is very easy. They only need to connect to communication channels rather than breaking into authenticated networks. Jamming is one of the easiest ways to launch physical layer DOS attacks [19-21], particularly for wireless systems. In smart grids, wireless systems are primarily used in local area communication [1,2,3,8,9], so jamming is primarily physical layer attack in smart grid network.

- **MAC Layer**: Responsibility of MAC layer is reliable point to point communication. An intruder may mislead by purposefully modifying its MAC parameters [6,7]. It will provide them with an option of accessing the communication network, and hence the performance of the network will degrade. Therefore, in smart grids, MAC layer malfunctioning can cause weak versions of DOS attacks. At MAC layer spoofing can be more destructive because it can affect both the integrity and availability. In smart grid networks spoofer can broadcast false Address Resolution Protocol (ARP) packets to shut down connections.

- **Network and Transport Layer**: these two layers are responsible for reliable hop to hop delivery. DOS attacks at both layers can severely affect the end to end communication performance. Intruders can use traffic flooding and worm propagation attacks [22-24] to deteriorate the performance of power system network.

- **Application Layer**: The DOS attacks on application layer exhaust the resources such as CPU and bandwidth. These attacks can easily flood a computer with computational intensive requests and hence capturing the resources like CPU and network bandwidth. Most of the devices used in smart grid network are of limited computational capabilities. So they can be easy target for application layer DOS attacks.

In comparison with Internet, smart grid communication requires more time critical messages.

---

**Table 1: DoS Attack in Power System**

<table>
<thead>
<tr>
<th>Communication Layer</th>
<th>Attacks in system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td></td>
</tr>
<tr>
<td>MAC Layer</td>
<td>ARP Spoofing[40]</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Buffer Flooding[41]</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>Substations and jamming [18]</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Traffic Flooding[40]</td>
</tr>
</tbody>
</table>

---

**Fig. 4: Classification of DoS attack detection schemes**
So a DOS attackers do not need to completely destroy the communication network, instead they may launch weaker versions of attacks to slow down the transmission of time critical messages. This can also be severe to power grid infrastructure. Therefore, goal of DOS attacker may be bothering the timely delivery of critical message exchange.

B. Attacks Targeting Integrity

These attacks generally occur at the application layer, since intruders try to manipulate data in the smart grid. These attacks attempt to modify data to corrupt the information in the smart grid. Customers details (e.g.: Balance, Billing and Pricing) or power system data (e.g. device status, voltage reading) are main target of integrity attacks. The false and manipulated data may be catastrophic to power system as well as for customers.

C. Attacks targeting confidentiality:

These attacks, like the integrity attacks occur at application layer. In such attacks intruders do not modify information over communication network; they just steal the desired data by eavesdropping on communication networks. They try to acquire customers’ information like customers’ account number and their usage details. Such attacks have very less impact on the Functionality of communication network, but are harmful because they can steal the unauthorized data.

V. Countermeasures of Cyber Attacks In Smart Grid Network

In this section we will discuss about the key steps taken in the case of DoS attacks to the smart grid and with some current solutions [37].

A. Discovery attacks

Power network as this is the first step to reveal all the attacks and take the counter and take the counter measures for it.

- Signal Strength Detection: - at the Mac layer or at the physical layer dos can be judged by the receiving of signal strength i.e. if RSS of many packets is larger than that of the threshold and the output is comes with the error then we cell it as attack [27,28-30].
- Packet transmission Detection:- If every the transmission result of the packet is found potential attacks by identifying a significant increase of a packet transmission Failure, [31,40,26].
- Proactive technique :- in this method is to identify the attacks on the prior basis and accordingly take action [32,33]
- Cross breed Method :- In this method we are combining all the method on the basis of the requirement of the situation and get best result for the traffic jamming [27]

B. Methods for attacks mitigation mechanism

The dos attacks can be prevents by the mitigation mechanism to save network nodes dos attract mitigation schemes mainly included in two layers i.e. on network layer and physical layer.

- Network layer:- The measures for network layer mitigations are:

  We can create rate limit on some of the packets which can be found malicious the fault detection mechanism discussed above

  Filtering mechanism can be done with black list provided by attack detection with the source address of the packets with the of the different attack detection method.

  By reconfiguring the network architect by switching among the topology of intermediate address to the victim to add more resources to the victim or isolate the attack a machine [24]
Physical layer:- Written network primary dos attack sources on the problem jamming network where wireless network is highly deployed in the local area system in the smart grid.

It is being seen that the scheme of deployment of jamming resilient scheme for deployment of network is done and they are majorly working on either coordinated or uncoordinated manner.[34,18].

Coordinated protocol is the traditional anti-jamming transmission schemes which are already discussed in wireless communication they can be defined as FHSS, DSSS and CSS. These protocols are opening for intentional about protocol [25,11]. Uncoordinated protocols don't repaired the sender & receiver to share a pre-known secret among them salver they time of transmission and couple the transmission.

VI. Conclusion

Smart grid, cyber security has become a new area of research that has attracted huge attention in government, academia and industry. This paper has presented a comprehensive survey that has reflected the security issues present in the smart grid. The survey paper states that cyber security is still in the development stage. There is a need to take information security into account with electrical power systems.

Few of the features of the smart grid communication network such as network architecture, heterogeneous devices, delay constraints on different time scales make it quite impractical to arrange strong security technicians all over the smart grid. Consequently, smart grid requires fine security solutions for different network applications in order to make cyber security challenging area of research in future.

References


Cyber Crime – A Threat to Mankind

Charul Nigam*
Vaishali Singhal**

Abstract

Presently, the cyber space has become the most indispensable part connecting the man, business and life all over the globe. The number of connections & number of users being connected is increasing very rapidly, each year millions of new users are added to the network in various fields of internet such as social networking, online marketing etc. As fast as cyber space is spreading connecting man to man and business to business so is spreading “the world of cyber-crime.” This paper discusses about the recent trends catching up in the Cyber Crime. It also focuses on the categorization and prevention measures of Cyber Crime.

Keywords: Cyber Crime, Cyber Space, Cyber Security, Hacking

I. Introduction

Cyber-crimes are being committed all over the world in various ways such as phishing, DOS attacks and Trojan attacks, email bombing and many more. Apart from this the cyber-crime also include criminal activities committed via internet such as online gambling, fake online sales of articles, theft of any sort of information present in electronic form, cyber defamation, unofficial access to computers etc. During the last decade a substantial growth has been observed in the cyber-crime failing all the several measures being adopted by different individuals and business organizations.

Although the term cyber-crime remains undefined by any justified decree still cyber-crime can be defined as the crime being committed using the computer system and network being used as the medium. Under this the computer system serves both as weapon and the affected victim. Cyber-crimes are being committed by various groups of individuals such as adolescents or children between 6 to 18 years of age group, various kinds of hackers (organized or professional) or discontented employees to name some. The reason behind the crime can be curiosity, business or revenge.

Although mostly being committed purposefully there are still chances of accidents as connecting the whole globe together can't be a cent percent safe road.

Presently cyber space has emerged as a region where both optimistic and pessimistic ideas are developed, enhanced and escalated as soon as they emerge. People not only get influenced by these, but also become part and parcel of them. Cyber space has become a better half of social life of most individuals around the globe and when it comes to society both defeatist and affirmative constitutes the surroundings. While the affirmatives consist of tech-friendly users and professionals the defeatists consist of the “criminals of cyber world” Cyber space is considered as a public space by the offenders where one is free to do anything of his/her choice and do not consider their act as criminal. These offenders exist as old as the internet itself does and are also somewhere to be held responsible for the internet’s present form. Cyber-criminals no longer consist of collegiate but also tech-savvy proficient who don’t only have apprehension of all do’s and don’ts but have also gained white-collar mastery of all the black jobs including blocking a website, posing obscene content(s), black marketing on the web etc. Unsurprisingly the cyber-criminal mostly constitutes the people among 15-34 years of age group.

Although it is practically indefinite to acknowledge how much a cyber-crime does cost they do have numerous monetary and non-monetary effects. While monetary forms include theft under online monetary transactions causing the loss of thousands or millions
and non-monetary may include spread of viruses in the form of applications or programs which may lead to the creation of botnets which can be further be used for the purpose of trafficking leading to the server failure of the host. By the elevating number of devices connecting to internet such as mobiles and tablets the exposure to cyber-crimes has increased several folds as the use of internet not only makes the device multi-tasking, but also provide multiple paths for crime to peek in. Out of all other cyber-crimes being committed theft of identity is considered to be one of the most dangerous in which the host grants the access to all the personal and confidential details including login, passwords, credential details related with online banking and business transactions.

II. History of Cyber Crime

The origin of cyber-crime goes back to 1960 when it started with the form of hacking. Hacking then evolved because of the activities committed by some MIT Model Train Engineers who revived the functioning of their model without actually re-engineering the model but by means of alteration of the source code of some early computers. Then in 1970 the hacking became evident, the hackers then known as phreakers developed codes that was capable of providing long distance service and embedded them in Bell Telephone Company in order to grab the personal information. This activity became a challenge for the legislation and evidence to the fact that the computer systems were a platform for the cyber-criminal activities as well.

The next cyber-crime was accounted in 1986 at Lawrence Berkeley national Laboratory where the malfunctioning of an accounting data was encountered. This was soon followed by the creation of Morris Worm virus by Robert Morris which resulted in the damage of around $98 million damaging 6000 computers and above. After this the legislation under Congress enforced acts and laws stating computer tampering a criminal and punishable offence.

III. Categorization of Cyber Crimes

In the present day, where cyber crimes are increasing day by day it has become strenuous to distinguish between a prevailing crime and a cyber crime. So as to make this demarcation feasible the cyber crime has been categorized as under:-

**Against persons:** These are the offences, which attempts to or actually vandalize the character of an individual. These are the crimes, which tend to degrade an individual’s morale either socially, financially or psychologically. These crimes take place such as by communicating harassing messages, comments, videos, images or by stealing e-banking credential details etc through various means. These crimes intend to defame an individual by accrediting content, either which lower downs individuals dignity or tend to make business by theft in terms of hacking or cracking.

**Against persons property:** These are the crimes, which tend to harm person’s possessions in particular. These
crimes generally come into picture because of the global enhancement of merchandising on the internet. Today both buyer and supplier are frequently making their hand to make business through internet thus leading to huge amount of data being stipulated on internet thus making pace for unauthentic access very common.

Many cases occur where domain names become inaccessible by the use of multiple users claiming the name to be registered either by them based on their registration priority or by accessing the same name. Crime also comes in when the user’s data on the network has intentionally been tempered to cause business failures. Hacking is one of the crucial crimes under this head. Hacking can take multiple forms such as time-theft (which occurs in the case when the charges of internet services are taken on hourly basis), cyber-trespassing (in this case no harm to the device or data is caused but is used unauthentic ally by non-permissible means such as connecting to Wi-fi without its owner’s permission) etc.

Against government: These are the offences done in order to hamper global peace and harmony by means of internet. These are of various forms such as cyber-terrorism (It is a matter of native and worldwide distresses, in this the jurisdiction and nobility of a state is exposed to danger.), cyber-warfare (It is a purposefully done militant act done for the sake of obstruction and counter-intelligence; form of hacking) etc. Internet has made information easily accessible for terrorists, which they use as a weapon for their civic, theological and communal aims.

Against society: Any illicit activity done with the objective to molest the network can be vulnerable to many users. These include both financial and non-financial offences. The financial offences include online gambling (these include different types of gambling offered online such as bingo, poker, casinos, lotteries etc; all these are offensive means of making money) and other financial crimes such as credit card and debit card frauds.

IV. Recent on Cyber Crime

Pakistan based group suspected for hacking revenue based website: Pakistan based group is suspected for hacking the web portal belonging to Income tax department under Indian Revenue service (IRS). The officials reported that the website has become inaccessible from Feb. 7 2016 leading to failure of communication between the central board of direct taxes and the IT department field office. The website had slogans promoting Pakistan territories have been reported by the officials accessing the website.

Japan, Singapore, Malaysia & India sign pacts for cyber security: Three pacts have been signed between Indian computer response team(CERN-In) and its analogue in Japan, Malaysia and Singapore on accounts of Cyber security. The pact was framed and sealed firstly under PM Narendra Modi’s trip to Malaysia in November 2015. This pact will focus on enhancement, development and enforcement of techniques and ideas amongst the three nations to boost cyber security.

Cyber criminals nagged from Kolkata: Three former employees stole the credentials of UK based clients and assaulted money on account of technical assistance into the account faking to be on the firm’s name. The trio maintained the directory for such prey’s using the cloud addressing from where the data was later on downloaded through PDA’s and money extracted was shared between the three.

UK police campaign’s for young hackers: A survey reported that the average cybercriminal age has turned down to 17 thus the Britain’s National Crime Agency has started a campaign aiming to be an alarm for parents of boys belonging to the age group of 12-15 that they should become alert keep an eye on the activities being committed by the youngsters around them as they can turn out to be young criminals in disguise.

900 hackers nagged down by China: After being criticized by the US over inflated cyber attacks by Chinese criminals intending American firms. China has nagged down 900 hackers under their online campaign. Most of those arrested already posed to have a criminal background.

Cyber Crimes to be checked through reporting helpline: A free online helpline has been launched in Delhi-
NCR for reporting cyber-crimes. After the helpline became functional more than 250 cases had been lodged in around a fortnight. Considering all the cases phishing and money-laundering were mostly reported followed by women harassment.

**Above 100 million Indians dissipated around Rs. 16000 on cyber-crime:** Nortan software security firm reported that around 100 million and above Indians have dissipated Rs.16000 on account of cyber-crime and suffered social, emotional and financial harassment. As per the nortan report the users of age group 55 and above considered as less tech-friendly have been to abide more cyber secure habits than the young & more tech-friendly users.

**More than 70 percent Indian firms duped by Cyber attacks:** A survey report concluded that more than 70 percent Indian firms have been duped by cyber attacks in year 2015. Cyber-attacks were considered to be most harmful for the corporate by about 94% said the report.

**Over 125,000 profiles suspended by twitter:** Twitter Inc. had reported that from 2015 onwards 125,000 profiles had been suspended which seemed to promote anti-socialism and terrorism especially related to ISIS.

### VI. Prevention Of Cyber Crime

**Safe-guard your device:** If the device is not properly secured then it is prone to be hampered by the offenders or the offenders can get the access to your credentials on the basis of your device. Always get the latest and authentic security software for your device and do keep them fully updated. Must get your device firewall protected.

**Have a safe “site”:** Be always sure about the links you visit. Always go for safe and familiar links. Do not just blindly follow hyper-links whether they are from emails, profiles or blogs these can be either malicious or fake copies of original one’s leading you to a dangerous situation.

**Obviate “yourself”:** It is highly recommended that one should never send his/her personal details through emails as in such cases the chances of cyber-attacks are highly rated. Authorized corporate never demand personal details through emails.

**Have compelling passwords:** Several software has been programmed having the capability to suspect the passwords. Passwords should be such that they are “hard to crack but easy to grasp”. Always make long passwords of mixed cases that is, including both lower and upper cases. Passwords preferably should be mixtures of characters, digits and symbols. It is endorsed to make multiple passwords for multiple accounts.

**Protect Yourself:** By means of search engines one can easily track other's public information. It is a suggested practice to set your search names difficult. The data provided by the data service providers is not guaranteed to be secured due to their complexity in terms of number of records and the compilation of data from diverse sources and thus there are chances of your public information being used by the offenders for their intended and harmful use.

**Limit your data:** Always make sure to remove the data from your profile as well from other’s profile relating to you and that is under your control once it becomes unwanted for you as it can become a threat in future. It would be rather a safer practice to avoid posting privileged information in the first place.

**Do review your accounts:** Mostly there are three options available on social networking accounts update privacy settings, delete the data or delete the account. If you ever go for deletion of your account always do make sure to delete all your data first. Always prefer for deletion of your account rather than deactivation.

**Communicate cautiously:** While communicating on internet being sure is highly unsure. Always cross check all your communications even those claiming to be trustworthy. Go for links which you are sure about or are familiar with in case of any doubt do not go for it at all.

**Avoid Spams:** Do not respond or reply to any spams as they are surely harmful.

**Prevention is better than cure:** Spotting of vulnerabilities will help associated firms and corporate deal with these challenges.
Avoid pop-up: Never give any credentials as input in any pop-up advertisements. If you want to go for the deals offered by means of pop-ups always contact the dealer by either going to the authentic websites or homepages and not by the links provided on the pop-ups or by any other permissible means.

Keep photographs in safe: due to increased pornography cases, it is recommended to avoid sharing of photographs amongst strangers online.

Keep a careful watch: For underage or less tech-friendly users parents guidance is an advisory in order to prevent future aggravation for children.

VII. Conclusion
Due to the multiplying number of computers and users of internet all around the globe and ease of accessibility of resources by means of internet in fraction of seconds the security has become a major issue of concern. It is neither simple nor practicable to abolish cyber-crime in a single go due to all technological enlargements. Although there is a scope to withstand and scrutinize the cyber-crimes. In order to gain this objective first the users worldwide should be made capable to identify such crimes, made to learn secure and safer tech practices and prevent such offences.

References
1. http://cyberlaws.net/cyberindia/articles.htm
5. www.indiancybersecurity.com/.../8_history_of_cyber_law_in_india.htm
Enhancing ATM Security Using Fusion of Biometric Techniques

Sakshi Singh*
Simranjeet Kaur**

Abstract
Security and authentication of customer’s account is of great concern for all the banks all over the world. Frauds are increasing day by day; hackers are using advance techniques for hacking PINs so there is a great need of strengthening the security and authentication system of banks. This paper focuses on the biometrics, its types, how biometric can be of help in the field of banking for authentication and security purpose. It especially focuses on biometric ATMs i.e. an ATM which takes humans physical traits template like fingerprint and iris scan along with OTP as an input instead of entering PIN.

Keywords: Biometrics, ATM, PIN, OTP, Iris, Fingerprints.

I. Biometrics
Biometrics is a science of recognizing the physical and behavioral traits such as fingerprint scan, iris scan, retina scan, hand geometry etc. of a person.
Biometrics is a security system which is based on these traits of a person which can be checked automatically as these traits are indistinguishable from one person to another person.
There are different levels of authentication based on:
1. Something you have like key, token or badge.
2. Something you know like PIN or Password.
3. Something you are like physical or behavioral traits.
Since biometrics security is based on something a person is i.e. his personal biological traits or characteristics it is considered more reliable than any key, PIN or password.
Biometrics can help in each and every field in the scope of security and authentication, and it is one of the safest ways used for security related issues as it reduces the chance of hackings and frauds.

II. Types of Biometrics
There are different types of biometrics like:
1. Fingerprints: Impression of a person’s finger, usually impression of index finger.
ii. Face detection: scanning a person’s face.
iii. Iris scan: Scanning the iris which is responsible for controlling the size of pupil.
iv. Retinal Scan: Scanning the blood vessels of eyes.
v. Voice Recognitions: Recognizing the sound and pitch of a person’s voice.
vii. Gait: Walking style of a person
viii. Vein: scanning the patterns of vein in the palms of a human.
ix. Signature Recognition: Recognizing a person’s signature which actually checks handwriting.

III. Current Implementation of Biometrics
Use of Biometrics is spreading in various fields. For e.g. In India, Adhaar Card is an initiative of Indian govt. which is based on Biometrics. Three behavioral traits of a person are used i.e. Face detection, iris scan and fingerprints of all the fingers of both hands, then he/she is given an unique 12 digit number known as Adhaar no. and it serves as an identity proof.
Another implementation is for the attendance of govt. employees. It is use to record the attendance and working hours of an employee.
Not only in government offices, but in many organizations in many fields biometric serve as attendance recording system which helps to eliminate fraud.
IV. Biometrics and Banking

World of banking is changing. It is a need of time to strengthen the security system of banks as there is increase of hackers, fraudsters, identity theft and data breaches which have become a major issue for banks.

If the customer will have their unique biometrics attached to their bank accounts, it would be difficult for fraudsters and hackers, and through a biometrics authentication platform banks can verify a customer’s identity.

Biometrics will support banks to enhance security, user experience and solves the problem of PIN and password management issues and provide secure and simplified experience to user.

Biometrics in banking will optimize customer’s interaction, fraud reduction and fraud prevention. Many banks do not feel the need to adopt biometric technology because of its complexity and cost, but recent development in the field of biometrics and customers behavior have helped in changing the views of banking sector. Thus, now banking sectors also feel the need of biometrics authentication in banking.

Customers’ today are not only looking for accessing methods which are convenient than memorizing PINs and passwords and security questions but they also demand methods of accessibility which ensures security.

Biometric based security along with OTP satisfy all of these criteria and it is an attractive way than the two step verification system or just OTP (One Time Password) and is more secure than these methods as well, because using only OTPs and security questions are suspect to be hacked or attacked by malwares.

Biometric is a long term investment not an expense as banks can reduce the frequency of frauds affecting their customers and can reduce the number of incidents of customers having their accounts compromised.

V. Need of Biometrics in Banking

1. It is important to make the bank facilities available to all the citizens of any developing country like India, since there are many people in India who are illiterate or moderately literate. So, biometric ATM will be of great help to the people in rural areas in doing transactions without the need of remembering any PIN or password and with the guidance of audio spoken in local language.

2. Since case of frauds are increasing due the low level of security and hackers can easily hack the PINs, so biometric will serve as a strong security system and customer’s personal data and account details will be secured.

3. Customers today are looking for the transaction methods which are more convenient than memorizing the PINs and the passwords and security questions but they also want the method which ensures security, so biometric is right choice which fulfills these criteria.

VI. Implementation of Biometrics in Bank Branches

In banks, biometrics can be used in bank branches for employees as well as customers. Many banks are already using biometrics for attendance recording.

For customers it can be used in bank branches at the counters of depositing money, withdrawing money, passbook updation and rest of the services provided by the banks. It can be implemented by installing any biometric supporting device at the counters which stores the data of customer containing all the important details of the customer like account no. customers name, his personal details saved with his biological trait used for biometric security system, so that when the customer need to do transaction his biometric template will be scanned and will be matched from the database and he can proceed with the transactions the moment template is matched. This will help people to get rid of filling forms and will save time also.

Adopting a biometric security system can provide banks a convenient and easy way to authorize customers identity accurately and will help in maintaining records of every transaction being processed. This will further prevent frauds as transaction will be processed only when customer’s template authenticated at the counter by biometric scanner will match from the database.
VII. Biometric ATM
An ATM (Automated Teller Machine) is an automatic system which is used to do transactions anywhere anytime. We can withdraw money as well as deposit money. For this a person need to insert his ATM card and PIN as an input.

A Biometric ATM is a machine which is used to perform transaction by taking account holders biometric template as an input and if the template is matched then an OTP will be generated and will be send to the customers via sms and then transaction will be proceeded further.

VIII. Process of Fingerprints Recognition
Fingerprint scanner is an electronic device which takes the digital image of patterns of fingers. The image is taken through lights emitted by specialized digital cameras or scanner. Top layer where we put our fingers is the touch surface. Below which there is layer of phosphor which emits the visible light responsible for illuminating the image and pattern of fingers, and then converted into digital form and is compared with the similar type of images stored in database.

IX. Process of Iris Recognition
In the process of iris recognition person keeps his eyes in front of camera maintaining 10-15 cm of distance then the camera takes digital image of the iris with the help of both the ordinary light and invisible infrared. The infrared rays helps in identifying the unique features of eyes then computer keeps image of iris only removing unnecessary details like eyelashes and identify around 240 feature which are unique from person to person and eye to eye and these unique features are converted into 512 digit number which is called as Iris Code which is different eye. Now this iris code is stored in database along with rest of the details of the person. When the person goes for iris scan, the system will check his iris code and the will match from the database.

X. Proposed System for Implementation of Biometrics in ATMs
Biometrics can also work for transaction processed in ATMs. It can be used as best suited technology for ensuring identity. It provides fast and accurate identification thus, enhancing security for authentication.

A typical ATM have two inputs one is card reader and other is keypads or touch screen display screens. Since ATM takes a magnetic card called ATM or debit card and PIN as input for performing a transaction. We can replace PIN by just putting or installing a biometric device as input device which will take combination of customer's Iris and Finger Print as an input. This fusion of customer's physical traits i.e. Iris and Finger Print will then be matched with the existing template in the database provided by network provider and then an OTP will be generated which will be sent to the customer via sms. After entering the OTP in the system the transaction will be processed.

XI. Advantages
1. *Strong and Robust Authentication:* Since biometric security is based on the physical or behavioral traits which are unique from any person to another. Its combination will provide a strong security system.
2. *Suitable for illiterate or barely literate people:* It is best suited security system for those people who are not literate and for those who have difficulty in remembering PIN.
3. *Accurate and quick Authentication:* Biometric system provides a convenient way for banks to authorize customers accurately and quickly.

XII. Conclusion
ATM is technology which provides financial services in many countries. Biometric is a technology which is already accepted by many for security purpose. Combining Finger Print and Iris and then generating OTP will give a robust security and authentication in ATMs. It will not be helpful only to people living in urban areas but also to the people living in remote areas. It is a complex and expensive method but it helps in reducing frauds and can reduce the no. of incidents of customers having their accounts compromised. Thus, it is an investment not expense.
References

Comparative Analysis of IDS Approaches and their Techniques

Osheen*
Manpreet Singh**
Raj Kumar Singh***

Abstract
With increase in the reliability of today’s generation on the computer systems and internet networks, it is important to maintain a secured network around us so as to retain security of data as well as the systems. During recent years, number of attacks on networks has dramatically increased and consequently interest in network intrusion detection has increased among the researchers. This research paper will provide an overview of the “Intrusion Detection System” as a whole. This paper will focus on the intrusion detection techniques, its approaches, the securities against the intrusions and the challenges to the techniques used against intrusion.

Keywords: IDS (Intrusion Detection System), NIC (Network Interface Card), Threshold, Anomalous

I. Introduction
The network based applications are becoming an attractive target for vulnerabilities which affects all the actors involved to it, be it the owner of the application and the application in itself too. The most common threat to computer security that we are all aware of are the viruses. There is yet another very common or in a specific way the most publicized threat called intrusion. The concept of intrusion detection was introduced by Anderson in 1980. According to him “An intrusion or threat is a potential possibility of deliberate unauthorized attempts to

- Access information
- Manipulate information, or
- Render a system unreliable or unusable”

Classification:- Anderson also identifies three classes of intruders:-

- Masquerader: These are the ones who are not authorized to use the computer and emerge into the systems access controls, exploiting the account they are likely to be outsiders.
- Misfeasor: A misfeasor is one who may not have an authority of access and he/she has an access authority, he/she misuses privileges. A misfeasor is generally an insider.
- Clandestine User: This one seizes control of the system and uses this control evade access controls or suppress audit collection. This user may be an insider or an outsider both.

II. IDS (Intrusion Detection System)
Before any attack could be prevented, it needs to be detected. The research of detecting the intrusions is called Intrusion Detection. Once the intrusion occurs in a system or a network, the intruder can be determined and the attack can be removed so that the future information leak could be prevented and data could be protected from future damage. A basic intrusion detection system is demonstrated in figure:-

The intrusion detection system primarily focuses on four things. First, identifying probable incidents. Second, monitoring information about them. Third, trying to stop them and fourth, reporting them to security administrators in real time as well as non-real time environment.

III. Intrusion Detection Approaches
The studies on intrusion detection have determined three main approaches of intrusion detection namely:
A. Statistical Anomaly Approach
The statistical anomaly detection approach involves collecting data regarding the behavior of legitimate users over a period of time. After this collection, statistical tests are applied on the observed data to gain a true assurance whether the behavior of the user is a legitimate user behavior or not. The following figure shows a typical statistical anomaly detection approach.

The statistical anomaly detection approach consists of two techniques which are “Threshold Detection” and “Profile Based Detection”.

Threshold Detection- While performing statistical test, we use flag value. During these tests there occurs possibilities like, the anomaly activities that are not prove to intrusion are flagged as intrusion and The anomalous activities that are prove to intrusion results in false negatives i.e. those activities which are intrusive are not flagged intrusive which are not supposed to occur. For this selection of threshold levels needs to be done which is itself an issue. In this technique, thresholds are defined independent of the user to measure the frequency of occurrence of various events.

Profile Based Detection- In the profile based detection technique; a set of profiles of each user activities is maintained and is used for detecting any change in the behavior of individual accounts. The figure three tells us about the change detected in user profile’s activities

B. Rule-based Detection Approach
Rule based detection approach involves a set of rules that are defined to detect the behavior of the intruders.
The rule based selection approach consists of two techniques which are “Anomaly Detection” and “Penetration Identification”. 

**Anomaly Detection**- The rule-based anomaly detection technique is one of among the oldest techniques of intrusion detection and has also been implemented in the recent years. Anderson’s report said that the masqueraders and the misfeasors could be detected by monitoring whether the user activities deviates from the normal usage patterns. Thus the anomaly detection providers certain rules which are needed for detection of usage pattern deviation in a user’s account.

**Penetration Identification**- Penetration identification is an expert technique of searching suspicious behavior in a user profile. This technique have become a common supplement in the intrusion detection system. It uses anomaly detection components as well. The penetration identification technique has the capability of detecting the adverse behavior even when the profile confirms to be applying the same usage patterns the way it followed generally.

**C. Misuse Detection Approach**

Misuses detection technique works on the scheme whose attacks can be represented in the form of patterns and signatures. Even if there are variations of the same attack, it can be detected as the pattern of that kind of attack is already represented. The main difference between the anomaly and misuse detection approach is that the “Anomaly” searches for the complement of adverse behavior whereas the “Misuse” searches for the known adverse behavior. The figure-4 consists of a typical structure of misuse detection technique approach.

The misuse detection approach consists of three techniques which are “Key Stroke Monitoring”, “Model Based Intrusion Detection” and “State Transition Analysis”.

**Keystroke Monitoring**- Keystroke monitoring is a simple technique in which keystroke for every attack pattern is monitored. This technique does not analyze the running program but only keystrokes. This resulted in the flagging the malicious data as intrusive.

**Model Based Intrusion Detection**- Model Based Intrusion Detection builds up models at higher level of abstraction. They maintain these models of patterns so that the administrator could represent the penetration abstractly. The main goal of this technique is to represent the characteristics behavior of intrusion.

**State Transition Analysis**- In this technique the system monitor is represented as a state transition diagram. As soon as the data is analyzed, the system changes
from one state to the other. This is generally done when some Boolean condition becomes true. For example: a user when tries to open a file, it checks for its existence which will return true if it exists and then it changes its state from one state to another.

IV. Intrusion Detection Tools

After all the discussed approaches were introduced, now it had to be implemented using some tools. Rather some effective tools which could retain the efficiency of the approaches as well. Certain effective tools for intrusion detection are listed as follows:-

Artificial Intelligence and Intrusion Detection-
Artificial Intelligence is a widely used technology for intrusion detection. Some researchers use the statistical approach with artificial intelligence whereas some wishes to use the rule based approach along with it.

Embedded Programming and Intrusion Detection-
This kind of technology is one approach in which involves the use of preprocessor hardware or in other words front end processes. In this some parts of the intrusion detection processing is done prior to the IDS to decrease the load of work for the IDS and the CPU as well. This can be done by programming code into the network interface card (NIC) which will be used as the front end processor.

Agent Based Intrusion Detection-
In this type of technical approach, the work of detection is divided among the individual processor. This technology not only decrease the work load but also acts as an advantage to the IDS that it can take the whole knowledge of the network working conditions.

Software Engineering and Intrusion Detection-
With increase in the complexity of IDS, the complexity of language used to develop the IDS code has also increased, steps have been taken to develop a programming language designed only to develop the IDS code. These languages improve the efficiency of the IDS code as well as the programming speed. The IDS developers can enjoy the benefits of the new language dedicated to the IDS only.

V. Challenges of IDS

Various challenges faced by organizations while installing an intrusion detection system are as follows:

Human Intervention-
Till now there is no such IDS installations that do not need human intervention. IDS is itself facing many enhancements due to which the organization needs to explain its prospects for installing IDS.

Deployment-
The efficiency of IDS is measured by the way the system is deployed. A lot of planning is required as for designing as well as for implementing the IDS.

False Positive and Negative Alarm Rate-
There is a possibility that the IDS may give false alarms. As discussed before, sometimes the IDS may list those activities intrusive which were not and leave those activities which are actually intrusive.

Signature Database-
Signature in before is the same as the usage of each attack. The main policy of IDS in detecting is to remember the signature of known attacks. The new threats are often not recognized and hence here is the challenge.

Historical Analysis-
Managing and monitoring the IDS log is still a very important task and a necessary task to be done.
VI. Conclusion

All the three approaches namely the statistical anomaly approach, Rule-Based detection approach and the misuse detection system are used depending on the purpose for which the IDS is installed in an organization. Statistical approach being the oldest of all is the most basic form of IDS and is often used in these times for the security while routing whereas the rule-based approach consists of the most expert rules for intrusion detection and provides with the utmost security and the misuse detection approach on the contrary fails to detect unknown intrusions.

VII. Comparative Analysis of IDS Approaches

<table>
<thead>
<tr>
<th>Approach</th>
<th>Protocols</th>
<th>Application</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Statistical Anomaly Detection Approach | Works on the network layer of the TCP/IP protocol, it even help in link state routing protocol. | Counters, gauge-numbers of logical connections assigned to it, resource utilization. | ● This approach can adaptively measure user behavior.  
● Potentially easy to maintain than rule-based intrusion detection. | ● False negative or positive generated depending on the threshold values that can be too high or too low.  
● Due to insensitivity of the order of events, relationship between the activities or events is missed.  
● It is unknown of what the subset of the possible measure of intrusive activity is. |
| Rule Based Detection Approach     | Works on the DNS network protocol.  
Works on the rules to create packets, exchange of packets, exchange of packets in a network etc. | Site specific application wisdom and sense (WDS) NADIR.                     | ● Expert rules offers high capability of an odd behavior in the user’s account.  
● In greater number of rules fired, greater is the suspicious rate.  
● Identifies both masqueraders and misfeasors.  
● Anomaly detection and penetration identification can be combined together for better security results. | ● Needs to be specially crafted to avoid infinite loops.  
● There is a possibility of contradictions i.e. under the set of rules for detecting intrusion activity, non-intrusive may fall.  
● It can become a complex system as thousands of rules may be needed for detecting first one type of intrusion. |
● Model based intrusion detection technique in this approach is a very clean approach.  
● Noise present in audit data can be filtered which leads to performance enhancements.  
● This system can predict attacker’s next moves before the attackers thinks of doing | ● Inability to identify unknown attacks.  
● Does not analyze running programs. |
References
1. Amit Kumar, Harish Chandra Maurya & Rahul Misra “A research paper on hybrid detection system”
2. Amrita Anand & Brajesh Patel “An overview on intrusion detection system and types of attacks it can detect considering different protocols”
3. Aurobindo Sundaram “An introduction to Intrusion Detection”
4. Chintan Bhatt, Asha Koshti, Hemant Agarwal, Zakiya Malek & Dr. Bhushan Trivedi “Architecture of intrusion detection system with fault tolerance using mobile agent”
5. Dr. Fengmin Gong “Next Generation Inrusion Detection System”
7. Jeramie Reese “Intrusion Detection System”
9. Karen Scarfone & Peter Mell “Guide to intrusion detection and Prevention System (IDPS)”
15. R. Rangadurai Karthick, Vipul P. Hattiwale & Balaraman Ravindran “Adaptive network intrusion detection system using a hybrid approach”
17. William Stallings “Network security Essentials, Applications and standards”
Big Data Security

Dr. Prerna Mahajan*
Geetika Gaba**
Nagendra Singh Chauhan***

Abstract

In today’s world, requirement of huge data is increasing rapidly with major security concern. Everyone wants their data to be secured with every aspect and dimension. If we talk about our personnel life everyone have data in huge quantity and of a huge variety (audio, video, text, chat, photos) and Professionally we have a large amount of data in field of media, healthcare, technology, private sector, science, sports which has to be stored so that security could be maintained with every aspect. Big data refers to management and analysis of huge amount of data that exceeds the capability and efficiency of traditional data with every dimension. Cloud computing can be viewed as a solution to store huge amount of data, but there are certain security concerns to deal with. Measures can be taken to provide incremental enhancements in securing the cloud that will ultimately provide us with a secure cloud.

To manage, identify and analyze complex data it is essential to store and share huge amount of data i.e. why big data is introduced to store large amount of data with great security. Big data was introduced to handle a large amount of data and also be processed massive quantity of data. Google has announced mapreduce framework to process large amount of data on hardware. Later on apache hadoop distributed file system is evolved as an efficient hardware component for cloud computing along with integrated part like map reduces. However hdfs and mapreduce were not quite efficient because they do not provide security to protect sensitive data. That is why hadoop was introduced to encourage security measures by using different technologies such as combining data mining technology. In this paper, we come up with some solution to provide security aspect in storing big data.

Keywords: FLUME, Hadoop, HBASE, HIVE, PIG, SQOOP, ZOOKEEPER

I. Introduction

Big data refers to the huge volume of data that cannot be stored and processed with in a time frame in traditional file system.

The next question comes in mind is how big this data needs to be in order to classify as a big data. There is a lot of misconception in referring a term big data. We usually refer a data to be big if its size is in gigabyte, terabyte, Petabyte or Exabyte or anything larger than this size. This does not define a big data completely. Even a small amount of file can be referred to as a big data depending upon the content is being used.

Dr. Prerna Mahajan*
Department of IT, Institute of Information Technology & Management, GGSIPU, New Delhi

Geetika Gaba**
Student - MCA, Institute of Information Technology & Management, GGSIPU, New Delhi

Nagendra Singh Chauhan***
Student - MCA, Institute of Information Technology & Management, GGSIPU, New Delhi

Let’s just take an example to make it clear. If we attach a 100 MB file to an email, we cannot be able to do so. As a email does not support an attachment of this size. Therefore with respect to an email, this 100mb file can be referred to as a big data. Similarly if we want to process 1 TB of data in a given time frame, we cannot do this with a traditional system since the resource with it is not sufficient to accomplish this task.

As you are aware of various social sites such as Facebook, twitter, Google+, LinkedIn or YouTube contains data in huge amount. But as the users are growing on these social sites, the storing and processing the enormous data is becoming a challenging task. Storing this data is important for various firms to generate huge revenue which is not possible with a traditional file system. Here is what Hadoop comes in the existence.

II. Big Data

Big Data simply means that huge amount of structured, unstructured and semi-structured data that has the ability to be processed for
information. Now a days massive amount of data produced because of growth in technology, digitalization and by a variety of sources, including business application transactions, videos, picture, electronic mails, social media, and so on. So to process these data the big data concept is introduced.

Structured data: a data that does have a proper format associated to it known as structured data. For example the data stored in database files or data stored in excel sheets.

Semi-Structured Data: A data that does not have a proper format associated to it known as structured data. For example the data stored in mail files or in docx files.

Unstructured data: a data that does not have any format associated to it known as structured data. For example an image files, audio files and video files.

Big data is categorized into 3 v's associated with it that are as follows:[1]

Volume: It is the amount of data to be generated i.e. in a huge quantity.

Velocity: It is the speed at which the data getting generated.

Variety: It refers to the different kind data which is generated.

A. Challenges Faced by Big Data

There are two main challenges faced by big data [2]

i. How to store and manage huge volume of data efficiently.

ii. How do we process and extract valuable information from huge volume data within a given time frame.

These main challenges lead to the development of hadoop framework.

Hadoop is an open source framework developed by duck cutting in 2006 and managed by the apache software foundation. Hadoop was named after yellow toy elephant.

Hadoop was designed to store and process data efficiently. Hadoop framework comprises of two main components that are:

i. HDFS: It stands for Hadoop distributed file system which takes care of storage of data within hadoop cluster.

ii. MAPREDUCE: it takes care of a processing of a data that is present in the HDFS.

Now let's just have a look on Hadoop cluster:

Here in this there are two nodes that are Master Node and slave node.

Master node is responsible for Name node and Job Tracker demon. Here node is technical term used to denote machine present in the cluster and demon is the technical term used to show the background processes running on a Linux machine.

The slave node on the other hand is responsible for running the data node and the task tracker demons.

The name node and data node are responsible for storing and managing the data and commonly referred to as storage node. Whereas the job tracker and task tracker is responsible for processing and computing a data and commonly known as Compute node.

Normally the name node and job tracker runs on a single machine whereas a data node and task tracker runs on different machines.

B. Features Of Hadoop:[3]

i. Cost effective system: It does not require any special hardware. It simply can be implemented in a common machine technically known as commodity hardware.

ii. Large cluster of nodes: A hadoop system can support a large number of nodes which provides a huge storage and processing system.

iii. Parallel processing: a hadoop cluster provide the accessibility to access and manage data parallel which saves a lot of time.

iv. Distributed data: it takes care of splitting and distributing of data across all nodes within a cluster and it also replicates the data over the entire cluster.

v. Automatic failover management: once and AFM is configured on a cluster, the admin needs not to worry about the failed machine. Hadoop replicates the configuration Here one copy of each data is
vi. **Data locality optimization:** This is the most powerful thing of Hadoop which make it the most efficient feature. Here if a person requests for a huge data which relies in some other place, the machine will sends the code of that data and then other person compiles it and use it in particular as it saves a log to bandwidth

vii. **Heterogeneous cluster:** node or machine can be of different vendor and can be working on different flavor of operating systems.

viii. **Scalability:** in Hadoop adding a machine or removing a machine does not effect on a cluster. Even the adding or removing the component of machine does not.

**C. Hadoop Architecture**

Hadoop comprises of two components

i. HDFS

ii. MAPREDUCE

Hadoop distributes big data in several chunks and store data in several nodes within a cluster which significantly reduces the time.

Hadoop replicates each part of data into each machine that are present within the cluster.

The no. of copies replicated depends on the replication factor. By default the replication factor is 3. Therefore in this case there are 3 copies to each data on 3 different machines.

**III. Big Data Over Cloud [4]**

The rise of cloud computing and data storage over cloud have facilitate in emergence of big data it is very easy to store big data and we can also say huge data over cloud and access more efficiently. Cloud computing have reduced computing time increased data storage capacity by using standardized technologies. Moreover we have many other advantages of big data storage over cloud it has major advantages over traditional file system as cloud platforms comes in different forms and sometimes have to be merged and integrated with traditional platforms.

As cloud is an enabler for advanced analytics with big data with its cost effective delivery models it is providing analytics-as-a-service(AaaS) for cloud based big data analytics.

Big data along with cloud computing is a compelling combination to handle huge amount of data with more efficiency and with more accuracy as data is becoming more valuable. Today conventions are shifting from what to store? To where to store with security and privacy.

Big data refers to huge data sets that are orders of eminence (volume) more manifold structured, semi structured, and unstructured data that are and approaching faster (velocity). This outpouring data is generated by different places. It is assorted and comes...
in many formats, including text, document, image, video, and more. The actual significance of big data is in the insights. When big organizations store there sensitive data in data warehouse unaware of all these facts some data is already located over cloud. Depending on requirement of security and place where to store data IT industry is focusing on budget which leads to analytics-as-a-service which supports internal, external as well as hybrid cloud.

Analytics-as-a-service aims to solve big data security and privacy problem. IT are not just solving the problem of storing data and also providing an infrastructure to perform analytics-as-a-service. Many companies done have cloud to store big and sensitive data so it allows to store data on public cloud which helps to reduce cost of storage with security and maintenance also.

DAaas(Data Analytics-as-a-service) represents an opportunity to extend platform that can provide cloud based analytical capability with huge variety and volume. It is a platform which provides end-to-end capabilities to handle data with an innovative concept to submit to our big data solution to extract and turn out sensitive data from data sources.

Apart from information leak, it can also corrupt the data which result in unpredicted results from data.

It can also perform some denial of services on big data solution too.

B. Input validation and filtering: since data is collect data from variety of sources, so the biggest issue to validate the input which involves making a decision of what kind of data is trusted and what kind of data is untrusted. Data Filtering: It also needs to filter the malicious data from good data.

Since GBs or TBs of continuous data flow over the internet there is a big challenge to filter out the data Signature data can lead to reduce the problem here.

C. Granular Access Controls Designed for performance and scalability with no security in mind. Table, Rows and cell level access control went missing in big data.

By default access control is disabled. No sql is provided for that and a user has to depend on third party software to enable its accessibility.

D. Insecure Data Storage: data at various nodes, Authentication, Authorization & encryption is challenging. Encrypting of real time data can have
E. Privacy pertains in Data Mining and Analytics: Legitimatize of big data generally involves Data mining and Analytics.

Here sharing of data involves multiple challenges such as invasion of Privacy, Invasive Marketing and an unintentional disclosure of information.

Example: AOL releases of anonym zed search logs, User can easily be identified.

V. Solution to Achieve Big Data Security:[6]

At some extent we can achieve big data security with the following solutions.

1. Secure your computation code just by implement access control, code signing, dynamic analysis of computational code.

2. Strategy to prevent data in case of untrusted code.

3. Implement comprehensive input validation and filtering: consider all internal and external sources, Evaluate input validation and filtering of your big data solutions

4. Implement Granular access Control: Review Permission to execute ad-hoc queries and enable access control explicitly which is disabled by default.

5. Secure you data storage and computation: Sensitive data should be segregated, Enable data encryption for sensitive data which is again disabled by default, Provide API security and audit administrative access on data nodes.

6. Review and employ privacy maintaining Data Mining and analytics: here users make sure that the analytics data should not disclose sensitive information and get your Big data pen tested.

7. Security for big data can also be achieved through Hybrid cloud i.e. hybrid cloud means private and public cloud together large companies are providing space to store huge amount of data over hybrid cloud which reduces the cost of storing and maintenance with public cloud and a maintaining security with private cloud

VI. Conclusion

The goal of big data along with cloud computing and hadoop architecture is to achieve privacy and security for big data i.e. huge amount of data with variety, velocity, volume. Somehow privacy and security can be achieved with hybrid cloud computing, if big data is integrated with hybrid cloud architecture. We can acquire security if big data is encrypted and divided into small clusters then it can be managed and processed with privacy. Data on clusters can be secured by using digital signatures. Security of data can also be maintained through analytics-as-a-service (AaaS). It also reduces the cost of storage and maintenance.
References

1. Roger Schell “Security –” A Big Question for Big Data” in 2013 IEEE International Conference on Big Data


5. “Cloud Security Alliance Top Ten Big Data Security And Privacy Challenges “by CSA Big Data Working Group

Biometrics: Human Body as a Password

Shriya Jain*
Ruby Dhaiya**
Ashi Chauhan***

Abstract
This paper examines biometry as an evolving technology. It explains the basic biometric system and their working. The characteristics of a biometric trait and the various techniques that can be used in a biometric system have also been elaborated upon. The paper also provides a comparison between the major techniques and elaborates on the applications of biometrics, specifically in India through the Aadhaar project.

Keywords: Aadhaar, Biometry, Identification, Verification, Comparison.

I. Introduction
Biometrics is the science of automatically identifying and/or verifying a person based on their physical, chemical and behavioural characteristics. It is a very convenient and almost fool proof method of ensuring the identity of a person, as biometric traits are unique to each individual and cannot be borrowed, stolen or forged.

A biometrics system can be used for two purposes, namely: Identification (One to One) and Verification (One to Many). A biometrics system can be used to identify an individual with or without their knowledge. The system compares the captured biometric data of the user with the stored template of the user in the database, to verify his/her identity. It is a one to one process as a single template is compared with a single set of captured data. For example, it can be used by the government to find an individual by scanning security feeds using facial recognition or they can be used by nefarious parties to identify citizens unknowingly. A biometric system may also be used to verify the identity of an individual. It can be used by anyone to ensure that the person is exactly who they say they are. The system uses already stored templates in the database to search for a possible match among many samples. Thus it is a one to many approach. For example, usage of palm prints to grant access to secure locations or activating/deactivating locks with speech recognition.

Physiological biometric traits include retina, iris, facial characteristics, ear, palm geometry, fingerprint and DNA. Behavioural biometric traits include gait, signature, odour, voice patterns and keystroke.

II. Characteristics of Biometrics Traits
For a trait to be used as biometric recognition technique, a personal trait must have some attributes that ensure that it is apt to be used in a biometric system. These characteristics are:

A. Acceptable
Taking samples of the attribute should be acceptable to the public and must not violate their dignity in any manner.

B. Comparable
The biometric trait should be able to provide a sample that can be effectively compared with other samples of the data without ambiguity.

C. Constant
For an attribute to act as an effective biometric trait, it must be invariant. The attribute should not change over time, location or chronic diseases.

D. Inimitable
The trait should be such that it cannot be forged. It is one of the most important characteristic as it ensures the security of the biometric system. The trait should not be reproducible.
E. Not violate privacy
The attribute should not violate the privacy of anyone in any manner. For the attribute to be accepted worldwide and have co-operating participants it must respect the privacy of users.

F. Quantifiable
The attribute should be capable of being measured so as to be useful in comparison of samples. It should not be an infinite or abstract value.

G. Reducible
The trait should be such that it can be reduced to a series of data that can be stored on files and used for analysis.

H. Reliable
The trait should be difficult to manipulate and prove to be a reliable source of identification.

I. Uniqueness
Each instance of the attribute must be singular to the individual. It should not be found in any other individual and should have enough unique properties to be distinguishable from the sample of other individual.

J. Universal
The trait should be possessed by each and every individual. It rules out any special features that only a select number of people may have, for example a sixth finger.

III. Operation of Biometric Systems
Although each biometric system is configured according to the biometric trait(s) it uses, the general working and operations of a biometric system remain the same. There are four main modules involved in the working of a biometric system, namely: Sensor Module, Feature Extraction Module, Comparison Module and Decision Making Module. Sensor module consists of the physical hardware or sensors that capture the biometric data from the user. For example, the iris scanner or the voice recorder. The Feature Extraction Module deduces a specified feature set from the data captured by the Sensor Module. Each individual set of biometric data needs to be able to provide the specified feature set for the data to be accepted as a valid sample. The comparison or matching module compares the features extracted by the previous module with the ones already stored in the database. This module only provided the hard facts about the similarities or the differences between the template and data. It does not provide any decisions. Based on the comparison done by the Matching Module, Decision Making module passes the final verdict on whether to accept or reject the user. All biometric system work on the same basic principle of capturing biometric data, identifying the salient feature set and storing the values into the database. When a user inputs some biometric data, the salient features are identified again and the samples are compared with the values in the database.

The two main operations performed in a biometric system are Enrolment and Comparison (which includes Identification and Verification).

Enrolment -This is the basic operation needed for both identification and verification purposes. This operation involves the capturing of user data for the first time. The user can enter their personal details such as name, age, designation etc. as well as provide the sample of the specific biometric trait. The quality of this sample is then checked and if found appropriate the features are extracted from the sample and stored in the database as a template. If the sample does not pass the quality check, the user needs to provide the data again.

Comparison -After enrolment when the user logs into the system, the user provides his/her biometric sample to the system. The system compares the current sample with the template in the database and passes the verdict stating whether the person is who they claim to be or not.

IV. Techniques of Biometric Systems
A. DNA
According to Oxford Dictionary, deoxyribonucleic acid, a self-replicating material which is present in nearly all living organisms as the main constituent of chromosomes. It is the carrier of genetic information. Although a major percentage of the DNA is same for each human being, 0.10 percent of the DNA is unique for every person and can be used to identify the person. The DNA is easy to acquire and can therefore be used for nefarious purposes. There is also the fact that DNA
is the same for identical twins thus they cannot be distinguished on a biometric system.

**B. Face**
Looking at a person’s face is the most common way of identifying a person and is used predominantly by humans. It is one of the most non-intrusive methods of biometric detection and are therefore one of the most widely used techniques. The face recognition techniques mainly uses the location and relative position of the facial features to determine a match.

**C. Fingerprint**
Fingerprints have long been used as an acceptable measure of a person’s identity. They are still used to identify illiterate people in many countries like India. This is therefore one of the most developed biometric technology and has proved to be quite reliable and accurate. Fingerprints are different for each individual so much so that each person has a different pattern on each of the ten fingers. It is also one of the cheapest methods and most widely used, for example it is present in laptops as well.

**D. Gait**
Gait, according to Oxford Dictionary, is a person’s manner of walking. It is a very non-intrusive method of detection and can be used to identify an individual without his/her consent. The biometric systems using gait extract a silhouette of the human body and track it as a combination of moving points. This trait, however, is not very consistent as the way a person walks is greatly affected by his/her choice of footwear, the ground s/he is walking upon and the physical condition of their legs.

**E. Hand Geometry**
This technique analyses the hand in detail for things like the length and width of fingers, the gap between each finger, the shape of the palm etc. to create a template. It is an easy to use trait that is non-intrusive and not easy affected by external factors. The drawback, however, is the fact that hand geometry is not a proven distinctive feature. Compared to other traits, hand geometry is more likely to be same for two people.

**F. Iris**
The iris is a flat and ring-shaped membrane behind the cornea of the eye with an adjustable circular opening in the centre called a pupil. Together with the pupil, the iris is responsible for regulating the amount of light that gets into the eye[6]. The iris is a distinctive feature and is different even for identical twins. Two people cannot have the same iris pattern.

---

**Fig. 1: Simple Biometric System**
and there is also technology to detect natural iris from the fake contact lenses. It is one of the most effective although a little expensive technology.

G. Odour

Body odour is a distinctive smell that can be used as biometric trait. Thesis an ancient method as it has been used by the police in tracking criminals by scent using bloodhounds. Finding people by scent could usually be done only by animals who have a highly developed sense of smell, like dogs. Now as technology evolves odour can also be tracked by computer systems. It is a relatively new technology hence it is not very developed as sensors have yet to achieve the accuracy of a dog’s sense of smell.

H. Signature

Signatures have long been used to determine the identity of an individual by authenticating the person,

### Table 1: Comparison of Various Biometric Techniques

<table>
<thead>
<tr>
<th>Technique</th>
<th>Acceptability</th>
<th>Comparability</th>
<th>Constancy</th>
<th>Inimitability</th>
<th>Non Violating</th>
<th>Quantifiability</th>
<th>Reducibility</th>
<th>Reliability</th>
<th>Uniqueness</th>
<th>Universality</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Face</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Gait</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Iris</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Keystroke</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Odour</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Signature</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Voice</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
be it on legal documents or attendance registers. The same principle can also be applied to biometrics where the signature of a person can be scanned and stored as a template that can be further compared to other samples to determine identity. However, professional forgers may be able to replicate the signature and fool the system. Signatures also change over time and are influenced by the physical and emotional state of the signatory.

I. Voice
Humans can often distinguish each other by voice; so can computers. Voice recognition is another widespread technology that is implemented in mobiles, laptops, TVs and security systems. Voice and speech recognition are cheap but forgeable traits as one can easily replicate voice via technological means. Also the fact that voice can be altered due to ailments such as sinus, make voice an inconsistent trait.

V. “Aadhar Project” Application of Biometric Systems in India
The use of biometric systems has drastically increased in the last few years as people across the globe pay more attention to security. Almost all countries have ongoing research projects on biometry to make things more secure.

The biggest application of biometry in India is the “Aadhaar” project. It is the world’s largest biometric identification system with the Unique Identification Authority of India (UIDAI) issuing nearly 82 crore cards [9]. The “Aadhaar” is our nation’s bid to provide a unique identification to each of its citizens. An Aadhaar card is an irrefutable proof of identity for any resident of India, verifiable online anywhere, any time. While creating an Aadhaar card, a person is required to provide his/her fingerprints and iris scan. These biometric scans solidify the individual’s identity ensuring that one person cannot have more than one Aadhaar card.

VI. Conclusion
Biometrics has emerged has a rapidly growing field of study today. As the security becomes more important each day and gets harder to achieve, biometrics seem to offer a viable solution. There are numerous techniques or traits that are already used as a biometric identifier and more are to come.

There are infinite areas in which biometrics can be used and has already started being used, defence, government, police, personal security are just a few examples. Although biometric systems have been researched on for quite a while now, their use has yet to be widespread due to their considerable disadvantages like intrusiveness and expensive technology. However, the field of biometry shows a strong promise of evolving and forever changing the outlook of data security.

References
Artificial Intelligence Impact on Cyber Security

Eshita Madhok*
Ashutosh Gupta**
Nidhi Grover***

Abstract

Information technology and the world of web are increasing at a very fast pace and so are increasing the crimes related with cyber world. Cyber systems are much prone to various kinds of threats, intrusions and dynamically evolving risks related with them. Software based on conventional security algorithms and mere and human involvement is inadequate for ensuring complete cyber security. Thus, there is an increasing requirement for more powerful and intelligent cyber defense systems to serve the purpose of providing cyber security. The innovative practices of Artificial Intelligence are getting more popular in assisting users to fight crimes and related problems in cyber space. The purpose of this paper is to review cyber security, its associated risks and the advancements made so far by applying Artificial Intelligence methods in cyber defense. The paper also aims in demonstrating the applicability and effectiveness of these AI techniques in present scenario.

Keywords: artificial intelligence, cyber space, cyber security, artificial expert system, artificial neuron system, artificial intelligence system, artificial immune system.

I. Introduction

In growing world of computers and internet the problem associate with them are also increasing. The technological advancement in the field of internet and telecommunication has brought the world in front of new kind of problems known as cyber crimes and cyber terrorism. The term like cyber security came into existence because of the incidence like cyber crime or cyber war. Cyber infrastructure is much vulnerable and poses threat to countries’ overall development [1]. Cyberspace has become a new platform for raging war or terror for many non-state actors. Now days, Cyber space is a source from where a person sitting in different continent can create terror in other continents by one click. Through cyberspace somebody can destroy not only the civil or government infrastructure but it can destroy the nuclear infrastructure also. Today, cyber weapons and tools have become so powerful that typical human supervised security systems are unable to protect against them. The advancements done so far in cyber technology have proposed the option of using AI (Artificial Intelligence) for protecting the networks and cyber infrastructure. Applications of Artificial intelligence are next step in the field of cyber security. Rapid developments in cyber space might lead to intelligent cyber weapons that are much powerful and tough to control and it may be impossible to use conventional methods to provide overall cyber security to users[2]. Cyber incidents become especially dangerous in network centric warfare (NCW) thus, advanced cyber defense techniques are immediately required [2].

A. Cyber Security and its Problems

In last decade, a new word “cyber” came into existence and create a whole new string of words Examples of terms that surface in academic papers include cyber society, cyber attacks, cyber security, offensive cyber capabilities and problems of cyber terrorism [3]. The parent term of cyberspace is “cybernetics”, this word is first introduced by Nobert Wiener for his work in communication and control science [4]. Cyber world is an environment in which communication over computer networks occurs [4]. In 21st century technology has moved to provide a platform where
humans can interact, exchange idea, share information, provide social support, conduct business, direct action, play game engage in political discussion and so on, using a virtual space or say global network or cyber space. In an era of continuous growth of cyber connectivity with ever increasing number of online applications from buying a needle to being a part of a team deployed to mars it comes essential to be conscious of potential threats looming over the cyber space. It became very essential to secure this cyberspace for potential threats. With increasing number of Computers and betterment of telecommunication networks number of cyber security problems are also increasing .Attacks like backdoor, zombies computer attack ,viruses , worms, Trojan ,D Dos, intrusion attacks , phishing targeting individuals ,business world and even government also. What make cyberspace so valuable for a country is because thousand's of GB data get processed and passes on computer and computing system. Cyberspace erased the barrier of language and country. Brenner (2010) argues that “Most of the cyber crime seen today simply represents the migration of real-world crime to cyberspace which becomes the tool criminals use to commit old crimes in new ways” [7].

B. Artificial intelligence(AI)

Artificial intelligence is the computer science that is concern with making computer behave like humans. This machine intelligence emerged in the form of summer research project of Dartmouth College in July 1956. But the idea of AI started back in 15th or 16th century.

AI can be described in two ways:

(i) As the science of developing intelligent machines.
(ii) As science of finding methods of solving the problem with more complexity that cannot be solved without applying some intelligence.

The second definition of AI that symbolizes a system as that has the capability of taking its own decisions without interference of others [5].

Some characteristics that a Artificial intelligence should exhibiter [5, 6]:

- Deduction, reasoning, problem solving (embodied agents, neural network)
- Knowledge representation
- Planning (multi agent planning)
- Learning (machine learning)
- Natural language process (information retrieval)
- Motion and manipulation
- Perception (speech recognition)

Although Alis based on individual human behavior, knowledge and representation on other hand Distributive Artificial intelligent system (DAI) is competitive system [6]. Although from 1956 till 2016 advancements have come so far in field of AI but there is a long way to go. But, not to forget that this is still a new or say young filed of science. It has to be cultured very carefully. Now a day's techniques of AI like Heuristics, Data Mining, Neural Networks, AISs, Artificial immune system, Expert systems, searching, genetic algorithms etc are being getting use in Cyber defense and cyber security. This paper is going to throw the light on the following applications of AI [7]:

- Artificial Neural Network: The idea of system is based on neural network technology.
- Artificial Intelligent System: It's a system that has Qualities like pro-activeness, understanding of agent Communication language
- Expert System: It is a system which is used to find answers to problems created by users.

II. Artificial Neural Networks

From thousands of year or say from the beginning of civilization, human body is one of the biggest mysteries. But, from the middle of 19th century facts and secret about human body started getting revealed by several scientists and like other discoveries or inventions human started using its knowledge for making their life’s comfortable. Neural system of brain is the idea used by two experts in their field’s mathematician Walter Pitts and Warren McCulloch in 1943 who wrote a paper on how neurons might work. For showing and describing the work of neuron...
working in brain, they modeled a simple neural network using electrical circuits [9][10]. The ANN (Artificial neural network) is parallel distributed process which tries to mimic like natural brain system [11]. The main reason for using of ANN (Artificial neural network) and its popularity in cyber defense is its high-speed. The high-speed and logical gates are the reason behind the popularity of ANN in cyber security. By reducing the switching time with logical gates, high-speed can be achieved by artificial neural network [13]. ANN is used to protect against cyber attacks:

Artificial neural network is explained in the figure 1.1. Inputs enter into the processing element from the left hand side. The first step is to multiply every inputs by their according weighting reason. These adapted inputs are then feed into the summing function, which perform different kind of function on it like average, smallest, summing etc these products. These operations can produce a number of different values, which are then move forward; the output is then sent into a transfer function from of the summing function, which turns this number into a real output[19].

A. Intrusion Detection and Prevention System

The name tell its story itself, it's a software or hardware that protect a network, it's like a smoke detector, it raise a flag of danger when it feel security is get bleached and some malicious activity is going on in the system or network. The work of prevention system is to give response to this bleach in network and take necessary step to protect the data of network from this breakout. In this kind of situation system like artificial neuron system can help the prevention system and it may also help the intrusion detection system fast and reliable[14]. The properties of artificial neuron system like to learn, process distributed adapt, information and self-organize are applicable to solving problems that require considering conditionality, imprecision and ambiguity at the same time[14,15], help in detecting as well taking counter measure in real-time world.

B. DDOS attack

DDOS is explained as Distributed denial-of-service attacks which has become one of the main internet security problems over the last decade [15]. DDOS is a type of DOS attack where multiple compromised systems, these computers are often infected with a Trojan; these are used to target a single system causing a Denial of Service (DOS) attack [17]. SOM (Self Organizing Map) is an artificial neural network, which is based on the competitive learning. Each neuron fight among them self to get activated, but...
only one get activated called winning neuron , this results in trigger of negative feedback path (lateral inhibition connection). This results in neurons are forced to organize themselves and through this a network is formed known as DDOS [17]. The SOM system (Self-Organizing Map system) changes the n-dimension maps into 2-or 3-dimension maps or grid. The data with similar pattern and similar statistical features get grid closer together. The basis of this classification is done according to the topological order [17]. Its became difficult for a normal system to discriminate between normal/genuine or abnormal request, Here system or mode like SOM help a normal network with help of its grid which control the flooding of packets or request and help in blocking unwanted or fake requests.

C. Virus Detection using Artificial Neural Networks

Computer virus is a kind of threat that causing billions of dollar to many companies and government. These are actually malicious programs that are made to replicate itself and causes damage to the host computer. The problem with today’s antivirus programs is they detect virus on basis of known pattern of virus, so detection of new virus is difficult. Again the models like SOM (Self-Organizing Map) of ANN help in solving the problem as SOM capability of gridding the analogous data and fast speed help in the detection of new virus. The SOM can be used to detect features hereditary to the problem and thus has also been called SOFM, the Self-Organizing Feature Map [18]. Its high-speed enable to respond towards the detection of virus very fast in comparison of common human being.

III. Artificial Intelligent Agents

Intelligent agents (IA) are software components that pose some feature of intelligent behavior that increase its importance in cyber security. Features like pro-activeness, understanding of Agent communication language, re-activeness, mobility, reflection ability increase the usage of AI with time in many fields [20]. Given that current cyber defense measures, in particular passive cyber defenses, are inadequate in comparison of increasingly sophisticated threats [22]. Nowaday’s intelligent malware and other advanced threats are increasing day by day this became necessary for defense sector to use agents (an autonomous entity which monitor through sensors and response upon an environment using actuators that is an agent [21]) with more advance intelligent. The characteristic that separate this Artificial intelligence tool from rest of other is two IA are able to communicate among them self in case they need to make plans or take some counter action for some threat in the system or network [23].

A. Agent-based distributed intrusion detection system: ABDIDS

ABDIDS is the system of hybrid technologies including intelligent agent and intrusion detection system (IDA) [22]. With time the most valuable thing is users’ online identity and the data which get transferred from several networks. The system like ABDIDS saves the data and transaction from theft and other malicious objects. A recent analysis by the UK Ministry of Defense proposes that advancement in robotics, powerful computing, sensors, precognitive science, energy efficient systems and nanotechnology together combine to produce rapid improvements [22]. Intelligent agent-based systems are classified into four categories namely: simple agents, multi agents, mobile agents, and ant-based agents [24].

B. Agent-Based Simulation of DDOS Attacks

DOS is one of the biggest attack problem of today’s computer networks, and it has been difficult to find its permanent solution properly but there is new kind of attack that marked its presence in the beginning of this century, called DDOS “Distributed Denial Of Service” attack. To perform this attack male factor needs to hack a set of computers (“zombies”) at first and to run on them DOS programs to attack next targets. Thus, it becomes hard to sense DDOS attack and to provide defense against it [25]. Agent-based modeling and simulation of network security assume that agents’ competition is represented as a large collection of semi-autonomous interacting agents. The aggregate system performance emerges from evolving local interactions of agents in a dynamically changing environment specified by computer network mode [25]. Agents of both teams compete with each other and defend themselves and their component. Each agent role and function is predefined.
C. Artificial intelligent system against virus

There is no paper that shows the effectiveness of intelligent system for countering computer viruses. The computer viruses have been mentioned here because it’s one of the most dangerous threat for the computer networks at present. There is so many anti-viruses in the market, but still this little piece of software is permanent threat. The reason behind this is the weakest link of chain that secure the cyber network, that is human beings [26]. For now there is hardly any permanent solution for computer viruses.

IV. Artificial Immune System (AIS)

Artificial Immune System is created to do the work like biological immune system i.e. to adapt itself in the changing environment and releasing the antibodies against the dangerous threat to a computer or network. It is also needed to look into biology for a little inspiration [27]. From thousands of year immune system of human being is fighting from several viruses and intruders, and the reason behind it is the efficiency of body in keeping on learning and improving itself along with the increasing ability of intruders. Another reason that makes immune system so flexible is its ability to discriminate between self and others and this makes it so powerful [27,28].

Basically Artificial immune system have following properties:

- Detection: classification or detection take place in immune system when infected elements get attached with sensory cell surface.
- Diversity: Immune system has number of sensory cell some of which work like lymph cell, which react to foreign element.
- Learning: As stated before Immune system capability to adjust itself and treat the foreign object as soon as possible. This structure of immune system help to find out and adjust themselves according to intruder.
- Tolerance: The particles which mark themselves as self bodies are contained in the chromosomal bodies [31]

A. Artificial Immune System (AIS) based on Intrusion detection system (IDS)

The purpose of the IDS is not only preventing the attack but also reporting all the abnormal behaviors of the system. (28). The properties of AIS like its support robustness, its lightweight Self-Organized, Multi-layer. These increases the capability of IDS and help in betterment of system. By the properties like robust is help IDS to work properly although if some part of IDS gets crippled. Other properties like Self-organized help in adaptability and global analysis, Without external help or say Management, maintenance or supervision [29].

B. Artificial Immune system against viruses

Viruses are the terms used for the malicious unwanted codes that can do malicious activity on the computer, this viruses can turn into worm, virus or Trojan horse its life can be divided in three stages, first when it attacks the host; second when it start replicate itself and last when it start causing harm. The basic theory of immune system is prevent a body or a system from the alien entities that may cause harm. Natural Immunity can be classified into two types; inborn or innate and acquired. Inborn mediates between the infection and the body while acquired develops slowly.
and mediates later. The artificial immune system theories such as the Clonal Selection Theory are based on the notion of acquired immunity [31].

V. Expert system

Expert system is one of the most widely used A.I tools. An Expert system software designed to find answers to various application domain questions posed either by a software or some user[32]. It is usually used to support some decision-making tasks. At present there are many expert system that is being used at present in many organization to solve the Complex and sophisticated problems. The expert system are the first successful form of expert system using AI technique. Expert systems are of two types namely: Inference Engine and Knowledge Base systems. A Knowledge base system represents facts and rules while Inference Engine is used to apply the rules to the know facts [17]. Inference Engine may also include explanation and debugging capability. With the development of computer application and network technology number of cyber attacks are also increasing. Commercial or say open source intrusion detection systems are independently not able to solve this problem alone.

Fig. 3: Artificial Immune System

VI. Conclusion

Cyberspace opens the new doors for businesses, governments and common people to achieve new heights in their work. This paper provides a glimpse of the cyber attacks, intrusion etc. cyber crimes. This situation forces to look up to more powerful techniques such as Artificial Intelligence based approaches to combat cyber crimes. The ever increasing DDOS attacks, computer viruses, worms, Trojans and logical bombs etc. give rise to the development of tools such as Artificial neural networks, Intelligent Agents, Expert Systems and Artificial Immune System to fix or avoid these problems. The network based systems are still under threat and present security techniques are inefficient to protect against these harmful threats. As thousands of GBs of data travels through network, mere human supervision and traditional security approaches are unable to match the ability and efficiency of artificially intelligent systems. Advancements in Artificial Intelligence have still a long way to go and much research needs to be done in this field. This field of study opens a complete new horizon of technology that in future will be able to secure cyber space and networks with greater efficiency and effectiveness.

Fig. 4: Expert System
References

2. https://en.wikipedia.org/wiki/Stuxnet ,This page was last modified on 15 February 2016, at 03:40 .
4. https://en.wikipedia.org/wiki/Cyberspace,This page was last modified on 12 February 2016, at 04:09.
5. https://en.wikipedia.org/wiki/History_of_artificial_intelligence,This page was last modified on 12 February 2016, at 09:45.
6. Selma Dilek1, Hüseyin Çakýr2 and Mustafa Aydýn3,”Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes”,
8. https://www.google.co.in/search?q=Sub+parts +of+Artificial+neuron+system&oq=Sub+parts+of+Artificial+neuron+system&aqs=chrome..69i57.22509j0j7&sourceid=chrome&es_sm=122&ie=UTF-8#,by BC Bangal- 2010 .
10. https://en.wikipedia.org/wiki/Artificial_neural_network,This page was last modified on 19 February 2016, at 19:28
17. Himali Jani1 ,Sathvik Shetty1 ,Kiran Bhowmick ,"Virus Detection using Artificial Neural Networks Shivani Shah1”.
18. “Artificial NEURAL NETWORK” https://en.wikipedia.org/wiki/Artificial_neural_network, This page was last modified on 16 February 2016, at 10:10
19. Enn Tyugu ,”Artificial Intelligence in Cyber Defense”, R&D Branch ,Cooperative Cyber Defense Center of Excellence (CCD COE)and


23. Vijayalakshmi, Palanichamy Yogesh and Arputharaj Kannan, Intelligent feature selection and classification techniques for intrusion detection in networks, Sannasi Ganapathy*, Kanagasabai Kulothungan, Sannasy, Muthurajkumar, Muthusamy

24. Igor Kotenko, Alexander Ulanov, "Agent-Based Simulation Of Ddos Attacks And Defe Nse Mechanisms ",

25. St.-Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, 39, 14th Liniya, St. Petersburg, 199178, Russia


27. Hua Yang, 1,2 Tao Li, 1 Xinlei Hu, 1 Feng Wang, 1 and Yang Zou 1 "A Survey of Artificial Immune System Based Intrusion Detection"

28. Jungwon Kim, Peter J. Bentley, Uwe Aickelin*, Julie Greensmith*, Gianni Tedesco†, Jamie Twycross* "Immune System Approaches to Intrusion Detection"


30. Hamza A. Ali and Duaa Jawad Hussain, "International Journal of Trends & Technology in Computer Science" (IJETTCS) Volume 3, Issue 2, March – April 2014 ISSN 2278-685 Computer Virus Detection Based on Artificial Immunity Concept

A Comprehensive Study of Contemporary Tools and Techniques in the Realm of Cyber Security

Dhananjay*
Aishwarya Raman**
Sheetal Kaushik***

Abstract

The Inherent Weaknesses in the cyber space and ever escalating cyber-attacks tend to continuously threaten the National Security, economy and Privacy. More than fifty countries, around the world, have framed their Cyber Security Strategies to address the serious issues of National Cyber Security. A cyber security strategy is particularly meant to be securing the national cyberspace from malicious cyber threat courses, but due to the unpredictable threat background, considerable variations can be seen in the invasive and defensive actions and methods adopted by different country.

This research paper analysis and Compares Cyber Security tools and techniques, also discusses about developed and developing countries with their identified standards, aims and explanation of cyber awareness, characterization of the cyber threats, and legislative measures, capacity building programs etc. The majority of the strategies have described the need of assigning an official body for leading the cyber security tasks at the national level and establishment of Computer Emergency Response Teams (CERT) to fight cyber-attacks targeting national cyberspace.

Keywords: Cyber Security, Cyber Security Strategies, Cyber Security Measures

I. Introduction

In this digital age everyone have the facility to send information from one part to the other within a fraction of second and that to with a click of a single button but only a fraction of those who click this button actually knows what is happening behind the scenes. “40 million People who were addicted to Ashley Madison a commercial website had no clue what nightmare they had to face after the cyber-attack by the impact group [1]. This is just one example out of the countless events that has happened in the previous year itself.

Cyber security has been there from quite some time but new and new ways of exchanging information has made older techniques used for securing confidential data obsolete. With crimes like these increasing day by day we need to come up with not just effective but intelligent solutions to safeguard confidential data. In this light we would like to take this opportunity to present our white paper on cyber security and threats. In simple terms cyber security means protecting the network, computer, programs or data from suspicious access. This paper brings forward the different cyber techniques and tools, strategies, ways of detection and the various kinds of cybercrimes. This paper shows a clear picture about various techniques being followed for eg: Authentication, encryption, firewall, digital signatures etc. and various tools such as Forensic Security tools, Vulnerability Scanner etc. This is the representation of the current condition of cyber-attacks in various places across the globe. The status clearly possesses an urgent need for the development of new cyber security techniques.

A. Worldwide Network Attacks Origin by Ranks

This information has been sourced from Symantec. This is a part of worldwide survey conducted in 2014, according to which China and United States remained in the top 2 positions in malicious activities. India
remains in the 8th position with least malicious attacks.

B. Top 5 Sectors Breached by Number of Incidents:
The following graph shows the top 5 sectors breached by number of incidents. The maximum breaches happened in health sector while the least in Financial Sector.

C. Incidents of Breach:
The following chart shows the timeline of data breaches that happened globally in 2014. While the maximum incidents numbering 34 happened in march 2014, the maximum identities exposed were 147.62 million in the month of May 2014.

II. Literature Review
With a view to make this research titled “A Comprehensive Study of Contemporary Tools and Techniques in the Realm of Cyber Security” more effective; it is prepared after detailed study of various research papers and journals. Certain facts have been considered. The papers discuss about various cyber-attack detection strategies. In view of the current state of increasing cyber crimes this paper brings forward the need for the development of new cyber-attack detection strategies. This paper also demonstrates about various types of cyber-attacks for eg:

(a) Denial of service attacks
Dos is basically a kind of cyber-attack where the attacker makes the memory resource too occupied or too heavy thereby limiting the user to use the machine. Here the network connection, or the computers or network may be targeted and prevents the user to legitimate commands [2].

(b) Remote to local(R2L)
In this kind of attack an attacker sends packets to machine over network so that he can illegally access the machine to gain the local access. The attacker usually doesn’t have an account on the machine and is able to send the packets to the system. [3]

(c) User to root attacks (U2R)
In this class of attack, the attacker uses the machine normally and is able to exploit the system to gain the root access of machine (sniffing passwords, hacking) [4]

(d) Probing
Probing is a system of gaining access to the computer and files by knowing the weak point in the system i.e. mostly external to the network. [5]

A. Some of the Attack Detection Strategies Include
(a) Intrusion detection strategies: An Intrusion detection is a sort of device that checks the network
system for malicious or suspicious activities going in the computer and reports it to the supervision system.

(b) Signature based approach: in this system the server can use existing software like antivirus and firewall, use their properties, inherit them and use in attack signatures in such a way that those signatures that create log files directly saves in the machine [6].

As per the study the analytical view for detecting the cyber-attacks is also very important. One of the major examples is: artificial immune system.

Bio-inspired methods such as artificial immune system gives a new dynamical method to defend entire data network from malicious attacks. It detects the affected cell named as pathogens such as virus and mal virus. Artificial immune system only detects the reactive cell in the system that are affected and process them to protect system data [6]. As much as analytical view is important for detection it is also important to know the classification of cyber-attack and the possible solution to it:

For eg: (1) Cyber Wars in which different nations are involved with the aim of disrupting the network to gain military. (2) Cyber Crimes—it uses computers and internet to abuse the users for monetary gains. One of the offered solutions to this kind of attacks includes: Agent based approach

III. Cyber Security Techniques and Tools

As per the survey it is founded that Cyber Security are gaining importance because of growing number of unauthorized attempts to rush into private data with the clear aim of stealing the same and forcing the users into information blackmailing. The tools and techniques [7]active to challenge cyber security concerns are:

A. Authentication

It proposes to verify the identity of user based on the credentials stored in the security domain of the system. The most common mode of governance is password technology; the main challenge encountered in authenticating process is when the unauthorized people try to spoil the attempts of authorized people only to listen to the authenticating message. The password transmitted over an insecure medium is responsible to be diverted by dishonest people who can use it to disguise as the original user. This problem is solved by encryption.

Techniques used for Authentication

1. Password and Pin Authentication

In this technique, privacy and confidentiality can be maintained up to some extent. User remember their passwords termed as Knowledge-based techniques. Passwords can be single words, numeric, phrases, any
grouping of these. But problem with this technique is that memorized passwords can be easily predicted or randomly explored by the hackers. The following fig.1 shows the working of authentication technique.

1. Biometric Authentication
As per the survey of previous year, detecting theft and loss or disclosure of data is increasing day by day. To overcome these security threats uses of different gestures come in the process such as:

(a) Fingerprint Authentication
As per the study of many years it is found that fingerprints are unique of every person in the world even twins also have different fingerprints and these are used for basic security in companies to access files and databases over the server. In this security it compares the pattern of ridges and creases on the fingers. As per the survey record it is found that it is the worst security in Biometric. For eg. China stolen the fingerprints of 5.6 million US Federal Employees in Year 2013 [8].

(b) Voice Recognition Authentication
As per the record it is most widely use security in cyber world. It is different from speech recognition and it is basically recognized the way of person speaks and the pitch of the voice.
(c) Iris Scanner Authentication
It is the latest technology used for authentication in different aspects and it recognizes the person by laser system that scan the retina of the eye that has unique pattern.

(d) Facial Recognition Authentication
This authentication application is capable to recognizing and confirming a person from the video sources and digital images. It recognizes the shape, size and pattern of the face of the person.

This Table shows the pros and cons of Biometric Authentication and which is designed by analyzing different articles:

<table>
<thead>
<tr>
<th></th>
<th>Fingerprint</th>
<th>Face</th>
<th>Iris</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniqueness</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Durability</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>How Well Trait can be Sensed</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Speed and Cost Efficiency of System</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Willingness of people to have trait used</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Difficulty of spoofing the trait</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>False Rejection Rate</td>
<td>0.4%</td>
<td>1-2.5%</td>
<td>1.1-1.4%</td>
<td>5-10%</td>
</tr>
<tr>
<td>False Acceptance Rate</td>
<td>0.1%</td>
<td>0.1%</td>
<td>0.1%</td>
<td>2-5%</td>
</tr>
</tbody>
</table>

**Algorithm used for Encryption**

1. **Triple DES**
Triple DES is designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry. Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it.

2. **RSA**
RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You’ve got your public key, which is what we use to encrypt our message, and a private key to decrypt it.

3. ** Blowfish**
Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. It’s definitely one of the more flexible encryption methods available.

4. **Two fish**
Computer security expert Bruce Schneider is the mastermind behind Blowfish and its successor Twofish. Keys used in this algorithm may be up to 256 bits in...
length and as a symmetric technique, only one key is needed. Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments.

Tools Used for Two Fish Encryption: Photo Encrypt, GPG, and the popular open source software True Crypt.

5. AES
The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes. AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

C. Digital Signatures
Digital signatures can be created out of the same mathematical algorithms that are used in asymmetric encryption. A user holds a private key for getting some information encoded with it. Anyone can get the same decrypted data by having the public key that will verify the person’s credentials. This process is the core of the exact reciprocal of public key encryption

D. Anti-virus
The threats of computer viruses or undesirable short programs that trigger unwanted commands without the explicit permission of user have assumed monstrous proportions. Anti-virus software carries out two functions; it prevents the installation of virus in a system and scans the systems for viruses that are already installed.

E. Firewall
Firewalls [9,10] effectively hold back any attempt of unauthorized access to a computer when it is connected on the internet by hackers directly or via other network connections. Firewalls come pre-installed with most operating systems and are turned on as default. The help of commercial firewalls can be required if the security level of the default firewall is not strong enough or if it is posing interference to legitimate network activities.

Working of Firewall
There are various different methods firewalls use to filter out data, and some are used in combination. These methods work at dissimilar layers of a network, which determines how specific the filtering options can be used. Firewalls can be used in a number of ways.
to add protection to user’s home or business. Large organization or corporations often have very complex firewalls in their workplace to secure their networks. On the other side, firewalls can be configured to avoid employees from sending certain types of mails or transmitting confidential data outside the network. On the inbound side, firewalls can be programmed to stop access to certain websites like social networking sites. Moreover, firewalls can prevent outside computers from accessing computers inside the network.

G) Some Cyber Security Tools

There are various tools used for cyber security such as:

1. Vulnerability Scanners
   (a) Nmap- It is the Network Mapper and available as free and open source license utility for network discovery and security auditing.
   (b) Nessus – For Security Practitioners who evaluate complex enterprise networks for security flaws and compliance issues, Nessus is the world’s most widely Deployed vulnerability and configuration assessment product.
   (c) Open VAS – Open VAS is a framework of several services and tools offering a wide-ranging and powerful vulnerability scanning and vulnerability management solution.

2. Forensic Security Tools
   (a) FTK Imager - It is a court accepted digital investigations platform which is built for speed, analytics and enterprise-class scalability. It is known for its in-built interface, email analysis, customizable data views and stability, FTK lays the framework for seamless expansion, so your computer forensics solution can grow with organization’s needs.
   (b) Sans Investigate Forensic Toolkit (SIFT) - The SIFT workstation is a VMware appliance, pre-configured with the necessary tools to perform detail digital forensic examination in the variety of settings. It is compatible with Expert Witness Format (E01), Advance Forensic Format (AFF), and raw(dd) evidence formats. The brand new version has been completely rebuilt on an Ubuntu base with many new capabilities and tools such as log2 timeline that provides a timeline that can be of enormous value to investigator.

3. Penetration Testing
   (a) Metasploit - Simplifies network discovery and vulnerability verification, Tool Used: Nexpose.
   (b) Paros - Web Scanner

4. Reverse Engineering
   (a) OllyDbg – It is an assembler level analyzing debugger for Microsoft® Windows®. Emphasis on binary code analysis.

5. Network and Security Traffic Analysis
   (a) Silk - Silk, the System for Internet-Level Knowledge, is a collection of traffic analysis tools developed by the CERT Network Situational Awareness Team (CERT NetSA) to facilitate security analysis of large networks.

IV. Review of Cyber Security Practices

This research study aims to highlight the conditions of Cyber Security in the world and the best cyber security practices. These are the countries that are top listed in the ITU’S cyber security ranking. This set of the particular countries contains a section of each of the following:

1. Developed Countries

This includes countries that lead the ITU’s ranking which regards to cyber attentiveness [11] shown in Table 1. The analysis of these strategies will provide a notion of advance and secure cyberspace practices to be measured while expressing a cyber security strategy documents.

The Cyber Security practices of USA, UK, France, Netherlands and Germany are particularly recognized worldwide for mentioning dual aspects of cyber security that is both offensive and defensive cyber security action plans [12]. Japan, Spain, Australia and Canada [13] have been selected because they have the highest ICT usage and cybercrime rate in the world after US and Germany; they also reveal potentially secure approaches for combating cybercrimes in the country. [14] Besides these Countries Czech Republic and Estonia are amongst the few countries that have
Table 1: Developed Countries with High Cyber Security Ranking

<table>
<thead>
<tr>
<th>Cyber Security Ranking</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USA</td>
</tr>
<tr>
<td>2</td>
<td>Canada</td>
</tr>
<tr>
<td>3</td>
<td>Australia</td>
</tr>
<tr>
<td>4</td>
<td>New Zealand</td>
</tr>
<tr>
<td>5</td>
<td>Estonia, Japan, UK, Germany</td>
</tr>
<tr>
<td>6</td>
<td>Austria, Israel, Netherland</td>
</tr>
<tr>
<td>8</td>
<td>Finland</td>
</tr>
<tr>
<td>9</td>
<td>France</td>
</tr>
<tr>
<td>12</td>
<td>Czech Republic</td>
</tr>
</tbody>
</table>

updated their first strategy draft. Netherlands has been selected as like the USA, it has two separate strategies one for Civil and other for military cyber defence. Finland and Israel are considered the prime example of cyber excellence according to many security researchers. [15] This is the reason why the strategies of these countries have been selected for the study.

2. Developing Countries
This includes countries which have high cyber security ranking, according to ITU, as shown in Table 2. Cross Comparison of Such Strategies will provide necessary information for developing nations development with such a quick step in cyber domain, Leave even many developed countries behind.

The Researchers regard Malaysia as the most cyber savvy country of Asia and hence, it is included in the set of countries for research [16]. India and Iran have extremely high cybercrimes rates, so the analysis of their strategies will provide considerable direction for protecting the cyberspace against miscellaneous threats and attacks.

3. Comparison Based on Identified standards
The Cyber Security strategies exist in various forms and length varying from nine pages (Netherlands Cyber Security Strategy of 2011) to ninety pages (Saudi Arabia’s Cyber Strategy of 2013). Most of the countries under study have developed separate strategies for National Defense and Cyber Security, whereas few added a portion of “Cyber Security” in national security strategy or the defense strategy.

(a) Development of Cyber Security Strategy
The Development of cyber security strategies gradually gained momentum after 2008 when the trend of Cyber-attacks shifted to massive targeted state-sponsored attacks. Table 3 below gives a timeline of NCSS of Various National Cyber Security Strategies that have been selected from research study. With the Exception of Iran, Israel and Malaysia, all the countries have published their strategies online. The data for these three countries have been take out from public documents relating to the cyber security methods in the country.

Table 2: Developing Countries with High Cyber Security Ranking

<table>
<thead>
<tr>
<th>Cyber Security Ranking</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Malaysia</td>
</tr>
<tr>
<td>5</td>
<td>India</td>
</tr>
<tr>
<td>7</td>
<td>Turkey</td>
</tr>
<tr>
<td>19</td>
<td>Iran</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Countries</th>
<th>Year Strategy/ Policy Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Strategy 2009, Revised strategy expected</td>
</tr>
<tr>
<td>Austria</td>
<td>Strategy 2013</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Strategy 2011, 2015</td>
</tr>
<tr>
<td>Finland</td>
<td>Strategy 2013</td>
</tr>
<tr>
<td>France</td>
<td>Strategy 2011</td>
</tr>
<tr>
<td>Germany</td>
<td>Strategy 2011</td>
</tr>
<tr>
<td>India</td>
<td>Policy 2013</td>
</tr>
<tr>
<td>Iran</td>
<td>NCSS not Public</td>
</tr>
<tr>
<td>Israel</td>
<td>Official NCSS not Published</td>
</tr>
<tr>
<td>Japan</td>
<td>Strategy 2013</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Policy 2006 (Document not Public) NCSS expected in 2017</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Strategy 2011, 2013</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Strategy 2011</td>
</tr>
<tr>
<td>Saudia Arab</td>
<td>Strategy 2013</td>
</tr>
<tr>
<td>Spain</td>
<td>Strategy 2013</td>
</tr>
<tr>
<td>Turkey</td>
<td>Strategy 2013</td>
</tr>
<tr>
<td>UK</td>
<td>Strategy 2009, 2011</td>
</tr>
</tbody>
</table>

The timeline infers that majority of the countries published their cyber security strategy in 2011. The United States of America, on the other hand, published the first strategy draft in 2003, when cyber-attacks were not very common. However, the continuously changing spectrum of cyber threats has made it imperative to update the cyber security strategy to encompass emerging threats and relevant countermeasures. Countries particularly the UK, USA, Netherlands, Czech Republic and Estonia have consequently published the subsequent versions of their strategy as well, with USA reviewing and updating their documents most frequently.

(b) Strategic Objectives outlined in NCSS

NCSS basically defines the vision of any country for addressing the cyber security challenges at the national level. Since all strategies are directed towards the ultimate goal of safeguarding the national cyberspace, they share many common themes and concerns. Except for Germany, which lists down some priority areas as the objectives, all other countries clearly state their strategic objectives in the document. The common objectives found in almost all NCSS are: [17]

1. To maintain a safe and resilient cyberspace,
2. To secure critical national cyber assets and infrastructures,
3. To define a cyber-security regulatory, legislative and assurance framework,
4. To raise cyber awareness amongst citizens, government officials, IT professionals etc.,
5. To develop cyber security incident detection and response capabilities e.g. Cyber-Security Incident Response Team (CSIRT) etc.,
6. To develop indigenous cyber-security technology,
7. To respect fundamental rights of citizens,
8. To promote public-private co-operation for enhancing the cyberspace security,
9. To stimulate international co-operation mainly with the neighboring and regional countries.

Beside the common ones, few strategies have also proposed objectives that are only specific to their country. For instance, France desires to become a world leader in cyber security domain in near future. Also, Japan desires for agile adaptation of evolving cyber threats and introduction of global outreach programs for cyber security, etc. The thorough study of the selected strategies also brings forward the fact, that with the passage of time, the scope of cyber security strategies is shifting from merely securing citizens or governments against cyber-attacks to securing the whole information society in general.

(c) Level of prioritization assigned to cyber security
In the last few years, besides terrorism, economic downturn, natural hazards, etc., cyber-attacks, cyber espionage and cyber terrorism have also become a global risk. The comparative analysis reveals that countries have now realized the importance of cyber security and, therefore, regard it as one of the top-tier national security issues. Countries especially USA, UK, Japan, Germany, Australia and France that have inflated rates of cybercrimes, have allocated significantly greater resources to cyber security measures than other countries under study. According to the publically available data, the UK spends £650m annually, India $500 million, France $1.2 billion, Canada $6 billion, and USA with the highest annual cyber security spending in the world amounting up to 10 billion dollars. [18] The facts indicate that despite same prioritization is assigned to cyber security in various documents, extensive variation lies in the budget allocated to national cyber security initiatives. [19]

(d) Characterization of Cyber Security Threats
For most of the countries, especially Canada, USA, UK, Germany, Netherlands etc. the potential risks and threats posed to the cyberspace revolve around organized cybercrimes, state sponsored attacks, cyber terrorism, unauthorized access to and interception of digital information, electronic forgery, damage and blackmail etc. For Germany and Netherlands, natural hazards and hardware/software failures too are regarded as the cyber threats. [20] In the cyber security strategies, there also exist some offenses that varies in terms of severity of the crime in different countries. Since Germany view cyber-attack as the attack on IT systems that compromises secrecy, availability and integrity of the information systems, USA considers it as an attack on the digital information, ICT devices and cyber networks. Hence, where probing is considered as a cybercrime in Germany, it is not an offense in USA. [21] Thus the varying observation of cyber security and the cyber threat landscape makes it difficult to adopt a holistic global approach to cyber threats and adversary. Apart from the traditional cyber-attacks, few countries have also taken account of emerging cyber risks in their strategies e.g. France, Japan and India have considered the risks of Cloud Computing, Japan mentions the need of addressing the security of Internet Protocol IPv6 and appliances attached to smart grids etc., in the document. Few countries such as Estonia, USA, Germany and Netherlands have also referred to cyber warfare in their documents. However, Finland and France have not defined any cyber threat topology explicitly in the strategy.

(e) Technical Measures:
(Threat Information Sharing/ Early Warning Approached) For a country to effectively deter targeted cyber threats and incidents, it is essential to have technical teams that efficiently spread threat information to the concerned authorities and provide cyber protection and resilience capabilities. Various forms of such teams include Computer Emergency Response Teams (CERTs), Computer Security Incident Response Team (CSIRT) and Information Sharing and Analysis Centre’s (ISAC). The cross comparison of the selected NCSS reveals that all the countries hold their own national CERT/ CSIRT for effectively responding to cyber-attacks. However, the missions and efficiency of these units greatly vary for one another. Table 4 below provides a timeline of the establishment of CERT/ CSIRTS in the countries under study. [22]
Table 4: Timeline of Cyber Security Strategies

<table>
<thead>
<tr>
<th>Countries</th>
<th>CERT Established</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>2010</td>
</tr>
<tr>
<td>Austria</td>
<td>2008</td>
</tr>
<tr>
<td>Canada</td>
<td>2003</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>2011</td>
</tr>
<tr>
<td>Estonia</td>
<td>2006</td>
</tr>
<tr>
<td>Finland</td>
<td>2014</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1997</td>
</tr>
<tr>
<td>Netherlands</td>
<td>2012</td>
</tr>
<tr>
<td>New Zealand</td>
<td>2011</td>
</tr>
<tr>
<td>Saudia Arab</td>
<td>2006</td>
</tr>
<tr>
<td>Spain</td>
<td>2008</td>
</tr>
<tr>
<td>Turkey</td>
<td>2007</td>
</tr>
<tr>
<td>UK</td>
<td>2014</td>
</tr>
<tr>
<td>France</td>
<td>2008</td>
</tr>
<tr>
<td>Germany</td>
<td>2012</td>
</tr>
<tr>
<td>India</td>
<td>2004</td>
</tr>
<tr>
<td>Israel</td>
<td>2014</td>
</tr>
<tr>
<td>Japan</td>
<td>1996</td>
</tr>
<tr>
<td>USA</td>
<td>2003</td>
</tr>
</tbody>
</table>

Few countries have also established coordinating bodies along with CERT/CSIRTS for information threat sharing. For example, Integrated Government of Canada Response Systems by Canada, Cyber Security Strategy Headquarter by Japan, etc.

To ensure that all public and private entities can handle cyber security challenges, it is necessary to establish an appropriate policy framework to frequently evaluate the progress of the proposed objectives of the strategy and revise the strategy accordingly. The research reveals that except for Spain, most countries within the scope of study have mentioned review and evaluation processes for the strategy in the documents. Since, Malaysia has not formulated the complete strategy yet, it, therefore, lacks annual cyber security audits and policy reviews too. Countries such as Austria, Estonia and Germany have even specified the actors to be involved in reviewing mechanisms. However, in all instances, the details of review mechanisms have been provided as a separate act or in implementation scheme. Several strategies have also mentioned the frequency of the review cycle i.e. yearly for Netherlands and Slovakia and biannual for Austria and UK. [23]. While USA, UK, Estonia and few other countries update their cyber security strategy very frequently, there are countries that have not even updated their initial cyber security strategies once.

(f) Cyber Security Capacity Building

All cyber security strategies mention the need of creating cyber defensive and preventive capabilities to better defend the national cyberspace. This subsection throws light on various cyber security capacity building initiatives e.g. training, awareness, R&D initiatives etc., as documented in the selected strategies.
(1) Manpower Development and Cyber Awareness Programs:

All cyber security strategies emphasize the need of raising cyber awareness in general public especially businessmen, IT professionals, government officials and lawmakers. But countries especially, Australia, Spain, Japan and the UK pay special attention to the cyber training of children and parents too. [24] Countries particularly UK, India and Malaysia have mentioned the usage of social media for launching widespread awareness campaigns. However, Netherlands and Turkey highlight the need of teaching cyber security at all academic levels and have thus suggested making it a part of academic curriculum. All the nations under study, except for the Czech Republic, have defined nation-wide cyber-security outreach programs for their citizens, where they provide cyber security tools and practical education. The most notable programs amongst them are Stay Safe Online campaign of Australia, Malaysia’s “Cyber Safe” Program, “Get Safe Online” program of UK, and organization of “Cyber Security Month” annually by Austria, UK, and US. [25] The study also reveals Japan’s desire for establishing various cyber security support services for the capacity building. Moreover, countries especially UK, Netherlands, India, Saudi Arab, Malaysia, and Turkey emphasize the need of commercial security certifications/ trainings for professionals and experts in their NCSS. [26]

(2) Research and Development:

To prevent inherent vulnerabilities of the ICT devices from being exploited by adversaries, it is required to lay stress on the development of local security products, thereby enhancing cyberspace security. The comparative study shows that except for Australia, Saudia Arab, Czech Republic, UK and Finland, all other countries have officially recognized entities for promoting R&D work at the national level. The tasks of the R&D divisions as mentioned in the various strategies are to sponsor academic and industrial projects related to cyber security, develop indigenous cyber security products, promote security standards and best practices at the national level, etc.

(g) Latest on Cyber Security Practices

Privacy and data theft will be the top security issues that organizations need to focus. All are living in a world where all information is in digital form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. There will be new attacks on Android operating system based devices, but it will not be on a huge scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8 and Windows 10, so it will be possible to develop malicious applications like those for Android [27] and infected them using network and web.

V. Conclusion

In the recent years, Cyber Security has gained more attention than the issue of National Physical Security. Countries around the world are, therefore, framing cyber security strategies to address this serious issue. Almost all documented strategies, selected by different countries, have mentioned the need of establishing incident prevention capabilities at the national level, raising cyber awareness in general public, and promoting public-private partnership for better security of the cyberspace, etc. However, the majority of the countries have practically tried less to achieve the above stated objectives. Despite similar aims and objectives, the research has shown many differences in the scope and approach of the twenty strategies that were selected for the study. For instance, the establishment of CERT has been mentioned in all the strategies, but the tasks assigned to it vary from country to country. Similarly, all strategies urge the need of running various cyber awareness programs, but the approach of each country is different from the other. From a detailed research, it is obvious that the strategies of UK, USA and Germany are particularly better than the rest in terms of development and enforcement of action plans. Despite stating defensive missions in the strategy, they have also highlighted on utilizing their cyber capabilities to defend valuable assets offensively, and this gives them an edge over the other countries.
References

10. Kuang Chu, network security and firewall technology, Chongqing university publishing house, 2005
24. ENISA. National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace. May 2012.
27. Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012
Comparative Analysis of Intrusion Detection System Schemes for MANETs

Ruby Dahiya*
Manpreet Singh**
Mohit Jalan***

Abstract

In current information age, the mobile wireless telecommunication becoming more innovative and attractive because of its applications in emerging fields. The attacks has been made from years ago, many schemes were launched to secure data from intruders.

In this paper, comparative study on Intrusion Detection System Schemes for Mobile Ad-hoc Networks has been made. It will present an analysis of performance of the algorithms used for securing data information over mobile network.

Keywords: Watchdog Algorithm, Mobile Ad-hoc Networks, Intrusion Detection Systems, Enhanced Adaptive Acknowledgement

I. Introduction

Intrusion
Intrusion is an unauthorized act of spying, snooping, and stealing information through cyber space. It is defined as a sequence of related actions performed by malicious attacks those results in the compromise of a aim system. It is assumed that the actions of the interloper violate a given security policy.

Intrusion Detection
Intrusion detection (ID) is the technique for identifying and responding to malicious activities targeted at computing and network resources. Intrusion detection is an approach that is complementary with respect to mainstream approaches to security, such as access control and cryptography.

Intrusion Detection System
Intrusion detection systems (IDSs) are software applications dedicated to perceive intrusions against a target network. IDS is placed out-of-band on the network infrastructure, meaning that it is not in the correct real-time communication path between the sender and receiver of information [5].

There are three major modules of IDS: Monitoring, Analyses and Response. The Monitoring Module is responsible for controlling the cluster of data. Analysis Module is responsible for deciding if the collected data indicated is an intrusion or not. Response Module is responsible for managing and using the response actions to the intrusion [5].

IDS in MANETs
A MANET is a mobile ad-hoc network that can change its locations and configure itself on the fly. It uses wireless connections to connect to diverse networks.

The limitation of MANETs is that its routing protocols and nodes assume that other nodes forever help with each other to transmit the data. The assumption leaves the attackers with the opportunities to achieve their target. To address this problem, IDS should be added to enhance the security level of MANETs [2].

Security issues in MANETs

1) MANET is highly vulnerable to attacks because node configuration and maintenance are done on their own [3].

2) One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment [3].
The ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious invader reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network.

In the next section, we will concentrate on the IDS Architecture for MANETs required for understanding this research topic.

**II. IDS Architecture For Manets**

In fig.1, MAC Layer is the data link layer from where the data packets are send one by one from sender to receiver by means of transmission techniques. To protect the data from intruders, IDS Layer is made in between to secure data.

The Local IDS Agent collects the data from the MAC Layer and sends it to Intrusion Detection Engine for analyzing and processing. The data is further sent to Intrusion Response Engine to give response to the network layer. In this, intruders will get less chances to track data from both the ends i.e. sender and receiver.

In the next section, we mainly concentrate on discussing the various schemes for IDS in MANETs required for understanding this research topic.

**III. Various Schemes of IDS in Manet's**

In this paper, we will be comparing four various schemes of intrusion detection system in mobile ad-hoc network security. Those are WATCHDOG, TWOACK, and AACK AND EAACK ALGORITHM.

**A. WATCHDOG**

A watchdog algorithm was made to cope with the problem of attack named as black hole. In this algorithm, [9] each network node connected to other node works as a spectator (watcher) to the next node connected to it. This continues till it reaches to the router or receiver. The watchdog algorithm defines the time limit to each node in which it checks the data by sending time and storing time. If the sending time is more than the storing time then that node is being marked up as a harmful/mischievous node. If something like this happens then the path rater gets active with routing algorithms and ignores that node in between the transmission [9].

**B. TWOACK**

This algorithm states that the communication between the dispatcher and the recipient is on the basis of the two hops or we can say the three nodes communication.
Fig. 2 states that S is the sender and R is the receiver just two hops far from S and I is the immediately knot in between the S and R. [1] So while transmitting the data, S will send the packet to the I (Intermediary) node and I will send that packet to the R. On completion of this process, R will send back the ACK (Acknowledgement) for the packet to the S. If TWOACK packet doesn’t get back to the S in define time period both the nodes I and R are defined as harmful/malicious nodes. This process goes up for all the nodes till destination.

C. AACK
Adaptive ACK ALGORITHM is being termed as end-to-end Acknowledgment. Basically, it is a combination of peer-to-peer Ack and TWOACK.[8] As TWOACK send the acknowledgment packet to the node two hops, in AACK this process is done from the sender to the receiver/destination end.

The S sender or source sends the packet to the R Receiver or Destination by the intermediate nodes i.e. A, B and C. Each node passes the packet to the next node and then get the Acknowledgment in the reverse order to the sending route. If the sender doesn’t get the acknowledgement then it sends it by TWOACK algorithm to find the harmful node in between.

D. EAACK
EAACK is being termed as Enhanced Adaptive Acknowledgement. [2] This algorithm is a combination of three things i.e. ACK, SACK and MRA.

ACK is being used for peer to peer communication when there is no such harmful node in between.
SACK is an advance form of the TWOACK which is used to detect the malicious node or the harmful node.
MRA is an algorithm which is used to search the routing path into its local databases. [5] If the algorithm does not get the path, then sender starts DSR routing algorithm to find another way to transmit the packet to the destination.

In the next section, we will concentrate on comparison of various schemes for IDS in MANETs.

IV. Comparison of Various IDS Schemes in Manets
Here, we have compared four schemes namely: Watchdog, TWOACK, AACK and EAACK for intrusion detection in MANETs. The factors used for their comparative analysis are: Ambiguous Collision, Receiver Collision, Limited Transmission Power, False misconduct report, Collusion, Partial Dropping, Network Overhead and Detection. The Table shown below represents the comparison of IDS Schemes for MANETs.

IV. Conclusion
The Mobile Ad-hoc Network is a new technology used in many applications. Because of its characteristics, the networks are more vulnerable to attacks and have most security problems. In this paper, the comparative analysis is made on IDS schemes for MANETs to explain best suited algorithm.
The Watchdog algorithm aims to improve the throughput of network in presence of malicious no design in the network. It has no network overhead compared to other schemes of IDS.

The TWOACK Algorithm aims to solve the receiver collision and limited transmission power. The network overhead is more as well as it fails to detect malicious nodes in the network with presence of false misbehavior report and forged acknowledgement packets.

The AACK algorithm combines TWOACK and an end-to-end acknowledgement scheme (ACK). It reduces network overhead compared to other schemes and it fails to detect malicious nodes in the network as TWOACK Scheme.

The EAACK has no network overhead and detects malicious nodes in the network. To prevent attackers from initiating forged acknowledgement attacks, a digital signature is incorporated in the scheme.

References
Scientific Research and Development of Mobile Application for Android Platform

Dimple Chawla*
Rahul Aggarwal**
Akansha Aggarwal***

Abstract
In recent years, the emergence of smart phones has changed the definition of mobile phones. Mobile phone is no longer just a communication tool, but also an essential part of the people’s communication and daily life. Various applications added unlimited fun for people’s lives. It is certain that the future of the network will be the mobile terminal. Now the android system in the electronics market is becoming more and more popular, especially in the Smartphone industry. Because of the open source, some of the development tools are free, so there are plenty of applications generated. This greatly inspired the people to use the android system. Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets. Android’s user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input.

The purposes for developing this android application for providing the services to the user. It maybe for providing information, communication, Image and video making, Entertainment, Recharge Bills and Storing data. Also giving chance to entrepreneurs and developers make their own application for income source and reach an even broader audience base.

This paper gives a complete knowledge of how to start working on eclipse and develop an application and get it run on emulator.

Keywords: Android SDK, ADT plug-in, AVD manager, Eclipse-IDE, java/xml, Android Development Architecture, Activities.

I. Introduction

To develop apps for Android, here to use a set of tools that are included in Android Studio or Eclipse. In addition to using the tools from Android Studio, also access most of the SDK tools from the command line. Developing with Android Studio is the preferred method because it can directly invoke the tools that required for developing applications.

App Workflow: The four basic steps for developing any application (with or without android studio) includes:

Environment Setup: During this phase you install and set up your development domain.
Project Setup and Development: In this phase you set up and develop your Android Studio project and application modules, which have all of the source code and resource files for your respective application.
Building, Debugging and Testing: During this phase you build your project into a debuggable.apk package(s) that you can install and run on the emulator or an Android-powered device.
Publishing: During this phase you configure and build your application for release and distribute your application to users.
Applications: These are the basics of Android applications:

Dimple Chawla*
Department of IT, DIAS, Rohini, Delhi
Rahul Aggarwal**
Student, DIAS, Rohini, Delhi
Akansha Aggarwal***
Student, DIAS, Rohini, Delhi
Each component accomplishes a different role in the final application behavior, and each one can be triggered individually (even by other applications).

The manifest file must declare all components in the application and should also declare all application demands, such as the minimum version of Android necessary and any hardware configurations that are essential.

Non-code application resources (images, strings, layout files, etc.) should include options for different device configurations (such as different strings for different languages).

**Android System Architecture**

**Applications:** Android gives a set of core applications plugining client, SMS program, calendar, maps, browser, contacts, and soon, all developed in Java.

**Application Framework:** The developer is allowed to access all the API framework of the core programs. The application framework simplifies the reuse of its segments. Any other app can release its functional components and all other apps can access and use this component by following the security aspects of the framework.

**Libraries and Android Run Time:** The library is divided into two parts, Android Runtime and Android Library. Android Runtime is comprised of a Java Core Library and Dalvik virtual machine.

**Linux Kernel:** The kernel system service provided by android inner nuclear layer is based on Linux 2.6 kernel; operations like internal storage, process management, internet protocol, bottom-drive and other core service are all placed on Linux kernel.

**Eclipse:** Eclipse is an integrated development environment (IDE). It contains a base workspace and an extensible plug-in system for customizing the environment. Eclipse is written mostly in Java and its primary use is for developing Java applications, but it may also be used to develop applications in other programming languages through the use of plugins.

1. **Tools and Environment**

Here we will discuss the installation details of software. Android SDK Tools, revision 20 or newer.
SDK Platform Android 3.0 (API 11). The minimal platform supported by Java API is Android 2.2 (API 8). But for successful compilation the target platform should be set to Android 3.0 (API 11) or higher. It will not prevent them from running on Android 2.2.

Eclipse IDE: There is a list of Eclipse versions that are well matched with the Android SDK. In this paper we are using Eclipse 3.7 (Indigo).

ADT plug-in for Eclipse: Android Development Tools (ADT) is a plug-in for the Eclipse IDE that is designed to give us a strong, integrated environment in which to build Android applications.

ADT unroll the capabilities of Eclipse to let us rapidly set up new Android projects, create an application UI, add packages based on the Android Framework API, debug applications using the Android SDK tools, and even export signed (or unsigned) .apk files in order to spread the application. Developing in Eclipse with ADT is highly recommended and is the fastest way to get started. With the guided project setup it provides, as well as tools unification, custom XML editors, and debug output pane, ADT gives us an incredible elevation in developing Android applications.

Following paragraph will explain, how to download and install the ADT plug-in:

Start Eclipse and then select Help, now you have to click on → Install New Software. Now, click on Add, it is present on the top-right corner of your screen.

After doing all this, a Add Repository dialog box will appear, enter “ADT Plug-in” for the Name and the URL refer to Figure 3.

Now, click OK and make sure that your system must be connected to the internet. In the Software dialog box, select the checkbox next to Developer Tools and then click next. A new window will appear and in that, we’ll see a list of the tools to be downloaded. You have to click on Next. License agreement will appear, read and accept that and then click Finish. After this installation bar will appear, wait for its completion and once it is completed restart eclipse.

AVD Manager: The AVD Manager provides a graphical user interface with the help of which we can create and manage Android Virtual Devices (AVDs), which are required by the Android Emulator. For emulation, a device is defined. Select Window and then from the menu select Android AVD Manager.
Create a Project with Android Studio

You have to create a new project in the android studio. Android studio already gives you a opened project in the welcome screen but If you don't have a project opened, in the Welcome screen, click on New Project but If you have a project opened the from the File menu, select the New Project. The Create New Project screen appears.

Now fill out the fields that appear on the screen, and then click on Next.

Application Name is the app name that appears to users. For this project, use “My First App.”(or anything you like)

Company domain provides a qualifier that will be appended to the package name; Android Studio will remember this qualifier for each new project you create.

Package name is the fully qualified name for the project (following the same rules as those for naming packages in the Java programming language). Make sure that your package name must be unique across all packages installed on the Android system.

You can also edit this value independently from the application name or the company domain. Project location is the directory on your system that holds the project files.

Under the Select form the factors on which your app will run on, check on the box for Phone and Tablet(For Minimum SDK, select API 8: Android 2.2 (Froyo)). Leave all of the other options (TV, Wear, and Glass) unchecked and then click on Next.

Activities An activity is one of the distinguishing features of the Android framework. Activities provide the user with access to your app, and there may be many activities. An application will usually have a main activity for when the user launches the application, another activity for when she selects some content to view, for example, and other activities for when she performs other tasks within the app.

After this Add an activity to <template>, select Blank Activity and then click on Next.

Under Customize the Activity option, change the Activity Name to MyActivity. The Layout Name will change to activity_my, and the Title name will change to MyActivity. The Menu Resource Name will be menu_my.now click on finish button and create your project.
Developing an Audio Player

Step 1: Open the project’s main layout file and replace its contents with the following layout:

```xml
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="fill_parent"
    android:layout_height="fill_parent"
    android:orientation="vertical"
    android:background="#FF330000"
    tools:context=".MainActivity">
  <ListView
    android:id="@+id/song_list"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content" />
</LinearLayout>
```

Step 2: Store the title strings in the `res/values/strings.xml` file. The two items refer to drawable files. Create your own or use these two images to start with:

```
<ListView
    android:id="@+id/song_list"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content" />
</LinearLayout>

Step 2: Store the title strings in the `res/values/strings.xml` file. The two items refer to drawable files. Create your own or use these two images to start with:

<table>
<thead>
<tr>
<th>AvD Name</th>
<th>Target Name</th>
<th>Platform</th>
<th>API Level</th>
<th>CPU/AB</th>
</tr>
</thead>
<tbody>
<tr>
<td>GalaxyNexus42</td>
<td>Android 4.2.2</td>
<td>4.2.2</td>
<td>17</td>
<td>ARM (armeb-v7x)</td>
</tr>
</tbody>
</table>
```

Figure 3: ADT Plug-in wizard to install

Figure 4: Android Virtual Device Manager Wizard
We will also use an icon to display in the playback notification. Create one now or use the one below:

▶

The code will refer to the images using the names `rand`, `end`, and `play` so make sure that you use the same file names. Copy the images to your project's `drawables` folder(s). We will implement the actions later.

**STEP 3:** Open the main Activity class and add the following imports:

```java
import java.util.ArrayList;
import java.util.Collections;
import java.util.Comparator;
import android.net.Uri;
import android.content.ContentResolver;
import android.database.Cursor;
import android.widget.ListView;
```

Declare the following instance variables before the `onCreate` method:

```java
private ArrayList<Song> songList;
private ListView songView;
```

We will store the songs in a list and display them in the `ListView` instance in the main layout. In `onCreate`, after setting the content view, retrieve the `ListView` instance using the ID we gave it in the main layout:

```java
songView = (ListView) findViewById(R.id.song_list);
```

Instantiate the list as shown below:

```java
songList = new ArrayList<Song>();
```

Next, in the main Activity class declaration, after the existing methods, create a helper method to retrieve the audio file information:

```java
private void getSongList() {
    // add songs to list
    do {
        long thisId = musicCursor.getLong(idColumn);
        String thisTitle = musicCursor.getString(titleColumn);
        String thisArtist = musicCursor.getString(artistColumn);
        songList.add(new Song(thisId, thisTitle, thisArtist));
    } while (musicCursor.moveToNext());
}
```

Now we can iterate over the results, first checking that we have valid data:

```java
if (musicCursor != null && musicCursor.moveToFirst()) {
    // get columns
    int titleColumn = musicCursor.getColumnIndex
        (android.provider.MediaStore.Audio.Media.TITLE);
    int idColumn = musicCursor.getColumnIndex
        (android.provider.MediaStore.Audio.Media._ID);
    int artistColumn = musicCursor.getColumnIndex
        (android.provider.MediaStore.Audio.Media.ARTIST);
    // add songs to list
    do {
        long thisId = musicCursor.getLong(idColumn);
        String thisTitle = musicCursor.getString(titleColumn);
        String thisArtist = musicCursor.getString(artistColumn);
        songList.add(new Song(thisId, thisTitle, thisArtist));
    } while (musicCursor.moveToNext());
}
```

We first retrieve the column indexes for the data items that we are interested in for each song, then we use these to create a new `Song` object and add it to the list, before continuing to loop through the results.

Back in `onCreate`, after the code we added, call this new method:

```java
getSongList();
```

**STEP 4:** Back in the main Activity class, in the `onCreate` method after sorting the list, create a new instance of the `Adapter class` and set it on the `ListView`:

```java
SongAdaptersongAdt = new SongAdapter(this, songList);
songView.setAdapter(songAdt);
```

II. Conclusion

Android is a full, open and free mobile device platform, with its powerful function and good user experience rapidly developed into the most popular mobile
operating system. This paper gives an overview of the different challenge and issues faced in android app development. It gives a detailed reference of a new music app. The experience of developing an android app is quite challenging, motivating as well as satisfying.

References
Cyber Security: A Brief Encounter

Anil Kumar Pandey*

I. Introduction
The digital domain has become more intertwined with our daily lives. Citizens, government bodies and businesses are using digital applications for online interactions, transactions, more efficient collaboration, communication and entertainment. More equipment with integrated ICT services is connected to the internet: computers and telephones, but also cars, thermostats and medical equipment. This increasing digitization is not only for ease, efficiency and pleasure, but is also an important drive behind innovation and economic growth.

Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems. There is a wide range of currently accepted cyber security definitions:

1. The Committee on National Security Systems defines cyber security as the ability to protect or defend an enterprise’s use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or, destroying the integrity of the data or stealing controlled information.

2. The National Institute of Standards and Technology defines cyber security as “the process of protecting information by preventing, detecting, and responding to attacks.” Similar to financial and reputational risk, cyber security risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers.

3. International Organization for Standardization defines cyber security or cyberspace security as the preservation of confidentiality, integrity and availability of information in the Cyberspace. In turn, “the Cyberspace” is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.” At its core, cyber security seeks to protect your enterprise from those who wish to do harm to your business, steal your information or your money, or use your systems to target peers in the market.

Cybersecurity is a shared responsibility – people, processes, tools, and technologies work together to protect an organization’s assets. Protecting your organization’s assets requires a focus on the following three fundamental goals:

A. Confidentiality Any important information you have that should be kept confidential. This information should only be accessed by people (or systems) that you have given permission to do so.

B. Integrity Maintain the integrity of information assets to keep everything complete, intact, and uncorrupted.

C. Availability Maintain the availability of systems, services, and information when required by the business or its clients.

II. Strategic Objectives

1. FUNDAMENTAL INTERESTS, DEFENSE AND SECURITY OF STATE INFORMATION SYSTEMS AND CRITICAL INFRASTRUCTURES, MAJOR CYBER SECURITY CRISIS. (Having the scientific, technical and industrial capabilities required to protect sovereign information, ensure cyber security and develop a trustworthy digital economy.)

2. DIGITAL TRUST, PRIVACY, PERSONAL DATA, CYBERMALEVOLENCE (Measuring cybercrime, Recommending technical solutions aimed at securing digital life and which are accessible to all businesses and the general public. Reinforcing the operational mechanisms of legal international mutual aid and universalizing the principles of the IT ACT 2000/1TA 2008)

Anil Kumar Pandey*
B.E. (Electronics) LL.B., PgD. Cyberlaws and IPR (Central University, Hyderabad)
3. RAISING AWARENESS, INITIAL TRAINING, CONTINUING EDUCATION (Integrating cyber security awareness into all higher and continuing education programmes. Children's awareness of digital security and responsible cyberspace behaviors as 'of school age. Initial higher education and continuing education will include a section dedicated to digital security adapted to the sector.)

4. THE ENVIRONMENT OF DIGITAL TECHNOLOGY BUSINESSES, INDUSTRIAL POLICY, EXPORT AND INTERNATIONALISATION (Develop an environment that is favorable to research and innovation and will make digital security a factor in competitiveness. It will support the development of the economy and the international promotion of its digital products and services. It will ensure that digital products and services with levels of ergonomics, trust and security adapted to the uses and cyber threats are available to its citizens, businesses and administrations.)

5. DIGITAL STRATEGIC AUTONOMY, CYBERSPACE STABILITY

III. Cyber Insurance

Information sharing and advanced cyber security technologies will not stop all cyber attacks—by now it seems clear that technically adept adversaries will always find new ways to circumvent cyber security safeguards. That's why many businesses are purchasing cyber security insurance to help Mitigate the financial impact of cybercrimes when they do occur. Cyber security insurance is, in fact, one of the fastest-growing sectors in the insurance market: cyber insurance market will reach $7.5 billion in annual sales by 2020, up from $2.5 billion this year. Today, first-party insurance products cover data destruction, denial of service attacks, theft and extortion; they also may include incident response and remediation, investigation and cyber security audit expenses. Other key areas of coverage include privacy notifications, crisis management, forensic investigations, data restoration and business interruption. The insurance industry is attempting to expand into policies that cover the value of intellectual property, reputation and brand image, as well as cyber related infrastructure failures.

IV. Challenges

Future developments in cyber security are hard to predict. However, a clear picture can be painted of the Challenges which currently and in the long-term influence the security and openness of the digital domain:

- The Internet of Things (everything is connected to the internet) and hyper connectivity (everything is connected to each other) promotes innovation and results in usability. At the same time, it raises the question of whether or not digitally linked products and services are actually safe and what the implications may be for privacy.—The amount of data available in digital form is only increasing; as will the interest in acquiring such data. Governments and businesses, increasingly working with large data files, which are also increasingly stored in the cloud, are faced with increased risks.

- The playing field in the digital domain is not only determined by states, but also by major private market parties. Governance in the digital domain is therefore complex and cannot always be solved in traditional forums, as it requires a multi-stakeholder approach. This applies to security standards as well as to the protection of fundamental rights and values.

- In the cyber domain, we see an increasingly interwoveness of civil and military domains due to substantial mutual dependence on similar ICT systems and application and the complex attribution issue. We have to take into consideration that civil targets prone to cyber attacks. Furthermore, in case of large-scale attacks, the Defense organization's cyber capabilities may be called upon to protect the vital national civil infrastructure. In view of the above, clear Parameters for strengthened cooperation in the digital domain are needed.

- The increased complexity and dependence on ICT-based products and services require a higher level of expertise. This both concerns the level of expertise of average internet users and sufficiently-qualified experts.