Combating Cyber Crime Using Artificial Agent Systems

L.S. Wijesinghe*, L.N.B De Silva *, G.T.A.Abhayaratne*, P.Krithika*, S.M.D.R. Priyashan, Dhishan Dhammearatchi***

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

Abstract- As this is the 21st century, the term “globalization” has become popular. Simply put, globalization is the process of international integration. Under this, as nations, people have lots of factors that must be definitely considered. Among those important areas, information technology (IT) is something that is being evolved day by day. As a negative aspect of IT, with the help of technological advancements, criminals are using cyberspace to commit numerous cyber-crimes. Since people are connected to the cyber space with their own devices, they are all vulnerable to intrusions and other various kinds of threats. Basic protection methods, such as internet security suits, are not just enough to protect the data and devices. Introducing effective and highly advanced cyber defense systems has become essential. As of today, with the technology, the globe is moving towards the artificial intelligence (AI). AI plays a major role in technology and has been involved with many technological aspects as well. Creating cyber defense systems, using intelligent agents has become a trend by today. Basically, an intelligent agent is a software component which can be emerged in an environment, take decisions, and has the ability of noticing and representing. The purpose of this study is to introduce a sophisticated cyber-crime defense system which involves intelligent agents that are based on artificial intelligence.

Index Terms- Cyber-crimes, Intrusion detection and prevention system, artificial agents, artificial intelligence.

I. Introduction

This research paper mainly focuses on how to combat cybercrimes, and also it demonstrates how intelligent and effective the tool “agent” that can be used in detection and prevention of cyber-attacks. Cyber-attacks tend to have a huge impact on the IT industry when it comes to data theft, many societies across the world have components or systems which depend on web applications. As web applications are used increasingly on basic and critical activities they have become a very vulnerable and a popular target for security attacks. It can be noticed that the increase of cyber-attacks are very high in today’s cyberspace. Any action that bypasses the security mechanisms of the targeted system using a computer and a network can be defined as a cybercrime. In a cybercrime the computer might be used as an intruder or it can be the target.

In cyberspace maintaining confidentiality, integrity and availability are essential. Most network-centric cyber-attacks are carried out by intelligent agents such as computer worms and viruses; hence, combating them with intelligent semi-autonomous agents that can detect, evaluate, and respond to cyber-attacks has become a requirement. Physical devices and human intervention are not sufficient for monitoring and protection of these infrastructures from attacks. Therefore, the study of cyber-attack detection strategies and systems are becoming a popular and interesting topic among the specialists in the network security field. Expansions of the intrusion systems are rapid in modern technological environment.

Intrusion detection systems (IDS) are one of the very popular systems which are deployed to detect cyber-attacks. It can be classified as host based systems or network based systems. Host-based systems are based on information’s of a single host while network-based systems are based on monitoring traffic of the information. It is critical that these cyber defense systems being flexible, adaptable and powerful, and being able to detect a wide variety of threats and making intelligent real-time decisions. Apart from IDS’s, Intrusion Prevention Systems (IPS) is also being used in this invention. These will not only detect and warn about cyber-attacks but will prevent them from entering into the system. IPS’s are placed in-line and are able to actively prevent/block intrusions that are detected, more specifically IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address which could be very troublesome for the cyber-attackers and perky for the users.

An Agent is a small program module that functions continuously and autonomously. Characteristics of an agent system should be reactivity, proactive in action and small in size. There are many advantages of building cybercrime detection systems using the agent technology. They can run independently. The agent can be reconfigured to newer version without interrupting to the rest of the system and also they can exchange information by deriving more complex results than on its own. This particular program module plays a major role in the system as all the algorithmic data is allocated into the Agent making this invention work as a whole. Agent is built in a way that it’s easy for the user to cooperate with the system without any issue; the agent basically makes stuff simple for the user. The in-depth analysis of an agent might seem pretty complicated but its main aim is to be user friendly for the user. In order to make things simpler for the users and for communication purposes a language called the Agent Communication language (ACL) is being used by the agent to interact with the users. Agent has administrative control over the system as the agent is used to formulate inner judgment when it comes to the system.

The content of the paper has been divided into four main chapters, according theirs topics. First chapter is the introduction chapter where it gives a basic idea about the research. Second chapter explains the characters or components which are being used in other related research papers. Solution for the identified problem is given in the third chapter. Fourth chapter includes the conclusion and in the last chapter possible future tasks to get better results are being mentioned.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Cyber attacking, it is a common word used in the present world. Daily thousands of computer networks or computer systems get attacked by an unknown systems or hackers in order to damage or destroy the system. In order to prevent and detect such attacks many systems are being developed. A background study was done in order to identify the available technologies, mechanisms etc.

A. Intrusion Detection System

An Intrusion Detection System or IDS is a network security technology originally built for spotting vulnerabilities that exploit against a targeted application or a computer system. It is the process of monitoring the events occurring in a computer system or in a network and analyzing them for possible incidents indications, which are violations or impending threats of destruction of computer security strategies, suitably used policies, or common security practices. An ID system gathers and analyzes information from various sources within a computer or a network to identify possible security breakings, which include both intrusions and attacks from the outsiders the organization and does not use them properly or attacks within the organization. Particular intruders can be pin pointed and shown through an algorithm [2] [9] [10]. Intrusion detection system only can identify intrusions, and it cannot prevent the system from attacks [5] [7]. It should be fast enough to identify the intruders (external or internal intruders) as soon as the attack is going on. In IDSs efficiency is a more important feature. Intrusion Detection System (IDS) technologies are not very effective as there are several limitations, such as performance, scalability and flexibility. Intrusion Prevention System (IPS) is a new approach to defense networking systems. Figure 01 indicates how an IDS is placed in a system.

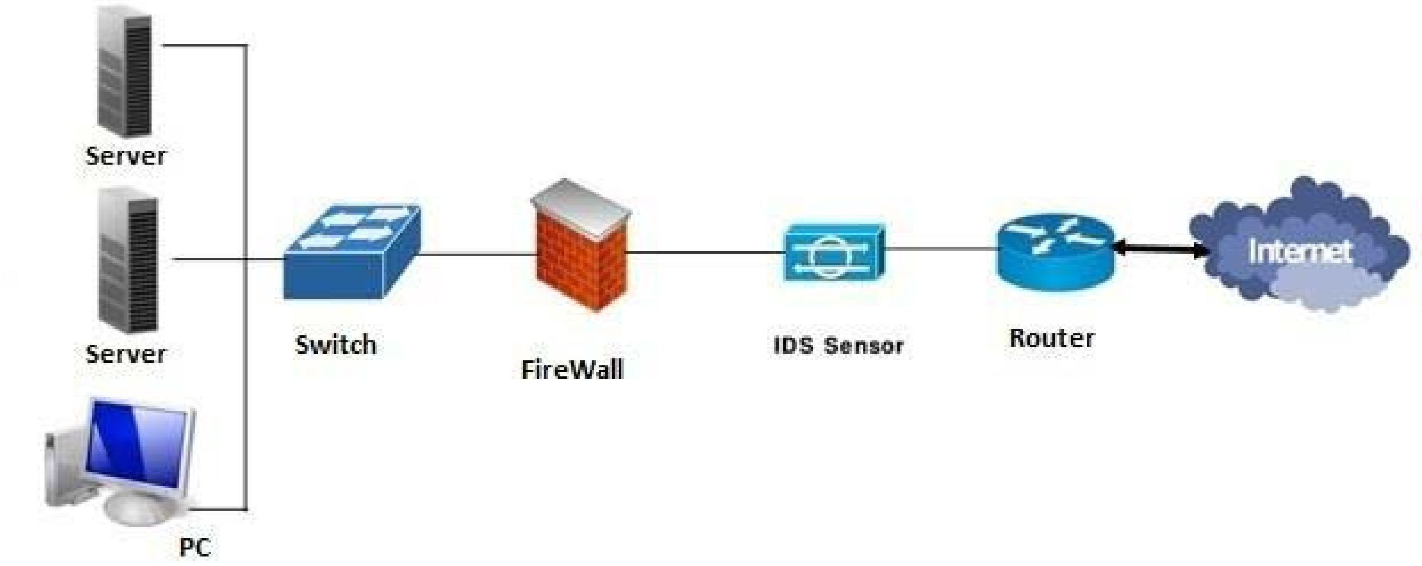

Figure 1: Intrusion detection system
(Source: https://www.google.lk/search?q=Intrusion+detection+system&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjxhKjK357LAhWKco4KHb5pBQ0Q_AUIBygB&biw=1366&bih=667#imgrc=bgoc5oyiXo2hwM%3A)

B. Intrusion Prevention System

Intrusion prevention systems or IPS, also known as intrusion detection and prevention systems or IDPS, are network security appliances that monitor networks and system activities for malicious activities. The IPS often lies directly behind the firewall and provides a complementary or integral layer of analysis that selects for dangerous contents. Intrusion prevention is a preemptive approach in network security which is used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) checks and controls network traffic. However, because an exploit may be carried out quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate actions, it’s about a bunch of rules created by the network administrator. As an example, IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port [9]. Legitimate traffic, meanwhile, it should be sent forward to the recipient with no sudden interruption or delay of service. Unlike its predecessor the Intrusion Detection System (IDS) is known to be a passive system that scans traffic and alerts back the threats the IPS is placed intact with (in the direct communication path between source and destination), automated actions will be taken on entire traffic flows that enter the network by actively analyzing them. Specifically, these actions include:

- Dropping the malicious packets;
- Sending an alarm to the administrator;
- Blocking traffic from the source address;
- Resetting the connection.

The IPS should work properly, as it one of the main frontline components used to avoid the degrading of network performance. It must also work fast because exploits could be caused in real-time. The IPS must also spot and react precisely, so it can eliminate threats and false positives. Figure 02 indicates how an IPS is placed in a networking environment.

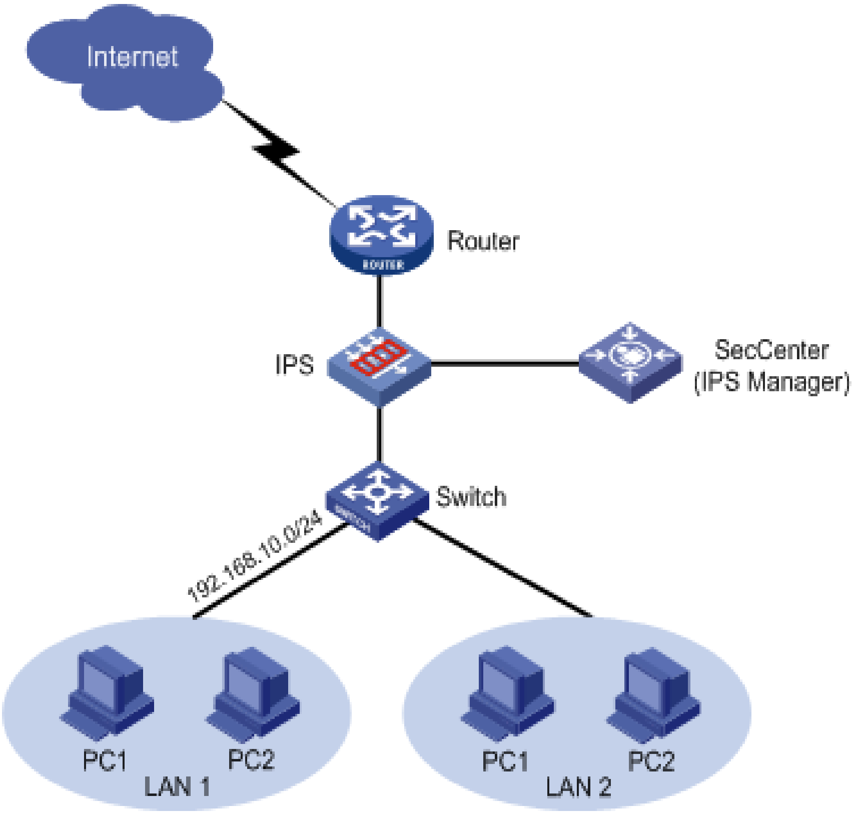

Figure 2: Intrusion prevention system
(Source: http://www.h3c.com.cn/res/201005/26/20100526_985682_image001_676465_30005_0.png)

C. Cyber Security System / Cyber Attack Detection Systems (CADS)

Cyber Attack Detection Systems (CADS) and its generic framework perform well for all the classes. This is based on Generalized Discriminant Analysis algorithm (GDA) for feature decrement of the cyber-attack datasets and a collective approach of classifiers for classification of cyber-attacks [1] [10]. Cyber Attack Detection System is having improved detection accuracy for all the classes of attacks.

Cyber Attack Detection Systems are of two types [2]. Host Intrusion Detection Systems (HIDS) and Network Intrusion Detection Systems (NIDS). Host intrusion detection refers to the class of intrusion detection systems that reside on and monitor an individual's host machine. There are several characteristics which is used by a host intrusion detection system that can be used in collecting data including File systems, Network Events, and System Calls. Network Intrusion Detection System is a network cyber-attack detection system (NCADS) which monitors the packets that traverse to a given network link. A NCADS is obviously of little use in spotting attacks that are launched through an interface on a host except for the network.

D. Detects denial-of-service (DOS) attacks

A DoS attack is an attack type which is used to make a computer or a network resource unavailable to the users, such as to temporarily or permanently interrupt or suspend services of a host connected to a network. By targeting user's computer and its network connection, or the computers and network of the sites the user is trying to use, an attacker may be able to prevent the user from accessing email, websites, online accounts (banking, etc.), or other products and services that reside on the affected computer. The most common type of DoS attack is a situation where an attacker floods a network with information. When the user types an URL for a particular website into web browser, he is sending a request to that site's server to view the page. Only a certain amount of requests will be processed by the server at a time, therefore requests will not be processed if an attacker swamps the desired server with. This is known as a "Denial of Service" because the user will not be able to access that site. There are many other types of cyber-attacks such as brute force attacks, browser attacks, shellshock attacks, SSL attacks, backdoor attacks and botnet attacks[3] [6] [7]. Figure 03 illustrates the mechanism of a Typical DoS attack.

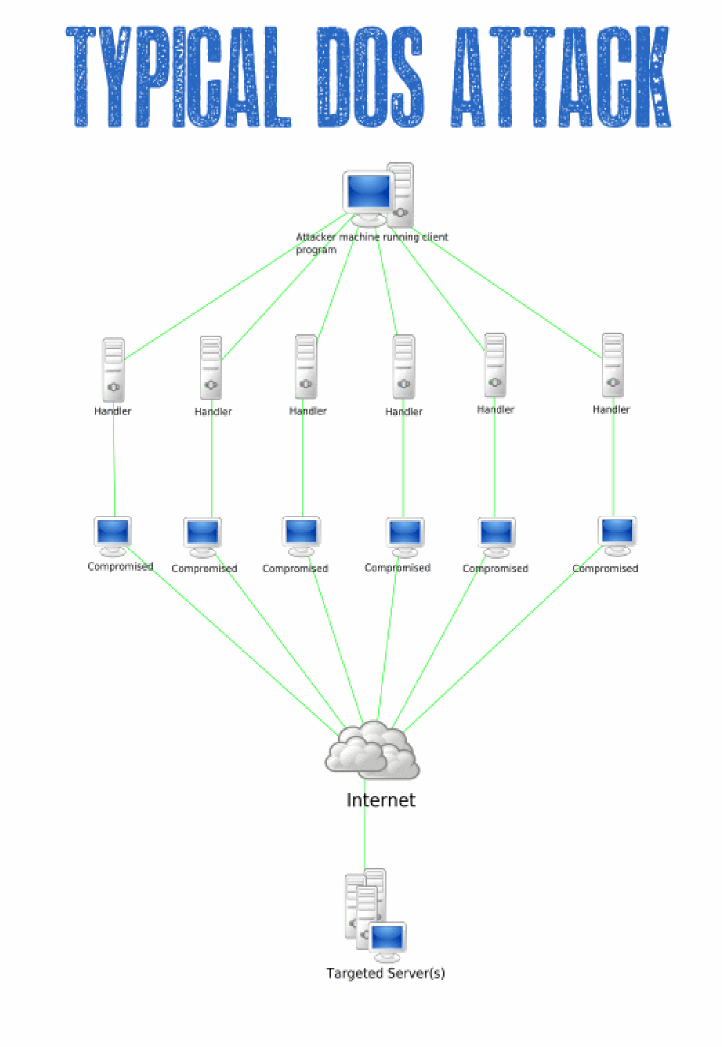

Figure 3: Typical DOS Attack
(Source:
https://www.concise-courses.com/security/wp-content/uploads/2013/08/dos-attack.png)

E. Agent Based / Artificial Agent

An entity that can be activated, autonomous and has the capability of formulating inner judgment can identify as an agent. An agent is a software program that gives assistance to user to complete some tasks or activities. Agents in a multi-agent system (MAS) must be able to cooperate and work together with every user of the system [4] [8]. Therefore, a common language is requisite for the purpose of communication, an Agent Communication Language, or ACL can be used for this. Intelligent agents are software components which have special features of intelligent behavior such as pro-activeness, understanding of an agent communication language [2] [3]. They may also possess features such as mobility, adaptability and collaboration. Multi-agent system is a system which consists of multiple agents interacting with each other to learn or exchange experience [4] [8]. Consequently more complete operational picture of the cyber space can be provided by these multi-agent tools.

F. Algorithms

An algorithm can be identified as a procedure or a formula which helps in solving a problem. A computer program can be viewed as an implementation of an algorithm. In mathematics and computer science, an algorithm usually means a procedure that helps to solve a recurrent problem. New approaches can be made by combining set of algorithms in order to detect and defeat cyber-attacks [5] [9]. Combining Fuzzy logic and Genetic Algorithm (GA) for identify intrusions has being developed since there is an essentiality of a high security approach to safe and confident communication of information between different organizations [7]. In creating new approaches FUZZY LOGIC algorithm and GENETIC algorithm are being used. Genetic Algorithm is an optimization algorithm that helps in finding appropriate fuzzy rules. Fuzzy rule is a machine learning algorithm. Fuzzy logic along with genetic based approach gives more powerful performance.

G. Data sharing between agents

Agents share its data with other agents in the system. In sharing data, the system has used wide varieties of sharing schemes such as, centralized data reporting on one side and decentralized sharing on the other. This article present a theoretical concept and framework based on peer-to-peer computing in order to integrate a multi-agent system. But this is sharing results in a scalability bottleneck due to the high volumes of incoming data; these systems often have slow performance or slow reaction [8].

H. Data mining

Data mining /data or knowledge discovery is the process of analyzing data from different perspectives and transforming it to useful information. It allows users to analyze data from many different dimensions, categorize it, and summarize the identified relationships. Typically, data mining is the process of identifying correlations or patterns among fields in large relational databases. Data mining concept can be used to analyze a multi-agent based approach in intrusion detection. Analyzing previous cyber attacking details using data mining techniques predictions regarding the future attacks can be done [10].

III. WRITE DOWN YOUR STUDIES AND FINDINGS

As been mentioned in the introduction the agent plays a key role in providing solutions to this system. The multi-agent system contains multiple agents which consist of the Agent Communication Language (ACL). This will tend to make things easier for the user. Cyber-attack detection systems (CADS's) are based on assumptions that intrusive activities are noticeably different from normal system activities and detectable. Cyber defense proposes a unique algorithm to identify cyber-attacks on web based applications. Cyber security systems in the other hand consist of a Broadway defense system, this will help the user to use the system and track many areas of cyber-crime occurrences.

CADS will make sure that external and internal cyber threats will be taken care of, through the web based algorithm used cyber defense will be able to track down the culprits within a short period of time. The IDS and IPS will also be used in tracking cyber-attacks. The IDS will identify and notify the users about cyber-crimes with the help of the agent system, whereas the IPS will identify, notify and prevent the attacks being caused. If a specific piece of valuable data is being compromised the IPS will be taking action against it and makes sure that malicious data does not harm the system or whatsoever. Using an IPS is more advantageous compared to using an IDS, as an IDS just identifies and notifies the system, whereas the IPS will prevent it from occurring.

If the agent based approach is taken into consideration, the multi-agent system consists of multiple agents with unique tasks to be done. The **IDS agent** is clear with the data collection and is curios with unwanted data, if any unwanted data is found the system notifies it through the IDS. According to a detection strategy suspicious occasions will indicate through the **classification agent. Decisions/Actions Agent** looks complicated in settling on decisions and performing particular assignments as the basic security strategies. **Alarm generation agent** handles all the interruption caution messages. The **configuration agent** makes sure that arrangement of data is done in a way so the decisions/actions agent will be able to retrieve data about cyber-attacks without any hassle.

When it comes to Intrusion Detection (ID), generally, ID can be defined as the problem of identifying or clarifying individuals who attempt to use a computer or a computer system without authorization and those who have legal access to the system but are abusing their privileges. It is also important to define an attempt as any action that try to compromise the integrity/confidentiality/availability of a particular resource. An Intrusion Detection System (IDS) watches over all network activity and identifies suspicious actions that may indicate a network attack from someone who is attempting to break into. Generally, and IDS can be divided into two categories. The first category is host-based, which includes analysis of the system's configuration files to detect suspicious settings, and inspection of other system areas to detect policy violations. The second category is network-based. In network-based, the mechanisms are set in place to act out known methods of attack and to record system responses.

While agents do not directly support the techniques for detection, they can change the way of applying theories. This means improving efficiency and effectiveness. Because agents can reproduce themselves and reside on multiple platforms, they potentially can eliminate attackers from trying to mislead IDS. Agents can maximize the strength of general IDS into robust, attack-resistant IDS. The agents are mainly focused on responding to an intrusion rather than its detection, because responses can be generated from anywhere in the network. Moreover, the following items can be described as advantages of using agents to respond to an intrusion.

- Tracing the attacker

Attackers often log into a network of many hosts before attacking a target and sometimes hide their source address. In order to catch the attacker, the IDS must trace back through the network and locate the actual host who is sending the packets. To fulfill this requirement, the infrastructure required would be expensive, but not with a widely installed agent platform.

- Responding to the attacker

When an attack is detected, it would be better if automatically respond at the target host. Such a response can prevent the attacker from establishing a better foundation and using the selected host to further compromise the network. It also helps to minimize the effort needed to recover the damage that was done by the attacker.

- Responding to the source

Responding to the attacker's host, gives an IDS much capabilities to break the attacker's mitigate plans. Without using agents, it will be hard for IDS to gain sufficient access to attacker's host in order to take necessary actions.

- Evidence gathering

Currently, it is impossible to gather evidence automatically of an attack from many different sources. Agents offer the ability to run anything, anywhere, at any time, including different hardware platforms, operating systems, and different applications such as web servers.

- Isolating the source and target

In case of action failed that was taken for source and the target, a network level response is needed to limit the attacker's actions such as block communication with the target host. The ability of agents to travel through network, it is possible to perform such an action.

Users will find it easy and user friendly to use the system along with the help of the multi-based agent systems. With the help of multiple agents Cyber Attack Detection Systems will also seem fair from the user's point of view. As it is the main component in this research area. IPS and IDS will also be beneficial as the agent based system will quickly determine threats and prevent those using prevention and detection systems.

IV. CONCLUSION

Fast development of information technology considerably impacts to human life styles. However it also generates issues such as emergence of cyber-crimes. Application of artificial agent is a new trend to combating cyber-crimes as they provide features such as mobility, rationality, adaptability and collaboration. This paper has briefly presented about the cyber-crimes and advances made so far in the field of applying artificial agent techniques in collaboration with Intrusion Prevention Systems, Intrusion Detection Systems, Cyber Attack Detection Systems and algorithms in order to combat cyber-crimes.

V. FUTURE WORK

In future works there are things which can be improved to have better results. Agents can help to improve IDSs in many areas, but they have no ability of identifying upcoming attacking strategies. In order to mitigate this issue, agents must be programmed with the ability of forecasting the future of attack types. When it comes to performance, IDSs might be running slowly when they are embedded with such agent based software. Since it is necessary to identify and respond to an attack quickly, combination of agents and IDS would delay the above mentioned identifying and responding processes. The client-server architecture is well known and has been stabilized as a technology. But the area of agent system technology is still evolving and is under construction. There should be new designs and implementations, to bring the mentioned technologies to a same level. The new methodologies must be introduced in order to overcome the issues mentioned above.

Acknowledgment

We would like to express our great appreciation to Lecturer-in-Charge (CNDI) Mr.Dhishan Dhammearatchifor his valuable and constructive suggestions given to make this research paper a success. His willingness to give his valuable time so generously has been very much appreciated.

References

[1] R. Hill, "Dealing with cyber security threats: International cooperation, ITU, and WCIT", *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pp. 119-134, 2015 [Online]. Available: http://ieeexplore.ieee.org/xpl/abstractReferences.jsp?tp&arnumber=7158473&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7158473. [Accessed: 13- Feb- 2016]

[2] S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 5, 2009 [Online]. Available: http://paper.ijcsns.org/07_book/200905/20090501.pdf. [Accessed: 08- Feb- 2016]

[3] J. Nogueira, "Mobile Intelligent Agents to Fight Cyber Intrusions", *The International Journal of FORENSIC COMPUTER SCIENCE*, vol. 1, pp. 28-32, 2006 [Online]. Available: http://www.ijofcs.org/V01N1-P03%20-%20Mobile%20Intelligent%20Agents.pdf. [Accessed: 10- Feb- 2016]

[4]S. Adebukola, Onashoga, Akinwale O. Bamidele and A. Taofik, "A Simulated Multiagent-Based Architecture for Intrusion Detection System", *(IJARAI) International Journal of Advanced Research in Artificial Intelligence*, vol. 2, no. 4, 2013 [Online]. Available: http://thesai.org/Downloads/IJARAI/Volume2No4/Paper_6A_Simulated_MultiagentBased_Architecture_for_Intrusion_Detection_System.pdf. [Accessed: 15- Jan- 2016]

[5] S. Dilek, H. Çakır and M. Aydın,"APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW", *International Journal of Artificial Intelligence & Applications (IJAIA)*, vol. 6, no. 1, 2015 [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf. [Accessed: 13- Feb- 2016]

[6] J.Raiyn, "A survey of Cyber Attack Detection Strategies", *International Journal of Security and Its Applications*, vol. 8, no. 1, pp. 247-256, 2014 [Online]. Available: http://www.sersc.org/journals/IJSIA/vol8_no1_2014/23.pdf. [Accessed: 13- Feb- 2016]

[7] A. Cerli and D. Ramamoorthy, "Intrusion Detection System by Combining Fuzzy Logic with Genetic Algorithm", *Global Journal of Pure and Applied Mathematics (GJPAM)*, vol. 11, no. 1, 2015 [Online]. Available: http://ripublication.com/gjpamspl/gjpamv11n1spl_20.pdf. [Accessed: 09- Feb- 2016]

[8] O. Oriola, A. Adeyemo and A. Robert, "Distributed Intrusion Detection System Using P2P Agent Mining Scheme", *African Journal of Computing & ICT*, vol. 5, no. 2, 2012 [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.411.3403&rep=rep1&type=pdf. [Accessed: 08- Feb- 2016]

[9] S. Simmons, D. Edwards, N. Wilde, J. Just and M. Satyanarayana, "Preventing Unauthorized Islanding: Cyber-Threat Analysis", *2006 IEEE/SMC International Conference on System of Systems Engineering*, pp. 5, 24-26 [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=165229&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1652294. [Accessed: 11- Feb- 2016]

[10] I. Ionita and L. Ionita, "An agent-based approach for building an intrusion detection system",*RoEduNet International Conference 12th Edition: Networking in Education and Research*, pp. 1-6, 26-28, 2013 [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6714184. [Accessed: 11- Feb- 2016]