Available online at http://acfa.apeejay.edu
APEEJAY JOURNAL OF COMPUTER SCIENCE AND APPLICATIONS
ISSN:0974-5742(P)
Vol. 2, January 2014

INTELLIGENT CYBER DEFENSE SYSTEM (ICDS): HYBRID APPROACH TO DETECT AND DEFENSE AGAINST CYBER CRIME

Neeru Mago
Assistant Professor, Panjab University SSG Regional Centre, Hoshairpur

ABSTRACT
Cyberspace is very lucrative area for criminals to spread cyber crimes in society. They commit various types of cyber crimes using technological advancements of IT field. Cyber infrastructures are highly vulnerable to intrusions and other threats which lead to the need for development of sophisticated, flexible, adaptable and robust Cyber Defense Systems (CDS). These systems need to be intelligent enough to be able to detect a wide variety of threats and make intelligent real-time decisions. Numerous techniques of Artificial Intelligence and Data Mining have been introduced which plays an important role in cyber crime detection and prevention. In this paper, various techniques in the field of AI & DM, for detecting and preventing cyber crime are presented and how these techniques can be an effective tool in CDS are demonstrated. This paper mainly focuses on study of survey on various existing techniques available and proposes a hybrid approach to detect and defense against cyber crime using Artificial Intelligence and Data Mining techniques. The proposed system is named as Intelligent Cyber Defense System (ICDS).
***Keywords**: Cyber crime. Cyberspace, Intrusion, artificial intelligence, data mining, intelligent cyber defense system.*

1. INTRODUCTION

The rapid growth in the development of computing technology and internet had made our life convenient and easy but it also had a negative impact such as emergence of new types of crimes. For instance, Cyber crimes can be attained through information technology. Moreover, with the evolvement of this technology, number and variety of criminal cases increase correspondingly. Information technology is increasingly used as a tool for committing crimes. Electronic devices and other high-tech products such as computers, phones, Internet and all other information systems developed for the benefit of humanity are susceptible to criminal activity. They typically target e-mail accounts, bank accounts, computers, servers, websites, personal data, and digital records of private and public institutions. These crimes are also known as “Digital Crimes”, “Computer Crimes”, “Crimes of Information Technologies”, “Network Crimes” or “Internet Crimes”[1].

Security is a vital and critical issue for the future of the cyberspace. Over the past few years, due to penetration of new technologies and high usage/dependency of the Internet in all sectors, there has been tremendous increase in the cyber threats. The problem is becoming severe with the increasing rate of attacks against the computer infrastructures. Cyber security involves protecting information by detecting, preventing and responding to attacks. Cyber security also referred to as information technology security, whose main focus is protection of computers, networks, programs and data from unauthorized access. Intruders need not to be computer experts. With the invention of various innovative tools that support various types of network attacks, they can attack or hack other’s system. Hence, effective methods for cyber crime detection have become an insisting need to protect the cyber crime. Many CDS were developed but there is a need to refine them by introducing various techniques of AI & DM.

This paper imparts number of applications for the artificial intelligence and data mining methodologies in cyber security. It have been developed and deployed to protect computer systems against network attacks. Combinations of different intelligent system approaches to form hybrid intelligent systems continue to find new applications. Hence, in this paper, Intelligent Cyber Defense System (ICDS) is proposed to make the defense system more effective.

2. RELATED WORK

Defining “cyber crime” in precise words is very difficult. Most of the existing definitions were developed experimentally. Gordon and Ford (2006) define cyber crime as: “any crime that is facilitated or committed using a computer, network, or hardware device” where “computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime” [2]. Dictionary.com defines cyber crime as “criminal activity or a crime that involves the Internet, a computer system, or computer technology” [3]. Fisher and Lab (2010) defined cyber crime as “crime that occurs when computers or computer networks are involved as tool, locations,

or targets of crime" [4]. Every day, as the people communicate, share, shop, work, and socialize using computers and Internet, the amount of digital data stored and processed on computers and other computing systems increases exponentially. Therefore cyber space has not stayed isolated from the concepts of crime and criminals either [5]. Brenner (2010) argues that "most of the cyber crime we see today simply represents the migration of real-world crime to cyberspace which becomes the tool criminals use to commit old crimes in new ways"[6].

The main goal of Cyber Defense Systems is to monitor resources to detect abnormal behavior and misuses[7]. In year 1980, the concept was projected by James P. Anderson[8] by providing various ways to improve security [2, 6] auditing and surveillance at customer sites. During the period 1984 and 1986 Peter Neumann and Dorothy Denning developed the first real time Intrusion Detection System, named as Intrusion detection Expert System (IDES). Initially IDES was trained to detect known malicious behavior using rule-based approach and further it was refined and named as Next-Generation IDS (NIDES) In the year 1988, University of California and U.S. Government funded for the research projects like Haystack (US Air Force). Research work have done by comparing audit with known patterns, Host based Pattern matching system evolved and it was included in the Distributed atmosphere(i.e. Distributed IDS) In 1990, NIDS (Networks bases Intrusion Detection) was introduced by UC Davis's Todd Heber lien and contributed in DIDS and deployed NSM (network Security Monitoring)and in early 90's Commercial IDS are developed like CMDS (Computer Misuse Detection System) host based approach. In 1994, ASM (Automated Security Measurement system) came in to the market.

Based on data provided by CERT/CC, vulnerabilities and number of virtual attacks have highly raised up from 1998 to 2002. Malek and Hamantiz (2004), indicated that the reports show 25,000 of intrusions happened in 2000 which means the intrusions have highly increased [9]. The number of attacks happened from 1990 to 2010 are illustrated in Fig. 1. Both the list of Common Vulnerabilities and Exposures (CVE) (Christey and Martin, 2007) and the recent research on security issues in the digital network of the world show that 25 percent of the total security threats were related to web application vulnerabilities (Vasudevan et al., 2011).

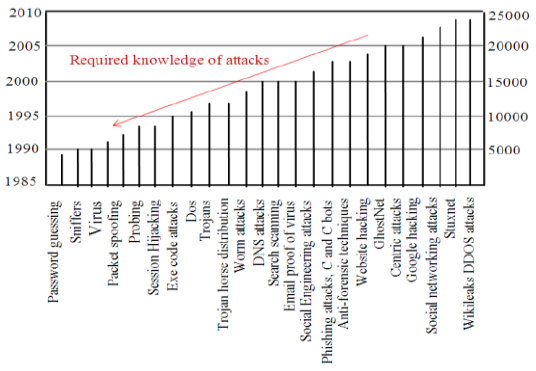

Fig. 1. Security Vulnerabilities and Threats (Malek and Harmantzis, 2004; Vasudevan *et al.*, 2011)

Many author presented their views on AI and DM techniques in security management from different perspectives. The author [11] present the intelligent techniques are applicable for network protocol security, monitoring, measurement, and accurate prediction. The social networking issues are quite serious issue hence the author [12] presents the Artificial Intelligence techniques can help to outline basic categories of privacy concerns, including solutions to them. The paper in [13] proposes a dynamic model Intelligent Intrusion Detection System, based on specific AI approach for intrusion detection. The author in paper [14] presents situation of rapidly growing attacks on cyberspace. Besides AI techniques for security, there has been a lot of work on applying data mining for cyber security. Various data mining techniques like classification. clustering, link analysis and association rule mining are being explored to detect abnormal patterns. After studying existing papers on the various techniques available for providing security, it becomes apparent that there is a need to develop an Intelligent Cyber Defense System (ICDS) that works on hybrid approach by using various AI and DM techniques to detect and protect against cyber crime.

3. **TECHNIQUES**

In this section, various techniques, methods and tools of Artificial Intelligence and Data Mining are discussed which can be used for providing cyber security. Each having its own applications, domain, advantages, limitations, issues and challenges associated with them. Where and how to apply them is the obvious question comes in our mind. AI techniques have several applications in dealing with cyber crimes. For instance, neural networks are being applied for detection and prevention of cyber crime[1]. In addition, it can also be applied in

"Denial of Service (DoS) detection, computer worm detection, spam detection, malware classification and forensic investigations" [15]. AI techniques such as Heuristics, Neural Networks, and AISs, have also been applied to new-generation anti-virus technology [16]. Data mining has many applications in security including national security, terrorist activities and cyber security. Some CDSs use intelligent agent technology which is sometimes even combined with mobile agent technology. This section will briefly present some existing applications of AI and DM techniques to cyber defense.

3.1. Artificial Neural Network

ANN is a computational mechanism that simulates structural and functional aspects of neural networks existing in biological nervous systems. They are ideal for situations that require prediction, classification or control in dynamic and complex computer environments [17]. Al-Janabi and Saeed (2011) designed neural network-based IDS that can promptly detect and classify various attacks [18]. Barman and Khataniar (2012) also studied the development of IDSs based on neural network systems. Their experiments showed that the system they proposed has intrusion detection rates similar to other available IDSs, however, it proved to be at least 20.5 times faster in detection of DoS attacks [19].

3.2. Intelligent Agent

Intelligent agents are autonomous computer-generated forces that communicate with each other to share data and cooperate with each other in order to plan and implement appropriate responses in case of unexpected events. Their mobility and adaptability in the environments they are deployed in, as well as their collaborative nature, makes intelligent agent technology suitable for combating cyber attacks. Shosha et al. (2011) proposed distributed IDS based on community collaboration between multiple agents for detecting cyber intrusions in Supervisory Control and Data Acquisition (SCADA) networks. The proposed architecture also incorporates the SCADA network topology and connectivity constraints [20]. Ionita and Ionita (2013) proposed a multi intelligent agent based approach for network intrusion detection using data mining [21].

3.3. Artificial Immune System (AIS)

AISs, just like the biological immune systems which they are based on, are employed to uphold stability in a changing environment. The immune-based intrusion detection comprises the evolution of immunocytes (self-tolerance, clone, variation, etc.) and antigens detection simultaneously. An immune system produces antibodies to resist pathogens and the intrusion intensity can be estimated by variation of the antibody concentration. Therefore, AISs play an important role in the cyber security research [22]. Mohamed and Abdullah (2009) presented an AIS-based security framework for securing mobile ad hoc networks, which is scalable, robust, and has traits of distributability, second response and self-recovery. Their architecture resolved some limitations found in the previous related studies such as scalability and bandwidth conservation [23].

3.4. Genetic Algorithm and Fuzzy Sets

Kim et al. (2004) proposed a learning algorithm for anomaly detectors which can detect attacks using genetic algorithm. They applied their algorithm to an artificial computer security system and showed its effectiveness in intrusion detection[24]. Jongsuebsuk et al. (2013) proposed a network IDS based on a fuzzy genetic algorithm. Fuzzy rules are used to classify network attack data, whereas genetic algorithm optimizes finding appropriate fuzzy rule in order to obtain the optimal solution. The evaluation results showed that the proposed IDS can detect network attacks in real-time (or within 2-3 seconds) upon the arrival of data arrives to the detection system with the detection rate of over 97.5% [25].

3.5 Expert systems

Expert systems are unquestionably the most widely used AI tools. An expert system is software for finding answers to questions in some application domain presented either by a user or by another software [26]. It can be directly used for decision support, e.g. in medical diagnosis, in finances or in cyberspace. There is a great variety of expert systems from small technical diagnostic systems to very large and sophisticated hybrid systems for solving complex problems. Example of a Cyber Defense expert system is one for security planning [27]. This expert system facilitates considerably selection of security measures, and provides guidance for optimal usage of limited resources[28].

3.6 Bayesian Classification

Bayesian classification works based on probability distribution function over a set of variables, in graphical representation form[29]. The intrusion analysis structure can be represented as Directed Acyclic Graph (DAG)[30], where each node represents a random variable and each edge represents the relation between two nodes and the individual attacks occurred are represented as a node in the graph with relation between the events which are represented as edge of the graph. However it needs to build a decision tree based on special features

and various types of attacks modeled by a Bayesian classifier network. Let X is a data sample whose class label is unknown. Let H be some hypothesis that X belongs to a class C. For classification determine P(H/X). P(H/X) is the probability that H holds given the observed data sample X P(H/X) is posterior probability. In this approach IDS is built by using naïve bayesian classifier and mostly it works on anomaly based intrusion detection. It works by recognizing all the features that have different probabilities of occurring in various attacks and also detecting normal traffic in TCP and UDP protocols. The Bayesian filter is trained with classified traffic and adjusts the probabilities for each feature whenever a new attack occurs. The process repeats by recalculating for each TCP connection to classify weather it is normal traffic or an attack.

3.7 Decision Tree

Decision tree approach proposed by [Mrutyunjaya] states that the targeted values are represented in the form of a tree, the tree is built up based on the principle of recursive partitioning of the data. In this approach attributes are selected as a partitioned attribute or a node with the information gain criteria and the process repeats for every child node till all selected attributes are considered and decision tree is constructed. For better results some pruning techniques can be used to reduce the size of the tree.

3.8 Support Vector Machine

Based on the proposed work of Weijun li, Zhenyu Liu[31]. The normal way of intrusion detection is based on gathering and analyzing data from different areas within a machine or network. A number of datasets with feature values which has large value range, such as numerous periods of Maximal and minimum in byte(s) among the target and source when normal and attack. SVM is a most popular way as it is moderately insensible to the no. of data points and the classification complexity doesn't dependson the dimensionality of the attribute space. So they can potentially learn a larger set of patterns and thus be able to scale better than some methods. For the reason normalization is a good quality way to decrease the difference of the data and improve the speed. Some normalization methods are brought forward. Since the routine data is extremely large, method of normalization should have simple rules and fast speed. Max Normalization and Min-MaxNormalization.

3.9 Data Mining Techniques

There are several major data mining techniques have been developed and used in data mining projects recently including association, classification, clustering, prediction and sequential patterns.

TABLE I: VARIOUS DATA MINING TECHNIQUE

Techniques Name	*Function*
Association	a pattern is discovered based on a relationship of a particular item on other items in the same transaction
Classification	Classify each item in a set of data into one of predefined set of classes or groups. Classification method makes use of mathematical techniques such as decision trees, linear programming, neural network and statistics
Clustering	Makes meaningful or useful cluster of objects that have similar characteristic using automatic technique.
Prediction	Discovers relationship between dependent and independent variables
Sequential Patterns	Discover similar patterns in data transaction over a period

Data mining approaches can be applied for intrusion detection. An important advantage of data mining approach is that it can develop a new class of models to detect new attacks before they have been seen by human experts. Classification model with association rules algorithm and frequent episodes is developed for anomaly intrusion detection. This approach can automatically generate concise and accurate detection models from large amount of audit data. However, it requires a large amount of audit data in order to compute the profile rule sets. More-over, this learning process is an integral and continuous pat? of an intrusion detection system because the rule sets used by the detection module may not he static over a long period of time. A team of researchers at Columbia University proposed the detection models using cost-sensitive machine learning algorithms. Audit data is analyzed by association rules algorithm in order to determine static features of attack data.

4. METHODOLGY

In this section, an Intelligent Cyber Defense System (ICDS) is proposed which will collectively use AI and DM techniques on cyberspace to make the CDS more intelligent. Defense against intelligent cyber weapons can be achieved only by intelligent software, and events of the last few years have shown rapidly increasing intelligence of malware and cyber-weapon. Here comes the need of Artificial Intelligence for developing intelligent system for Cyber Defense. Data mining is being applied to problems such as intrusion detection and auditing. For example, anomaly detection techniques could be used to detect unusual patterns and behaviors.

Link analysis may be used to trace self-propagating malicious code to its authors. Classification may be used to group various cyber attacks and then use the profiles to detect an attack when it occurs. Prediction may be used to determine potential future attacks depending in a way on information learnt about terrorists through email and phone conversations. Data mining can also be used for analyzing web logs as well as analyzing the audit trails. Based on the results of the data mining tool, one can then determine whether any unauthorized intrusions have occurred and/or whether any unauthorized queries have been posed. Other applications of data mining for cyber security include analyzing the audit data. One could build a repository or a warehouse containing the audit data and then conduct an analysis using various data mining tools to see if there are potential anomalies. For example, there could be a situation where a certain user group may access the database between 3 and 5am in the morning. It could be that this group is working the night shift in which case there may be a valid explanation. However if this group is working between say 9am and 5pm, then this may be an unusual occurrence. Another example is when a person accesses the databases always between 1 and 2pm; but for the last 2 days he has been accessing the database between 1 and 2am. This could then be flagged as an unusual pattern that would need further investigation.
The proposed system for Intelligent Cyber Defense using AI and DM techniques is shown in Fig 2.

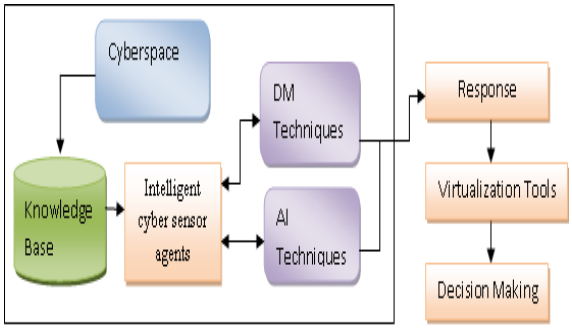

Fig 2: Intelligent Cyber Defense System (ICDS)

Various modules of ICDS are as follows:

- Cyberspace: The term originated by author William Gibson in his novel Neuromancer. The word Cyberspace is currently used to describe the whole range of information resources available through computer networks. It is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.
- Knowledge Base: Whenever a user uses cyberspace for any purpose, it is stored in the knowledge base as a web log file that maintains the history of all the activities performed in the cyberspace. It must get more and more intelligent with every activity made in the cyberspace. It becomes the basis for detection and analysis of any suspected/false activity performed.
- Intelligent cyber sensor agents: Intelligent cyber sensor agents are computer-generated forces which detect, evaluates and responds to cyber attacks in a timely manner.
- DM Techniques: Data mining is being applied to problems such as intrusion detection and auditing to detect unusual patterns and behaviors. Some data mining techniques (like clustering, classification, association rules and prediction) can be applied to identify some unusual patterns in the web log file.
- AI Techniques: Once the DM techniques applied to data for pattern recognition, some AI techniques (like neural network, genetic algorithms, etc) can also be applied to make the system more intelligent to monitor, analyse and find the actual cyber crime. DM and AI techniques together use cyberspace for performing their functions at various stages.
- Response: After detecting the actual cyber crime performed by criminals/intruders on a cyberspace, the results in the form of alerts, alarms, etc are provided.
- Visualization tools: Results can also be shown by various visualization techniques like GUI, graphs, charts, etc.
- Decision making: Once the results are shown, appropriate decision can be made by the concerned authorities.

In contrast to traditional Cyber Defense Systems (CDS), AI & DM anomaly detection methods/techniques have been used in ICDS in the domain of cyberspace data for detection and prevention against cyber threat. AI & DM techniques/methods and tools are widely recognized as popular and important intelligent and automatic tools to assist humans in big data security analysis and anomaly detection over CDSs.

5. CONCLUSION AND FUTURE SCOPE

In the present situation of rapidly growing intelligence of malware and sophistication of cyber attacks, it is unavoidable to develop intelligent cyber defense method. As Security is key important issues, the integration Artificial Intelligence and Data Mining (AI & DM) Techniques certainly improve the performance of the existing security system. Main thing related to security is alert the user before unwanted things going to happened. This paper consists of overview of different AI & DM techniques and proposal of Intelligent Cyber Defense System useful in enhancing the security infrastructure. Use of different AI & DM techniques together in security management protects against the security attacks/threads by warning the user on appropriate time.

When planning the future research, development and application of AI & DM methods in Cyber Defense, one has to distinguish between the immediate goals and long-term perspectives. There are numerous AI & DM methods immediately applicable in Cyber Defense, and there are immediate Cyber Defense problems that require more intelligent solutions than have been implemented at present. Until now we have discussed these existing immediate applications. In the future, one can see promising perspectives of the application of completely new principles of knowledge handling in situation management and decision making.

REFERENCES:

[1] Selma Dilek, Hüseyin Çakır, Mustafa Aydın "APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES:A REVIEW" International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015 .

[2] S. Gordon, R. Ford, (2006) "On the definition and classification of cybercrime", Journal in Computer Virology, Vol. 2, No. 1, pp. 13 20.

[3] http://dictionary.reference.com/browse/cybercrime

[4] B. S. Fisher, S. P. Lab, (2010) Encyclopedia of Victimology and Crime Prevention, SAGE Publications, Vol. 1, pp. 251, USA

[5] H. Dijle, N. Doğan, (2011) "Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı", Bilişim Teknolojiler Dergisi, Vol. 4, No. 2

[6] S. W. Brenner, (2010) Cybercrime: Criminal Threats from Cyberspace, Greenwood publishing group, Library of Congress Cataloging-in-Publication Data,USA.

[7] Anderson, James P., "Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co., 1980.

[8] Mohsen Kakavand, Norwati Mustapha, Aida Mustapha, Mohd Taufik Abdullah and Hamed Riahi "A Survey of Anomaly Detection Using Data Mining Methods for Hypertext Transfer Protocol Web Services", Journal of Computer Science 2015, 11 (1): 89.97 DOI: 10.3844/jcssp.2015.89.97.

[9] Swapnil Ramesh Kumbhar, "An Overview on Use of Artificial Intelligence Techniques in Effective Security Management", International Journal of Innovative Research in Computer and Communication Engineering ISO 3297: 2007 Certified Organization)Vol. 2, Issue 9, September 2014Copyright to IJIRCCE.

[10] Emmanuel Hooper "Intelligent Techniques for Effective Network Protocol Security Monitoring, Measurement and Prediction",International Journal of Security and Its ApplicationsVol.2,No.4,October, 2008

[11] Sattikar, Dr. R. V. Kulkarni, "A Role of Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking", IJCSET , Vol 2, Issue 1, January 2012.

[12] Idris, N.B.Shanmugam.B.," Artificial Intelligence Techniques Applied to Intrusion Detection" INDICON2005 Annual IEEE Conference, pp 52 –55,Dec. 2005.

[13] Enn Tyugu , "Artificial Intelligence in Cyber Defense" , 3rd International Conference on Cyber Conflict,2011.

[14] E. Tyugu, (2011) "Artificial intelligence in cyber defense", 3rd International Conference on Cyber Conflict (ICCC 2011), pp. 1–11.

[15] X. B. Wang, G. Y. Yang, Y. C. Li, D. Liu, (2008) "Review on the application of Artificial Intelligence in Antivirus Detection System", IEEE Conference on Cybernetics and Intelligent Systems, pp. 506 509.

[16] C. Bitter, D.A. Elizondo, T. Watson, (2010) "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI 2010), pp. 949 – 954.

[17] S. T. F. Al-Janabi, H. A. Saeed, (2011) "A Neural Network Based Anomaly Intrusion Detection System", Developments in E-systems Engineering (DeSE), pp. 221 – 226.

[18] D. K. Barman, G. Khataniar, (2012) "Design Of Intrusion Detection System Based On Artificial Neural Network And Application Of Rough Set", International Journal of Computer Science and Communication Networks, Vol. 2, No. 4, pp. 548-552.

[19] A. F. Shosha, P. Gladyshev, W. Shinn-Shyan, L.Chen-Ching, (2011) "Detecting cyber intrusions in SCADA networks using multi-agent collaboration," 16th International Conference on Intelligent System Application to Power Systems (ISAP), pp.1-7.

[20] I. Ionita, L. Ionita, (2013) "An agent-based approach for building an intrusion detection system," 12th International Conference on Networking in Education and Research (RoEduNet), pp.1-6.

[21] L. Rui, L. Wanbo, (2010) "Intrusion Response Model based on AIS", International Forum on Information Technology and Applications (IFITA), Vol. 1, pp. 86 – 90.

[22] Y. A. Mohamed, A. B. Abdullah, (2009) "Immune Inspired Framework for Ad Hoc Network Security", IEEE International Conference on Control and Automation, pp. 297 – 302.

[23] D. W. Kim, J. W. Yang, K. B. Sim, (2004) "Adaptive Intrusion Detection Algorithm based on Learning Algorithm", The 30th Annual Conference of the IEEE Industrial Electronics Society, Vol. 3, pp. 2229 – 2233.

[24] P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, (2013) "Real-time intrusion detection with fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp.1-6.

[25] http://en.wikipedia.org/wiki/Expert_system. Expert System. Wikipedia.

[26] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.

[27] Enn Tyugu, "Artificial Intelligence in Cyber Defense", International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.)Tallinn, Estonia, 2011 © CCD COE Publications.

[28] Hesham Altwaijry , Saeed Algarny, Bayesian based intrusion detection system, Journal of King Saud University – Computer and Information Sciences, (2012) 24, 1–6.

[29] Dickerson, J. E. and J. A. Dickerson, "Fuzzy network profiling for intrusion detection", In Proc. of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, pp. 301306. North American Fuzzy Information.

[30] Dasgupta, D. and F. A. Gonzalez, "An intelligent decision support system for intrusion detection and response", . In Proc. Of International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS), St.Petersburg. Springer-, 21-23 May,2001.

[31] Anita Rajendra Zope, Amarsinh Vidhate, and Naresh Harale "Data Mining Approach in Security Information and Event Management", International Journal of Future Computer and Communication, Vol. 2, No. 2, April 2013.