International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||06||Pages||5582-5587||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i6.33

Computer Security and Intrusion detection System-A Data Mining Based Approach

Neetu Anand [1]***, Tapas Kumar*** [2]
[1]Maharaja Surajmal Institute, New Delhi
neetuanand@msi-ggsip.org,
[2]Lingayas University, Faridabad
Kumartapas534@gmail.com

Abstract**-With an increased understanding of how systems work, intruders have become skilled at determining weaknesses in systems and exploiting them to obtain such increased privileges that they can do anything on the system. Intruders also use patterns of intrusion that are difficult to trace and identify. They frequently use several levels of indirection before breaking into target systems and rarely indulge in sudden bursts of suspicious or anomalous activity. They also cover their tracks so that their activity on the penetrated system is not easily discovered. We must have measures in place to detect security breaches, i.e., identify intruders and intrusions. Intrusion detection systems fill this role and usually form the last line of defense in the overall protection scheme of a computer system. They are useful not only in detecting successful breaches of security, but also in monitoring attempts to breach security, which provides important information for timely countermeasures. This paper focused on how data mining is used for Intrusion detection System**

Keywords – Intrusion Detection, Data Mining, Data Analysis, Denial of service, Anomaly detection

I. Introduction

Computer Security and its Role: One broad definition of a secure computer system is given by Garfinkel and Spafford as one that can be depended upon to behave as it is expected to. The dependence on the expected behavior being the same as exhibited behavior is referred to as trust in the security of the computer system. The level of trust indicates the confidence in the expected behavior of the computer system. The expected behavior is formalized into the security policy of the computer system and governs the goals that the system must meet. This policy may include functionality requirements if they are necessary for the effective functioning of the computer system.
A narrower definition of computer security is based on the realization of confidentiality, integrity, and availability in a computer system

Data confidentiality: Data that are being transferred through the network should be accessible only to those that have been properly authorized.
Data integrity: Data should maintain their integrity from the moment they are transmitted to the moment they are actually received. No corruption or data loss is accepted either from random events or malicious activity.
Data availability: The network should be resilient to Denial of Service attacks.
By this definition, an unreliable computer system is unsecured if availability is part of its security requirement.
In addition to the well-established intrusion prevention techniques such as data encryption and message integrity, user authentication and user authorization, as well as the avoidance of security flaws inherent to many off-the-shelf applications, intrusion detection techniques can be viewed as an addition safeguard for networked computers. Thus, intrusion detection systems are useful even when strong preventive steps taken to protect computer systems place a high degree of confidence in their security.

II. Literature Reviewed

Eric Bloedorn, et al.(2001)suggested data mining techniques to consider and types of expertise and infrastructure needed for making an IDS.

Wenke Lee, et al.(2000) utilized auditing programs to extract an extensive set of features that describe each network connection or host session, and apply data mining programs to learn rules that accurately capture the behavior of intrusions and normal activities. These rules can then be used for misuse detection and anomaly detection. New detection models are incorporated into an existing IDS through a meta-learning (or co-operative learning) process, which produces a meta detection model that combines evidence from multiple models.

Sattarova Feruza Yusufovna (2008) presented the application of a number of data mining techniques that have been proposed towards the enhancement of IDS. It was shown that data mining has been known to aid the process of intrusion detection and the ways in which the various techniques have been applied and evaluated by researchers. The integration of data mining approaches can contribute significantly in the attempt to create better and more effective intrusion detection systems.

Tao Peng, Wanli Zuo (2005) implement the architecture of data mining based NIDS in real time. They analyze a frequent patterns mining algorithm that integrate Apriori candidate generation into FP-growth method .FP-growth adopts a divide-and-conquer strategy that compresses the database representing frequent items into a frequent –pattern tree(FP-tree),and proceeds mining of FP-tree, and proceed mining of FP-tree.

Norbik Bashah et al. (2005) proposed system is a hybrid system that combines anomaly, misuse and host based detection. Simple Fuzzy rules allow us to construct if-then rules that reflect common ways of describing security attacks. For host based intrusion detection we use neural-networks along with self organizing maps. Suspicious intrusions can be traced back to its original source path and any traffic from that particular source will be redirected back to them in future. Both network traffic and system audit data are used as inputs for both.

Hu Zheng Bing, Shirochin V. P. (2005) proposed an algorithm to use the known signature to find the signature of the related attack quickly.

.

P.J. Stanford, et al. (2006), presented an approach to Internet misuse detection that combines the use of an efficient signature detection filtering mechanism with statistical summaries and data mining algorithm to provide a highly configurable adaptive network intrusion detection system.

QU Zhiming, et al. (2009), used rough set and clustering algorithm to mine network security evaluation rules which are utilized to build a model of network security system to assess decision making.

Hu Zhengbing, et al. (2008) focused on misuse detection and collected the attack signature in a database and proposed an algorithm to find the signature of the related attack quickly.

Stefano Zanero et al.(2006), described an innovative model of Anomaly Based Network Intrusion Detection System, totally based on unsupervised learning techniques.

Hongyu Yang et al.(2006), performed clustering to group training data points into clusters, from which they selected some clusters as normal and known-attack profile according to certain criterion. For those training data excluded from the profile, they used them to build a specific classifier. During the testing stage, they utilized influence based classification algorithm to classify network behaviors

Liu Dihua et al.(2001), utilized auditing program to extract an extensive set of features that described each network connection or host session ,and applied data mining program to learn rules that accurately captured the behavior of intrusion and normal activities .These rules can then be used for misuse and anomaly detection.

Wenke Lee et al.(1998), outlined a data mining framework for constructing intrusion detection models. The key idea is to apply data mining programs to audit data to compute misuse and anomaly detection models, according to the observed behavior in the data. To facilitate adaptability and extensibility, they proposed the use of meta-learning as a means to construct a combined model that incorporate evidence from multiple (lightweight) base models. This mechanism makes it feasible to introduce new ID components in existing IDS possibly without significant re-engineering. They extended the basic association rules and frequent episodes algorithms to accommodate the special requirements in analyzing audit data. They showed that the frequent patterns mined from audit data can be used as reliable user anomaly detection models, and as guidelines for selecting temporal statistical features to build effective classification models.

Ye Changguo, et al.(2009), adopted fuzzy associate rules mining method and apriori algorithm to abnormal detecting experiment based on network, and improved the support and credit, and compared and analyzing the experiment result

Joong-Hee Leet, et al.(2008),they generate the decision trees for DoS attack,R2L attack, U2R attack, and Scan attack. The ID3 algorithm is used as the learning algorithm to generate the decision tree automatically, and the DARPA Set is adopted for the training data. They described the process of generating the decision tree step by step, and evaluate the decision tree by DARPA Set Testing Data. Their proposed model achieves the improvement in detecting new kinds of attacks in anomaly detection.

III. Intrusion Detection

A. What is Intrusion Detection?

An intrusion is defined by any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. An intrusion is a violation of the security policy of the system. Whereas policy defines the goals that must be satisfied in a system, detecting breaches of policy requires knowledge of steps or actions that may result in its violation [20].

Intrusion Detection System (IDS) is an important detection used as a counter measure to preserve data integrity and system availability from attacks. Intrusion Detection Systems (IDS) is a combination of software and hardware that attempts to perform intrusion detection. Intrusion detection is a process of gathering intrusion related knowledge occurring in the process of monitoring the events and analyzing them for sign or intrusion.

B. Characterizing Intrusion Detection Systems

IDS systems vary according to a number of criteria. First and foremost, it’s possible to distinguish IDSs on the basis of the kinds of activities, traffic, transactions, or systems they monitor. In this case, IDSs may be divided into network-based, host-based, and application-based IDS types[21]. IDSs that monitor network backbones and look for attack signatures are called network-based IDSs, whereas those that operate on hosts defend and monitor the operating and file systems for signs of intrusion and are called host-based IDSs. Some IDSs monitor only specific applications and are called application-based IDSs. (This type of treatment is usually reserved for important applications such as database management systems, content management systems, accounting systems, and so forth.) Hybrid intrusion detection systems offer management of and alert notification from both network and host-based intrusion detection devices. Hybrid solutions provide the logical complement to NID and HID - central intrusion detection management.

(i) Network-based IDS characteristics

Pros: Network-based IDSs can monitor an entire, large network with only a few well-situated nodes or devices and impose little overhead on a network. Network-based IDSs are mostly passive devices that monitor ongoing network activity without adding significant overhead or interfering with network operation. They are easy to secure against attack and may even be undetectable to attackers; they also require little effort to install and use on existing networks.

Cons: Network-based IDSs may not be able to monitor and analyze all traffic on large, busy networks and may therefore overlook attacks launched during peak traffic periods. Network-based IDSs may not be able to monitor switch-based (high-speed) networks effectively, either. Typically, network-based IDSs cannot analyze encrypted data, nor do they report whether or not attempted attacks succeed or fail. Thus, network-based IDSs require a certain amount of active, manual involvement from network administrators to gauge the effects of reported attacks.

(ii) Host-based IDS characteristics

Pros: Host-based IDS can analyze activities on the host it monitors at a high level of detail; it can often determine which processes and/or users are involved in malicious activities. Though they may each focus on a single host, many host-based IDS systems use an agent-console model where agents run on (and monitor) individual hosts but report to a single centralized console (so that a single console can configure, manage, and consolidate data from numerous hosts). Host-based IDSs can detect attacks undetectable to the network-based IDS and can gauge attack effects quite accurately. Host-based IDSs can use host-based encryption services to examine encrypted traffic, data, storage, and activity. Host-based IDSs have no difficulties operating on switch-based networks, either.

Cons: Data collection occurs on a per-host basis; writing to logs or reporting activity requires network traffic and can decrease network performance. Clever attackers who compromise a host can also attack and disable host-based IDSs. Host-based IDSs can be foiled by DoS attacks (since they may prevent any traffic from reaching the host where they're running or prevent reporting on such attacks to a console elsewhere on a network). Most significantly, a host-based IDS does consume processing time, storage, memory, and other resources on the hosts where such systems operate.

(iii) Application-based IDS characteristics

Pros: An application-based IDS concentrates on events occurring within some specific application. They often detect attacks through analysis of application log files and can usually identify many types of attack or suspicious activity. Sometimes application-based IDS can even track unauthorized activity from individual users. They can also work with encrypted data, using application-based encryption/decryption services.

Cons: Application-based IDSs are sometimes more vulnerable to attack than the host-based IDS. They can also consume significant application (and host) resources.

The goal of IDS is to detect malicious traffic. In order to accomplish this, the IDS monitor all incoming and outgoing traffic. There are several approaches on the implementation of IDS. Among those, two are the most popular:

Anomaly detection: This technique is based on the detection of traffic anomalies. The deviation of the monitored traffic from the normal profile is measured. For example, if user X only uses the computer from his once between 9 AM and 5 PM, an activity on his account late in the night is anomalous and hence, might be an intrusion. Another user Y might always login outside working hours through the company terminal server. A late night remote login session from another host to his account might be considered unusual. Anomaly detection attempts to quantify the usual or acceptable behavior and flags other irregular behavior as potentially intrusive.

Misuse/Signature detection: This technique looks for patterns and signatures of already known attacks in the network traffic. A constantly updated database is usually used to store the signatures of known attacks. The way this technique deals with intrusion detection resembles the way that anti-virus software operates.

Main problems: manual and ad-hoc

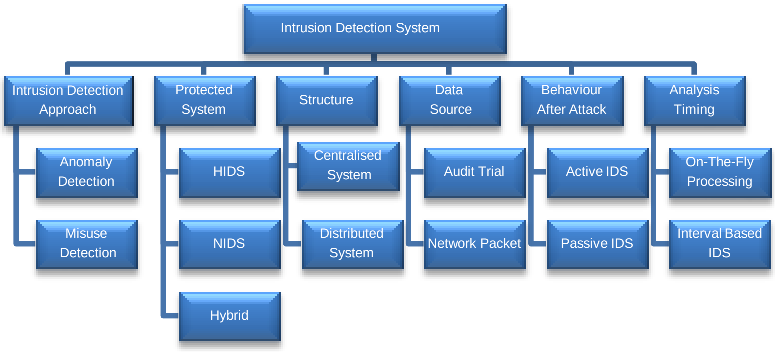
– *Anomaly detection:*

- Selecting the right set of system features to be measured is ad hoc and based on experience
- Unable to capture sequential interrelation between events

– *Misuse detection*:

- Known intrusion patterns have to be hand-coded
- Unable to detect any new intrusions (that have no matched patterns recorded in the system)

IV. ORGANIZATION OF IDS



The aim of an IDS is to inform the system administrator of any suspicious activities and to recommend specific actions to prevent or stop the intrusion In order to be able to implement these actions, the IDS must, among other tasks, analyze network traffic data in order to determine whether there is evidence of an attack, or whether the data are anomalous with respect to normal traffic. As for attack patterns, four categories were identified [22]:

Denial of Service (DoS) attacks, which prevent a computer from complying with legitimate requests by consuming its resources.

Probe attacks, which are scanning and polling activities that gather information on vulnerabilities for future attacks.

DOI: 10.18535/ijsrm/v5i6.33

Remote-to-local (R2L) attacks, which are local non-authorized access attempts from a remote machine.

User-to-root (U2R) attacks, which have the goal of obtaining illegal or non-authorized super-user or root privileges.

Intrusion Detection mechanism based on IDS are not only automated but also provides for a significantly elevated accuracy and efficiency. Unlike manual techniques, Data Mining ensures that no intrusion will be missed while checking real time records on the network. Credibility is important in every system. IDS are now becoming important part of our security system, and its credibility also adds value to the whole system. Data mining techniques can be applied to gain insightful knowledge of intrusion prevention mechanisms. They can help detect new vulnerabilities and intrusions, discover previous unknown patterns of attacker behaviors, and provide decision support for intrusion management.

V. **Data Mining**

*A. KDD (Knowledge Discovery in Database)***:**It is the process of identifying valid, useful and understandable patterns in data. Different Steps involved are: understanding the application domain, data preparation, data mining**,** interpretation, and utilizing the discovered knowledge. Data Mining is the automated extraction of previously unknown data that is interesting and potentially useful. Data mining is an iterative process that typically involves the following phases:

Phase I: Problem definition -A data mining project starts with the understanding of the problem, define the project objectives and the requirements. The project objective is then translated into a data mining problem definition. In the problem definition phase, data mining tools are not yet required.

Phase II: Data exploration-Data is collected, described, and explored. Identify quality problems of the data. In the data exploration phase, traditional data analysis tools, for example, statistics, are used to explore the data.

Phase III: Data preparation -Build the data model for the modeling process. Collect, cleanse, and format the data because some of the mining functions accept data only in a certain format. Create new derived attributes, for example, an average value. In the data preparation phase, data is tweaked multiple times in no prescribed order. Preparing the data for the modeling tool by selecting tables, records, and attributes, are typical tasks in this phase. The meaning of the data is not changed.

Phase IV: Modeling -Select and apply various mining functions. Some of the mining functions require specific data types. Assess each model. In the modeling phase, a frequent exchange with the domain experts from the data preparation phase is required. The modeling phase and the evaluation phase are coupled. They can be repeated several times to change parameters until optimal values are achieved. When the final modeling phase is completed, a model of high quality has been built.

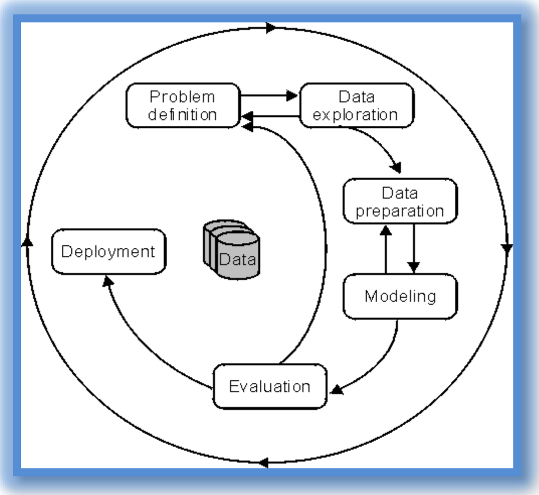
Phase V: Evaluation-Evaluate the model. If the model does not satisfy expectations, then go back to the modeling phase and rebuild the model by changing its parameters until optimal values are achieved. When you are finally satisfied with the model, then extract explanations and evaluate the following questions:

- Does the model achieve the objective?
- Have all the issues been considered?

At the end of the evaluation phase, decide how to use the data mining results.

Phase VI: Deployment -Use the mining results by exporting the results into database tables or into other applications. The following figure shows the phases for data mining (DM) process

Model.



.

B. Techniques of data mining

- *Classes*: Stored data is used to locate data in predetermined groups. For example, a restaurant chain could mine customer purchase data to determine when customers visit and what they typically order. This information could be used to increase traffic by having daily specials.
- *Clusters*: Data items are grouped according to logical relationships or consumer preferences. For example, data can be mined to identify market segments or consumer affinities.
- *Associations*: Data can be mined to identify associations and/or correlation relationships among large set of data items.
- *Sequential patterns*: Data is mined to anticipate behavior patterns and trends. For example, an outdoor equipment retailer could predict the likelihood of a backpack being purchased based on a consumer's purchase of sleeping bags and hiking shoes.
- *Decision trees:* Tree-shaped structures that represent sets of decisions. These decisions generate rules for the classification of a dataset. Specific decision tree methods include Classification and Regression Trees (CART) and Chi Square Automatic Interaction Detection (CHAID).
- *Rule induction*: The extraction of useful if-then rules from data based on statistical significance.
- *Data visualization:* The visual interpretation of complex relationships in multidimensional data. Graphics tools are used to illustrate data relationships.

VI. Approach

A .Objective of Study

- To develop an overall framework for defending against attacks and threats to computer system.
- To Identify analyze different data mining techniques best suited for developing IDS.
- To train the algorithm with the wide variety of parameters on various subsets of dataset.
- To build tools that will convert manually encoded intrusion patterns and profiles into learned rules.
  - To design and develop an intrusion detection system that would be accurate, low in false alarm and not easily cheated.
  - To refine the existed intrusion detection systems.

B. Statement of the research problem

Current IDS have a number of significant drawbacks [23]:
• Current IDS are usually tuned to detect known service level network attacks. This leaves them vulnerable to original and novel malicious attacks.
• Data overload: Another aspect which does not relate directly to misuse detection but is extremely important is how much data an analyst can efficiently analyze. That amount of data he needs to look at seems to be growing rapidly. Depending on the intrusion detection tools employed by a company and its size there is the possibility for logs to reach millions of records per day.
• False positives: A common complaint is the amount of false positives IDS will generate. A false positive occurs when normal attack is mistakenly classified as malicious and treated accordingly.
• False negatives: This is the case where an IDS does not generate an alert when an intrusion is actually taking place. (Classification of malicious traffic as normal)
Data mining can help improve intrusion detection by addressing each and every one of the above mentioned problems.

C. Methods

The main motivation behind using intrusion detection in data mining is automation. Pattern of the normal behavior and pattern of the intrusion can be computed using data mining. To apply data mining techniques in intrusion detection, we will use the following stages:

Stage I: Understanding the application domain: In depth knowledge is required to understand the application domain and to achieve the stated objective.

Stage II: Feature Selection: To select the subset of features from the collected data set that are used for creating useful result.

Stage III: Preprocessing: Data will be preprocessed and convert it into the format suitable for mining processing.

Stage IV: Data analysis and Techniques: Data analyzing involves detecting attacks and building a model using data mining technique. This process requires various tool and techniques and their usefulness for IDS will be evaluated.

Stage V: Interpretation and validation of discovered pattern: The result obtained will be compared with the current available Intrusion Detection System based on different criterion.

Stage VI: Evaluation and performance checking: New IDS will be assessed for several research issues such as performance, delay and many others to validate it.

D. Data analysis and Interpretation

We will use the available data set for IDS. Data mining techniques or frequently occurring pattern will be used to identify features to detect various attack categories. The types of analysis that can be possible for detecting attacks are:
-Pattern matching/Signature comparison of contents to detect malware signatures.
-Behavioral analysis of traffic rates to detect DOS attack.
-IP clustering analysis to determine significance of attack.
For Developing an IDS we will use following available tools like WEKA, MatLab, SPSS Clementine, DB Miner, R, RIPPER and explore them to make the best IDS.
We will apply different data mining approaches like classification, clustering, association rule, and outlier detection by using the above mentioned tools to analyze network data to gain intrusion related knowledge. The following are the list of techniques and their outcomes:
Clustering: Clustering discovers complex intrusions occurred over extended periods of time and different spaces, correlating independent network events. The sets of data belonging to the cluster are modeled according to pre-defined metrics and their common features. It is used to detect hybrids of attack in the cluster. Clustering is an unsupervised machine learning mechanism for finding patterns in unlabeled data with many dimensions.
Classification: Classification categorizes the data records in a predetermined set of classes used as attribute to label each record; distinguishing elements belonging to the normal or abnormal class. This technique has been popular to detect individual attacks but has to be applied with complementary fine-tuning techniques to reduce its demonstrated high false positives rate. Classification approach can be useful for both misuse detection and anomaly detection, but it is more commonly used for misuse detection. In intrusion detection, data mining classification can be applied to a standard set of malicious virus and benign executable using derived features. Secondly, RIPPER, Naive Bayes and multi-Bayes classifiers can be used to detect malicious virus code. A decision Tree can be exploited to formulate genetic algorithm to create rules that match a set of anomalous connection.
Outlier Detection: Outlier detection is very useful in anomaly based intrusion detection. With outlier detection approach, we can detect novel attack/intrusion by identifying them as deviation from normal behavior.. Outlier detection approaches can useful for detecting any unknown attacks. This is the primary reason that makes outlier detection a popular approach for intrusion detection systems.
Association Rule: Use of association rule in analyzing network data in intrusion detection is useful in many ways. Basic steps for incorporating association rule for intrusion detection as follows. (1) First network data need to be formatted into a database table where each row is an audit record and each column is a field of the audit records. (2) There is evidence that

intrusions and user activities shows frequent correlations among network data. For example, one of the reasons that "program policies", which codify the access rights of privileged programs, are concise and capable to detect known attacks is in that the intended behavior of a program, e.g., read and write files from certain directories with specific permissions is very consistent. These consistent behaviors can be captured in association rules. (3) Also rules based on network data can continuously merge the rules from a new run to the aggregate rule set of all previous runs. Thus with the association rule, we get the capability to capture behavior in association rule for correctly detecting intrusion and hence lowering the false alarm rate.

VII. **Conclusion**

In this paper, various data mining techniques are described for the IDS. This review will be helpful to researchers for gaining a basic insight of various approaches for the intrusion detection. Every day new unknown attacks are witnessed and thus there is a need of those approaches that can detect the unknown behavior in the data set stored, transferred or modified. Our continuing objective is to develop an overall framework for defending against attacks and threats to computer systems.

References

[1] Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, Jonathan Tivel,"Data Mining for Network Intrusion Detection: How to Get Started", The MITRE Corporation 1820 Dolley Madison Blvd.

[2] Tao peng, Wanli Zuo, Data Mining For network Intrusion Detection System in Real Time, August 2005

[3] Norbik Bashah, Idris Bharanidharan Shanmugam and Abdul Mahan Ahmed,"Hybrid intelligent Intrusion Detection System." proceedings of world academy of science, engineering and technology volume 6 June 2005 issn 1307-6884

[4] HuZheng Bing, Shirochin V.P,"Data Mining Approaches For Signature Search In Intrusion Detection ", IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 5-7 September 2005, Sofia, BulgariaI.

[5] P.J. Stanford, D.J. Parish, J M Sandford, " Detecting security threats in network core using Data Mining techniques", IEEE 2006.

[6] QU Zhiming, WANG Xiaoli, "Study of Rough Set and Clustering Algorithm in Network Security Management", International Conference on Network Security, Wireless communication and trusted computing, IEEE, 2009.

[7] Hu Zhengbing1,2, Li Zhitang1,Wu Junqi2¸ "A Novel Network Intrusion Detection System(NIDS) Based on Signatures Search of Data Mining", 2008 Workshop on Knowledge Discovery and Data Mining

[8] Stefano Zanero, Sergio M. Savaresi," Unsupervised learning techniques for an intrusion detection system", *SAC'04* March 1417 ,2004, Nicosia, Cyprus.

[9] Hongyu Yang, Feng Xie, and Yi Lu,"Clustering and Classification Based anomaly Detection", FSKD 2006, LNAI 4223, pp. 1082–1091, 2006.

[10] Liu Dihua, Wang Hongzhi,Wang Xiumei,"Data mining for intrusion detection ",IEEE,2001.

[11] Wenke Lee, Salvatore J. Stolfo,Kui W. Mok," A Data Mining Framework for Building Intrusion Detection Models" in Proceeding of the IEEE Symposium on Security and Privacy,1999. pp. 153 -157.

[12] Sattarova Feruza Yusufovna," Integrating Intrusion Detection System and Data Mining", 2008 International Symposium on Ubiquitous Multimedia Computing.

[13] Wenke Lee, Salvatore J. Stolfo,Kui W. Mok" A Data Mining Framework for Building Intrusion Detection Models", IEEE,2000.

[14] Ye Changguo, Wei Nianzhong, Wang Tailei, Zhang Qin, Zhu Xiaorong," The Research on the Application of Association Rules Mining Algorithm in Network Intrusion Detection", 2009 First International Workshop on Education Technology and Computer Science.

[15] Joong-Hee Leet, Jong-Hyouk Leet, Seon-Gyoung Sohn+, Jong-Ho Ryu+, and Tai-Myoung Chungt," Effective Value of Decision Tree with KDD 99 Intrusion Detection Datasets for Intrusion Detection System",IEEE 2008.

[16] Website: www.itsecurity.com/features/intrusion-detection-030807

[17] Website: www.acm.org/crossroads/xrds11-1/csid.html

[18] Website: www.acm.org/crossroads/xrds2-4/intrus.html

[19] Website : http://discovery.csc.ncsu.edu/Courses/ csc774-S03/ IDTechniques.pdf

[20] Yanjie Zhao,Network intrusion detection system model based on data mining 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD),Year: 2016

[21] Reddy E., Reddy V., Rajulu P., "A Study of Intrusion Detection in Data Mining", Proceedings of the World Congress on Engineering 2011 Vol III WCE 2011, July 6 - 8, 2011, London, U.K

[22] Eszter Katalin BOGNÁR ,Data Mining in Cyber Threat Analysis – Neural Networks for Intrusion Detection, AARMS Vol. 15, No. 2 (2016) 187–196

[23] QIU, C., SHAN, J.: Research on Intrusion Detection Algorithm Based on BP Neural Network. International Journal of Security and its Applications, 9 4 (2015) 247–258