International Journal of Advanced Technology and Engineering Exploration, Vol 5(47)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2018.546013

Review Article

A survey on network intrusion detection system techniques

K. Nandha Kumar[1*] and S. Sukumaran[2]
Ph.D Scholar, Department of Computer Science, Erode Arts and Science College, Erode, Tamilnadu, India[1]
Associate Professor, Department of Computer Science, Erode Arts and Science College, Erode, Tamilnadu, India[2]

Abstract
Security is the emerging trend in today's modern world. Whole world is connected with some network capabilities and transmission of data becomes easier and faster. Nowadays, several places were implemented with network like schools, banks; offices etc. and many individuals are adopted with social network media. Several techniques were developed for improving the security aspects for network related issues. But still, vulnerable attacks are taken place and dominate the security aspects to pertain their strength towards various kinds of attack possibilities. For this reason, several network intrusion detection systems (NIDS) were proposed to protect computers as well as networks. It safeguards data integrity, system availability, and confidentiality from several kinds of attacks. In this paper, we study about the various types of network attacks and intrusion detection system to prevent from these attacks. Also, challenges that are faced by NIDS are discussed and comparison of different techniques and analysis are given in detail. The performance accuracy of each classifier that is previously proposed is comprised.

Keywords
Network security, Network intrusion detection system (NIDS), Network attacks, Deep learning.

1.Introduction
Sharing of resources is the main concept of using computer networks which is group of computers connected together. The rapid development of communication and network technologies leads to improvement in security related issues. Two kinds of attackers are available that are commonly known as 'insider' and 'outsider'. The insider attack is defined as the person who has full authorization for accessing the system can misuse the authentication for obtaining other system resources who has no authorization to access. The outsider attack is accessed from outside of the premises that are pertaining unauthorized access towards the system resources. Such examples for the outside attackers are organized criminals accessing through internet or some international terrorists or other governments [1].

Two main components are consisted in computer networks and these are hardware and software. These components have its own vulnerabilities and different kinds of risk. The first component is hardware which several threats that can be detected easily and can rectify the errors since it affects the device parts rather than the data.

Four types of hardware threats are available and these are Electrical, Maintenance, Physical, and Environmental. Whereas, the second component is software threat, here the main problem is that it affects data rather than the device which could be a huge loss and cannot recover that easily [2−5].

In previous years, the expert in programming skills can only write programs for hacking the data and steal it. Nowadays, people having basic knowledge in programming are becoming hackers by just downloading hacking tools from the websites [6, 7]. Furthermore, high featured software was used by the people due to its attracting application feature that makes attackers easily interfere into their system. Lack of security is dealt with using of high features into the system which are prone to attack easily. There are three main goals of software security threat and these are Integrity, Availability, and Confidentiality [3, 8−11].

Three main contributions are concerned for contributing network security challenge. The first is the volume of network data that grow rapidly from years that is set to be continued. New techniques are required to deal with this data which analyze increasingly efficient, effective, and rapid manner. The second one is to improve accuracy and effectiveness by using granularity and in-depth

*Author for correspondence

monitoring. The final cause is data traversing using different protocols and diversity using modern networks [4]. In this section, basic class of attacks is presented which is responsible for reducing the performance of network and creating uncontrolled traffic and sending viruses etc. The network attacks are caused by malicious nodes present in the network. Two types of attacks are classified and these are active and passive attack [12−14]. In "Active attack", the system resources are altered by some actions from the attacker by bypassing or breaking the secured systems. It mainly modifies the data completely or reveals the sensitive information from the system. Some examples of the active attacks are viruses, Trojan horses, and penetrating network data, inserting malicious code, worms, and stealing login information. Different types of active attacks are available and these are Modification of messages, masquerade, denial of service, and session replay [5].

A "Passive Attack" is to find some important files from the system and obtain the information from it without affecting the system. Some sniffer tool is used by these kinds of attackers and always waits for the information to be captured that could be applied for some other attacks. Some of the basic passive attack examples are packet sniffer tools, Traffic analysis software, and filtering the passwords [6].

There are different types attacks that performed in the networks and these are classified as follows:

1. **Distributed Denial of Service (DDoS):** It is one kind of attack where systems are compromised to the attacker which is affected by Trojan. It is targeted to a single system which causes denial of service (DoS) attack.
2. **Denial of Service (DoS):** It is one type of cyber-attack that make network resources not visible to the users for a while or permanently disrupting the services of main host that connected to the network [7,15].
3. **IP Spoofing:** The devices connected to the network are impersonate by malicious party for launching the attacks to the network host and spread malware, steal data, or bypass access control.
4. **Sniffers:** This attack takes place using network traffic for capturing the data using a sniffer [8].
5. **Man-in-the-Middle:** The communication is altered and secretly relays on network between two parties that they communicating the right person.
6. **Privilege Misuse:** This attack is mentioned as insider attack that the person who has permission can do malicious activities that could not be detected that easily.
7. **Password Cracking:** The stored password for data in a system is recovered using this password cracking or it can transmit to other devices.

Challenges faced by NIDS

Network monitoring is used widely for the purposes like forensics, anomaly detection, and security. Several issues have been created in recent years and become a barrier for NIDSs and some of these are as follows [10].

Volume-Increase in storing and communicating of data through the network and its volume are continuous. A recent survey has been viewed that by 2020 44ZB amount of data will comes in existence. The observed volume of traffic is increasing and the capacity also improved drastically for modern networks [12]. Nowadays, NIDS needs to handle 148,809,524 packets sending in 100Gbps link and analysis should complete within 6.72ns. For ensuring such speed with effectiveness and efficiency with level of accuracy will be significantly challenging.

Diversity-New or customized protocols have been increasing in recent years that utilized by modern networks. Still, the problem persists for differentiating the abnormal traffic with normal or its behaviors due many number of devices connected to internet.

Accuracy-Many existing techniques are not relied for performing accurate level of accuracy. For providing more accurate view and holistic the requirement of depth, greater levels of granularity, and contextual understanding are needed. Hence, the financial cost, time and computational expenses are a major drawback.

Low-frequency attacks-Previous anomaly detection techniques and artificial intelligence approaches are not that much preventable from different kinds of attacks. Weaker detection precision is offered by NIDS which is imbalance towards the training dataset when facing low frequency attacks.

Dynamics-The modern network has given flexibility and diversity which is dynamic and problem in predicting such instances. In turn, reliable behavioral form is difficult for establishing. Learning models lifespan also considered by this kind of difficulty.

Adaptability-Many new technologies were adopted by modern networks for reducing their reliance on management styles and static technologies. Dynamic technologies were used more wisely and these are virtualization, containerization and software defined networks. Side effects could be ensured when using such kind of NIDS technologies.

The main objective of this paper is to survey and discuss the aspects of network intrusion detection system techniques.

2.Related works

In this section, the comparative analysis of IDS techniques and method were discussed.

In [16] author suggested a technique for finding malicious websites. For processing the signatures, a self-developed JAVA program is used for static content web pages with regular expression that is used for accelerate the analyzing process. The type of web page is concluded finally when Honeypot is used for browsing web pages. Four modules are present in Microsoft operating system and these are behavior recording, proxy source code analysis, and behavior analysis. The static analysis of this operating system shows low accuracy even when it is Automated and Active detector of malicious nodes in which time and resource are consumed high.

In [17] proposed a method for IDS, that it produces large number of unimportant, false, and redundant alerts when it finds an attack in the network. Hence, it is the drawback of this system. ShahidRajaee Port Complex dataset and DARPA 1999 dataset is used for proposing an online approach. Number of alerts is reduced with a percentage of 94.32% when obtaining result from this approach. Some cases, this approach gives a high false alarm rate and high detection rate. For online analysis, this approach is not suitable so a new system have to design so that it can reduce false alarm rate and increase the detection rate.

In [18] author proposed a method for detecting SQL injection attack which is a technique for stealing the sensitive data or information from the back-end databases like credit card numbers. An SQL Injection detection using query transformation and document similarity (IDS-SQLiDDS) is proposed for detecting various kinds of SQL injection attacks. Five honeypot web applications are used for testing that were developed using MySQL and PHP. This helps for capturing all kinds of SQL attacks and its patterns.

In [19] author analyzed the advanced persistent threat (APT) that uses different kinds of attack methods for accessing unauthorized system at the initial stage afterwards it slowly mingle throughout the network. For improving the results, "packet-level" IDS are extended at its design approach. This model is built with event classes (C), rules (R), hypothesis (H), and search-patterns (P). By using the combination of log information, the system model is extracted from distributed systems and without the knowledge of log-lines the nodes in the network also extracted. Different meaningful subsets are distinguished and detected using this model form log-lines. The SCADA dataset is used for the experimental purpose and the result after implementing using this model is true positive rate with 1 while false positive rate is denoted by 0.

In [20] author proposed a method for code injection attack that is performed by cross-site scripting attack (XSS) for exploiting the existing vulnerabilities in the web application by injecting java script functions. Different kinds of XSS attacks are presented and works in two types and these are tracing out the cross site vulnerabilities in the web application. Three steps are used namely for this system and these are Sanitization, Encoding, and Regular Expressions Matching. All html tags are removed by sanitization from the user for preventing malicious code insertion. The Java script code is defined by the possible malicious regular expressions. Predefined regular expressions are matched with every users input for checking valid or not. Most commonly used techniques are also discussed in [21, 22].

In [23] proposed a method for detecting the malicious JavaScript. The linear regression and 3 layers stacked denoising auto-encoders (SDA) are used in this proposed method. Furthermore, the experimental results are compared with other classifiers which it gives high positive rate and second best false positive rate.

In [24] built a flexible and effective NIDS using a deep learning based approach. This method is known as Self-taught learning (STL) which helps in combining softmax regression and sparse auto-encoder. The benchmark NSL-KDD dataset is used for implementing and evaluating the proposed method. The classification accuracy is obtained to a promising level for both 5-class and binary classification. An average f-score of 75.76% is achieved by using their 5-class classification. In this method for learning normal network flow using unsupervised learning. In this method, dropout concepts of deep learning, RNN, and auto encoder are used. The accuracy is not fully enclosed and accuracy is not that exact for proposed method. Furthermore, a proposed a concept for monitoring network flow data. Exact algorithm is not discussed

in this paper but an evaluation over NSL-KDD dataset is shown and an accuracy of 75.75% is claimed using six basic features.

In [25] proposed a model for NIDS within health monitoring using the state-of-art survey of deep learning applications. The conventional machine learning methods are compared experimentally with four common deep learning methods like restricted Boltzmann machine (RBM), auto-encoders, recurrent neural network (RNN), and convolutional neural network (CNN). From the experiment result concluded that conventional methods are lack behind and deep learning methods give high accuracy.

In [26] suggested a work for advanced persistent threats and 100 hidden units were used in the proposed deep neural network (DNN) and combined with ADAM optimizer and Rectified Linear Unit activation function. KDD dataset is used for evaluation and obtained an accuracy rate of 99% and as future scope the summarization of both long short term memory (LSTM) and RNN models are need.

In [27] discussed a survey about NIDS approaches and produced a comprehensive taxonomy that utilized by deep and shallow learning. Most pertinent results are aggregated from this work. *Table 1* shows the overall comparison of learning from techniques of NIDS.

Table 1 Comparison of different IDS techniques

IDS Techniques	Proposed By	Processing overhead		Overhead communications	Unfair load distribution
		Space complexity	Time complexity		
Fuzzy c-means clustering	Hore et al. [28]	k-means: O((N+C)D) and O(ND+NC)	k-means: O(NCID) and $O(NDC^2I)$	Predefined feature set are extracted from packets and exchanged	N/A
Self-organizing map and wavelets	Li et al. [29]	Wavelet: O(N)	Wavelet: O(N)	The base station acquire full data records	N/A
Multi agent and refined clustering	Guan and Truk [30]	SOM: $O(N^2)$	SOM: O(NDR)	Full records exchanged between nodes	N/A
Agglomerative clustering	Tan et al. [31]	$O(N^2)$	$O(N^3)$	Summaries of clustering is exchanged	N/A
Support vector machine	Tsang et al. [32]	$O((ND)^2)$	$O((ND)^3)$	Support vector only exchanged between nodes	Common nodes are overloaded unfairly
Back propagation neural network	Chauvin and Rumelhart [33]	O(RT) per cycle	$O(R^2T)$ per cycle	All data records exchanged between nodes	Cluster heads overloaded unfairly
Naïve bayesian classifier	Fleizach and Fukushima [34]	O(DVC)	O(ND)	Full data record are transferred to cluster heads	Cluster heads unfairly overloaded

3.Network intrusion detection system (NIDS)

A NIDS mainly concentrate on detecting intrusions such as computer misuse, spread of viruses, and malicious activity etc. Data packets travelling through network are analyzed and monitored by NIDS for watching suspicious activities for monitoring all traffic, NIDS is installed as a backbone network that is directed to the particular server, gateway, switch, or route. Furthermore, for scanning the system files NIDS is set up in a centralized server for analyzing suspicious activity or unauthorized access for maintaining data integrity [9]. The perimeter of the firewall is employed outside and traffic entering the enterprise network/local host is scanned by NIDS. At a high speed link, the network intrusion detection system remains in a single tapping locater and serve potentially to large number of hosts. Therefore, the signatures configuration and management are kept up-to-date which are very easy to handle. The main drawback of this system is undetectable when the attack is undergone within the firewall perimeter. Every network interfaces have been attached with inbuilt NIDS which acts as an anti-virus to each host. The key benefit of NIDS is that it can decouple the operating system of host [9]. There are two main approaches for implementing NIDS and these are

signature based and anomaly detection based methods. These are the trending approaches for detecting attackers in the network and most commonly used techniques [21]. In *Table 2* shows comparative analysis of existing work for different kinds of techniques used in intrusion detection system with optimization techniques.

Table 2 Comparative analysis of different methods

Authors	Methodology used	Outcome
Tian and Liu [35]	Particle swarm optimization and neural network combined and used for detecting intrusion detection	Proposed obtained 90% of accuracy
Cleetus and Dhanya [36]	Multi objective PSO algorithm is proposed with two different fitness function	The accuracy obtained is 91.71%
Shin, and Kita [37]	In PSO, two dimensional packaging problem is focused	85.56% of accuracy is obtained
Aljarah and Ludwig [38]	Fitness function for PSO is proposed	Obtained accuracy about 85%
Bratton and Kennedy [39]	PSO is proposed with Map reduce using clustering algorithm	0.91% TPR is obtained
Altwaijry and Algarny [40]	Bayesian based IDS	89.5% detection rate is obtained
Panda and Patra [41]	Used Naïve Bayes for detecting NIDS	53.64% DR is obtained
Peddabachigari et al. [42]	Used Decision Tree and SVM for IDS	77.08% is obtained

(i) Signature based NIDS

The packets on the network are monitored by this signature based IDS. The attributes or database of the signatures are compared from the known malicious threats. Packet content inspection and packet header are combined for identifying anomalous traffic flow when signature is specified. Filter on packet 5-tuple is consisted in packet header rule that includes IP addresses of source and destination and its ports. Regular or string expression pattern is included in content inspection rule that packet load must match with this expression. Ternary Content Addressable Memories (TCAM) is used for implementing classification techniques that required by packet header matching. Every byte of the packet load is scanned when deep packet inspection is involved when required for pattern matching [11]. Recently, many string matching algorithms are proposed with high speed and efficient due to importance and wide adaptation of patterns [22].

Figure 1 shows the basic architecture of signature based NIDS. Some standard string matching algorithms of the signature based NIDS are Aho-Corasick, Wu-Manber, and Commentz Walter. To perform high-performance matching, preprocessed data structure is used and Aho-Corasick is the best model and used widely.

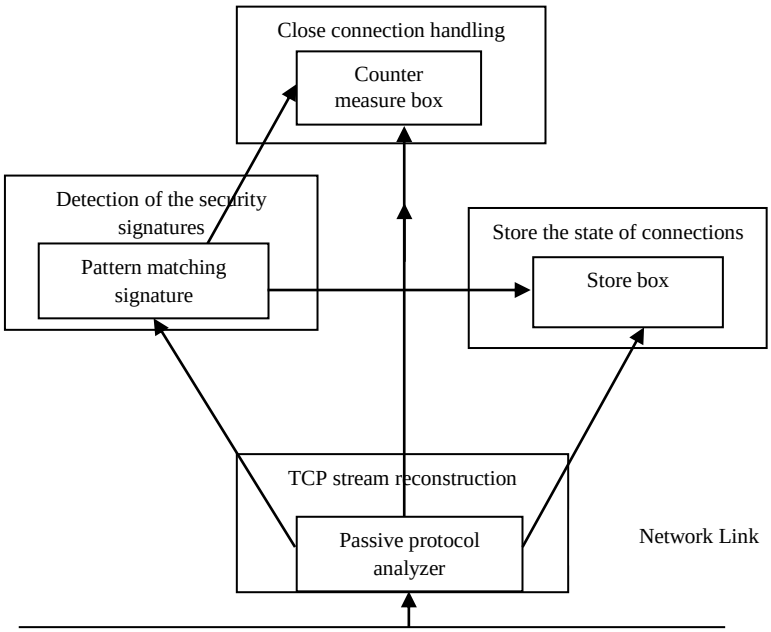

Figure 1 Signature based NIDS architecture

Aho-Corasick algorithm

Aho-Corasick algorithm is the perfect multi-pattern string matching which is earliest and most efficient algorithm.

By the size of the input the string matching is enabled by this algorithm. Using the strings, a finite automaton is generated by Aho-Corasick. The structure of the strings is similar to trie and the same are encoded for searching in multiple stages. No partial match is represented when empty root node is started while construction strings. The patterns each character is added by the nodes for matching. It is started from the root node and travel up to the end of the pattern. The common prefix and the corresponding set of parent nodes are shared by the strings in the trie. Aho-Corasick has two main variants and these includes deterministic and non-deterministic. At the beginning of the root node, state machine is traversed for the non-deterministic version of trie. Each node is added a failure pointers to the longest prefix that leads to a valid node in the trie. In deterministic version, one traversal per input character is enabled by avoiding automaton for using failure pointers [12].

Regular expression signature

When comparing regular expressions with exact-match strings, it is proved that this type of signature is fundamentally more flexible and efficient when specifying signatures for NIDS. The character classes, optional elements, union, and closures are used for achieving expressiveness in a high degree which makes more flexibility. The effective schemes increase the efficiency for performing pattern matching. For specifying rules, Snort and Bro which are open source NIDS system are used nowadays for regular expressions. Many NIDS commercial products are using regular expression as a choice of language. There are two primary kinds of finite automata that are represented by regular expression [11].

The first one is Deterministic Finite Automaton (DFA) which consists of alphabets that has a finite set of input symbols and having a initial state and a transition function as a finite set of states. Generally, 256 ASCII characters are available in alphabets when comes to networking applications. For any given input symbol, single next state is returned by the transition function which is a key property of DFA. Therefore, DFA has only one state is active at any time. Lots of memory is required by DFA even if it is faster. Gigabytes of memory are required for implementation process.

The transition function lies in the distinction of NFA and DFA for returning a single state that could be an empty set. Multiple states can be active simultaneously for Non-deterministic Finite Automaton (NFA) [12]. Merits arrangement is easier and usage is simple. Demerits attacks outside the rule can't be detected, signatures are handicapped which make false positives. Occasional refreshing of signatures required for powerful against new threats.

(ii) Anomaly detection based NIDS

This design is hailed as a future scope for network intrusion detection system which is commercially not available. The unknown attacks are inferred automatically by anomaly based NIDS which is key success and gives more effectiveness. Two different steps are included in anomaly based detection and these are profile for normal traffic is generated and it is known as training phase and second one is looking for any deviations that applied to the current traffic by learned profile and it is known as anomaly detection. Recently, for detecting deviations of the traffic some of the anomaly detections techniques are proposed and categorized into machine learning methods, data mining methods, and statistical methods [13].

Detecting anomalies using machine learning

It is the algorithmic method that learns from the given input automatically and time to time the performance is improved. The traffic feature deviations are the main aim for this machine learning to determine. Using some mechanism, the anomalies are detected by the methods based on machine learning. It is mainly based on false positive or not concept is used to improve the mechanism. Some models like Bayesian network, support vector machine, and neural networks are used for the detection of anomalies [14].

Data mining algorithms

It consists of advanced set of techniques which input is taken as set of data and the patterns are detected and deviations could be difficult to detect. Not only data mining algorithms are used for anomaly detection but also used for constructing profiles of normal traffic. Some of the applied data mining techniques are Fuzzy logic algorithms that use set of fuzzy sets and rules for observing every feature which individual attacks are detected. Other optimization and search problems like genetic algorithm are used. Clustering methods are also used for the anomaly detection [12].

Statistical anomaly detection

Certain traffic characteristics are deviated from normal which is a result from using statistical

schemes. It is defined in terms of volumes like packets, number of bytes, and a certain set of IP ports or addresses. Large traffic changes are identified by this volume based schemes such as bandwidth flooding attacks. If the attacker is smart for disrupting then the volume based schemes will not be effective and analyze for alternative schemes. Fine changes in traffics are detected by number of algorithms and various traffic characteristics and its relative distributions are detected. Rate of scanning ports can be reduced simply by the attacker for keeping the traffic volume unaffected. Signature based system are added with this statistical anomaly scheme for detecting attacks automatically for generating a signature [43]. Merit is Based on anomalies the worms are identified and baselines are self-arranged and Demerit large networks cannot be profiled precisely. The critical changes could cause false positive in a substantial network.

4.Conclusion

In this paper, the study about different kinds of network attacks and IDS techniques are discussed. Several data mining techniques are proposed for improving the classification mechanism for NIDS. Different types of network attacks like DDoS, DoS, probe attack and IP spoofing etc. are discussed and description of each attack are analyzed. For evaluating network security and network attacks, the deep learning shows a promising effectiveness and gained prominence due to its increase in detection rate. Nowadays, increase in data become a trend and traditional network security models lack behind and failing to increase effectiveness. The survey shows the performance of each classifier and ability of detection rate towards the attackers. Deep learning approaches are used for analyzing different kinds of datasets and the experiment results obtained are given some promising outcome. For future work, new model for detecting the attackers on NIDS could be modelled using some hybrid technique by combining some optimization techniques with machine learning classifiers.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Jyothi V, Addepalli SK, Karri R. DPFEE: A high performance scalable pre-processor for network security systems. IEEE Transactions on Multi-Scale Computing Systems. 2018; 4(1):55-68.

[2] Zha Y, Li J. CMA: a reconfigurable complex matching accelerator for wire-speed network intrusion detection. IEEE Computer Architecture Letters. 2018; 17(1):33-6.

[3] Tsikoudis N, Papadogiannakis A, Markatos EP. LEoNIDS: a low-latency and energy-efficient network-level intrusion detection system. IEEE Transactions on Emerging Topics in Computing. 2016; 4(1):142-55.

[4] Liu J, Zhang S, Sun W, Shi Y. In-vehicle network attacks and countermeasures: challenges and future directions. IEEE Network. 2017; 31(5):50-8.

[5] Zou CC, Duffield N, Towsley D, Gong W. Adaptive defense against various network attacks. IEEE Journal on Selected Areas in Communications. 2006; 24(10):1877-88.

[6] Yang C, Feng L, Zhang H, He S, Shi Z. A novel data fusion algorithm to combat false data injection attacks in networked radar systems. IEEE Transactions on Signal and Information Processing over Networks. 2018; 4(1):125-36.

[7] Yin D, Shen Y, Liu C. Attribute couplet attacks and privacy preservation in social networks. IEEE Access. 2017; 5:25295-305.

[8] Deng S, Gao X, Lu Z, Gao X. Packet injection attack and its defense in software-defined networks. IEEE Transactions on Information Forensics and Security. 2018; 13(3):695-705.

[9] Wu SX, Banzhaf W. The use of computational intelligence in intrusion detection systems: a review. Applied Soft Computing. 2010; 10(1):1-35.

[10] Zhengbing H, Zhitang L, Junqi W. A novel network intrusion detection system (NIDS) based on signatures search of data mining. In proceedings of the 1st international conference on forensic applications and techniques in telecommunications, information, and multimedia and workshop 2008 (p. 45). ICST.

[11] Liu RT, Huang NF, Kao CN, Chen CH, Chou CC. A fast pattern-match engine for network processor-based network intrusion detection system. In international conference information technology: coding and computing, 2004 (pp. 97-101). IEEE.

[12] Subaira AS, Anitha P. Efficient classification mechanism for network intrusion detection system based on data mining techniques: a survey. In international conference on intelligent systems and control 2014 (pp. 274-80). IEEE.

[13] Bhuyan MH, Bhattacharyya DK, Kalita JK. Network anomaly detection: methods, systems and tools. Communications Surveys & Tutorials. 2014; 16(1):303-36.

[14] Maciá-Pérez F, Mora-Gimeno FJ, Marcos-Jorquera D, Gil-Martínez-Abarca JA, Ramos-Morillo H, Lorenzo-Fonseca I. Network intrusion detection system embedded on a smart sensor. IEEE Transactions on Industrial Electronics. 2011; 58(3):722-32.

[15] Kabir MF, Hartmann S. Cyber security challenges: an efficient intrusion detection system design. In international young engineers forum 2018 (pp. 19-24). IEEE.

[16] Koo TM, Chang HC, Hsu YT, Lin HY. Malicious website detection based on honeypot systems. In international conference on advances in computer science and engineering 2013 (pp. 76-82). Atlantis Press.
[17] Barghi MN, Hosseinkhani J, Keikhaee S. An effective web mining-based approach to improve the detection of alerts in intrusion detection systems. International Journal of Advanced Computer Science and Information. 2015; 4(1):38-45.
[18] Kar D, Panigrahi S, Sundararajan S. SQLiDDS: SQL injection detection using query transformation and document similarity. In international conference on distributed computing and internet technology 2015 (pp. 377-90). Springer, Cham.
[19] Friedberg I, Skopik F, Settanni G, Fiedler R. Combating advanced persistent threats: from network event correlation to incident detection. Computers & Security. 2015; 48:35-57.
[20] Kour H, Sharma LS. Tracing out cross site scripting vulnerabilities in modern scripts. International Journal of Advanced Networking and Applications. 2016; 7(5):2862-7.
[21] Dong B, Wang X. Comparison deep learning method to traditional methods using for network intrusion detection. In proceedings of ICCSN 2016 (pp. 581-5). IEEE.
[22] Alrawashdeh K, Purdy C. Toward an online anomaly intrusion detection system based on deep learning. In international conference on machine learning and applications 2016 (pp. 195-200). IEEE.
[23] Wang Y, Cai WD, Wei PC. A deep learning approach for detecting malicious JavaScript code. Security and Communication Networks. 2016; 9(11):1520-34.
[24] Javaid A, Niyaz Q, Sun W, Alam M. A deep learning approach for network intrusion detection system. In proceedings of the EAI international conference on bio-inspired information and communications technologies 2016 (pp. 21-6). ICST.
[25] Zhao R, Yan R, Chen Z, Mao K, Wang P, Gao RX. Deep learning and its applications to machine health monitoring: a survey. IEEE Transactions on Neural Networks and Learning Systems. 2016.
[26] Kim J, Shin N, Jo SY, Kim SH. Method of intrusion detection using deep neural network. In international conference on big data and smart computing 2017 (pp. 313-6). IEEE.
[27] Gao N, Gao L, Gao Q, Wang H. An intrusion detection model based on deep belief networks. In international conference on advanced cloud and big data 2014 (pp. 247-52). IEEE.
[28] Hore P, Hall LO, Goldgof DB. Single pass fuzzy c means. In international fuzzy systems conference 2007 (pp. 1-7). IEEE.
[29] Li T, Li Q, Zhu S, Ogihara M. A survey on wavelet applications in data mining. ACM SIGKDD Explorations Newsletter. 2002; 4(2):49-68.
[30] Guan H, Turk M. The hierarchical isometric self-organizing map for manifold representation. In conference on computer vision and pattern recognition 2007 (pp. 1-8). IEEE.
[31] Tan PN, Steinbach M, Kumar V. Data mining cluster analysis: basic concepts and algorithms. Introduction to Data Mining. 2013.
[32] Tsang IW, Kwok JT, Cheung PM. Core vector machines: fast SVM training on very large data sets. Journal of Machine Learning Research. 2005; 363-92.
[33] Chauvin Y, Rumelhart DE. Backpropagation: theory, architectures, and applications. Psychology Press; 2013.
[34] Fleizach C, Fukushima S. A naive Bayes classifier on 1998 KDD Cup.
[35] Tian W, Liu J. Network intrusion detection analysis with neural network and particle swarm optimization algorithm. In Chinese control and decision conference 2010 (pp. 1749-52). IEEE.
[36] Cleetus N, Dhanya KA. Multi-objective functions in particle swarm optimization for intrusion detection. In international conference on advances in computing, communications and informatics 2014 (pp. 387-92). IEEE.
[37] Shin YB, Kita E. Solving two-dimensional packing problem using particle swarm optimization. Computer Assisted Methods in Engineering and Science. 2017; 19(3):241-55.
[38] Aljarah I, Ludwig SA. Mapreduce intrusion detection system based on a particle swarm optimization clustering algorithm. In congress on evolutionary computation 2013 (pp. 955-62). IEEE.
[39] Bratton D, Kennedy J. Defining a standard for particle swarm optimization. In swarm intelligence symposium 2007(pp. 120-7). IEEE.
[40] Altwaijry H, Algarny S. Bayesian based intrusion detection system. Journal of King Saud University-Computer and Information Sciences. 2012; 24(1):1-6.
[41] Panda M, Patra MR. Network intrusion detection using naive Bayes. International journal of computer science and network security. 2007; 7(12):258-63.
[42] Peddabachigari S, Abraham A, Thomas J. Intrusion detection systems using decision trees and support vector machines. International Journal of Applied Science and Computations, USA. 2004; 11(3):118-34.
[43] Villalba LJ, Castro JD, Orozco AL, Puentes JM. Malware detection system by payload analysis of network traffic. In international workshop on recent advances in intrusion detection 2012 (pp. 397-8). Springer, Berlin, Heidelberg.

K. Nandha Kumar received his MCA degree from Dr. MGR University, Chennai, Tamilnadu, India in 2009 and M.Phil Computer Science Degree from PRIST University, Tanjore, Tamilnadu, India in 2010. Currently, He is doing Ph.D. Degree in Computer Science at Bharathiyar University, Tamilnadu. His research interests include Computer Networks, Network Security and Data Mining.
Email: nandha.k07@gmail.com

Dr. S. Sukumaran graduated in 1985 with a degree in Science. He obtained his Master Degree in Science and M.Phil in Computer Science from the Bharathiar University. He received the Ph.D degree in Computer Science from the Bharathiar University. He has 28 years of teaching experience starting from Lecturer to Associate Professor. At present he is working as Associate Professor of Computer Science in Erode Arts and Science College, Erode, Tamilnadu. He has guided 11 Ph.D Scholars and more than 56 M.Phil research Scholars in various fields. Currently he is Guiding 5 M.Phil Scholars and 6 Ph.D Scholars. He is member of Board studies of various Autonomous Colleges and Universities. He published around 68 research papers in national and international journals and conferences. His current research interests include Image Processing and Data Mining, Networking.