A Survey on Anomaly Based Host Intrusion Detection System

IOP Conf. Series: Journal of Physics: Conf. Series **1000** (2018) 012049 doi:10.1088/1742-6596/1000/1/012049

A Survey on Anomaly Based Host Intrusion Detection System

Shijoe Jose[1], D.Malathi[2], Bharath Reddy[3], Dorathi Jayaseeli[4]

Department of Computer Science and Engineering, SRM University, Kattankulathur.

shijoe8@gmail.com, malathi.d@ktr.srmuniv.ac.in, bharathreddy.s@ktr.srmuniv.ac.in, dorathijayaseeli.jd@ktr.srmuniv.ac.in

Abstract. An intrusion detection system (IDS) is hardware, software or a combination of two, for monitoring network or system activities to detect malicious signs. In computer security, designing a robust intrusion detection system is one of the most fundamental and important problems. The primary function of system is detecting intrusion and gives alerts when user tries to intrusion on timely manner. In these techniques when IDS find out intrusion it will send alert massage to the system administrator. Anomaly detection is an important problem that has been researched within diverse research areas and application domains. This survey tries to provide a structured and comprehensive overview of the research on anomaly detection. From the existing anomaly detection techniques, each technique has relative strengths and weaknesses. The current state of the experiment practice in the field of anomaly-based intrusion detection is reviewed and survey recent studies in this. This survey provides a study of existing anomaly detection techniques, and how the techniques used in one area can be applied in another application domain.

1. Introduction

Intrusion detection refers to detection of malicious activity (break-ins, penetrations, and other forms of computer abuse) in a computer related system. These malicious activities or intrusions are interesting from a computer security perspective. Intrusion detection systems are one of the major parts of computer security. An Intrusion Detection System (IDS) is a system security technology for detecting vulnerability exploits against a computer system that analyses Network / system functions. Different categories of IDS include Host-based IDS (HIDS), Network-based IDS (NIDS), (HIDS), and Wireless IDS [1]. There is Hybrid IDS which combines various IDS categories. Host-based IDS monitors the activities of a single host and detects if any malicious activity happen. HIDS mainly monitors the process activities and ensure security policies of system files, system logs and registry keys. Anomaly detection techniques are useful in intrusion detection systems since an intrusion activity is different from the normal activity of the system. Host based intrusion detection systems run on individual systems which includes the techniques for collecting and analyzing the information on a particular system [3].

HIDS is different from Anti-virus. Anti-virus monitors all the activities inside the system but not sufficient to detect and analyze some system specific attacks like buffer overflow attacks in memory, memory leakage, malfunctioning of operating system process but HIDS collect and analyze system data such as status of file system, system call pattern and system events to detect any anomaly has occurred or not. HIDS system uses audit trail information and system logs to detect malicious activities inside the system. The intrusions can be detected by recognizing the sequence of anomalies in system traces. The malicious programs, malicious behavior and security policy violations collectively form the anomalous

subsequences. The normal and anomalous behavior can be identified by analyzing the alphabets in the co-occurrence of events. The alphabet represents the individual system calls and the data will be in sequential form. These calls could be generated by programs or by users. The major advantage of host-based systems is that it can keep track of user specific information. [3], [4].

HIDS can detect an improper use of company resources. If the activity pattern is similar to past attacks, the activity with that company resource can be stopped, thus prevent the attack. Host-based intrusion detection system are designed to monitor, detect, and respond to user system activity and attacks on a given host [3]. Some robust tools offer centralized audit policy management, supply data forensics, statistical analysis and evidentiary support, as well as provide some measure of access control. Host-based intrusion detection is best suited to combat internal threats and abnormal behaviors in the local networks, because of its ability to monitor and respond to specific user actions and file accesses on the host.Anomaly detection refers to the methods of identifying items, patterns and events in data that normally not occur in normal behavior of system process. These malicious data patterns are also known as outliers, exceptions, aberrations, surprises, discordant observations, peculiarities or contaminants in different application domains. In anomaly detection the most commonly used terms are anomalies and outliers. Anomaly detection is applicable in a variety of domains such as fraud detection, system health monitoring, fault detection, event detection in sensor networks, detecting ecosystem disturbances, intrusion detection for cyber-security and military surveillance.

2. Categories of intrusion detection systems

Intrusion detection systems can be classified based data collection methods into two categories as Host-based and Network-based. A network-based intrusion detection system (NIDS) is used to monitor and analyze data from network traffic to protect a system from network-based attacks. A Host-based intrusion detection system (HIDS) monitors and analyzes data from system's log files that runs on a particular system. Intrusion detection systems can also be classified based on intrusion detection techniques into three categories as misuse- detection, specification-based detection and anomaly-based detection.

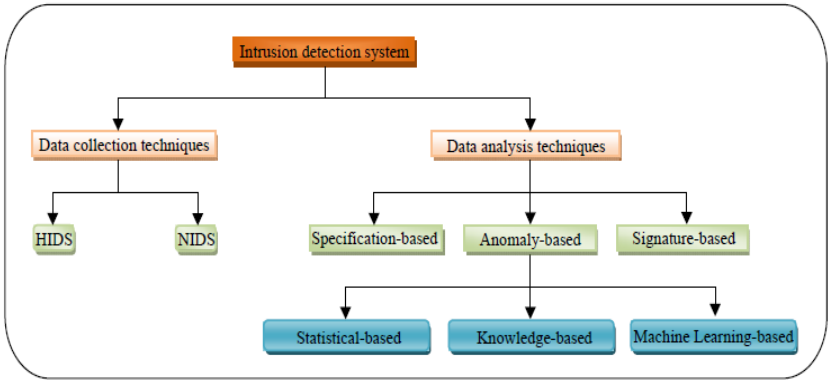

Figure 1. Classification of intrusion detection system

2.1. Signature based detection

A Signature based Intrusion Detection Systems references a stored collection of previous attack signatures such as specific patterns, known malicious instruction sequences, byte sequences in network traffic and known system vulnerabilities. Each intrusion gives a specific maliciousssignaturessuch as failed logins, failed attempt to run an application, failed file and folder access and nature of data packets. Signature based intrusion detection system uses these signatures to detect and prevent the same attacks in the future. The main advantage of signature based intrusion detection system is that it is very easy to develop and understand if we know the behaviour of network traffic and system activity. For example, to exploit particular buffer-overflow vulnerability the signature based intrusion detection system uses a signature that looks for particular strings. On modern systems pattern matching can be more efficiently

performed with minimum amount of computational complexity. For example if the system can only communicate via DNS, ICMP and SMTP it can enable the specific signatures and disable all other signatures.

The main disadvantages of signature-based intrusion detection systems are the collection of signatures must be continually updated and maintained and signature-based intrusion detection systems may fail to identify unique attacks. Signature-based intrusion detection systems work well against attacks with fixed behavioral pattern, but it is hard to works with self-modifying behavioural characteristics. Intrusion detection is further difficult when the user uses advancing exploit technologies such as payload encoders, encrypted data channels and nop generators that permit malicious users. To works against these kinds of attacks the collection of signatures must be continually updated and maintained which decreases the efficiency of the signature based systems also reduces the performance of the system. To address this issue modern systems which uses signature based intrusion detection system uses many IDS engines with multi processors and multi Gigabit network cards. The efficiency of the system determine by the speed of creation of the new signatures between the developers and attackers.

2.2. Anomaly based detection

Anomaly based Intrusion Detection Systems (IDS) references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered. Events in an anomaly detection engine are caused by any behaviors that fall outside the predefined or accepted model of behavior.

The major drawback of anomaly detection system is the difficultly of defining rules. All protocol being analysed must be well defined, implemented and tested for accuracy. The rule defined process for various protocols is also compoundedbydifferencesinvendorimplementations. Defining rule in customized protocols needs great efforts. Detailed information of normal network behaviorneeds to be collected and maintained by system memory for detection to occur correctly. Once the behavior is defined and rules for the protocol have been well structured and built the system can scale more quickly and easily than the signature-based model and works well for anomaly detection. There is a chance for malicious behavior gets unnoticed if it is considered as a normal usage patterns. For example a directory traversal activity with server, which complies with network protocol, does not trigger any payload or bandwidth limitation flags or any other flags. However, anomaly detection has an advantage over signature-based systems to detect new automated worms, in that a new attack for which a signature does not exist can be detected if it falls out of the normal traffic patterns. When a new system is infected with a worm it usually starts scanning for other vulnerable systems at an abnormal rate flooding the network with malicious traffic, thus triggering a network bandwidth abnormality rule. If any abnormal behaviour or intrusive activity occurs in the computer system which deviates from system normal behaviour then an alarm is generated. So this have follows a continuous monitoring process.

The key advantage of anomaly detection is that it does not necessitate preceding information's or data of intrusion, so it can thus detect new intrusions. Based on behavior model processing type of the system anomaly based detection techniques can be classified in to three groups as statistical-based, knowledge-based and machine learning-based.

3. Anomaly detection

Anomaly detection is a technique used to detect unusual patterns that do not conform to normal behavior. Anomaly detection has many applications in various domains varies from intrusion detection to system health monitoring and from fraud detection in credit card transactions to fault detection in operating environments.

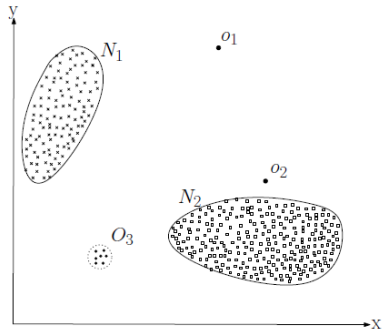

Figure 2. A simple example of anomalies in a 2-dimensional data set.

Figure 2 illustrates a simple example of anomalies in a 2-dimensional data set. The data has two normal classified regions, N1 and N2. Points that are sufficiently far away from these regions are anomalies.

The traces of malicious activities used to reflect in the data, careful analysing of this data reveals the presence of the intruder. The anomaly traces in the data have common characteristics which makes anomaly detection possible to analyst.

3.1. Challenges in anomaly detection

In data domain anomaly can be seen as a data pattern which does not belong to normal data pattern therefore a region can be created to represent normal behavior, any data patterns which do not belongs to this region can be classified as intrusion. But several factors make this apparently simple approach very challenging:

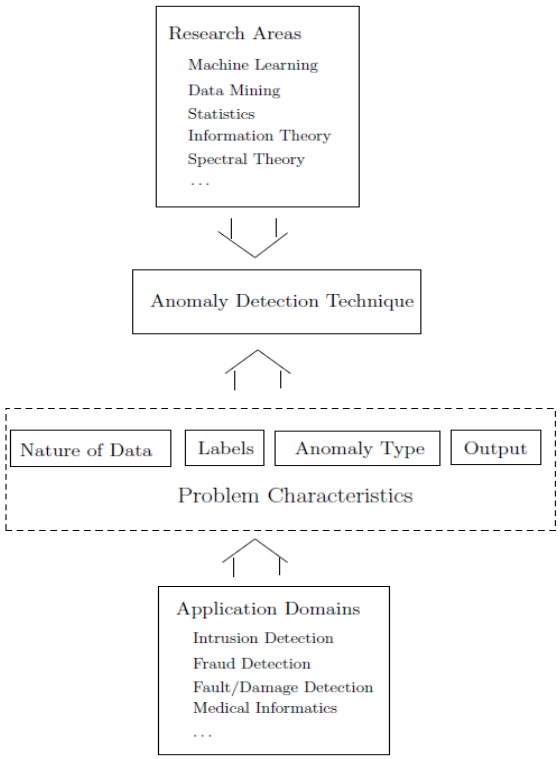

Figure 3. Key components associated with anomaly detection technique.

Defining a normal region which includes all possible data patterns that are normal is very difficult. Differentiate data patterns near the boundary regions between normal behavior and anomalous behavior

is difficult. The data patterns close to the boundary classified as normal can be a malicious data pattern. When anomalies are the result of malicious actions, the malicious adversaries often adapt themselves to make the anomalous observations appear like normal, thereby making the task of defining normal behavior more difficult. The current notion used to represent the normal behavior in a domain might not be sufficient to represent the same in the future. The notion used to represent normal behaviorand anomaly is different for different application domains. For example, in the medical domain small deviations in the normal behavior data pattern might be an anomaly, while similar deviation in the stock market domain might be considered as normal. Hence anomaly detection technique developed for one domain is not directly applicable for another domain. The labeled data used to train the models for anomaly detection might not be sufficiently available. The normal data pattern may contain noises hence it is very challenging to differentiate the actual anomalies and normal data patterns.

The existing anomaly detection systems often used various factors such as type of anomalies to be detected, availability of labeled data and nature of the data to generate specific formulation of the problem. The factors are different for different application domains in which the anomalies need to be detected.To develop a well formed problem formulation various concepts from disciplines such as data mining, machine learning, natural language processing, information theory and statistics have been adopted.Based on type of processing various models are used they are: Statistical based, Statistical Moments or mean and standard deviation model, Machine Learning based, Cognition based, Multivariate Model, Univariate Model, Markov Process or Marker Model, Description script Model, Operational or threshold metric model, Genetic Algorithm model, Time series Model, Finite State Machine Model, Adept System Model, Neural Network Model, Bayesian Model, Fuzzy Logic Model, Computer Immunology based, User Intention based.

3.2. Anomaly detection approaches

Statistical anomaly based intrusion detection system, Data mining based approach, Knowledge based detection technique and Machine learning based detection technique are commonly used for anomaly detection.

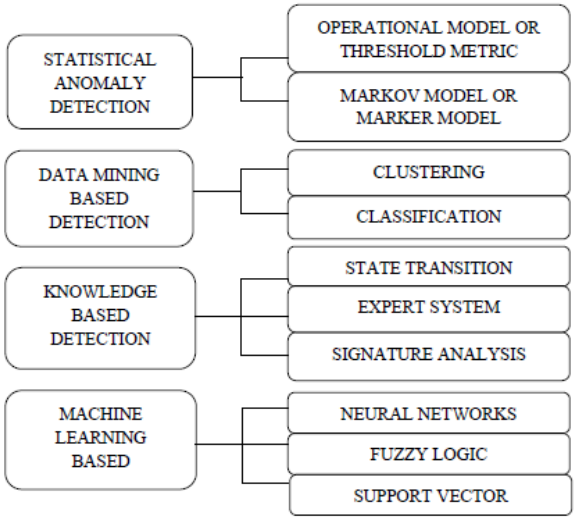

Figure 4. Taxonomy of Anomaly based Intrusion Detection System [12].

3.2.1. Statistical anomaly based intrusion detection system. The statistical anomaly based intrusion detection system uses statistical analysistoanalyze the user or system behaviour by checking the values of various variables such as login session variables, resource overflow flags and various timers periodically. Find precise threshold values and decrease false alarm rate is crucial in this approach. In Statistical Anomaly based intrusion detection system (SABIDS) the malicious behavior is differentiate from normal behavior by using statistical properties such as mean and variance of normal activities and

statistical test which determine the deviation of activities from normal behavior [13].A scoring mechanism is used to score an anomalous activity, when the calculated score exceeds certain threshold value then an alarm will be generated. InSABIDSto detect any kind of anomaly it first creates profiles for current activities and normal activities. Next the created profiles are compared to detect any kind of deviation from the normal behavior. The main advantage of SABIDS is that it does not require prior knowledge of security issues and it can detect new attacks. This approach is well suitable for finding malicious actions occurred in long duration of time and this approach can indicate the chances for denial-of-service attacks. In statistical methods the behaviors are to be modeled using accurate statistical distributions but for most of the application domains it is difficult to represent the problem formation using statistical methods. Many statistical anomaly detection methods require assumption based parameters of a process which cannot be suitable for accurate anomaly detection systems [14, 15, 16].SABIDS can be classified into Operational models and Markov process models[17, 14].

Markov process modelanalyzes the event sequences for determine the regularity of particular events by using an event counter. A state transition matrix stores each event states and this matrix is used to predict the probability of occurrence of a succeeding event.This model is very useful for a system which keeps the state of each event [19]. Markov model used in two main approaches as Markov chain and hidden Markov models [20].The Markov chain maintains a record of system states by examine the system at regular interval of time. When a system state change happens it calculates the probability of new system state and if the probability is less than it is considered as anomaly [13]. The Hidden Markov model is similar to a dynamic Bayesian network. This model can be used to model a system which contains finite system states, the state changes are hidden to the user of the system and the generated state is always dependent on the immediate previous state only.

*3.2.2. Data mining approach.*Often IDS is unable to efficiently detect insider attacks and also needs to keep large amount of data to analyze current state of the system with all possible attacks. Data mining approach is useful for extracting patterns from large data store. This approach reduces storage of large amount of data by creating the metadata useful for anomaly detection [21, 22]. It allows analysts to reduce false alarm by removes normal activity from alarm data. Various data mining approaches have also been used in order to detect known and unknown attacks more accurately. The data mining based approach can be classified into Clustering and Classification models.

Clustering is a method of grouping objects as clusters in such a way that objects in the same cluster are more similar to each other than to those in other clusters. It is an unsupervised method to detect patterns similarity. K-means clustering is the leading algorithms used for clustering. In IDS normal patters are gathered in a cluster and patterns that far away from the cluster are considered as anomalies [23].

Anomaly detection can be represented as a classification problem and classification algorithms are used for anomaly detection. Classify the attacks detected by anomaly-based detection systems is a significant task.The main objective of a classification method used for anomaly detection is to learn the characteristics of various classes. In this learning process the IDS uses labeled training data sets. After learning phase the IDS can be able to classify the new or previously unseen data.The main advantage of classification algorithms is that it can efficiently distinguish the classes of data. The classification-based techniques are comparatively fast and each new activity needs to be compared only with existing classes of data.

3.2.3. Knowledge based detection. Both signature based intrusion detection systems and anomaly based intrusion detection systems can use the knowledge based detection approach. Knowledge based detection uses the gathered knowledge about the attacks and this knowledge can be used to detect any attacks or system vulnerabilities. If the system does not have the knowledge about a particular attack then it is unable to identify the attack hence the system require significant amount knowledge of several of attacks. The main advantage of knowledge based detection is that this type of systems normally produces less false alarm rate and produces more accurate results. The regular updating of knowledge

repository is required for this type of systems [25]. The knowledge based detection technique can be classified intoState transition analysis, Expert system and Signature analysis.

State transition analysis was initially proposed and implemented in UNIX by Porras and Kemmerer [26]. In this state transition analysis the attacks are defined as a sequence of states with a goal state. These states are representing various activities of an intruder. The states are graphically represented as a state transition diagram.The intrusion activity changes the state of a system and propagates the state to a specific compromised system state. The key actions of system penetration are identified and listed. State transition analysis diagrams are useful to recognize the malicious state transitions occurring while the intruder penetrates the system security [28].

Expert systems are rule based systems. These systems are mainly used in knowledge-based IDS. The expert system contains set of facts, rules and inference methods. Each event occurred in the system is translated in to corresponding facts and rules. The inference methods are able to generate conclusions from the existing rules and facts. The attached semantics structure to each event will increase the level of event data abstraction [29]. Both signature based intrusion detection systems and anomaly based intrusion detection systems can use the expert system approach.

Signature analysis contains the same knowledge-acquisition approach as in an expert system, but the way of knowledge acquired is different. The exact evidence of every attack is available in the audit trail and this information is consolidated as semantic description of the attack. For example, the unique sequence of audit events and data patterns created during an attack contains the attack circumstance information. This technique can be efficiently implemented in different commercial application domains and products such as Haystack [30].Systems which use this technique to detect new attacks and system vulnerabilities need frequent knowledge updates.

*3.2.4. Machine learning based detection.*Machine learning is a method of data analysis, in which the system learns and gathers knowledge from the tasks performed by the system. The system will improve the performance by using the knowledge learned from the previous results it means that machine learning provides the ability to a system to enhance the execution strategy [31]. The systems with machine learning techniques can be used for various applications but these types of systems are expensive. In many application context the machine learning technique uses methods similar to that of the statistical techniques and data mining techniques [20]. Machine learning technique can be classified into Neural networks, Fuzzy logic approach and Support vector machines.

Neural Networks machine learning technique use neural network concepts acquire the ability to use the sequence of commands by the user to anticipate for the next command. The neural network model is well suitable for developing user behavior model since it does not require the explicit information on user behavior. A well trained neural network with back propagation and feed forward mechanism works efficiently as signature matching system [32].Multilayer Perceptron's, Radial Basis Function-Basedneural networks are used for anomaly based intrusion detection systems. IDS using neural network consists of three phases [28].In first phase the audit log is analyzed to obtain sufficient training data. Next phase is to train the neural network for understand the each user behavior. In the final phase each user behavior is compared with trained data to detect malicious behavior of the user if there exist any such user activities an anomaly is alarmed.

Fuzzy logic is useful for many applications. It can produce acceptable reasoning of data and helps to deal with the uncertainty in the data set. The various techniques using fuzzy logic have been used since 1990's [33]. Fuzzy logic is an important technique used in anomaly based intrusion detection systems. The fuzzy logic system can handle large volume of input data which may also contain uncertain parameters. The systems that use fuzzy logic can reduce the size of input data using data mining techniques and extract features from the given input parameters. There are many the Fuzzy Intrusion Recognition Engines available which uses fuzzy sets and fuzzy rules [22].There are many characteristics of fuzzy logic technique that makes the techniques suitable to be correlated with intrusion detection system [34, 35]. The many parameter used for intrusion detection are fuzzy in nature. For example, user activity frequency, CPU usage time etc.

Support vector machines: Support vector machines (SVMs) uses supervised learning approaches. SVMs are suitable to analyze data used for classification. With the labeled training data SVM can outputs an optimal classification results. The concepts used in SVM are relatively simple. In SVM initially it maps parameters in the given input vector into a multi-dimensional space graph. After all parameters are mapped in a well-structured feature space and then the optimal separation can be done. The support vector machines is efficient for anomaly detection since the SVM uses calculated separating hyper-plane for the classification rather than analyzing the entire training samples. Usually SVM classifier is used for binary classification it means that the classifier classify the training set into two different classes.

3.3. Genetic Algorithm in optimization

Genetic Algorithm belongs to wide group of evolutionary algorithms. These algorithms are commonly used to produce optimal solutions to optimization and search problems. Many high complexity real world applications use genetic algorithms to find optimal solutions.GA has been widely used for optimal feature selection from the large data set and it provides a good framework for many integrated application environments.

4. Research challenges

Intrusion Detection System is important for any organization. Many researches going on for enhancing IDS technology. Nowadays IDS technology is highly automated in case of any malicious activities happened, the IDS notify the administrator and it can also able to take actions to prevent further attacks. The maintenance of IDS logs are very important, the logs are monitored regularly for analyzing the activities. For implementing efficient IDS and decrease false alarm rate, it is mandatory to define baseline policy strategies. Many intrusion detection systems are not able to handle false positive results.

Many researches are going on for the development of real time intrusion detection systems with virtualization technologies. Virtualization technologies are capable of handling various aspects of intrusion detection system. In most cases customization in the virtualization can be possible. Host based intrusion detection systems are using the advantages of modern development in real time intrusion detection system. One of the main challenges in intrusion detection system is to reduce the usage of computational power and memory consumption. Even though there are many enhancements made in intrusion detection system, false positive rates is not sufficiently low for many applications. The HIDS is considered as an important part of intrusion detection systems. HIDS provides mechanisms to detect attacks prevent malicious activities and restore the system into a secured state. To reduce the false positive alarm rate the more manual input is required in HIDSs unless the inputs are semantically balanced. If HIDS is designed efficiently it can prevent the attacks like outgoing denial-of-service attacks. When the HIDS detects outgoing denial-of-service attacks it informs the administrator that the system or the resources of the system are being compromised. The data traces and the basic system properties are used for detecting any malicious activity in the host system.

HIDS can be a part of a large intrusion detection system and can act as a source of basic information. There for design an efficient self-learning HIDS is a major challenge in intrusion detection domain.

More research is needed to develop a HIDS which utilizes trusted platform modules and cryptographic technologies.

Another major research challenge is to develop intrusion detection system for smart phones and tablets. Providing good intrusion detection rate under a compromised operating system is a challenging task. In shared system environment the HIDS need to be work as an independent module since the shared parameters may cause the attack. The ability of a HIDS to recover quickly from attacks is dependent on the attacks. In HIDS the monitoring of various events and process are performed in virtual machine.

5. Conclusion

The main objective of this paper is to provide an overview of various aspects of anomaly based host intrusion detection system. Nowadays HIDS are becoming more important and plays a major role in

most of the intrusion detection systems. Various methods of anomaly detection and their merits and demerits have been reviewed. It is observed that HIDS with various data mining algorithms and cluster based approaches can give more accurate results with less false alarm rates. Hybrid solution of network based and host based HIDS can also be used in various application domains. The selection of intrusion detection systems is dependent on the requirements of organizations. This survey discussed multiple ways of the formulation of anomaly detection problem. The proper theoretical understanding of various anomaly types will help to develop better intrusion detection systems. It is observed that anomaly detection domain has various promising research directions, many anomaly detection methods requires large amount of test date set for detecting anomalies. Major directions towards the researches in anomaly detection are to develop efficient anomaly detection systems which work with complex systems (eg. aircraft system) and interaction between various components in real time.

References

[1] Syed ShariyarMurtaza, WaelKhreich, AbdelwahabHamou-Lhadj and Stephane Gagnon 2015 A trace abstraction approach for host-based anomaly detection *Computational Intelligence for Security and Defense Applications (CISDA)* pp. 1-8
[2] Bukac V., Tucek P and Deutsch M. 2012 Advances and Challenges in Standalone Host-Based Intrusion Detection Systems. *In: Fischer-Hübner S., Katsikas S., Quirchmayr G. (eds) Trust, Privacy and Security in Digital Business. TrustBus*
[3] V. Jyothsna and V. V. Rama Prasad 2011 A Review of Anomaly based IntrusionDetection Systems *International Journal of Computer Applications* vol 28
[4] Jiankun Hu and Xinghuo Yu 2009 A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection *IEEE Network Journal* vol. 23
[5] DavoodKheyri and MojtabaKarami 2012 A Comprehensive Survey on Anomaly-Based Intrusion Detection in MANET *Computer and Information Science*vol. 5
[6] Asmaa A and Sharad G 2011Importance of Intrusion Detection System (IDS) *International Journal of Scientific & Engineering Research*vol.2
[7] Parvathi Devi and Siva Prasad 2012 Study of Anomaly Identification Techniques in Large Scale Systems*International Journal of Computer Trends and Technology*vol.3
[8] Varun C, Arindam B and Vipin K 2009 Anomaly Detection: A Survey *ACM Computing Surveys*vol. 41
[9] Gideon Creech and Jiankun Hu. 2014 A semantic approach to host-based intrusion detection systems using contiguousanddiscontiguous system call patterns*IEEE Transactions on Computers* vol63 pp 807–819
[10] XuanDau Hoang, Jiankun Hu, and Peter Bertok 2003 A multi-layer model for anomaly intrusion detection using program sequences of system calls. *In Proc. 11th IEEE Intl. Conf. Citeseer*
[11] Lokendra Singh Parihar and AkhileshTiwari 2016 Survey on Intrusion Detection Using Data Mining Methods *International Journal for Science and Advance Research in Technology*, vol 2
[12] Kymie Tan and Roy A Maxion 2003 Determining the operational limits of an anomaly-based intrusion detector*IEEE Journal on Selected Areas in Communications*vol 21 pp 96–110
[13] Christina Warrender, Stephanie Forrest, and Barak Pearlmutter 1999 Detecting intrusions using system calls: Alternative data models.Proceedings of the 1999 IEEE Symposium on Security and Privacypp 133–145
[14] Qayyum, A.; Islam, M.H.; Jamil, M 2005 Taxonomy of statistical based anomaly detection techniques for intrusion detection*Proceedings of the IEEE Symposium on Emerging Technologies* pp 17-18
[15] ShikhaAgrawal and JitendraAgrawal 2015 Survey on Anomaly Detection using Data Mining Techniques *Procedia Computer Science*, vol 60 pp 708-713
[16] James C and Jay HA 1996 Comparative Analysis of Current Intrusion Detection Technologies*Proceedings of Technology in Information Security Conference (TISC)*, pp. 212-218
[17] Dorothy D 1987 An Intrusion-Detection Model *IEEE Transactions on Software Engineering*vol13

pp. 222, 232
[18] Vasilios S and Fotini P 2006 Application of anomaly detection algorithms for detecting SYN flooding attacks*Elsevier, Computer Communications* vol. 29 pp 1433, 1442
[19] Li Yang and Guo Li 2007 An active learning based TCMKNN algorithm for supervised network intrusiondetection, *Elsevier, Computers & Security* pp 459–467
[20] Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel M and Enrique V 2009Anomaly-based network intrusion detection: Techniques, systems and challenges*computers & security*vol 28 pp 18, 28
[21] Narayana Prasad, SrividhyaReddy 2011 DataMining Machine Learning Techniques – A Study on Abnormal Anomaly Detection System *International Journal of Computer Science and Telecommunications*vol. 2
[22] Dickerson, John E, Julie D 2000 Fuzzy network profiling for intrusion detection*In 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS), Atlanta, GA* pp. 301, 306
[23] Jian P., Shambhu U., Faisal F., Venugopal G 2004 Data Mining for Intrusion Detection – Techniques, Applications and Systems*Data Mining Techniques for Intrusion Detection and Computer Security, University at Buffalo, New York*
[24] S. Chebrolu, A. Abraham, and J. P. Thomas 2005 Feature deduction and ensemble design of intrusion detection systems*Comput. Secure.*, vol. 24pp. 295–307
[25] Herve D.; Marc D.; Andreas W 1999 Towards a Taxonomy of Intrusion Detection Systems", *Elsevier, Computer Networks*, vol. 31, pp. 805, 822
[26] Phillip A.; Porras; Alfonso V 1998 Live traffic analysis of tap/IP gateways*Proceeding ISOC Symposium on Network and Distributed System Security*, *San Diego, CA*
[27] Koral I., 1993 Ustat: A real- time intrusion detection system for Unix*Proceeding IEEE Symposium on Research in Security and Privacy, Oakland, CA*, pp. 16, 28
[28] Biermann, Elmarie; Elsabe C., Lucas V 2001 A comparison of Intrusion Detection systems", Elsevier, *Computers & Security*vol. 20, pp. 676, 683
[29] Lunt, Teresa F., Jagannathan 1988 A prototype real-time intrusion detection expert system*Proceeding of Symposium on Security and Privacy, Oakland, CA*, pp. 59, 66
[30] LeventKoc, Thomas A. Mazzuchi, ShahramSarkani. 2012 A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. *Expert Systems with Applications*vol 39pp 13492–500.
[31] Animesh P.; Jung-Min P 2007 An overview of anomaly detection techniques: Existing solutions and latest technological *trends Elsevier, Science Direct, Computer Networks*, vol. 51, pp. 3448, 3470
[32] Sreenath.M, 2014 A Comprehensive Review on Intrusion Detection Systems, *CiiT International Journal of Networking and Communication Engineering* vol 6
[33] Esra N. Yolacan, David R. Kaeli 2016 A Framework for Studying New Approaches to Anomaly Detection, *International Journal of Information Security Science, E.N. Yolacan* vol.5
[34] SumalathaPotteti, NamitaParati 2015 A Review on Hybrid Intrusion Detection System using TAN & SVM*IPASJ International Journal of Computer Science (IIJCS)* vol 3
[35] Abhaya, K. Kumar, R. Jha and S. AfrozData Mining Techniques for Intrusion Detection: A Review *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3 pp. 6938- 6941
[36] Eskin, Eleazar; Andrew A., Michael P., Leonid P., Sal S 2002 A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data*In D. Barbar and S.*