Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.3, 2018, pp.20-27

DOI: https://doi.org/10.51983/ajcst-2018.7.3.1905

A Literature Survey on the Importance of Intrusion Detection System for Wireless Networks

D. Selvamani[1] and V Selvi[2]
[1]Assistant Professor, Department of Computer Science, SIVET College, Gowrivakkam, Chennai, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India
E-Mail: selvamani.bhaskar@gmail.com, selvigiri.s@gmail.com

(Received 23 August 2018; Revised 4 September 2018; Accepted 29 September 2018; Available online 7 October 2018)

Abstract **- Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the importance of security, types of attacks in the networks. This paper elaborates theliterature study on network security in various domains in the year 2013 to 2018. Finally, it summarizes the research directions by literature survey.**

Keywords: **Network Security, Cloud Computing, Sensor Networks, Ad Hoc Networks, Internet of Things**

I. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet.

Network security starts with authorization, commonly with a username and a password. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Basically network security involves the authorization of access to data in a network, which is controlled by the network admin. It has become more important to personal computer users, and organizations. If this authorized, a firewall forces to access policies such as what services are allowed to be accessed for network users. So that to prevent unauthorized access to system, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion detection system (IDS) helps detect the malware. Today anomaly may also monitor the network like wire shark traffic and may be logged for audit purposes and for later on high-level analysis in system. Communication between two hosts using a network may be uses encryption to maintain privacy policy.

II. IMPORTANCE OF NETWORK SECURITY

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well- developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered:

1. *Access* – authorized users are provided the means to communicate to and from a particular network.
2. *Confidentiality* – Information in the network remains private.
3. *Authentication* – Ensure the users of the network are who they say they are.
4. *Integrity* – Ensure the message has not been modified in transit.
5. *Non-repudiation* – Ensure the user does not refute that he used the network.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack.

III. TYPES OF ATTACKS

This section describes the basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks can be categories in two: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

A. Active Attacks

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

1. *Spoofing:*When a malicious node miss-present his identity, so that the sender change the topology.
2. *Modification:*When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.
3. *Wormhole:*This attack is also called the tunneling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network.
4. *Fabrication:*A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices.
5. *Denial of services:*In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.
6. *Sinkhole:*Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack.
7. *Sybil:* This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network.

B. Passive Attacks

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring.

1. *Traffic analysis:* In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.
2. *Eavesdropping:* This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.
3. *Monitoring:* In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

IV. LITERATURE SURVEY ON INTRUSION DETECTION SYSTEM

Reda M. Elbasiony[1] proposed hybrid framework, the anomaly part is improved by replacing the k-means algorithm with another one called weighted k-means algorithm, moreover, it uses a proposed method in choosing the anomalous clusters by injecting known attacks into uncertain connections data.

S.A.Joshi[2] introduced to deal with these new problems of networks, data mining based IDS are opening new research avenues. Data mining is used to identify new patterns which were not known previously from large volume of network dataset.

Sannasi Ganapathy[3] a survey on intelligent techniques for feature selection and classification for intrusion detection in networks based on intelligent software agents, neural networks, genetic algorithms, neuro-genetic algorithms, fuzzy techniques, rough sets, and particle swarm intelligence has been proposed.

Panos Louvieris[4] presented a novel anomaly detection technique that can be used to detect previously unknown attacks on a network by identifying attack features. This effects-based feature identification method uniquely combines k-means clustering, Naive Bayes feature selection and C4.5 decision tree classification for pinpointing cyber-attacks with a high degree of accuracy in order to increase the situational awareness of cyber network operators.

Jaehak Yu[5] proposed a traffic flooding attack detection and an in-depth analysis system that uses data mining techniques.

Monowar H. Bhuyan[6] presented a comprehensive survey of DDoS attacks, detection methods and tools used in wired networks. The paper also highlights open issues, research challenges and possible solutions in this area.

Iftikhar Ahmad[7] depicted that several intrusion detection approaches are available but the main problem is their performance, which can be enhanced by increasing the

detection rates and reducing false positives. This issue of the existing techniques is the focus of research in this paper.

Wenying Feng[8] introduced a new machine learning based data classification algorithm that is applied to network intrusion detection. A new approach combines SVM with Clustering based on Self-Organized Ant Colony Network (CSOACN) to take the advantages of both while avoiding their weaknesses.

Wenchao Li[9] proposed a new intrusion detection system based on K-nearest neighbor (K-nearest neighbor, referred to as KNN) classification algorithm in wireless sensor network. This system can separate abnormal nodes from normal nodes by observing their abnormal behaviors.

Fangjun Kuang[10] proposed a novel support vector machine (SVM) model combining kernel principal component analysis (KPCA) with genetic algorithm (GA) is proposed for intrusion detection.

Roshan Chitrakar[11] proposed Half-partition strategy of selecting and retaining non-support vectors of the current increment of classification e named as Candidate Support Vectors (CSV) which are likely to become support vectors in the next increment of classification.

G.V. Nadiammai[12] introduced data mining concept which is integrated with an IDS to identify the relevant, hidden data of interest for the user effectively and with less execution time.algorithms like Efficient Data Adapted Decision Tree (EDADT) algorithm, Hybrid IDS model, Semi-Supervised Approach and Varying Hopping Period Alignment and Adjustment (HOPERAA) have proposed.

Gisung Kim[13] introduced a new hybrid intrusion detection method that hierarchically integrates a misuse detection model and an anomaly detection model in a decomposition structure is proposed.

Shahaboddin Shamshirband[14] given a game theoretic method, namely cooperative Game-based Fuzzy Q-learning (G-FQL). G-FQL adopts a combination of both the game theoretic approach and the fuzzy Q-learning algorithm in WSNs.

EunHee Jeong[15] proposed an IP Traceback Protocol (ITP) that uses a Compressed Hash Table, a Sinkhole Router and Data Mining based on network forensics against network attacks.

Shengyi Pan[16] presented a systematic and automated approach to build a hybrid IDS that learns temporal state-based specifications for power system scenarios including disturbances, normal control operations, and cyber-attacks.

Mustafa Amir Faisal[17] proposed a realistic and reliable IDS architecture for the whole Advanced Metering Infrastructure (AMI) system which consists of individual IDSs for three different levels of AMI's components: smart meter, data concentrator, and AMI head end.

Salma Elhag[18] considered the use of Genetic Fuzzy Systems within a pairwise learning framework for IDS. The advantages of using this approach are twofold: first, the use of fuzzy sets, and especially linguistic labels, enables a smoother borderline between the concepts, and allows a higher interpretability of the rule set. Second, the divide-and-conquer learning scheme, in which we contrast all possible pair of classes with aims, improves the precision for the rare attack events, as it obtains a better separability between a ''normal activity'' and the different attack types.

Adel Sabry Eesa[19] presented a new feature-selection approach based on the cuttlefish optimization algorithm which is used for intrusion detection systems (IDSs). The proposed model uses the cuttlefish algorithm (CFA) as a search strategy to ascertain the optimal subset of features and the decision tree (DT) classifier as a judgement on the selected features that are produced by the CFA.

Khattab M. Ali Alheeti[20] designed an intrusion detection mechanism for the VANETs using Artificial Neural Networks (ANNs) to detect Denial of Service (DoS) attacks.

Kelton A.P. Costa[21] proposed a nature-inspired approach to estimate the probability density function (pdf) used for data clustering based on the optimum-path forest algorithm (OPFC).

Opeyemi Osanaiye[22] proposed an ensemble-based multi-filter feature selection method that combines the output of four filter methods to achieve an optimum selection.

K. Keerthi Vasan[23] focused on the efficiency of Principal Component Analysis(PCA) for intrusion detection and determine itsReduction Ratio (RR), ideal number of Principal Components needed for intrusion detection andthe impact of noisy data on PCA.

Nathan Keegan[24] explored current research at the intersection of these two fields by examining cloud-based network intrusion detection approaches that utilize machine learning algorithms (MLAs).

Soo-YeonJi[25] focused on designing a multi-level network detection method. Mainly, it is composed of three steps as (1) understanding hidden underlying patterns from network traffic data by creating reliable rules to identify network abnormality, (2) generating an predictive model to determine exact attack categories, and (3)integrating a visual analytics tool to conduct an interactive visual analysis and validate the identified intrusions with transparent reasons.

Seyed Mojtaba Hosseini Bamakan[26] proposed an effective intrusion detection framework by using a new adaptive, robust, precise optimization method, namely,

time-varying chaos particle swarm optimization (TVCPSO) to simultaneously do parameter setting and feature selection for multiple criteria linear programming (MCLP) and support vector machine (SVM).

Abdulla Amin Aburomman[27] proposed a novel ensemble construction method that uses PSO generated weights to create ensemble of classifiers with better accuracy for intrusion detection. Local unimodal sampling (LUS) method is used as a meta-optimizer to find betterbehavioral parameters for PSO.

Rana Aamir Raza Ashfaq[28] proposed a novel fuzziness based semi-supervised learning approach by utilizing unlabeled samples assisted with supervised learning algorithm to improve the classifier's performance for the IDSs.

Jasmin Kevric[29] developed a combining classifier model based on tree-based algorithms for network intrusion detection.

Wathiq Laftah Al-Yaseen[30] proposed a multi-level hybrid intrusion detection model that uses support vector machine and extreme learning machine to improve the efficiency of detecting known and unknown attacks. A modified K-means algorithm is also proposed to build a high-quality training dataset that contributes significantly to improving the performance of classifiers.

Elike Hodo[31]has given a taxonomy and survey reviews machine learning techniques and their performance in detecting anomalies. Feature selection which influences the effectiveness of machine learning (ML) IDS is discussed to explain the role of feature selection in the classification and training phase of ML IDS.

Sumaiya Thaseen Ikram[32] proposed an intrusion detection model using chi-square feature selection and multi class support vector machine (SVM). A parameter tuning technique is adopted for optimization of Radial Basis Function kernel parameters.

M.R. Gauthama Raman[33] presented a novel approach based on Helly property of Hypergraph and Arithmetic Residual based Probabilistic Neural Network (HG AR - PNN) to address the classification problem in IDS.

Abien Fred M. Agarap[34] presented an amendment to this norm by introducing linear support vector machine (SVM) as the replacement for Softmax in the final output layer of a Gated Recurrent Unit (GRU) model.

Syed Ali Raza Shah[35] investigates the performance of two open source intrusion detection systems (IDSs) namely Snort and Suricata for accurately detecting the malicious traffic on computer networks.A hybrid version of SVM and Fuzzy logic produced better detection accuracy.

Weizhi Meng[36] proposed a way of combining Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure.

Krzysztof Cabaj[37] presented a novel Software-Defined Networking (SDN) based detection approach that utilizes characteristics of ransomware communication. Based on the observation of network communication of two crypto ransomware families, namely Crypto Wall and Locky.

Yanfang Ye [38] proposed a heterogeneous deep learning framework composed of an AutoEncoder stacked up with multilayer restricted Boltzmann machines and a layer of associative memory to detect newly unknown malware.

Sandeep Kumar Singh[39] proposed Joint Transformation based scheme to detect FDI attacks in real time. The proposed method is built on the dynamics of measurement variations. Kullback-Leibler Distance (KLD) is used to find out the difference between probability distributions obtained from measurement variations.

Longjie Li[40] presented a novel hybrid model was proposed with the purpose of detecting network intrusion effectively. In the proposed model, Gini index is used to select the optimal subset of features, the gradient boosted decision tree (GBDT) algorithm is adopted to detect network attacks, and the particle swarm optimization (PSO) algorithm is utilized to optimize the parameters of GBDT.

Konstantinos Demertzis[41] proposed a network-based online system, which uses minimum computational power to analyze only the basic characteristics of network flow, so as to spot the existence and the type of a potential network anomaly.

Igor Santos[42] proposed a new method to detect unknown malware families. This model is based on the frequency of the appearance of opcode sequences.

Cristian I. Pinzón[43] presented a multiagent architecture aimed at detecting SQL injection attacks, which are one of the most prevalent threats for modern databases. The proposed architecture is based on a hierarchical and distributed strategy where the functionalities are structured on layers.

David Zhao[44] proposed a new approach to detect botnet activity based on traffic behavior analysis by classifying network traffic behavior using machine learning.

Yuxin Ding[45] proposed an API (Application Programming Interface)-based association mining method for detecting malware.

Neminath Hubballi[46] reviewed existing false alarm minimization techniques in signature-based Network Intrusion Detection System (NIDS). The authors give taxonomy of false alarm minimization techniques in

signature-based IDS and present the pros and cons of each class.

Gideon Creech[47] introduced a new host-based anomaly intrusion detection methodology using discontiguous system call patterns, in an attempt to increase detection rates whilst reducing false alarm rates.

Wei Wang[48] proposed a novel framework of autonomic intrusion detection that fulfills online and adaptive intrusion detection over unlabeled HTTP traffic streams in computer networks.

Ammar Alazab[49] proposed a combination of an SIDS and an AIDS, namely, the Intelligent Intrusion Detection and Prevention System (IIDPS). This paper presents a novel approach by connecting the IIDPS with a response action using fuzzy logic

Ismaila Idris[50] has given a method to cope with the trend of email spam, a novel model that improves the random generation of adetector in negative selection algorithm (NSA) with the use of stochastic distribution to model the datapoint using particle swarm optimization (PSO) was implemented.

Youngjoon Ki[51] proposed a novel approach for dynamic analysis of malware. The authors adopt DNA sequence alignment algorithms and extract common API call sequence patterns of malicious function from malware in different categories.

Prof. Bhavin Shah[52] Surveyed the existing mobile agent based intrusion detection systems clearly shows poor response time and large agent size as major challenges.

Ming Zhang[53] proposed an anomaly detection model based on One-class SVM to detect network intrusions. The one-class SVM adopts only normal network connection records as the training dataset. But after being trained, it is able to recognize normal from various attacks.

Nattawat Khamphakdee[54] proposed a procedure for improving Snort IDS rules, based on the association rules data mining technique for detection of network probe attacks.

S. Sangeetha[55] proposed Application level Signature based Semantic Intrusion Detection System, which concentrates on the application level to detect application specific attacks.

Yujie Fan[56] proposed an effective sequence mining algorithm to discover malicious sequential patterns, and then All-Nearest Neighbor (ANN) classifier is constructed for malware detection based on the discovered patterns.

Hisham Shehata Galal[57] proposed a behavior-based features model that describes malicious action exhibited by malware instance. To extract the proposed model, first perform dynamic analysis on a relatively recent malware dataset inside a controlled virtual environment and capture traces of API calls invoked by malware instances.

Akash Garg [58] discussed on Snort, mostly used signature based IDS because it is an open source software. It is used world widely in intrusion detection and prevention domain. In this paper, the authors used IDEVAL data set we detect attacks using Snort on this dataset.

Kristof Bohmer[59] proposed a novel automatic signature generation approach for textual business process instance data while respecting its contextual attributes.

Andrea Saracino[60] presented MADAM, a novel host-based malware detection system for Android devices which simultaneously analyzes and correlates features at four levels: kernel, application, user and package, to detect and stop malicious behaviors.

Eduardo Viegas[61] demonstrated that a hardware (HW) implementation of network security algorithms can significantly reduce their energy consumption compared to an equivalent software (SW) version.

Mirza M. Baig[62] presented a cascade of ensemble-based artificial neural network for multi-class intrusion detection (CANID) in computer network traffic. The proposed system learns a number of neural-networks connected as a cascade with each network trained using a small sample of training examples.

Cheng Feng[63] discussed the approach time-series anomaly detection by proposing a stacked Long Short Term Memory (LSTM) network based softmax classifier which learns to predict the most likely package signatures that are likely to occur given previously seen package traffic.

Weizhi Meng[64] focused on MSNs and present a compact but efficient trustbased approach using Bayesian inference to identify malicious nodes in such an environment.

Zhengbing Hu[65] aimed to demonstrate developed anomaly detection system in secure cloud computing environment, show its theoretical description and conduct appropriate simulation.

Eduardo K. Viegas[66] presented a new method for creating intrusion databases. The authors proposed a new evaluation scheme specific to the machine learning intrusion detection field. The authors proposed a new multi-objective feature selection method that considers real-world network properties.

Shadi Aljawarneh[67] developed a new hybrid model that can be used to estimate the intrusion scope threshold degree based on the network transaction data's optimal features that were made available for training.

Anderson Hiroshi Hamamoto[68] has demonstrated the scheme combining Genetic Algorithm and a Fuzzy Logic for network anomaly detection is discussed. The Genetic Algorithm is used to generate a Digital Signature of Network Segment using Flow Analysis, where information extracted from network flows data is used to predict the networks traffic behavior for a given time interval.

Yu Wan [69] proposed a privacy-preserving framework for signature-based intrusion detection in a distributed network based on fog devices.

Yehonatan Cohen[70] showed that malicious webmail attachments are unique in the manner in which they propagate through the network. The authors leverage these findings for defining novel features of malware propagation patterns.

Mohsen Rezvani[71] proposed a novel assessment methodology for anomaly-based IDSs in cloud computing that takes into account both the network and system-level information for generating the evaluation dataset.

Soroush M. Sohi[72] applied a Recurrent Neural Networks (RNNs) known as powerful tools in finding complex patterns and generating similar ones.

Vajiheh Hajisalem[73] proposed a new hybrid classification method based on Artificial Bee Colony (ABC) and Artificial Fish Swarm (AFS) algorithms. The Fuzzy C-Means Clus- tering (FCM) and Correlation-based Feature Selection (CFS) techniques are applied to divide the training dataset and remove the irrelevant features, respectively.

Nachiket Sainis[74] evaluated the use of five ML classification algorithm to deal with the attack classification problem. They are SVM, Naive Bayes, KNN and the Decision Tree based C4.5 (J48) and Random Forest Algorithm.

V. RESEARCH DIRECTION

Following table I depicts the research direction in network security.

TABLE I RESEARCH DIRECTION IN NETWORK SECURITY

S. No.	Security Threats	Security Requirement	Research Direction
1	Denial-of-service (DoS)	Availability	Intrusion detection
2	Unauthenticated or unauthorised access	Key establishment and trust setup	Random key distribution
3	Node capture and compromised node	Resilience to node compromise	Inconsistency detection and node revocation
4	Routing attacks	Secure routing	Secure routing protocols
5	Message modification	Integrity and authenticity	Keyed secure hash function
6	Message disclosure	Confidentiality and privacy	Link/network layer encryption
7	Intrusion and high-level security attacks	Secure group management, intrusion detection,	Intrusion and high-level security attacks

VI. CONCLUSION

In this paper, we have evaluated many researchers approaches for network security in WSN, IoT, Cloud Computing, WBAN, and Big Data. This article suggests a research area in the domain of security threats for WSN, WBAN, Cloud computing, IoT. In future smart home conditions, there will be multi-modal sensor explications that include the advantages reported. However, there are still problems to surmount to perform these pervasive context-aware applications.

REFERENCES

[1] M. Elbasiony, Reda, *et al*, "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.

[2] S. A. Joshi and Varsha S. Pimprale, "Network Intrusion Detection System (NIDS) based on data mining," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, Vol. 2, No. 1, pp. 95-98, 2013.

[3] Sannasi Ganapathy, *et al.*, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," *EURASIP Journal on Wireless Communications and Networking*, Vol.1, pp.271, 2013.

[4] Louvieris, Panos, Natalie Clewley and Xiaohui Liu, "Effects-based feature identification for network intrusion detection," *Neurocomputing*, Vol. 121, pp. 265-273, 2013.

[5] Jaehak Yu, *et al.*, "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques," *Journal of Systems Architecture*, Vol.59, No.10, pp.1005-1012, 2013.

[6] Monowar H. Bhuyan, *et al.*, "Detecting distributed denial of service attacks: methods, tools and future directions," *The Computer Journal*, Vol.57, No.4, pp.537-556, 2013.

[7] Iftikhar Ahmad, *et al.*, "Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components," *Neural computing and applications*, Vol.24, No.7-8, pp.1671-1682, 2014.

[8] Wenying Feng, *et al.*, "Mining network data for intrusion detection through combining SVMs with ant colony networks," *Future Generation Computer Systems*, Vol.37, pp.127-140, 2014.

[9] Li, Wenchao, *et al.*, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, 2014.

[10] Kuang, Fangjun, Weihong Xu and Siyang Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," *Applied Soft Computing*, Vol.18, pp.178-184, 2014.
[11] Roshan Chitrakar and Chuanhe Huang, "Selection of candidate support vectors in incremental SVM for network intrusion detection," *computers & security*, Vol.45, pp.231-241, 2014.
[12] G. V. Nadiammai and M. Hemalatha, "Effective approach toward Intrusion Detection System using data mining techniques," *Egyptian Informatics Journal*, Vol.15, No.1, pp.37-50, 2014.
[13] Gisung Kim, Seungmin Lee and Sehun 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.
[14] Shamshirband and Shahaboddin, *et al.*, "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks," *Engineering Applications of Artificial Intelligence*, Vol.32, pp.228-241, 2014.
[15] Jeong, EunHee and ByungKwan Lee, "An IP Traceback Protocol using a Compressed Hash Table, a Sinkhole router and data mining based on network forensics against network attacks," *Future Generation Computer Systems*, Vol.33, pp.42-52, 2014.
[16] Shengyi Pan, Thomas Morris and Uttam Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, Vol.6, No.6, pp.3104-3113, 2015.
[17] Mustafa Amir Faisal, *et al.*, "Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study," *IEEE Systems journal*, Vol.9, No.1, pp.31-44, 2015.
[18] Elhag, Salma, et al, "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems," *Expert Systems with Applications*, Vol.42, No.1, pp.193-202, 2015.
[19] Eesa, Adel Sabry, Zeynep Orman and Adnan Mohsin Abdulazeez Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications* ,Vol.42, No.5, pp.2670-2679.2015.
[20] Alheeti, Khattab M. Ali, Anna Gruebler and Klaus D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," *Consumer Communications and Networking Conference (CCNC)*, 2015 12th Annual IEEE. IEEE, 2015.
[21] Kelton AP Costa, *et al.*, "A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks," *Information Sciences*, Vol. 294, pp. 95-108, 2015.
[22] Opeyemi Osanaiye, *et al.*, "Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing," *EURASIP Journal on Wireless Communications and Networking*, 2016. Vol.1, pp. 130.2016.
[23] Vasan, K. Keerthi and B. Surendiran, "Dimensionality reduction using Principal Component Analysis for network intrusion detection," *Perspectives in Science*, Vol.8, pp.510-512.2016.
[24] Nathan Keegan, *et al.*, "A survey of cloud-based network intrusion detection analysis," *Human-centric Computing and Information Sciences*, Vol.6, No.1, pp.19, 2016.
[25] Soo-Yeon Ji, *et al.*, "A multi-level intrusion detection method for abnormal network behaviors," *Journal of Network and Computer Applications*, Vol. 62, pp. 9-17, 2016.
[26] Bamakan and Seyed Mojtaba Hosseini, *et al.*, "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization," *Neurocomputing*, Vol. 199, pp.90-102, 2016.
[27] Aburomman, Abdulla Amin and Mamun Bin Ibne Reaz, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," *AppliedSoftComputing*, Vol. 38, pp.360-372, 2016.
[28] Ashfaq and Rana Aamir Raza, *et al.*, "Fuzziness based semi-supervised learning approach for intrusion detection system," *InformationSciences*, Vol. 378, pp. 484-497, 2017.
[29] Kevric, Jasmin, Samed Jukic and Abdulhamit Subasi, "An effective combining classifier approach using tree algorithms for network intrusion detection," *Neural Computing and Applications*, Vol. 28, No.1, pp.1051-1058, 2017.
[30] Al-Yaseen, Wathiq Laftah, Zulaiha Ali Othman and Mohd Zakree Ahmad Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems with Applications* Vol. 67, pp.296-303.2017.
[31] Elike Hodo, *et al.*, "Shallow and deep networks intrusion detection system: A taxonomy and survey," *arXivpreprintar*, Vol. *Xiv*: 1701. 02145, 2017.
[32] Thaseen, Ikram Sumaiya and Cherukuri Aswani Kumar, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM," *Journal of King Saud University-Computer and Information Sciences*, Vol. 29, No.4, pp.462-472, 2017.
[33] MR Gauthama Raman, *et al.*, "A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems," *NeuralNetworks*, Vol. 92, pp.89-97, 2017.
[34] Abien Fred M. Agarap, "A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data," *Proceedings of the 2018 10th International Conference on Machine Learning and Computing*, *ACM*, 2018.
[35] Syed Ali Raza Shah and Biju Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Future Generation Computer Systems*, Vol. 80, pp.157-170, 2018.
[36] Weizhi Meng, *et al.*, "Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data," *IeeeAccess*, Vol. 6, pp.7234-7243, 2018.
[37] Cabaj, Krzysztof, Marcin Gregorczyk and Wojciech Mazurczyk, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," *Computers & Electrical Engineering*, Vol. 66, pp.353-368, 2018.
[38] Yanfang Ye, *et al.*, "DeepAM: a heterogeneous deep learning framework for intelligent malware detection," *KnowledgeandInformationSystems*, Vol. 54, No.2, pp.265-285, 2018.
[39] Sandeep Kumar Singh, *et al.*, "Joint-Transformation-Based Detection of False Data Injection Attacks in Smart Grid," *IEEE Transactions on Industrial Informatics*, Vol. 14, No.1, pp. 89-97, 2018.
[40] Li, Longjie, *et al.*, "Towards Effective Network Intrusion Detection: A Hybrid Model Integrating Gini Index and GBDT with PSO," *Journal* of *Sensors*, 2018.
[41] Demertzis, Konstantinos and Lazaros Iliadis, "A hybrid network anomaly and intrusion detection approach based on evolving spiking neural network classification," *International* Conference on e-Democracy, *Springer, Cham*, 2013.
[42] Igor Santos, *et al.*, "Opcode sequences as representation of executables for data-mining-based unknown malware detection," *Information Sciences*, Vol. 231, pp.64-82, 2013.
[43] Cristian I. Pinzon, *et al.*, "idMAS-SQL: intrusion detection based on MAS to detect and block SQL injection through data mining," *Information Sciences*, Vol. 231, pp.15-31, 2013.
[44] David Zhao, *et al.*, "Botnet detection based on traffic behavior analysis and flow intervals," *Computers& Security* Vol. 39, pp.2-16, 2013.
[45] Yuxin Ding, *et al.*, "A fast malware detection algorithm based on objective-oriented association mining," *computers &security*, Vol.39, pp. 315-324, 2013.
[46] Hubballi, Neminath and Vinoth Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Computer Communications*, Vol. 49, pp.1-17, 2014.
[47] Gideon Creech, and Jiankun Hu, "A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns," *IEEE Transactions on Computers*, Vol. 63, No.4, pp. 807-819.
[48] Wei Wang, *et al.*, "Autonomic intrusion detection: Adaptively detecting anomalies over unlabeled audit data streams in computer networks," *Knowledge-Based Systems*, Vol. 70, pp.103-117.2014.
[49] Ammar Alazab, *et al.*, "Using response action with intelligent intrusion detection and prevention system against web application malware," *Information Management & Computer Security*, Vol. 22, No.5, pp.431-449, 2014.
[50] Ismaila Idris and Ali Selamat, "Improved email spam detection model with negative selection algorithm and particle swarm optimization," *Applied Soft Computing*, Vol. 22, pp.11-27.2014.

[51] Youngjoon Ki, Eunjin Kim and Huy Kang Kim, "A novel approach to detect malware based on API call sequence analysis," *International Journal of Distributed Sensor Networks*, Vol. 11, No. 6, pp. 659101, 2015.

[52] Bhavin Shah and Bhushan H. Trivedi, "Improving performance of mobile agent based intrusion detection system," *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on IEEE*, 2015.

[53] Zhang, Ming, Boyi Xu and Jie Gong, "An anomaly detection model based on one-class svm to detect network intrusions," *Mobile Ad-hoc and Sensor Networks (MSN), 2015 11th International Conference on. IEEE, 2015*.

[54] Khamphakdee, Nattawat, Nunnapus Benjamas and Saiyan Saiyod, "Improving intrusion detection system based on snort rules for network probe attacks detection with association rules technique of data mining," *Journal of ICT Research and Applications*, Vol. 8, No.3, pp. 234-250, 2015.

[55] S. Sangeetha, *et al.,* "Signature based semantic intrusion detection system on cloud," *Information Systems Design and Intelligent Applications. Springer, New Delhi*, pp. 657-666, 2015.

[56] Yujie Fan, Ye Yanfang and Lifei Chen, "Malicious sequential pattern mining for automatic malware detection," *Expert Systems with Applications*, Vol. 52, pp. 16-25, 2016.

[57] Galal, Hisham Shehata, Yousef Bassyouni Mahdy, and Mohammed Ali Atiea, "Behavior-based features model for malware detection," *Journal of Computer Virology and Hacking Techniques*, Vol. 12, No.2, pp.59-67, 2016.

[58] Akash Garg and Prachi Maheshwari, "Performance Analysis of Snort-based Intrusion Detection System," *Advanced Computing and Communication Systems (ICACCS), 3rd International Conference on IEEE*, Vol. 1, 2016.

[59] Kristof Böhmer and Stefanie Rinderle-Ma, "Automatic signature generation for anomaly detection in business process instance data," *Enterprise, Business-Process and Information Systems Modeling. Springer, Cham*, pp.196-211, 2016.

[60] Andrea Saracino, *et al.,* "Madam: Effective and efficient behavior-based android malware detection and prevention," *IEEE Transactions on Dependable and Secure Computing*, 2016.

[61] Eduardo Viegas, *et al.,* "Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems," *IEEE Transactions on Computers*, Vol. 66, No.1, pp.163-177, 2017.

[62] Mirza M. Baig, Mian M. Awais and El-Sayed M. El-Alfy, "A multiclass cascade of artificial neural network for network intrusion detection," *Journal of Intelligent & Fuzzy Systems*, Vol. 32, No.4, pp.2875-2883, 2017.

[63] Feng, Cheng, Tingting Li and Deeph Chana, "Multi-level anomaly detection in industrial control systems via package signatures and lstm networks," *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on IEEE*, 2017.

[64] Weizhi Meng, *et al.,* "A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks," *Journal of Network and Computer Applications*, Vol. 78, pp. 162-169, 2017.

[65] Zhengbing Hu, *et al.,* "Anomaly detection system in secure cloud computing environment," *International Journal of Computer Network and Information Security*, Vol. 9, No.4, pp.10, 2017.

[66] Eduardo K. Viegas, Altair O. Santin and Luiz S. Oliveira, "Toward a reliable anomaly-based intrusion detection in real-world environments," *ComputerNetworks*, Vol. 127, pp. 200-216, 2017.

[67] Aljawarneh, Shadi, Monther Aldwairi and Muneer Bani Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, Vol. 25, pp.152-160. 2018.

[68] Hamamoto, Anderson Hiroshi, *et al.,* "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Systems with Applications*, Vol. 92, pp. 390-402, 2018.

[69] Yu Wang, *et al.,* "A fog-based privacy-preserving approach for distributed signature-based intrusion detection," *Journal of Parallel and Distributed Computing*, Vol. 122, pp. 26-35, 2018.

[70] Cohen, Yehonatan, Danny Hendler and Amir Rubin, "Detection of malicious webmail attachments based on propagation patterns," *Knowledge-Based Systems*, Vol. 141, pp. 67-79, 2018.

[71] Mohsen Rezvani, "Assessment Methodology for Anomaly-Based Intrusion Detection in Cloud Computing," *Journal of AI and Data Mining*, Vol. 6, No. 2, pp. 387-397, 2018.

[72] Soroush M. Sohi, Fatemeh Ganji, and Jean-Pierre Seifert, "Recurrent Neural Networks for Enhancement of Signature-based Network Intrusion Detection Systems," *arXivpreprintarXiv*: 1807.03212, 2018.

[73] Hajisalem, Vajiheh, and Shahram Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," *Computer Networks*, Vol. 136, pp.37-50, 2018.

[74] Sainis, Nachiket, Durgesh Srivastava, and Rajeshwar Singh, "Feature Classification and Outlier Detection to Increased Accuracy in Intrusion Detection System," *International Journal of Applied Engineering Research*, Vol. 13, No.10, pp.7249-7255, 2018.