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 he applicability and effectiveness of these AI techniques in present scenario.

Keywords: artificial intelligence, cyber space, cyber security, artifical expert system, artificial neuron system, artificial intelligeence 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

Eshita Madhok*
BCA Student,
Institute of Information Technology and Management, Janakpuri, New Delhi
Ashutosh Gupta**
BCA Student,
Institute of Information Technology and Management, Janakpuri, New Delhi
Nidhi Grover***
Department of IT,
Institute of Information Technology and Management, Janakpuri, New Delhi

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 AIis 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
- Artificial Immune System: Idea of Artificial Immune System based on natural Immune system.
- 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

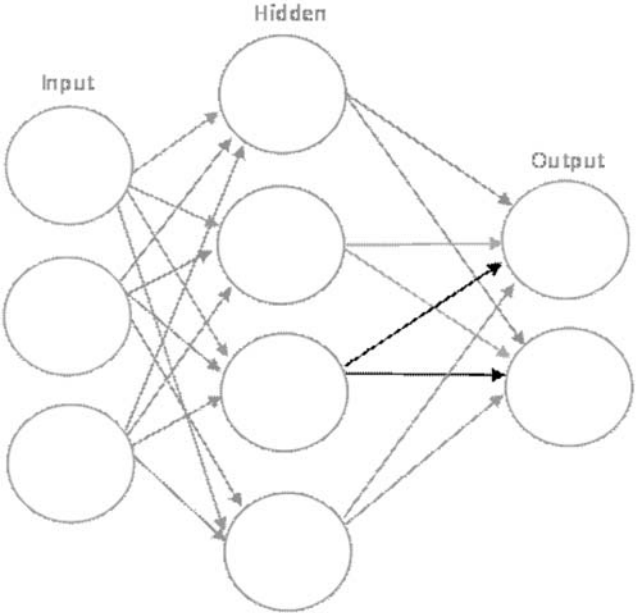

Fig. 1: Three layers of artificial neural network [19]

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 it's 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 to weighting reason. These adapted inputs are then fed 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. IntrusionDetectionandPreventionSystem

The name tell its story itself ,it's a software or hardware that protect a network ,it works 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 and help in blocking unwanted or fake requests.

C. Virus Detectionusing 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].Now aday'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.

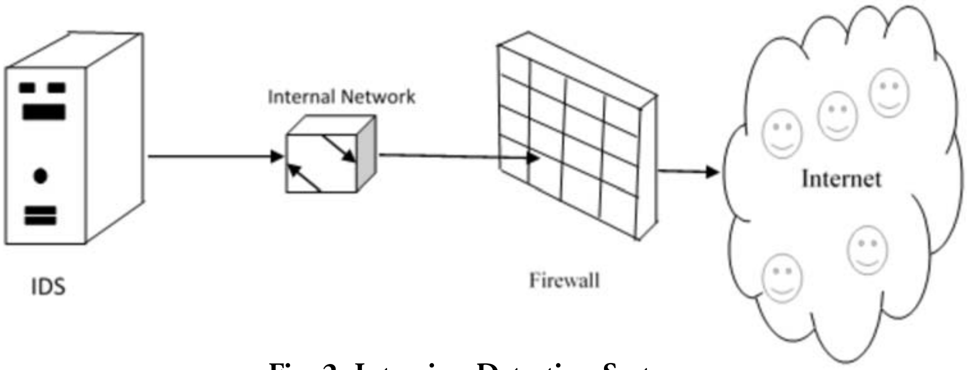

Fig. 2: Intrusion Detection Systems

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 isthe 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

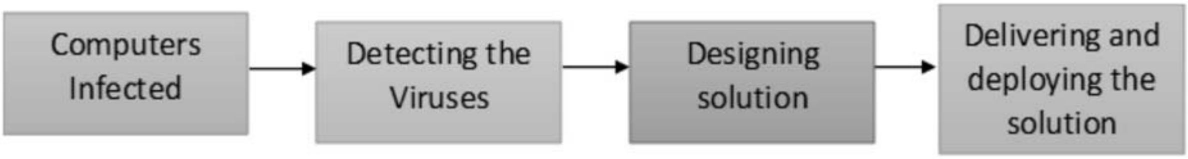

Fig. 3: Artificial Immune System

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.

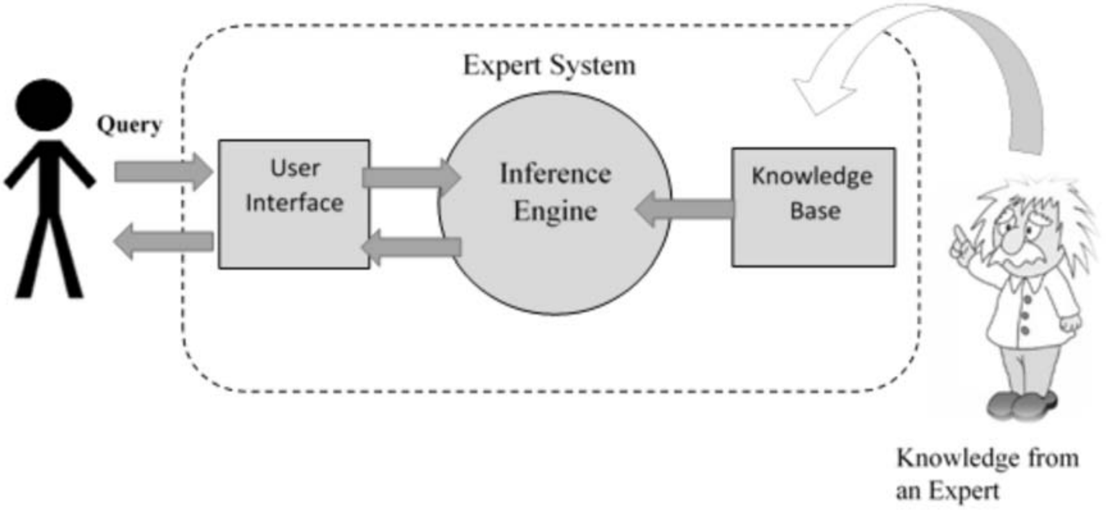

Fig. 4: Expert System

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.

References

1. Mary Ellen O'Connell, "Cyber Security without Cyber War , *, To Defend The Web: Using Artificial Intelligence As Online Security"
2. https://en.wikipedia.org/wiki/Stuxnet ,This page was last modified on 15 February 2016, at 03:40 .
3. Rain Ottis and Peeter Lorents," Cyberspace: Definition and Implications" , Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.
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",
7. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015 DOI : 10.5121/ijaia.2015.6102 21
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 .
9. https://cs.stanford.edu/people/eroberts/courses/soco/projects/neural-networks/History/history1.html.
10. https://en.wikipedia.org/wiki/Artificial_neural_network,This page was last modified on 19 February 2016, at 19:28
11. Jyothsna S Mohan1, Nilina ,"Prospects of Artificial Intelligence in Tackling Cyber Crimes ",International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438, 1Department of Computer Science and Engineering, College of Engineering, Vadakara, Kozhikode, Kerala, India.
12. Artificial Intelligence in CyberDefense,Enn TyuguR&D Branch,Cooperative Cyber Defense Center of Excellence (CCD COE)and Estonian Academy of Sciences2011 3rd International on Cyber Conflict.
13. Raul Rojas, Neural Networks Systematic introduction, book. Prospects of Artificial Intelligence in tackling cyber crime.
14. http://www.ijsr.net/archive/v4i6/SUB155595.pdfInternational Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438,
15. Selma Dilek1, Hüseyin Çakýr2 and Mustafa Aydýn3,"Applications of Artificial Intelligence, Techniques To Combating Cyber Crimes", International Journal Of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015, wwww.webopedia.com/TERM/D/DDoS_attack.html".html
16. John A. Bullinaria , 2004. Introduction to Neural Networks : Lecture 16
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
20. Estonian Academy of Sciences 2011, 3rd International Conference on Cyber. https://en.wikipedia.org/wiki/Intelligent_agent, This page is modified at 10:29 pm

21. P.Brangetto,M.Maybaum,J.Stinissen(Eds.),Caitríona H. Heinl,"Artificial (Intelligent) Agents and Active Cyber Defence"2014 6th International Conference on Cyber Conflict, Research Fellow,,Centre of Excellence forNational Security (CENS) S. Rajaratnam School of International Studies Singapore
22. http://www.ijsr.net/archive/v4i6/SUB155595."International,Journal of Science and Research (IJSR)", ISSN (Online): 2319-7064, Index ,Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438,"Prospects of Artificial Intelligence in Tackling cyber crime"
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 AttacksAnd Defe Nse Mechanisms ",
25. St.-Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, 39, 14th Liniya, St. Petersburg, 199178, Russia Cornelius T. Leondes, Intelligent Systems: Technology and Applications, Six Volume Set [book] .
26. By Shelly Fan," How Artificial Immune Systems May Be the Future of Cybersecurity", on Dec-27-2015,ArtificialIntelligence, Computing, Featured, Tech
27. Hua Yang,1,2 Tao Li,1 Xinlei Hu,1 Feng Wang,1 and Yang Zou1 "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 "
29. Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont,An Artificial Immune System Architecture for Computer Security Applications
30. Hamza A. ali1 and Duaa Jawad Hussain2,"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
31. https://en.wikipedia.org/wiki/Expert_system , 8 February 2016, at 13:32.