Role of Cloud computing in the Era of cyber security

Shilpa Taneja*
Vivek Vikram Singh**
Dr. Jyoti Arora***

Introduction

Cloud computing is taking the IT landscape further away from the organization. There are numerous benefits of cloud based system where software is managed and upgraded. Cost of hardware is very low as it requires only internet connection and browser, so other hardware devices become unnecessary. Cloud computing in simplification is considered as a form of outsourcing. With this the major issue is lying with most important asset for any organization i.e. information. Most of the IT organizations are losing control of their technology. As the cloud computing is emerging so as the cyber security trends of today are evolving at high speed pace. Prediction and detection of attack in cyber security is the shifting of incident response which is a continuous process. It generates the requirement of a security architecture that integrates prediction, prevention, detection and response. Cloud computing in cyber security provides the advantages of a public utility system in aspect of economic, flexibility and convince; but simultaneously raises the issue on security and loss of control. This paper presents the user centric measure of cyber security and provides the comparative study on different methodology used for cyber security.

Cloud computing in cyber security

Cloud computing provides high level of security and uptime than typical network. It is the simplest form of outsourcing. There are numerous benefits of cloud based system. Cost of hardware is lowers down and on the offside software is managed and upgraded. It saves cost and time as it controls the buying and upgrading of servers and other hardware. It diminishes the requirement of large IT staff. It provides faster time to market and increased employee productivity. Cloud computing provide the next generation of IT resources through a platform which is scalable and easy to manage the local area network. The legal system is running behind to adopt cloud computing. As most of the cloud vendors donot take responsibility for data loss, downtime or loss of revenue caused by cyber-attacks there is a need of taking preventive as well as corrective measures for solving the problem. According to foster, the cloud computing market will have a tremendous growth of $191 billion by 2020 which is $91 in 2015.

Risks to cloud computing

The study has revealed the 9 cloud risks. It follows high profile breaches of cloud platform evernote, adobe creative cloud, slack and lastpass. The lastpass breach is problematic as it stores all of user's website and cloud service password. It is protected with password especially those belonging to administrator with extensive permission for a company's critical infrastructure, a critical criminal could launch a devasting attack.

1. Loss of intellectual property

Cyber criminals are benefited by gaining the access on sensitive data. Skyhigh in its report says that21% of the uploaded files share services contains responsive data. A few services can even pose risk if the terms and conditions claim ownership of data uploaded to them.

2. Compliance violations and regulatory actions

Most of the companies these days follow some regulatory control of their information being it is about health information or student record. It becomes requirement for the companies to know about the location of their data and about its protection. It is also required to know about the person who will access it.

Shilpa Taneja*
Assistant Professor, IITM
Vivek Vikram Singh**
Assistant Professor, IITM
Dr. Jyoti Arora***
Assistant Professor, IITM

3. Loss of control over end user actions

Employees can harm the company by downloading a report of all customer contacts, upload the data to a personal cloud storage service and then access that information once he left the company and joins some competitor. It can be misused when companies are in dark about the working moment of their employees. It is one of the more common insider threats today.

4. Malware infections that unleash a targeted attack

Cloud services are the vector of data exfiltration. Study reveals that a novel data exfiltration technique is that where attackers encoded sensitive data into video files and uploaded them to social media. There are numerous malware that exfiltrates sensitive data via a private social media accounting the case of the Dyre malware variant, cyber criminals used file sharing services to deliver the malware to targets using phishing attacks.

5. Contractual breaches with stake holders

Contracts among business parties often restrict how data is used and who is authorized to access it. When employees move restricted data into the cloud without authorization, the business contracts may be violated and legal action could ensue. The cloud service maintains the right to share all data uploaded to the service with third parties in its terms and conditions, thereby breaching a confidentiality agreement the company made with a business partner.

6. Diminished trust of customer

Data breaches results in diminished trust of customers. The biggest breach reported was that where cyber criminals stole over 40 million customer credit and debit card numbers from different Target. The breach led customers to stay away from Target stores, and led to a loss of business for the company, which ultimately impacted the company's revenue.

7. Data breach requiring disclosure and notification to victims

If sensitive or regulated data is put in the cloud and a breach occurs, the company may be required to disclose the breach and send notifications to potential victims. Certain regulations like the EU Data Protection Directive require these disclosures. Following legally-mandated breach disclosures, regulators can levy fines against a company and it's not uncommon for consumers whose data was compromised to file lawsuits.

8. Increased customer churn

If customers even suspect that their data is not fully protected by enterprise-grade security controls, they may take their business elsewhere to a company they can trust. A growing chorus of critics is instructing consumers to avoid cloud companies who do not protect customer privacy.

9. Revenue losses

According to the Ponemon BYOC study, 64% of respondents confirmed that their companies can't confirm if their employees are using their own cloud in the workplace. In order to reduce the risks of unmanaged cloud usage, companies first need visibility into the cloud services in use by their employees. They need to understand what data is being uploaded to which cloud services and by whom. With this information, IT teams can begin to enforce corporate data security, compliance, and governance policies to protect corporate data in the cloud. The cloud is here to stay, and companies must balance the risks of cloud services with the clear benefits they bring.

In this era of digitization, data security is paramount to every business. In past, on-premise servers were the business technology model, but now there are more choices. For the last several years, a debate has flowed through businesses. How will cloud computing affect them? Should they adopt a public cloud approach, opt for private cloud, or stick with their on-premise servers? The use of cloud computing is steadily rising. In fact, a recent study has shown that cloud services are set to reach over $130 billion by 2017. Before making any decisions, it's important to think about how this shift towards cloud computing will affect cyber security for your business.

Measures or models of cloud computing in cyber security

Boehm et al. poised that all dilemmas that arise in software engineering are of an economic nature rather than a technical nature, and that all decisions ought to be modeled in economic terms: maximizing benefit; minimizing cost and risk. Their work is perfectly compatible with the philosophy of value-based software engineering, as it models system security not by an arbitrary abstract scale but rather by an economic function (MFC), quantified in monetary terms (dollars per hour), in such a way as to enable rational decision making.

Brunette and Mogull (2009) discuss the promise and perils of cloud computing, and single out security as one of the main concerns of this new computing paradigm. They have cataloged and classified the types of security threat that arise in cloud computing. Their work can be used to complement and provides a comprehensive catalog of security threats that are classified according to their type.

Black et al. (2009) discussed about categorization of metrics and measures and among different type of metrics. These metrics can be used as standard by organization to compare between current situations and expected one. This provides the organization facility to raise the level in order to meet the goal.

Jonsson and Pirzadeh (2011) proposed a framework to measure security by regrouping the security and dependability attributes on the basis of already existing conceptual model applicable on application areas varying from small to large scale organization. They discussed how different matrices are related to each other. They categorize the security metric into protective and behavior metrics. Choice of measures affect the results and accuracy of a metric.

Carlin and Curran (2011) founded that using cloud computing companies can decrease the budget by 18%. The findings comprise mainly three services Software-as-a-service (SaaS), Platform-as-a-service (PaaS) and Infrastructure-as-a-service (IaaS). Three kinds of model public private and hybrid, encryption is not a way to fully protect the data.

Chow et al. (2009) discusses the three types of security concern raised in cloud computing- provider-related vulnerabilities, which represent traditional security concerns; availability, which arises in any shared system, and most especially in cloud computing; and third party data control, which arises in cloud computing because user data is managed by the cloud provider and may potentially be exposed to malicious third parties. They also discuss strategies that maybe used to mitigate these security concerns.

Center for Internet Security (2009)used mean time to incident discovery, incident rate, mean time between security incidents, mean time to incident recovery, vulnerability scan coverage, percentage of systems without known severe vulnerabilities, mean time to mitigate vulnerabilities, number of known vulnerability instances, patch policy compliance, mean time to patch and proposed a set of MTTF-like metrics to capture the concept of cyber security.

Benefits of Cyber security in Cloud Computing

Cyber security has numerous benefits in cloud based applications like improvement in gathering and threat model, enhanced collaboration, reduction of lag time between detection and remediation. With the increase in cyber-attacks in era of cloud computing organization need to take precautions and adequate measures to deal with threats. The four pillars of cloud based cyber security comprise updated Technologies, extremely protected platforms, skilled manpower and high bandwidth connectivity. Learning collection can support real time integrated security information. Usage of cyber security ensures that security while maintaining sensitive data. The concept of out-of-band channels can be used to deal with cyber-attacks. 41% of business employ infrastructure-as-a-service (IaaS) for mission-critical workloads. Cloud-based cyber security solution developed by PwC and Google can provide advanced detection, analysis, collective learning, high performance, scalability in analytic processes to enable an advanced security operations capability (ASOC).This will create honeypots and dummies for maintaining connection to end point for analysis and learning.

Conclusion

This paper discusses about numerous benefits of cloud based system and various risks related to it. We also discussed the various models which talks about how to maximize the benefits, minimizing cost and risks. On the basis of classification of metrics and measures of cloud computing we can facilitate organization to raise the efficiency and to meet their goals. Various strategies maybe used to mitigate these security concerns. At last we can say that usage of cyber security ensures security while maintaining sensitive data as well.

References

1. Rabia, L., Jouini, M., Aissa, A., Mili, A., 2013. A cybersecurity model in cloud computing environments. Journal of King Saud University –Computer and Information Sciences.
2. Boehme, R., Nowey, T., 2008. Economic security metrics. In: Irene, E.,Felix, F., Ralf, R. (Eds.), Dependability Metrics, 4909, pp. 176–187.
3. Brunette, G., Mogull, R., 2009. Security guidance for critical areas offocus in cloud computing V 1.2. Cloud Security Alliance.
4. Black, P.E., Scarfone, K., Souppaya, M., 2009. Cyber Security Metricsand Measures. Wiley Handbook of Science and Technology forHomeland Security.
5. Jonsson, E., Pirzadeh, L., 2011. A framework for security metricsbased on operational system attributes. In: International Workshopon Security Measurements and Metrics – MetriSec2011,Bannf, Alberta, Canada.
6. Carlin, S., Curran, K., 2011. Cloud computing security. InternationalJournal of Ambient Computing and Intelligence.
7. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuok, R.,Molina, J., 2009. Controlling data in the cloud: outsourcingcomputation without outsourcing control. In: ACM Workshop onCloud computing Security (CCSW).
8. The Center for Internet Security, The CIS Security Metrics v1.0.0, 2009. <https://www.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.0.0.pdf>.