Review on Anomaly based Network Intrusion Detection System

Rafath Samrin
Computer Science and Engineering
ISL Engineering College
Hyderabad, India

D Vasumathi
Computer Science and Engineering
JNTUH
Hyderabad, India

***Abstract*— In computer system and network, Intrusion detection is an important research area. A lot of mechanisms are available for detect the network intrusion, but that is not able to identify the new kind of attacks. Various techniques have already been implemented for finding and categorizing intrusions. The Intrusion Detection system (IDS) is two types, namely Network based IDS and Host IDS (HIDS). The manual classification of network data inspection is time consuming task, expensive as well as repetitive job. IDS mechanism is very helpful to find the network attacks and anomalies. In IDS, data mining methods is broadly used for extracting useful information from the massive amount dataset. This paper presents the investigation of different techniques and intrusion classification on KDD Cup 99 dataset. So, by classifying the different network issues a new and effective technique is implemented which can categorize and identify intrusions in the KDD Cup 99 dataset.**

Keywords—Anomaly Detection; Classification; Clustering; Intrusion Detection System; Network based Intrusion detection system; Signature based Detection;

I. INTRODUCTION

As internet is growing rapidly security is the vital aspect in the computer networks. IDS is very helpful and act as a safeguard for data integrity, confidentiality and system availability for different kinds of attacks [1]. Firewalls and IDS are primary elements of the security framework [2, 3]. An IDS is one of the framework security foundations that attempts to identify harmful activities, for example, Denial of Service (DOS) attacks and port scans by observing and investigating activities occurring on systems and networks. IDS includes two types Host-based (HIDS) and Network-based (NIDS) approaches [4, 5]. HIDS is the primary sort of IDS, its fundamental capacity is internal observing (inside a computer or machine), yet numerous variations of HIDS have created which can be utilized to monitor network [6]. HIDS decide whether a system has been compromised and caution administrators correspondingly. A NIDS is utilized to control and investigate network traffic activity to protect a framework from network based threats [7]. In any case, there are numerous issues in the conventional IDS, for example, the low identification ability against the unknown network attack, high false alarm rate, and deficient investigation capacity and etc. [8].

For the most part, Intrusion discovery techniques are ordered into two strategies, namely Misuse Detection or Signature based recognition and Anomaly Detection [9, 10]. The Misuse identification calculations identify attacks in light of the known attack signatures [11]. They are helpful in identifying known attacks with fewer errors. In any case, misuse detection is can't identify new unclear attacks. To conquer this issue, Anomaly interruption detection can anticipate another attack by identifying any deviation from the client's ordinary profile [12]. A conventional technique of clustering is an unsupervised method, useful for identifying the unknown attacks. Using clustering technique database is divided into dissimilar sets based on it similarities. The particular methods detect the normal and attacked instances in groups [13, 14]. The classification is the supervised data mining technique, which construct the classified model depends on data [15]. This model helps to classify the new data into one predefined classes depends on the attribute values. The class's information can be categorized into different types of classification approaches using some classifier such as Artificial Neural Networks, Decision Trees, evolutionary algorithms, Rule Induction, Bayesian methods, K-Nearest Neighbors, etc. [16].

II. BACKGROUND OF INTRUSION DETECTION SYSTEM

An intrusion identification is to monitor irregular behavior and misuse in the network. Intrusion recognition was presented in 1980's after the development of internet with surveillance to monitor the risk presents in the network. The reputation and incorporation of security infrastructures are suddenly increased. From that point onward, a few activities in IDS innovation have advanced detection of network interruption in its present state. In 1980s to 1990s, James P. Anderson worked on Intrusion Detection Expert System (IDES). During this period, the U.S. government funded most of this research. To identify the intrusions several projects are used such as Haystack, Discovery, Network Audit Director and Intrusion Reporter (NADIR) and etc. The detection technique verifies the data and this led to excellent improvements in operating system. IDS and HIDS were first defined. Approximately, in 1990s they achieved the revenues and intrusion recognition market was increasing at that moment. Genuine secure is an intrusion detection network, created by ISS. Afterward, Cisco perceived the need for network intrusion identification and acquired the Wheel Group

978-1-5386-2361-9/17/$31.00 ©2017 IEEE

for overcoming the security arrangements. The administrative activities like Federal Intrusion Detection Networks (FID Net) were planned under Presidential Decision Directive 63 is likewise added motivation to the IDS [17].

A. Intrusion Detection System

It is a security service that controls and examine the system activities and challenges to access and identify the system resources as well as unauthorized activities. An intrusion in a network is described as set of actions that attempts to compromise the confidentiality, integrity and availability of resource [18]. A IDSs are typically used with the other protective security techniques namely authentication and access control. Several research works already addressed that IDS is a significant part of whole defense system. First, various conventional systems and applications were developed without security.

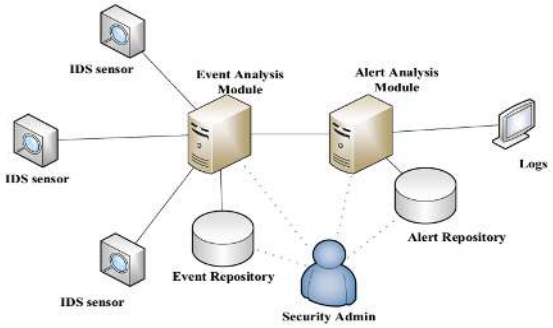

Fig. 1. General Architectural diagram of IDS

The Figure.1 represents the general architectural diagram of IDS. An IDS is a combination of hardware and software, which identify the external and internal user's unauthorized activities from the system. The NIST definition of IDS is the process of controlling the activities that are placed in the network or system [19]. These log files helps to recognize the intrusions [20]. On the other hand, in various environment to handle different kinds of works a lot of applications and systems are developed and to improve the system security various protective mechanisms are used. Additionally, the defensive security strategies protect the information systems effectively, but still required in intrusion related information [21]. There are two types of IDS namely,

- Host Based IDS
- Network Based IDS

Network based IDS detects network attacks as the payload is analyzed. The HIDS sense the local attacks before they hit the networks [22, 23]. Many methodologies are employed in IDS to detect the occurrence of intrusion in network. For accurate detection of network interruption IDS use multiple detection methods either hybrid methods or individual methods. The IDS detection models can be classified as,

- Misuse based IDS
- Anomaly based IDS

These two are the primary detection approaches for IDS. Misuse identification depends on the known features in the database. Anomaly detection is identifying the both computer and network interruptions and monitors the misuses of system activities and categorizes the normal attacks and anomalous attack. In additional, the detection rates of Misuse IDS are high for known intrusion but, not able to detect the unknown attacks [24]. All models and types of IDS are described in below section.

1) Host Based Intrusion Detection system

The objective of the HIDS is the controlling state and dynamic behavior of the computer system. This detection system checks all the activities of inspected packets on a network. HIDS recognize what resources are being utilized and which program gets to those resources. If in the network any alternations or adjustment happens, system administer receive some network alerts. HIDS is progressively becoming essential to ensure the host computer frameworks and its network activities. HIDS with host based information is incorporated into the computer frameworks to identify the intruder abnormal activities, noxious Behavior, application abnormalities and preserve the Information Systems from intruders and report the occasions to the HIDS System Administrator. The Figure.2 indicates to the HIDS.

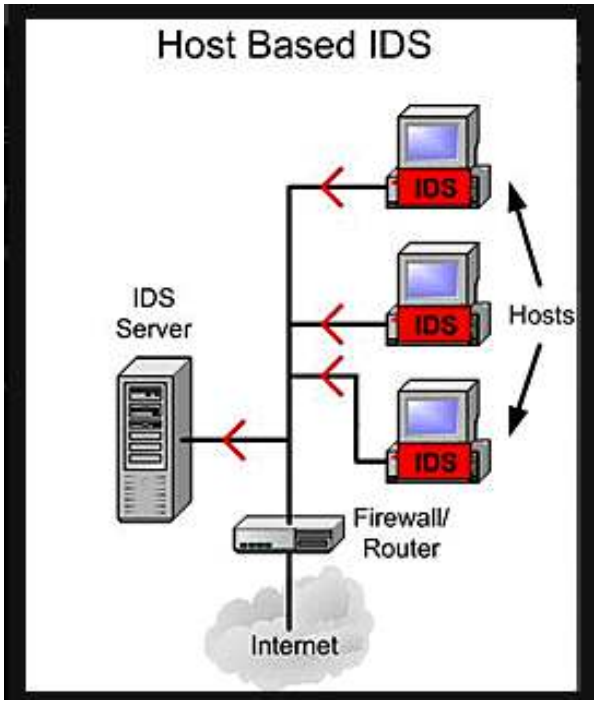

Fig. 2. Architecture of Host based IDS

A HIDS controls the software and investigate the activities occurring in the systems. After that, HIDS detect the abnormal activities in the computer systems. In a computer system, security is the significant element. A HIDS provide the security to the computer system. A lot of security violations in systems happens because of malicious code and unauthorized events are penetrated to the system barriers. The abnormal activities and misuse code affect the system. The HIDS approach avoids the unwanted access in a host system and provide higher security for the user's information [25].

2) Network Based Intrusion Detection System

NIDS is the attribute function of target system and function modules are observed in network. The investigation of NIDS based on either manually or automatically. The NIDS is significantly used in the security infrastructure of the system. In NIDS to control the incoming and outgoing threads, anti-thread software is installed on the servers [26]. It is very essential to provide security for the several fields such as government application, business, industries and educational institution and so on. The Figure.3 represents the architecture of network based IDS [27].

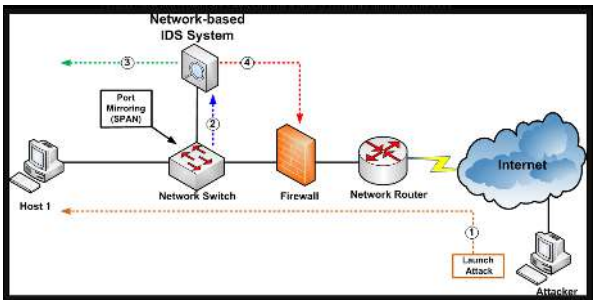

Fig. 3. Architecture of Network based IDS

The NIDS consist of signature based classification, which identify the abnormalities by comparing with previous log files or signatures. Anomaly based technique, identify the misuse as well as computer abnormalities, then classified as normal or attack depends on heuristics of signatures. The NIDS controls the device's outgoing and incoming packets. NIDs also classified as host based and network based [28].

III. Misuse Detection or Signature based detection of IDS

This detection system identifies abnormal behavior depends on the signatures of the known attacks and known framework vulnerabilities. Misuse detection compares the signatures of well-known attack with observed behavior to recognize the possible attacks. Misuse detection framework has a drawback that an unknown attack cannot be recognized as its signature is unavailable. In signature based IDS, if new attacks are discovered, it's signatures are manually updated in database. In addition, security products have some limitations such as antivirus software's. They can protect the dataset and identifies the misuses. Antivirus software's signature files are updated on daily or weekly basis. Consequently, computer users are not safe with respect to the unknown intrusions intervals between the updates. This is a challenging issue because the new attacks can be increased across the Internet in a few minutes [29].

A. Merits of Misuse attack

- It is frequently measure the known attacks of intrusion attempts and efficiently identified.
- Less time consumed due to system administrator takes less time for handling the false positive rate.

B. Demerits of Misuse attack

- Misuse based systems can detect only intrusion attempts matches a known feature on the database but, not identify the unknown attacks.
- This attack recognizes the new attacks but it requires dealers to update their patterns in datasets.

IV. Anomaly based detection of IDS

This is majorly consists of three kinds of methods: machine learning, statistical and knowledge based. The statistical based techniques indicate the network traffic activity [30, 31]. In anomaly detection process statistical based methods are used for network traffic of two datasets. The first database based on time observe the present network profiles and second dataset is the previously trained statistical profile. The network activities occurred, the present profile is defined, after that by comparing two activities anomaly score is calculated. The score typically represents the abnormality degree for a particular activity. The knowledge based strategy is significantly employed in IDS. Here, using a set of rules label of input data is determined and set of rules include two stages. Initially, in input training data the dissimilar classes and network activities are identified. In second step, the group of classification events are extracted from normal activities [32, 33].

The Anomaly based identification system includes three sections such as semi supervised, supervised, and managed anomaly discovery. The supervised anomaly detection system tries to construct the model and separately constructs the abnormal records and normal records. The semi-supervised anomaly detection methods attempt to construct the model depend on normal data. If records are not match with the model, then it's an anomaly. Now, the semi supervised methods can build the model depends on abnormal data but, very difficult to identify all the anomalies. For this purpose, semi-supervised detection required labeled database and frequently represents the high false positive rate. To solve this problem and find some new anomalies, unsupervised anomaly detection system is used. This method not required labeled dataset and installed in any system without alteration [34].

A. Advantages of Anomaly based IDS

- The database updation is not required for identifying the new attacks.
- After the software is installed, it needs some maintenance time.
- In parallel, it observes the network behavior and create network activities profiles.
- Most efficiently identify threats in a larger system.

B. Disadvantages of Anomaly based IDS

- The abnormal behavior of the network in normal traffic, it will not send the alert to administrator.
- In anomaly based setup, the false positives can become more.

There are many difficulties in both misuse and anomaly detection parts, one challenge is the imbalance between intrusion sorts in genuine system associations datasets which are utilized as training data to misuse recognition framework. A few sorts of intrusions like Denial of Service (DoS) have many network associations than other intrusion sorts like User

to Root (U2R); in this way, any information mining methodology will be interested on reducing the general error rate of the framework regardless of intrusion types, which causes rise in the error rate of the minority attacks like U2R, although these attacks are very dangerous than majority attacks [35, 36].

V. MAJOR ISSUES IN INTRUSION DETECTION SYSTEM

In security infrastructure, IDSs is one of the essential elements, which allows the networks administrators to identify the policy variations. In IDS, the different types of alarm rates are increased based on that anomaly and misuse based attacks are classified. The current limitations of IDS systems are:

- Data overload: The data overload is the significant issue in present IDS. In IDS the data source, which evaluates the data must be distinct volume for efficient study.
- False Positives: The major problem is IDS predict the false intrusion attacks. If this rate is high, then normal attack predicted as malicious. Reduction of false positive rates in IDS is the complex task.
- False Negatives: If the false negative rates are high then it is a problem because when intrusion occurred, IDS doesn't produce any alert.
- True Positive: An occurs when an actual attack occurs and the IDS responds to it by raising the appropriate alarm.
- True Negative: When no attack happens, the IDS does not raise alarm.

The comparative study of various existing work techniques of Anomaly based and misuse based detection technique of clustering and classification techniques, their merits, demerits and performance analysis are described in Table 1.

TABLE I. REVIEW OF LITERATURE

Author and Publication	Methodology Employed	Dataset	Advantage	Limitation	Performance Analysis
Mukherjee [1], 2012	Naïve Bayes Classification (NBC) and Feature Vitality Based Reduction Method (FVBRM)	NSL-KDD	FVBRM method recognize the significant input features. After that apply NBC on decrease the datasets for intrusion detection.	The training and testing speed is slow	This feature reduction method improves the classification accuracy.
Wang [3], 2010	The Fuzzy clustering and ANN used for classification	KDD CUP 1999	The fuzzy clustering divides the heterogeneous training set to subset. The complexity of each sub training set is reduced and detection performance is increased.	Unable to handle the noisy data and complex in large dataset	FC-ANN achieved higher detection precision of IDS, low-frequent attacks and stronger detection stability.
Al-Yaseen [11], 2017	Multi-level Hybrid Support Vector Machine and Extreme Learning Machine Based on Modified K-Means	KDD Cup 1999	This system significantly reduces the training time of classifiers and improves efficiency of detecting known and unknown attacks.	This method is applied in KDD dataset and difficult to perform in other database like DARPA.	The proposed model achieves good accuracy with false alarm rate of 1.87%.
Saleh [22], 2017	Hybrid IDS based on Prioritized K-Nearest Neighbors (P-KNN) and	KDD-Cup-99	An OSVM is applied for outlier rejection and PKNN is used for	For the larger dataset with high dimension the technique doesn't	The classification accuracy is high and IDS detection rate is maximum.

	Optimized SVM (OSVM) Classification		detecting input attacks.	provides sufficient rules with dependent attributes for the detection of attributes.	
Azad [26], 2017	Particle Swarm Optimization technique and Fuzzy min-max Neural Network classification	KDD CUP 99	This system provides the online adaption facility and less time taken for the learning.	The technique effectively detects the intrusions in the packet but the false alarm rate is increased.	Classification accuracy and classification error rates are taken as a performance evaluation parameter.
Amiri [29], 2011	Modified Mutual Information based Feature Selection (MMIFS) for IDS	KDD Cup 1999	This feature selection method is select the maximum relevant features and reduces the feature redundancy.	High false alarm and limited by training data	Detecting Intrusion with higher accuracy especially in R2L and U2R attack.
Elbasiony [35], 2013	Hybrid network IDS based random forest and weighted k-means	KDD-99	Feature importance values calculated by the RF algorithm are used in the misuse detection part to improve the detection rate	Slow classifying testing tuples	This framework reduces the false positive rate
Altwaijry [37], 2012	Bayesian classification based IDS.	KDD-99	This classifier able to detect intrusion in superior detection rate.	The assumptions made in class conditional independence and lack of availability probability data	To improve the accuracy of IDS.
Zhang [38], 2008	Random Forest (RF) based IDS system	KDD-99	This algorithm applied in both Anomaly and Misuse detection framework.	Cannot detect behavioral attack and difficult to apply in large dataset	RF algorithm achieves higher detection rate with lower false positive rate
Thaseen [39], 2016	Chi-Square Feature Selection and Multi class SVM	KDD Cup 99	This model improves network attack classification accuracy	It takes more time for training and testing	The detection rate is better and decrease the alarm rate.
Sindhu [40], 2012	Decision tree based light weight intrusion detection using a wrapper approach	KDD	This approach removes the redundant features and identifies the suitable subset of features and minimizes the computational complexity of classifier.	Since the technique is efficient in terms of accuracy and better classification of intrusions but can't be applied on missing attributes.	The overall detection rate of IDS is high.

VI. CONCLUSION

In computer system, the security is the essential element in the computer networks. In computer network security, identifying the intrusion attacks is the most challenging issues. The IDS is majorly classified into two techniques namely misuse and anomaly detection. Based on the detection strategy IDS is classified as two types such as misuse and anomaly detection. In misuse and anomaly detection approaches used numerous exiting techniques. The methods of anomaly detection include predictive pattern generation, neural network, sequence matching, statistics and supervising. These two techniques detect the network based issues. The presented information constitutes an important point to start for addressing Research & Development in the field of IDS. Based on this survey various limitations are addressed such as high false alarm rate, difficult to apply in massive datasets, high network traffic, time complexity in training and testing process, etc. After surveying the various Anomaly based IDS technique concluded that single technique is not able to provide accurate detection rate. For boosting the anomaly detection method, an efficient automatic hybrid technique is suggested to achieve accurate detection rate. Also, helps to reduce the false prediction rate as well as decrease the time complexity. Additionally, machine learning techniques reduce the network traffic.

REFERENCE

[1] S. Mukherjee, and N. Sharma, "Intrusion detection using naive Bayes classifier with feature reduction," Procedia Technology, vol.4, pp.119-128, 2012.

[2] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," Journal of Electrical and Computer Engineering, 2014.

[3] G. Wang, J. Hao, J. Ma, and L. Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering," Expert systems with applications, vol. 37, no. 9, pp. 6225-6232, 2010.

[4] M.S.M. Pozi, M.N. Sulaiman, N. Mustapha, T. Perumal, "Improving anomalous rare attack detection rate for intrusion detection system using support vector machine and genetic programming," Neural Processing Letters, vol. 44, no. 2, pp. 279-290, 2016.

[5] M. Vadursi, A. Ceccarelli, E.P. Duarte, and A. Mahanti, "System and Network Security: Anomaly Detection and Monitoring," Journal of Electrical and Computer Engineering, 2016.

[6] A. Sultana, and M.A. Jabbar, "Intelligent network intrusion detection system using data mining techniques," In the Proceedings of 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp. 329-333, 2016.

[7] A.P. Singh, and M.D. Singh., "Analysis of Host-Based and Network-Based Intrusion Detection System," International Journal of Computer Network and Information Security, vol. 6, no. 8, pp. 41, 2014.

[8] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," Applied Soft Computing, vol.18, pp.178-184, 2014.

[9] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1690-1700, 2014.

[10] L. Khan, M. Awad, and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering," The VLDB Journal-The International Journal on Very Large Data Bases, vol. 16, no. 4, pp. 507-521, 2007.

[11] S. Ganapathy, P. Yogesh, and A. Kannan, "Intelligent agent-based intrusion detection system using enhanced multiclass SVM," Computational intelligence and neuroscience, vol. 9, 2012.

[12] S.W. Lin, K.C. Ying, C.Y. Lee, and Z.J. Lee, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection," Applied Soft Computing, vol. 2, no. 10, pp. 3285-3290, 2012.

[13] W.M. Tammi, N.A. Biswas, Z. Nasim, K.Z. Shorna, F.M. Shah, "Artificial Neural Network based System for Intrusion Detection using Clustering on Different Feature Selection," International Journal of Computer Applications, vol. 126, no. 12, 2015.

[14] W.L. Al-Yaseen, Zulaiha Ali Othman, and Mohd Zakree Ahmad Nazri., "Hybrid Modified-Means with C4. 5 for Intrusion Detection Systems in Multiagent Systems", The Scientific World Journal, 2015.

[15] S. Mabu, S. Gotoh, M. Obayashi, and T. Kuremoto, "A random-forests-based classifier using class association rules and its application to an intrusion detection system," Artificial Life and Robotics, vol. 21, no. 3, pp. 371-377, 2016.

[16] G. Kalyani, and A.J. Lakshmi, "Performance assessment of different classification techniques for intrusion detection," IOSR Journal of Computer Engineering (IOSRJCE), vol. 7, no. 5, pp. 25-29, 2012.

[17] F. Jiang, Y. Sui, and C. Cao, "An incremental decision tree algorithm based on rough sets and its application in intrusion detection," Artificial Intelligence Review, pp.1-14, 2013.

[18] J. Kevric, S. Jukic, and A. Subasi, "An effective combining classifier approach using tree algorithms for network intrusion detection," Neural Computing and Applications, pp. 1-8, 2016.

[19] T. Garg, and Y. Kumar, "Combinational feature selection approach for network intrusion detection system," IN proceedings of International Conference on Parallel, Distributed and Grid Computing (PDGC), 2014.

[20] N.A. Alrajeh, and J. Lloret, "Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 9, no.10, pp. 351047, 2013.

[21] S. Masarat, S. Sharifian, and H. Taheri, "Modified parallel random forest for intrusion detection systems," The Journal of Supercomputing, vol. 72, no. 6, pp. 2235-2258, 2016.

[22] K. Demertzis, and L. Iliadis, "A hybrid network anomaly and intrusion detection approach based on evolving spiking neural network classification," Inproceedings of International Conference on e-Democracy, Cham, pp. 11-23, 2013.

[23] M. Belhor, and F. Jemili, "Intrusion Detection Based on Genetic Fuzzy Classification System".

[24] A.A. Sivasamy, and B. Sundan, "A Dynamic Intrusion Detection System Based on Multivariate Hotelling's T2 Statistics Approach for Network Environments," The Scientific World Journal, 2015.

[25] F.L. Catherine, R. Pathak, and V. Vaidehi, "Efficient host based intrusion detection system using Partial Decision Tree and Correlation feature selection algorithm," In proceedings of International Conference on IEEE, Recent Trends in Information Technology (ICRTIT), 2014.

[26] K. Shafi, and A.A. Hussein, "Evaluation of an adaptive genetic-based signature extraction system for network intrusion detection," Pattern Analysis and Applications, vol. 16, no. 4, pp. 549-566, 2013.

[27] N.G. Relan, and D.R. Patil, "Implementation of network intrusion detection system using variant of decision tree algorithm," In proceedings of International Conference on Nascent Technologies in the Engineering Field (ICNTE),., 2015.

[28] A.B. Ashfaq, M.Q. Ali, and S.A. Khayam, "Accuracy improving guidelines for network anomaly detection systems," Journal in computer virology, vol. 7, no. 1, pp. 63-81, 2011.

[29] F. Amiri, M.R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems,"

Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1184-1199, 2011.

[30] P. Ganeshkumar, and N. Pandeeswari, "Adaptive neuro-fuzzy-based anomaly detection system in cloud," International Journal of Fuzzy Systems, vol. 18, no. 3, pp. 367-378, 2016.

[31] S. Ohtahara, T. Kamiyama, and Y. Oyama, "Anomaly-based Intrusion Detection System Sharing Normal Behavior Databases among Different Machines," In Proceedings of Ninth IEEE International Conference on Computer and Information Technology, vol. 1, pp. 217-222, 2009.

[32] M. Mohammadi, A. Akbari, B. Raahemi, B. Nassersharif, and H. Asgharian, "A fast anomaly detection system using probabilistic artificial immune algorithm capable of learning new attacks," Evolutionary Intelligence, vol. 6, no. 3, pp. 135-156, 2014.

[33] P. Ganeshkumar, and N. Pandeeswari, "Adaptive neuro-fuzzy-based anomaly detection system in cloud," International Journal of Fuzzy Systems, vol. 18, no. 3, pp. 367-378, 2016.

[34] B. Subba, S. Biswas, and S. Karmakar, "Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis," In Proceedings of International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, 2016.

[35] R.M. Elbasiony, E.A. Sallam, T.E. Eltobely, and M.M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," Ain Shams Engineering Journal, vol. 4, no. 4, pp. 753-762, 2013.

[36] N. Pandeeswari, and G. Kumar, "Anomaly detection system in cloud environment using fuzzy clustering based ANN," Mobile Networks and Applications, vol. 21, no. 3, pp. 494-505, 2016.

[37] H. Altwaijry, and S. Algarny, "Bayesian based intrusion detection system", Journal of King Saud University-Computer and Information Sciences, vol. 24, no. 1, pp. 1-6, 2012.

[38] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 5, pp. 649-659, 2008.

[39] I.S. Thaseen, and C.A. Kumar, "Intrusion Detection Model using fusion of chi-square feature selection and multi class SVM," Journal of King Saud University-Computer and Information Sciences, 2016.

[40] S.S. Sindhu, S.G. Sivatha, and A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach," Expert Systems with applications, vol. 39, no. 1, pp. 129-141, 2012.