Proceedings of the International Conference on Inventive Computation Technologies (ICICT-2018)
IEEE Xplore Part Number: CFP18F70-ART; ISBN:978-1-5386-4985-5

A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks

Atul S Choudhary [1], Pankaj P Choudhary [2], Shrikant Salve [3]
School of Computer Engineering and Technology
MIT Academy of Engineering, Alandi(D), Pune
aschoudhary@it.mitaoe.ac.in [1], ppchoudhary@it.mitaoe.ac.in [2]

***Abstract*— World is moving rapidly towards the digital transformation. The internet across the world is growing rapidly which gives rise to many opportunities in every field including entertainment, finance, education, sports etc. As every coin has two aspects, the internet also has many advantages and disadvantages. We know about the advantages, but the only major disadvantage that everyone should be aware of is the increase in cyber-attacks. It is nothing, but the illegal activity committed on the internet. Many government websites and systems were hacked in the past few years and it has caused a huge loss to the nations like India, USA and China. These governments have already taken various steps to counter these crimes & attacks. But still, the attackers are coming up with new ways of attacking every time. There is need for some concrete solution which is not in the reach of the attackers. For developing such systems and tools we have done a deep analysis of various types of cybercrime and attacks happened in past along with existing solutions proposed by many researchers. Therefore, this paper presents a study on various cyber-attacks that were triggered in India and other countries in the past few years. The various prevention methods proposed in past to deal with these kinds of attacks. These prevention methods are based on machine learning algorithms like a random forest, k-means clustering, support vector machine and artificial neural network applied in order to prevent cyber-attacks. Also, in this paper, we have reported proposed intelligent system which is based supervised and unsupervised learning techniques to avoid these cyber-attacks. This proposed system might provide high efficiency with a minimum human intervention which can be implemented and used as a universal solution to most of the common cyber-attacks.**

Keywords—Cybercrimes, Attacker, Machine Learning, Cyber-attack

I. INTRODUCTION

Cyber-crime denotes any misconduct that includes the computer and a network. The computer may be used for performing the attack or it may be the target device [1]. Cyber-crime can be stated in few statements with a broad meaning as, Crimes that are turned against any person or group of persons with a criminal intention to deliberately harm the status of the victim or cause physical or psychological destruction to the victim directly or indirectly using modern telecommunications network such as internet, emails, cell phones etc. Cyber-attack on the other side is a type of crime conducted using the various types of cyber crimes.

With the initiative of Making Digital India lot of work is already being done for digitization of various domains. Digitization is rapidly implemented in the industries related to the domains like Transportation, Healthcare, Real-State, Education Sector, Automobiles and Finance. All this digitization is only possible because of the existence of Information Technology which this has resulted in the phenomenal increase in the cyberspace. The number of internet users in the past few years in India has increased tremendously. Technology advancement in IT and Internet together has opened a lot of opportunities for people to perform various kinds of transactions like online shopping, banking, advertising, social network and many other small and big transactions in their day to day life. Billions of transactions are performed by people on day to day basis across the globe. [2]

A global trend for internet usage is maintained by www.internetworldstats.com. The statistic shows that Asian countries contribute 55.1% to the world's total population till 2018 and a total percentage of internet users is 48.7% of the entire world. In Asian countries, India is ranked the second highest internet usage country after China. Below is the statistic recorded by the internet resources [3] which gives information about internet users in India.

TABLE 1: Internet users in India adopted from [3]

Criteria	Figures
Population (2018)	1,354,051,854
Internet users in Dec/2017	462,124,989
Internet penetration as per IAMAI (Internet and Mobile Association of India)	34.1%

This has eventually given birth to a new domain of crime popularly known as cybercrime. The crime performed on the cyberspace using electronic devices like computers, mobiles etc. The attackers perform various attacks on cyber space which ultimately leads to a cybercrime.

As per the statistics are given in an article at Indiatimes in the month of April-17, a study reveals that India ranks fourth when it comes to online security breaches, accounting for over 5% of global threat detections. The US and China occupy the top two slots and together make for almost 34%, followed by Brazil and then India [4]. The study also tells that, unlike other countries where the rate of cyber-attacks has decreased there is a substance from 3.4% in 2015 to 5.1% in 2016 [4]. According to the recent study done by the Ministry of State for Electronics and IT reveals that India has witnessed more than 27,000 cyber-attacks in the first half of the year 2017 [5].

As per the reports of Indian Computer Emergency Response Team (CERT-In)," the number of cyber-attack incidents reported was: [5]

- 2014: 44,679
- 2015: 49,455
- 2016: 50,362
- 2017 (up to June): 27,482

II. CLASSIFICATION OF CYBER ATTACKS

Cyber-attacks can be classified broadly into various categories. The classification is given below in Fig 1.

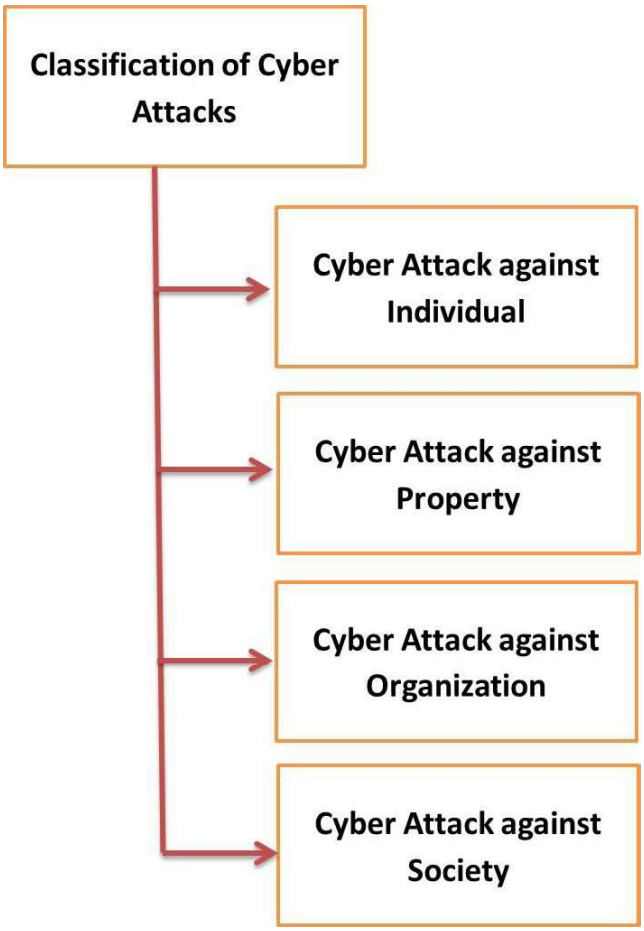

Fig 1: Classification of Cyber Attacks

A. Cyber-attack against individual

Email Spoofing: It is the formation of email messages by impersonating correspondent identity. It shows the origin of the email different from which it actually originated. The originators of this email are always unidentified.[6]

Cyber Defamation: it is an act of charging an individual with the intention to inferior the person in the estimation of the right thinking members of the society generally or to cause him to be ignored or side-stepped or to rendering him to hate, disrespect or ridicule. Cyber defamation is like conventional defamation except for the involvement of a virtual medium.

Cyber Stalking: When a victim is followed by the attacker all across the internet and posting threatening messages against the victim on a various social platform where the victim visits very frequently. Sometimes when the attacker continuously attacks the victims with emails messages is also a type of cyberstalking.[6]

B. Cyber-attacker against Property

Credit Card Fraud: Online fraud and cheating are a most money-spinning trades that are rising now a day in the cybersecurity. It may have diverse forms. Some of the cases of online fraud and cheating that are uncovered are referred to credit card offences or contractual crime.

Intellectual Property Crimes: It includes a list of crimes like any illegal act due to which the owner is deprived entirely or partly of his human right is a crime. Some of the very common IPR crimes include Software Piracy, Copyright infringement, Trademark and service mark violation and theft of computer source code.[7]

Internet Time Theft: Basically it comes under hacking. It is used by an unofficial individual of the internet hours paid for by another individual. The individual who gets entrance to someone else's ISP user ID and password either by hacking or by gaining access to it by unlawful means and uses it to access the internet devoid of the other person's knowledge.

C. Cyber-attack against Organizations

Unauthorized Access: This is generally denoted to as hacking and performed in a similar fashion.

Denial of Services Attack: In simple words, Denial of service is referred to as an act by which a user of any website or service denied to use the service or website. In this category of cyber-attacks, the offender aims the web server of the websites and flow a large number of requests to that server. This causes the use of the maximum bandwidth of the website due to which the website goes down or not available for some time.

Virus Attack: A computer virus is a type of malware that when executed replicates by implanting replicas of itself into the other computer programs, data files or the boot sector of the hard drive. Viruses are self-duplicating computer programs which mount themselves without the user's approval.[6] This affects the system by

a. Stealing hard disk space or CPU time
b. Retrieving private information
c. Corrupting data
d. Displaying radical or funny emails on the user's display
e. Spamming user's links or logging their keystrokes

Email Bombing: In this type of an attack a user sends the vast number of emails to the target address. Because of this the email addresses or mail server crashes and incurs denial of service.[6]

Salami Attack: It comes into execution when a minor attack makes up a major attack which becomes untraceable because

of its nature.it is also called as salami splicing which is frequently used to transport an unlawful activity, it is only a plan for gaining benefit over time by collecting it in small increments. In this, the attacker uses an online database to seize the information of the customer that is bank/credit card details and deducting a very small amount every time the transaction is made. The customer remains unaware of this slicing and hence no complaint is launched. [7]

Logic Bomb: It is a piece of code that is inserted purposefully into a system. The code triggers under some definite conditions to perform some mischievous features.[7]

Trojan horse: It is a malware program which is not self-duplicating but comprises of some malicious code which on execution carries out some actions determined by the nature of the Trojan, generally causing damage or stealing of data.[6]

Data Diddling: It is illegal modifying of data when an individual enters some data to his system and output is different from input then he may be a victim of data diddling. It is implemented by a virus program that changes the entered data.[7]

D. Cyber-attack against Society:

Forgery: When a perpetrator alters document saved in electronic form, the crime committed may be a forgery. In this case, computer systems are the target of criminal activity however they can be also used as tools with which a forgery can be committed. A new generation of fake modifications or forging arose when electronic colour laser duplicators become accessible. These duplicators are capable of-

a. High-resolution repetition
b. Alteration of documents
c. Formation of false documents without getting an original document
d. Form documents whose quality is differentiated from that of authentic documents

Cyber Terrorism: It is an international concern which has domestic as well as international consequences. The common form of these terrorist attacks on the internet is by dispersed denial of service attacks.

Web Jacking: It comes from hijacking, in this type of cybercrime the criminals hacked the control of a website. They may be able to change the content of that website. The attacker uses that website as like the owner and the real owner has no control over the content of the website. [7]

From the above classification and various stats discussed in this section, it is crystal clear that some strict action is the necessity of an hour to make digitization a grand success in India.

In the next section, we will be discussing the various cyber-attacks that took place in India in the past few years and what are some counters proposed and implemented by researchers to prevent the cyber-attacks.

III. Cyber-attack Cases in India

As already discussed, India is ranked fourth in the world in terms of the number of cyber-attack incidents happened. Times of India reports that in the year 2017 an attack named ransomware hits millions of systems including phishing and scanning. The survey says there is at least one cybercrime attack in every 10 minutes and as per the report from Computer Emergency Report Team (CERT), a total of 27,482 cases of cyber-attacks were reported in the first half of 2017 in India from the month of January to June.[8] Similar stats are observed every year in India where cyber-attacks like phishing, scanning, probing, intrusions, defamations, virus, worms, malicious code, ransomware, denial of services, SMS Scams, Credit Card Fraud, Website Hacking, Botnet Malware, and many other data breaches attacks took place in past few years. Here, we are discussing some famous cyber-attack incidents that caused some serious damage to related businesses.

A. Ransomware

Reported by KPMG, approximately 69% of the company committed that they have encountered ransomware as the biggest risk in the year 2017. Total 40 incidents of ransomware were reported to the Indian Computer Emergency Response Team (CENT-In) out of which around 34 incidents included ransomware. It was first reported in the month of May 2017 with the name WannaCry and another version of the same attack reported in June 2017 with name Petya. [9]

B. WannaCry:

Majority of ransomware attack was attempted by the malicious WannaCry virus. The main target and victims of this attack were the enterprises. It intruded mainly on the computers those were running the older versions of Microsoft Operating Systems. It locked the devices and prevented the users from accessing data from those devices until any ransomware is paid for it to the criminals.[10]

C. Petya:

Petya was one of the wipers that aimed for deleting all the data stored in the computer storage area. It even attacked the data stored in the first sector of the disk where the information about the operating system is generally stored. The main objective behind Petya was to root enormous devastation of the data to the financial sector. [9]

D. BSNL Malware Attack

The BSNL Karnataka circle observed a malware attack which affected over 60,000 modems. The main objective behind this attack was to get access to the modems and denying the victims from any internet usage. The modems were affected with default credentials for username and password “admin-admin”. The infected modems then could not connect to the internet. [8]

E. Data Breaches:

Food service provider Zomato was attacked in the month of May for data breaching. The company officials reported that the company’s database was breached and personal details of about 8 million users were being stolen. The stolen information was even listed for sale on the Darknet market.[9]

India's biggest telecommunication network service provider Reliance Jio was also once the victim of data breach. A website called magicapk.com suddenly went live overnight and anyone could search for personal details of Jio Customers on this website. [8]

F. Mirai Botnet Malware:

Mirai botnet malware took the world by targeting routers and IoT devices. The malware affected in total 2.5 million IoT devices over the globe.

G. Union Bank of India Heist:

Union Bank of India reported a phishing attack in July 2016. A phishing email was sent to one of the employees of the bank. The hacker stole the credentials of the employee and got an access to funding transfer. [10]

These were some famous cyber-attack incidents that were reported in India. There is a huge list of similar major and minor attacks those were reported by various agencies functioning in this domain. The next section of the paper discussed some of the research work done for detecting and preventing the various categories of cyber-attacks.

IV. Related Work

Considering the criticality of domain lot of research is done for countering the cybercrimes and attacks. Some of the key research done is discussed below.

Cagri B Aslan et al. in 2018 developed a system for automatic detection of attacks on the online social network (OSN). The system identified for experimentation is Twitter. The proposed system used a machine learning algorithm to learn about the various activities on the Twitter account. The machine learning algorithms include Support Vector Machine (SVM), Decision Tree, and Random Forest. All these algorithms are given three different set of behavioural features as input. The results obtained concluded that Random Forest algorithm showed better performance with accuracy of over 95%. [11]

Dennis Edwards et al. proposed a system for prevention, detection and recovery from cyber-attack using Multilevel Agent Architecture. At each level, a verifiable agent is used having a specific allied duty. The agents used in this system are communication agent who takes care of the communication with external entities, the distribution agent which validates the incoming data and replicated computational agent which performs the tasks like authentication, validity assurance, response computation and sending the response to the external entities. [12]

Ge Jin et al. in 2018 proposed a game based learning methodology for educating the high school students about cybersecurity. In this method, the students of Perdue University Northwest were given the training for developing various cybersecurity-related games. The game category identified was social engineering games, secure online behaviour games, cyber defence tower games, 2D GenCyber card game, 3D virtual reality games etc. At the end of the camp, a survey was taken to evaluate the students' knowledge of cyber-crime. The results showed the knowledge in terms of rating at 4.26 out of 5. [13]

Teik-Toe Teoh et al. in 2018 adopted a neural network concept for cybersecurity anomaly detection. In this approach, they classified attacks into different classes like attack, unsure and no attack. Using this attack 3 different clusters were formed using a k-means clustering algorithm. Finally, the data in every cluster is labelled and train the neural network multilayer perceptron. The experimentation was done on the data set provided by Singapore Technology Engineering which includes malware like a virus, worms, Trojan etc. The highest accuracy achieved with multilayer perceptron is 90.18%. As part of future work, the process of data integration will be automated. [14]

Igor Skrjanc et al. in 2017 proposed an algorithm for monitoring cyber-attacks using Cauchy Possibilistic Clustering. The algorithm calculates the Cauchy density for data stream and clustering is done on the basis of various mathematical models. The experimentation was done on a data set of 20,000 samples. The results obtained using the algorithm showed a relatively good performance. [15]

Keeping the importance of cyber-attack prevention, in this paper we are discussing a new approach based on the concept of machine learning. In the following section, we are discussing our concept of preventing users from being the victim of various cybercrimes. The proposed idea is only at the conceptual level.

V. Proposed Architecture

On the basis of the literature studied and comparison of various methods motivated us to propose a novel idea for detecting and preventing users from various cyber-attacks. As per the study, the methodology mentioned in [11] uses machine learning algorithms and concluded that random forest showed better performance with an accuracy of 95%. But the random forest algorithm has less interoperability and does not give good results with similar data sets. Another game based learning method [13] is a manual process of educating the students to prevent their data from attacks. The methodology used in [14] uses the concept of a neural network and achieve the accuracy of 90%, but the data integration process is not automated. Hence, in this paper, an idea for automating the data integration process and detection of suspicious attack by training the machine learning model is proposed. We believe machines are always a better alternative to a human when any task is to be processed repeatedly. In this approach, human intervention is the minimum and most of the tasks will be done by the machines trained using machine learning. Fig. 2 shows the proposed conceptual diagram and below is the stepwise procedure elaborating the proposed system flow.

Stepwise Procedure

The input to the algorithm is the data generated from the user's activity on a computing device.

Step 1: Collect a considerable amount of data through logs generated in a computing device.

Step 2: Set some indicators to map with the behaviour of the user's activity and feed it to the unsupervised learning module.

Step 3: The data gathered in Step 2 on the basis of identifiers feed it to unsupervised learning to generate the list of suspicious activities.

Step 4: Maintain the list of all the suspicious activities and ask the human analyst to manually tag the actual suspicious activities.

Step 5: Human analyst manually identifies the activities which are actually suspicious.

Step 6: The output of step 5 is given as feedback to the supervised model for analysis.

Step 7: The output of the supervised model is forwarded to the simulated analyst.

Step 8: Now, the simulated analyst is used in aggregation with the unsupervised model and step 2 is repeated.

Step 9: Repeat Step 1 to Step 6 until the device will be powered off.

VI. Supplementary Preventive Measures

In this section, some preventive measures are discussed. These are some measures which in addition to the availability of technology everyone should follow in order to keep their system secure.

a. Using of strong password for all the accounts that you hold. Password must be created in such a way that it becomes difficult for any password cracking tool to guess it. Do not use the same password for the different accounts and avoid creating sequential passwords. Always use the combination of Upper case, lower case, numeric and few special characters while creating your passwords.

b. Provide software security to your system. Always use a reputed antivirus system and keep it update continuously. The antivirus will help you to keep your system secure.

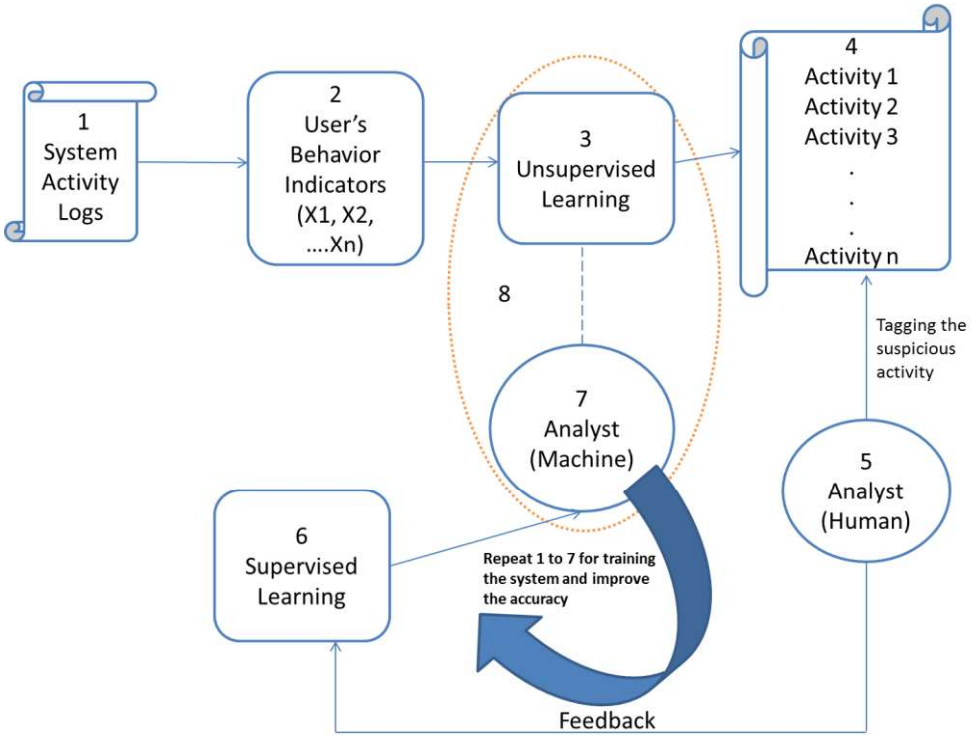

Fig 2. Proposed Idea

c. Always keep your firewall active, they are the first place which the attackers try to breach.

d. The operating system is another very important thing which the attacker always tries to breach, so always keep the operating system up-to-date. Regularly update the OS patches so that the attacker may not take the advantage of your OS vulnerability.

e. Avoid visiting websites which lure you to click on various links. These types of scenario generally come when you visit any online shopping websites. They ask you to enter your personal information and even payment is done online using the payment gateway. These websites are the best source of cross-site scripting attacks. Always ensure the security certificates of the websites.

f. Be aware of the emails containing harmful links. These types of emails generally ask you to verify your personal information and confirm the credentials. These types of emails can trigger the phishing or pharming attacks.

g. Wireless networks are the simplest to breach and vulnerable to various attacks. Keep your wireless network authenticated with strong password types.

h. Keep all of your sensitive data encrypted using the various software.

These are some of the very basic and general preventive measures that everyone should take care of. Everyone needs to get educated when working on the internet and using online systems.

VII. CONCLUSION AND FUTURE SCOPE

Cyber-attacks are one of the most dangerous threats in cyberspace. With the advancement of technology, hackers are also coming up with new ways of breaching security. There is a need to always be one step ahead of the hackers and it can only be achieved by doing some quality work in this domain. In this paper, we have discussed the broad scale classification of cyber-attacks. We have also unveiled a few very serious cyber-attacks that were the cause of huge loss to India as a whole nation. Looking at the importance of this situation we have proposed a novel solution for detection of cyber-attacks using the concept of machine learning. As the part of our future work, we will implement the algorithm using machine learning tools and develop a tool which will help to counter the cyber-attack attempts.

VIII. REFERENCES

[1] June Iqbal, Bilal Maqbool Beigh, "Cybercrime in India: Trends and Challenges" International Journal of Innovations & Advancement in Computer Science, Vol-6, Issue-12, December 2017, ISSN 2347 – 8616, pp. 187-196.

[2] The Internet World States, Accessed on 15/08/2018 from https://www.internetworldstats.com/

[3] Cyber Law Cases in India and World, Retrieved on 22/9/2018 from http://www.cyberlawsindia.net/cases.html

[4] India Fourth In List Of Countries That Faced Most Cyber Attacks, US And China On Top, Accessed on 21/09/2018 from https://www.indiatimes.com/news/india/india-fourth-in-list-of-countries-that-faced-most-cyber-attacks-us-and-china-on-top-276590.html.

[5] Cybersecurity issues in India, Retrieved on 20/09/2018 from https://www.medianama.com/2017/07/223-india-witnessed-27482-cyber-security-threat/.

[6] Jitender Kumar, "Cyber Crime in India: An Overview" Imperial Journal of Interdisciplinary Research, Vol-3, Issue-4, 2017, ISSN: 2454-1362, pp. 963-967.

[7] Praveen Paliwal, "Cyber Crime" Nations Congress on the Prevention of Crime and Treatment of Offenders, March 2016.

[8] One cybercrime in India every 10 minutes, Retrieved on 20/09/2018 from https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

[9] Cyber attacks that affected India in 2017, Retrieved on 20/09/2018 from https://www.gizbot.com/internet/features/cyber-attacks-that-affected-India-in-2017-046533.html

[10] V. K. Saraswat, Cyber Security, Accessed on 19/09/2018. http://niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

[11] Cagri B Aslan, Rahime Belen Saglam, Shujun Li, "Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an example", SMSociety, July 2018, Denmark.

[12] Dennis Edwards, Sharon Simmons and Norman Wilde, "Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture", US Department of Energy under Grant No. DE FG0205CH1292.

[13] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, Jonathan White, " Evaluation of Game-Based Learning in Cybersecurity Education for High School Students" Journal of Education and Learning (EduLearn), Vol.12, No.1, February 2018, pp. 150~158.

[14] Teik-Toe Teoh, Yok-Yen Nguwi, Yuval Elovici, Wai-Loong Ng and Soon-Yao Thiang, "ANALYST INTUITION INSPIRED NEURAL NETWORK BASED CYBER SECURITY ANOMALY DETECTION", International Journal of Innovative Computing, Information and Control, Volume 14, Number 1, February 2018, pp. 379{386.

[15] Igor Skrjanc, Seiichi Ozawa, Tao Ban, Dejan Dovzan, "Large-scale cyber attacks monitoring using Evolving CauchyPossibilistic Clustering", Applied Soft Computing 62 (2018) 592–601, Elsevier, 2017, pp. 592-601.