International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Survey on Intrusion Detection System

Jesu Jayarin. P[1], Blessing Solomon. B.C[2]

[1] Associate Professor, Department of Computer Science Engineering, Jeppiaar Engineering College, Chennai, Tamil Nadu, India

[2]PG Scholar, Department of Computer Science Engineering, Jeppiaar Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

Intrusion Detection Systems (IDSs) are a major line of defense for protecting network resources from illegal penetrations. A typical approach in interruption discovery models, particularly in irregularity recognition models, is to utilize classifiers as finders. Selecting the best set of features is central to ensuring the performance, speed of learning, accuracy, and reliability of these detectors as well as to remove noise from the set of features used to construct the classifiers. In most current systems, the features used for training and testing the intrusion detection systems consist of basic information related to the TCP/IP header, with no considerable attention to the features associated with lower level protocol frames. This survey paper aims at disclosing different strategies followed in Intrusion Detection Systems (IDSs) over the years. Due to the advancement in technologies, our coherent view is only on the latest trends.

Keywords: Anomaly Detection, Computer Security, Intruders, Intrusion Detection System

I. INTRODUCTION

Internet is a global public network. With the growth of the Internet and its potential, there has been subsequent change in business model of organizations across the world. More and more people are being connected to the Internet every day to take advantage of the new business model popularly known as e-Business. Internetwork network has along these lines turn out to be extremely basic part of the present e-Business. There are two sides of business on the Internet. On one side, the Internet brings in tremendous potential to business in terms of reaching the end users. At the same time, it also brings in lot of risk to the business. There are both harmless and harmful users on the Internet. While an organization makes its information system available to harmless Internet users, at the same time the information is available to the malicious users as well. The nature of mobility creates new vulnerabilities that do not exist in a fixed wired network, and yet many of the proven security measures turn out to be ineffective. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. We need to develop new architecture and mechanisms to protect the wireless networks. Malicious users or hackers will get access to an organization's internal systems in numerous reasons.

These are,

- ✓ Software bugs called vulnerabilities
- ✓ Lapse in organization
- ✓ Leaving frameworks to default arrangement

The vindictive clients utilize diverse strategies like Password breaking, sniffing decoded or clear content activity and so on to misuse the framework vulnerabilities said above and trade off basic frameworks. In this manner, there should be some sort of security to the association's private assets from

the Internet and additionally from inside clients as review says that 80% of the assaults occur from inside clients for the very truth that they know the frameworks substantially more than an outsider knows and access to data is simpler for an insider.In this manner, there should be some sort of security to the organization's private assets from the Internet and additionally from inside clients as review says that 80% of the assaults occur from inside clients for the very truth that they know the frameworks substantially more than an outsider knows and access to data is simpler for an insider.

II. INTRUSION DETECTION SYSTEM

Intrusion detection can be characterized as the computerized discovery and consequent age of a caution to alarm the security contraption at an area if interruptions have occurred or are occurring.
An IDS is a defence system that detects hostile activities in a network and then tries to possibly prevent such activities that may compromise system security.

IDSs achieve detection by continuously monitoring the network for unusual activity. The prevention part may involve issuing alerts as well as taking direct preventive measures such as blocking a suspected connection. In other words, intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. What's more, IDS devices are fit for recognizing insider assaults beginning from inside the system and outer ones. Unlike firewalls, which are the first line of defense, IDSs appear only after an intrusion has occurred and a node or network has been compromised. That is why IDSs are aptly called, the second line of defense.

Generally speaking, an IDS:

- ✓ is NOT an antivirus program designed to detect malicious software's such as viruses, Trojans, and worms.
- ✓ is NOT a network logging system used, for example, to detect complete vulnerability to any DoS attack across a congested network. These are network traffic monitoring systems.
- ✓ is NOT a vulnerability assessment tool that checks for bugs and flaws in operating systems and network services. Such an activity would fall under the purview of security scanners.

With so much advancement in hacking, if attackers try hard enough, they will eventually succeed in infiltrating the system. This makes it important to monitor what is taking place on a system and look for suspicious behavior. Intrusion Detection Systems do just that. The wireless links between nodes are highly susceptible to link attacks, which include passive eavesdropping, active interfering, and leakage of secret information, data tampering, impersonation, message replay, message distortion, and denial of service.

III. INVESTIGATION IN INTRUSION DETECTION SYSTEM – REVIEW FROM DIFFERENT AUTHORS

A. [1] "Bandwidth Spoofing and Intrusion Detection System for Multistage 5G Wireless Communication Network", (2018)

With the growing number of users in the network, it has become very important to maintain the security. In the present generation, the level of the security need to be raised. [1] analyzed the different aspects of security threats in 5G WCN. The major goal of 5G WCN is to increase the capacity as well as to reduce the load at the BS. To achieve this, [1] introduced the concept of relays, SCAs and wi-fi hotspots. However, this introduction has paved the way for the possible security breach in to the network, as they provide active sites for the attackers. Hence, 5G WCN has now become highly vulnerable to security threats. The key focus of [1] is on the security threats, particularly, the bandwidth spoofing attack on the Relay, SCA and BS. [1] concluded that the prisoner's dilemma game theory is a suitable method for investigating the bandwidth spoofing attack in the

multi stage 5G WCN and this is supported with the results, in which the intruder is successfully spoofing the bandwidth from the valid client with a substantial winning percentage. After the successful intrusion-using prisoner's dilemma game theory, [1] has provided an adaptive intrusion detection system for the multi stage 5G WCN. The proposed adaptive intrusion detection system is capable of detecting and eliminating an intruder attack, which is intended for the bandwidth spoofing attack on the Relay, SCA and BS. [1] has incorporated the concept of power levels of the Relay, SCA and BS with probability of the intruder to intrude in to the network. It is concluded from the simulation results that in the multi stage 5G WCN, the BS is having the maximum intruder detection capability as compared to the SCA and Relay because of the more power levels.

Remark: All over the world, there is a gigantic stir in the number of subscribers, which gave rise to numerous challenges, like interference management and capacity enhancement. The enabling candidates to deal with this plight are the enabling technologies of the 5G wireless communication networks.

B. [2] "A Literature Survey on Intrusion Detection and Protection System using Data Mining", (2018)

In the cutting edge universe of security, numerous analysts have proposed different new methodologies; among those procedures, use of information digging for Intrusion identification is outstanding amongst other reasonable methodologies. The system proposes a security system; name the Intrusion Detection and Protection System (IDPS) at system call level, which creates a personal profile for the user to keep track of user usage habits as the forensic features. The IDP utilizes a nearby computational network to distinguish malignant conduct in a continuous way. In [2], a security system named the IDPS is proposed to detect insider attacker at SC level by using data mining and forensic techniques.

Remark: In [2], Intrusion Detection and Identification System (IDIS), which mines log data to identify commands and their sequences (together named command sequences) that a user habitually submits and follows respectively as the user's forensic features. At the point when an obscure client sign in to a PC, the IDIS begins observing the client's information orders, to recognize whether the clients are issuing an assault. IIDPS can square interior gatecrashers and recognize the aggressor in the system.

C. [3] "Zero-Knowledge Authentication and Intrusion Detection System for Grid Computing Security", (2018)

[3] gives, an interest to the insider threats in the Grid computing. Thus, to address these security issues [3] proposed a solution based on a mutual authentication using zero-knowledge proof and an IDS that benefits from the flexibility and interoperability of mobile agents to conserve traces and proofs of the jobs execution. The practical evaluation of the solution, when compared to Client/Server architecture, demonstrates very promising results: low response time, less network load and high intrusion detection capacity.

Remark: For future works, [3] thinks to associate the detection with suitable prevention policy and make use of heuristics to replace the random scheduling and optimize agent's mobility.

D. [4] "Optimized Packet Filtering Honeypot with Snooping Agents in Intrusion Detection System for WLAN", (2018)

Wireless LAN networks are widely used and efficient infrastructure used in different domains of communication. [4] worked on Network Intrusion Detection System (NIDS) to prevent intruder's activities by using snooping agents and honeypot on the network. The thought behind utilizing snooping specialists and honeypot is to give network administration in term of checking. Honey pot is placed just after the Firewall and intrusion system have strongly coupled synchronize with snooping agents Monitoring is considered at packet level and pattern level of the traffic. Simulation filtered and

monitor traffic for highlight the intrusion in the network. Further attack sequence has been created and have shown the effects of attack sequence on scenario which have both honey pot and snoop agent with different network performance parameters like throughput, network load, queuing delay, retransmission attempt and packet. The simulation scenario shows the impact of attack on the network performance.

Remark: An intrusion detection system (IDS) enables the administrators to detect suspicious packets, activities, network vulnerabilities and attacks. All network traffic can be observed with the help of IDS and it is easy to detect as well as decode malicious traffic on a honey net and log some malicious packets at a centralized database. Honey pot have many advantages such as small data sets which collect limited amount of information instead of gigabytes of data logging, reduced false positive for legitimate activity, catching false negatives for malicious activities, working with encrypted and IPV6 environment, highly flexible and simple, require minimal resources to capture bad activity.

E. [5] "Network intrusion detection system for drone fleet using both spectral analysis and robust controller / observer", (2018)

[5] proposes a robust controller / observer for anomaly estimation inside UAV networks. This method is based on both Lyapunov Krasovkii functional and dynamic behavior of TCP (Transmission Control Protocol). This observer considers, as a preliminary step, a statistical signature of the traffic exchanged in the network. Both observer and spectral signature provide an accurate estimation of the traffic which is used to detect and characterize the different anomalies that can be observed in the UAV network. Consequently, the different signatures that we can process, based on the different types of intrusion we generate in the network, are used to select the accurate model for robust control estimation. This selection is conducted by choosing a specific controller / observer among a dedicated bank of models. The first statistical signature extraction of the analyzed traffic is run with a multi-fractal analysis. This solution based on wavelet analysis has been selected because it offers a wide spectral characterization of the entire traffic process. The wavelet-based analysis methodology has been widely used for the last decade for Internet traffic characterization but this is the first time that this tool has been used on a UAV ad hoc network traffic. Moreover, several research studies on network anomaly estimation have been carried out using automatic control techniques. These studies provide methods for designing both observer and command laws dedicated to time delay problems while estimating the anomaly or intrusion in the system. As a first result, the designed controller / observer system has been successfully applied to some relevant practical problems such as ad hoc networks for aerial vehicles and the effectiveness is illustrated by using real traffic traces including Distributed Denial of Service (DDoS) attacks.

Remark: [5] shows promising perspectives for Intrusion Detection System (IDS) in a fleet of UAVs. Indeed, different types of anomaly have been considered and the intrusion detection process accurately detects them all.

F. [6] "Intrusion Detection based on a Novel Hybrid Learning Approach", (2018)

[6] proposed a hybrid learning approach through a combination of K-Medoids clustering, Selecting Feature using SVM, and also Naïve Bayes classifier. The KDD CUP'99 benchmark dataset was used for evaluation. The experimental results obtained showed that our proposed approach was an efficient one. In [6], a new training dataset is created by K-Medoids clustering and Selecting Feature using SVM. Then it's performance is evaluated by the Naïve Bayes classifier. The results obtained showed that [6] performed well in terms of accuracy, detection rate, and also false alarm rate.

Remark: An interesting aspect that can be developed in the future is to consider a hybrid approach that performs better in detecting the R2L, U2R, and Probe attacks. Another emphasis to put on the research work was to find a new way to choose the number of clusters and also the initial cluster medoids.

G. [7] "A Data Classification Model: For Effective Classification of Intrusion in an Intrusion Detection System Based on Decision Tree Learning Algorithm", (2018)

In modern era of technology, the need of data and computation is increasing continuously. Every individual's hand is mounted with the new generation gadgets and smart devices, which is increasing the data exponentially. Data classification makes the things easier. It categorizes the voluminous data. In addition, it increases the accuracy of the result. [7] presented a data classification model for intrusion detection system by decision tree learning and this model calculates information gain in a different way by giving more significance to more important attribute instead of an attribute which is having more different values. The accuracy of proposed classifier is better.

Remark: [7]implemented the existing ID3 and the modified ID3 on JAVA platform. The experimental study has proved that the accuracy of the proposed ID3 is better as compared to the existing one.

H. [8] "Intrusion Detection System for Electronic Communication Buses: A New Approach", (2018)

With innovation and PCs winding up increasingly, modern and promptly accessible, cars have taken action accordingly by coordinating increasingly microcontrollers to deal with errands extending from controlling the radio to the brakes. Handling all of these separate processors is a communication system and protocol known as Controller Area Network (CAN) bus. However, this presents an opportunity for an outside party to interfere with the operations of a car. An existing node for the CAN bus could be swapped out for one that has been tampered with, causing potentially fatal accidents. To guard against this possibility, [8] will present an algorithm designed to recognize nodes based on the noise content of their signal so that any new hardware will trigger a flag that an unrecognized source is trying to interfere. The algorithm makes use of the MATLAB and Python programming languages to calculate certain characteristics of the noise in the signal and pass those through a machine learning algorithm. This algorithm is able to learn through mathematical means what each node "sounds like". With over 99% accuracy, [8] is able to predict which node sent a given signal.

Remark: [8] presents a promising method for identifying devices on a communication bus. While this work focused mainly on the CAN bus, such identification has obvious security benefits for any communication bus. Knowing the origin of a message can identify both the addition of new units to the bus, as well as compromised units that are attempting to take control of functionality for malicious purposes.

I. [9] "A two-stage flow-based intrusion detection model for next-generation networks", (2018)

[9] proposed a two-arrange stream based interruption discovery display for cutting edge systems. Cutting edge systems give voice, video and information benefits on a focalized IP-based system. Our stream based interruption location framework is especially helpful with regards to cutting edge systems (NGN) where distinctive systems are joined to an all IP stage. Our proposed show forms the stream information in a two-organize recognition process. The primary stage utilizes a one-class SVM for effective discovery of noxious streams. The one-class SVM disposes of every single typical activity and forward the malignant movement to second stage location process. Because of the two-arrange interruption recognition process, just vindictive streams are broke down in detail. Another essential component of our framework is the utilization of unsupervised learning. The unsupervised learning does not require a marked preparing datasets which are hard to get for cutting

edge systems. We have approved the approach on three stream based datasets and results demonstrate that the proposed show gives promising outcomes. In future, the proposed interruption discovery model can be executed utilizing extra stream characteristics. The IPFIX/Netflow v9 characterize around 280 stream traits which give top to bottom data about the system activity. These extra ascribes can be utilized to fabricate interruption recognition plans for location of novel and stealth assaults.

Remark: [9] utilizes an upgraded one-class SVM in the main stage. One-class SVM strategies give better outcomes for interruption identification in malignant stream records. A limitation of enhanced one-class SVM is the requirement that malicious flows in the training set are in sufficiently higher than normal flows. In second stage identification, [9] utilized SOM for programmed bunching of malevolent streams. The results show that SOM correctly places the majority of flows in the correct cluster. However, domain knowledge of the traffic is required to determine the number and label of attack clusters. Our system uses unsupervised learning techniques, and no labeled datasets are required for training. [9] evaluated the proposed IDS on the three flow-based datasets. The results demonstrate that [9] is accurate in the separation of malicious flows and grouping of malicious flows in different attack clusters.

J. [10] "High-Throughput Low-Power Variable Rate Network Intrusion Detection System Using Unique SRAM Controller", (2018)

[10] proved the merits of input payload driven multi-rate parallel matching in NIDS system in terms of high throughput and power efficiency. The problem over multi-rate is also being mitigated through reconfigurable clock divider with fully digitalized PLL whose dynamic range can be changed dynamically. To extend the merits of early detection during bitwise pattern matching clock gated controller is used for controlling both FSM and rule selection. The power efficiency is proved to be tolerable one over area overhead.

Remark: However, the computational accuracy and overall power reduction largely depend on a number of patterns used and user rate. Finally, Payload drove digital frequency synthesizer is also verified and its dynamic range is proved to be in several GHz since payload-incoming speed can be started from Kbps to Gbps.

K. [11] "An Enhanced Intrusion Detection System Based on Clustering", (2018)

In [11] detection rates for k-means clustering with and without SOM training are shown for refined algorithm and the approach leads to the conclusion that when SOM is trained for detecting unlabelled intrusions, it may or may not be able to generate good results. Thus, the SOM must be trained repeatedly using different numbers of nodes until the improved results are found. The false-positive alarm rates can be increased by clustering the data efficiently so that it is able to differentiate correctly between the normal data and abnormal data and the training of SOM must be done accordingly.

Remark: The initialization of cluster in the beginning helps us in working with a finite number of clusters. K-means clustering helps in fast computing since the number of clusters is defined beforehand. However, the initialization plays an important role as different values will give different results. The k-means clustering algorithm is able to reduce the percent of false-positive alarm rate.

L. [12]"Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition",(2018)

An intrusion detection system (IDS) is primarily used to protect nuclear power plants from external threats, such as sabotage and malicious attacks. However, earlier versions of IDSs are configured to detect an intrusion from visual inspection by an operator. This has the disadvantages of requiring standby human resources and relying on operator capabilities. [12] propose an image-based intelligent intrusion detection system (IIDS) with a virtual fence, active

intruder detection, classification, and tracking, and motion recognition to solve these limitations. An integrated acquisition device was manufactured combining optical and thermal cameras to compensate for the disadvantages of optical cameras, which have difficulty detecting an intrusion at night, under adverse weather conditions, and when the intruder is camouflaged. The virtual fence has a function to set the boundary between surveillance and external areas in a graphical user interface, and to define an early pre-alarm area if necessary. The background model is designed to detect moving objects, and detected objects are segmented into bounding boxes. We implemented a network model based on a convolutional neural network (CNN) to classify moving objects as either intruders or wild animals. If an intruder is detected in real time and is crossing the virtual fence, the alarm tile blinks with the associated color. Five types of intruder behavior patterns are recognized by optimizing a long-term recurrent convolutional network (LRCN) model. The proposed IIDS meets the physical protection requirements recommended in the nuclear regulatory guidelines, and can be used as an unmanned surveillance system. It is expected to perform more active and reliable intrusion detection in combination with existing sensors, such as microwaves, electric fields, and fence disturbance sensors in a nuclear power plant.

Remark: [12] provides a) IIDS used to protect nuclear facilities from external threats. b) Virtual fence with multi-level intrusion alarms. c) Automatic intruder classification feature with wild animals. d) Five intruder behaviors (Running, Walking, Crawling, Jumping and Climbing)

M. [13] "Proposed Network Intrusion Detection System Based on Fuzzy c Mean Algorithm in Cloud Computing Environment", (2018)

Nowadays cloud computing is an integral part of IT industry and cloud computing provides the working environment to share data and resources over the internet. Virtual grouping of resources offered over the internet lead to different matters related to the security and privacy in cloud computing. Consequently, making interruption discovery is imperative to distinguish outcast and insider interlopers of distributed computing with high identification rate and low false positive alert in the cloud condition. [13] proposed network intrusion detection module using fuzzy c mean algorithm and used kdd99 dataset for the experiments.

Remark: [13] characterized by a high detection rate with low false positive alarm.

N. [14] "Network intrusion detection system based on recursive feature addition and bigram technique", (2018)

[14] proposing a NIDS in light of a component choice strategy called Recursive Feature Addition (RFA) and bigram technique. [] tested the model on the ISCX 2012 data set, which is one of the most well-known and recent data sets for intrusion detection purposes. Furthermore, [14] proposing a bigram technique to encode payload string features into a useful representation that can be used in feature selection. In addition, a new evaluation metric called (combined) that combines accuracy, detection rate and false alarm rate in a way that helps in comparing different systems and selecting the best among them. The designed feature selection-based system has shown a noticeable improvement on the performance using different metrics.

Remark: Usually, for the stealthy and low profile attacks (zero – day attacks), there are few neatly concealed packets distributed over a long period to mislead firewalls and NIDS. Besides, there are many features extracted from those packets, which may make some machine learning-based feature selection methods to suffer from over fitting especially when the data have large numbers of features and relatively small numbers of examples.

O. [15] "Research and Application of Intelligent Intrusion Detection System with Accuracy Analysis Methodology", (2018)

In [15], as perimeter intrusion detection is of great value to security defense, an innovative intelligent intrusion detection system is analyzed and applied. The system is systematically designed through network topology, consisting of Infrared Image Collection and Pre-processing Module, Data Transmission Module, Intelligent Analysis and Automatic Alarm Module. Infrared Imagery Pre-processing is achieved through innovatively application of FLIR Tau 2336 based on advanced wavelet algorithm, considerably minimizing noises and enhancing details. Besides, synergistic action of intelligent analysis and automatic alarm are achieved through intelligent comparison between extracted imagery and models of pedestrian and vehicle. Additionally, creative arrangement design of thermal infrared cameras is connected to maintain a strategic distance from daze zone of intrusion detection. Through mix deployment of clockwise and anti-clockwise cameras, full coverage of security perimeter is achieved through only 14 thermal cameras, which is of great economic advantage. At last, precision investigation methodology is proposed and test results are out - Detection Rate for all test areas is 100%, and over 90% of test areas are with high caution exactness (over 90%). Alarm Accuracy and Missed-Alarm Rates are dependent on the distance between test and cameras, and the best alarm distance is 175.72m. In [15] results are acceptable, being of great efficiency and economic advantage.

Remark: Many international companies propose integrated solutions for perimeter intrusion detection. In complex outdoor scenarios with masking background texture or lack of illumination, the thermal signature of persons is more prominent compared to the visual optical signature.

IV. CONCLUSION

This survey paper specifies that IDS are turning into the sensible subsequent stage for some associations in the wake of sending firewall innovation at the system border. IDS can offer security from outside clients and interior aggressors, where movement doesn't go past the firewall by any means. Tight mix amongst host and system based IDS is particularly fundamental. It is encouraged to utilize arrange based IDS inside and outside the firewall or between every firewall in a multi-layered condition and host construct IDS with respect to all basic or key hosts. Additionally, it is critical in spite of the fact that not generally important to have an incorporated organization of host based and arrange based Intrusion Detection Systems.

As security keeps on moving to the inside stage, chiefs and system directors alike are starting to concentrate on interruption discovery innovation. While cutting edge IDSes are a long way from impenetrable, they can increase the value of built up data security programs. With merchants chipping away at dispensing with the weaknesses of Intrusion Detection Systems, the future looks brighter for this innovation.

V. REFERENCES

[1]. Akhil Gupta, Rakesh Kumar Jha, Pimmy Gandotra, "Bandwidth Spoofing and Intrusion Detection System for Multistage 5G Wireless Communication Network", IEEE Transactions on Vehicular Technology, Vol.67, 1(2018), DOI: 10.1109/TVT.2017.2745110

[2]. Chaitali Choure , Leena H. Patil, "A Literature Survey on Intrusion Detection and Protection System using Data Mining", International Journal of Advance Research, Ideas and Innovations in Technology, Vol.4, 1(2018), 61 - 65.

[3]. Ennahbaoui M., Idrissi H, "Zero-Knowledge Authentication and Intrusion Detection System for Grid Computing Security", Information Innovation Technology in Smart Cities, (2018), 199-212, https://doi.org/10.1007/978-981-10-1741-4_14

[4]. Gulshan Kumar, Rahul Saha, Mandeep Singh and Mritunjay Kumar Rai, "Optimized Packet Filtering Honeypot with Snooping Agents in Intrusion Detection System for WLAN", International Journal of Information Security and Privacy, 12,1(2018), DOI: 10.4018/IJISP.2018010105

[5]. Jean Philippe Condomines, Riad Chemali, Nicolas Larrieu, "Network intrusion detection system for drone fleet using both spectral analysis and robust controller / observer", ENAC – Ecole Nationale de l'Aviation Civile, (2018), https://hal-enac.archives-ouvertes.fr/hal-01652296/

[6]. Khalvati. L, M. Keshtgary and N. Rikhtegar, "Intrusion Detection based on a Novel Hybrid Learning Approach", Journal of AI and Data Mining Vol. 6, 1(2018), 157-162. DOI: 10.22044/JADM.2017.979

[7]. Latika Mehrotra, Prashant Sahai Saxena and Nitika Vats Doohan, "A Data Classification Model: For Effective Classification of Intrusion in an Intrusion Detection System Based on Decision Tree Learning Algorithm", Information and Communication Technology for Sustainable Development, Vol. 9(2018) Springer, DOI: https://doi.org/10.1007/978-981-10-3932-4_7

[8]. Matthew Spicer, "Intrusion Detection System for Electronic Communication Buses: A New Approach", (2018), https://vtechworks.lib.vt.edu/handle/10919/81863

[9]. Muhammad Fahad Umer, Muhammad Sher, Yaxin Bi, "A two-stage flow-based intrusion detection model for next-generation networks", https://doi.org/10.1371/journal.pone.0180945

[10]. Nagaraju. S, Sudhakara Reddy. P, "High-Throughput Low-Power Variable Rate Network Intrusion Detection System Using Unique SRAM Controller", Proceedings of 2nd International Conference on Micro-Electronics, Electromagnetics and Telecommunications, Vol. 434(2018), DOI: https://doi.org/10.1007/978-981-10-4280-5_18

[11]. Samarjeet Borah, Ranjit Panigrahi and Anindita Chakraborty, "An Enhanced Intrusion Detection System Based on Clustering", Progress in Advanced Computing and Intelligent Engineering, (2018), 37-45.

[12]. Seung Hyun Kim, Su Chang Lim, Do Yeon Kim, "Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition", Annals of Nuclear Energy, Vol.112, (2018), 845-855.

[13]. Shawq Malik Mehibs, Soukaena Hassan Hashim, "Proposed Network Intrusion Detection System Based on Fuzzy c Mean Algorithm in Cloud Computing Environment", Journal of University of Babylon, Vol. 26, 2(2018), 27-35. https://doi.org/10.29196/jub.v26i2.471

[14]. Tarfa Hamed, Rozita Dara, Stefan C. Kremer, "Network intrusion detection system based on recursive feature addition and bigram technique", Computers & Security, Vol.73 (2018), 137-155, DOI: https://doi.org/10.1016/j.cose.2017.10.011

[15]. Xianwei Hu, Tie Li, Zongzhi Wu, Xuan Gao, Zhiqiang Wang, "Research and Application of Intelligent Intrusion Detection System with Accuracy Analysis Methodology", Infrared Physics & Technology, (2018), https://doi.org/10.1016/j.infrared.2017.11.032