International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

Proficient Approach for Intrusion Detection using Behaviour Profiling Algorithm and Prevention Using Statistical Model in Cloud Networks

[1*]D.Rajagopal[1], [2]Dr.K.Padmanabhan

[1]Research Scholar and Assistant Professor, PG and Research Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Namakkal Dt, Tamilnadu, India.

[2]Professor, PG and Research Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Namakkal Dt, Tamilnadu, India.

*Corresponding author: email: sakthiraj2782007@gmail.com, rajagopal@vicas.org;

Abstract:

Objectives:

The objective of the paper is to discuss the proposed dynamic software model to detect and prevent intrusion in the cloud network.

Methods:

The Behavior Profiling Algorithm (BPA) has been used to detect the intrusion in cloud network. For finding the intruder in the network the Event Log Entries and the network Unique Identification Address (UIA) has been fetched from the server and then the collected attribute values have been transferred to prevention module. In the prevention module the dynamic statistical approach model has been used to prevent the network systems and data which are available in the Cloud Network.

Findings:

For testing the proposed model the 100 cloud network systems were taken and based on the loss of packets (in MB) ranges the samples were classified as 0-100, 101-200, 201-300, 301-400, 401-500, 501-600, 601-700 respectively. The range of data loss is assumed to be an interval of 100 Mbps. It is assumed that the higher the data loss ranges, the more data is lost. The mean, variance, and standard deviation were calculated to verify the data loss ranges. The mean (average) of the data loss in the ranges 0-100 is 060.77 and the mean in the ranges 101-200 is 144.714 data losses, which gradually increases in proportion to the data loss ranges, and in the ranges 601-700 it is 665.769 data losses. From the statistical approach model, the differences between mean and variance indicated that the intruder attacked the files during the data transformation in the network. Therefore, the administrator has to monitor the warning message from the proposed IPS model and get data packet losses in the transformation. If the frequency of data loss is low, the administrator can assume that the data flow is low due to network problems. On the other hand, if the frequency of data loss in the network system is high, he can block the transformation and protect the data file. This paper concludes that the behavioral profiling algorithm combined with a statistical model achieves an efficiency of over 96% in wired networks, over 97.6% in wireless networks, and over 98.7% in cloud networks.

Novelty:

In the previous paper discussed the approach which has been implemented with 40 nodes and the result of the proposed algorithm produced above 90%, 96% and 98% in the wired, wireless and cloud network respectively. Now, the model has been implemented with 100 nodes the result has been increased. This study concluded that, the efficient algorithm to detect the intrusion is behaviour profiling algorithm, while join with the statistical approach model, it produces efficient result.

Keywords: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Behavior Profiling Algorithm, Statistical Approach Model.

1. Introduction

Many services offered by cloud computing are free to users, including the ability to store and retrieve data from anywhere in the world. Due to the fact that data in a distributed system can be accessed from anywhere in the world, distributed systems and cloud computing are similar technologies. In contrast, in cloud computing, all data is stored online and can be accessed from any location [17]. Three cloud computing models are available to users. They are private, public and hybrid [8]. The public model is an open model that can be accessed by anyone in the world [2]. The cloud servers are always managed and operated by third parties, as it is created exclusively for a company and only it can use it. The private cloud is much more reliable and secure than the public clouds [5]. Many companies have moved from using public clouds to private clouds. The third type of cloud computing is called hybrid cloud and combines the best elements of the first two clouds [17].

Nowadays, a variety of devices are available to satisfy users' needs, including fast networks and powerful computer processors [7, 14]. Unfortunately, security issues have increased with our growing reliance on IT [14]. Many

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

organizations rely on NIDPS to protect their data sources and systems as computer network and Internet security face growing challenges [14, 16]. Because leaked information can cause significant damage, it is critical for both businesses and individuals to protect computer and network information. Intrusion detection systems are critical to prevent such situations. Recently, various machine learning strategies have been developed to improve the performance of intrusion detection systems [20]. For this reason, network security is of critical importance and an entire industry has emerged to develop better software and hardware platforms to detect and eliminate network threats [13]. There are limitations in the capacity to perform certain software activities, despite the fact that researchers have designed hardware IDPS to process millions of packets simultaneously in the communication.

Moreover, hardware-based NIDPS solutions have problems with limited memory size [9, 10, 13]. To properly identify the malicious node and prohibit it from further communication, an abuse detection and prevention system must be developed [23]. The Intrusion or Abuse or Anomaly Detection System is a programming instruction that detects suspicious activities and network policy violations [4, 6, 12]. The intrusion detection system is capable of detecting cloud-based malware [3]. When a hacker tries to attack the cloud data center, it sends an alert to the administrator [17].

Security tools such as adaptive security applications, intrusion detection system (IDS) intrusion prevention system (IPS) and re-walls all have misuse detection as a core component [8]. Various intrusion detection methods are used, but their effectiveness is a problem [6]. The performance of intrusion detection depends on the accuracy, which needs to be increased to reduce false positives and increase the detection rate [20]. The three basic categories of malware detection techniques are static, dynamic, and hybrid [25]. Static techniques, often referred to as misuse-based or signature-based, maintain an up-to-date database of dangerous code patterns or attack signatures and scan the code for these signatures without actually executing it [15].

Each network-connected device that is attacked and the network-wide attack frequency are tracked [11, 13, 35]. The cloud server is protected from attacks using a variety of solutions [17]. Although open source is the most popular type of NIDPS software with configured platforms, their communication performance is still a major problem in high-speed networks [13]. Moreover, hardware-based NIDPSs are relatively expensive but offer a wide range of processing speeds. Software solutions are preferred over hardware solutions because they are flexible and inexpensive [14]. Dynamic approaches, on the other hand, which track the activity of an application as it runs, are sometimes referred to as behavior-based or anomaly-based. They build a model of typical behavior. Any observation that deviates significantly from this paradigm is considered deviant behavior [15].

2. Review of Literature

The real-time Intrusion Detection Expert System (IDES) described **Dorothy E. Denning (1987)**. It is based on the idea that exploiting system vulnerabilities entails aberrant use of the system. Therefore, anomalous patterns of system usage could be used to identify security infractions. They came to the conclusion that the suggested model offers a solid foundation for the development of effective real-time intrusion detection systems that can identify a variety of intrusions related to attempted break-ins, masquerading, system penetrations, Trojan horses, viruses, leakage and other abuses by legitimate users and some covert channels. They do not propose to replace any security controls with IDES, however.

Sathish Kumar et al. in 2007 presented statistically based on intrusion detection framework for computer networks, and it employed the six-sigma technique to determine the thresholds for the critical network. Network data was used to identify the thresholds, which were then used to monitor unusual network behavior. DARPA has employed a benchmark for performance evaluation. The suggested model uses SBID based on six sigma approaches to provide 75% to 80% accuracy.

Mahboubian and Nor I Udzir (2013) suggested a new IDS model based on an Artificial Immune System (AIS) which has used a statistical approach model. With the use of binary detector sets, the model improved in terms of speed and detection rate, leading to increased performance. DARPA data set has been used to examine the model. The Probe channel recorded the highest accuracy rate since (91.32%). They choose to raise the model's accuracy % and put it in a real network as their future enhancement.

Waskita et al. (2014) suggested a creative method to statistically analyze network traffic. An ID has assessed a vast amount of network traffic's raw data to determine whether any of it is malicious. Each server in a network continuously analyzes incoming and outgoing packets by employing active ports. This behavior makes it possible to spot the infiltration. By using the raw data, such as time scales like Minute, Hour, Day, and Month, as well as the quantity of packets, a graph can be drawn. The model weakness, according to scientists, is that it only saves a small quantity of preprocessed data and performs dynamic calculations over a range of time scales and data collection periods.

Aneetha et al. (2015) used preprocessing, multivariate statistical analysis, and other components to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

create the Hotellings T2 approach and a multivariate statistical strategy for intrusion detection. The KDD Cup'99 dataset used for validation and testing, producing high detection rates or 100% detection rates in normal, R2L. The threshold range calculated using the Central Limit Theorem (CLT). The detection rates for DOS and probe classes are 99.77% and 97.32%, respectively. Because there are not as many traffic profiles in U2R (User to Root), the false alarm rate is higher.

Luca Boero et al. in 2016 proposed Statistical fingerprint-IDS (SF-IDS), a network based IDS that can be determined, if IP traffic is infected with malware or not**.** The model was divided into two phases: training and classification/decision-making. A group of IP flow statistical parameters represents the statistical fingerprints that are extracted in both phases. The fundamental tenet is that each flow's nature, whether malicious or not, can be determined by its statistical fingerprint.

Anup Ingle et al. (2016) provided a method for identifying aberrant network traffic for the detection of UDP spoofing attacks and other spoofing attacks. They used the application Wireshark to analyze UDP packets in regular traffic and to compare that traffic to that produced by a UDP spoofing assault in a Linux-based environment. They also used their own custom-built Windows interface to investigate the network. The researchers finally came to the conclusion that IP spoofing attacks are inevitable given the nature of the network packets they generate. Their network from damaging spoofing as well as hacking techniques can be protected by understanding how spoofing attacks are developed and implemented in combination with a straightforward network monitoring method or tool. Cracking those techniques is a long-term process that is open to the networking community.

By comparing the expected and observed frequencies, **Rajvirkaur and Gauravdeep (2017)** introduced a statistically based intrusion detection technique based on the chi-square to identify DDoS attacks. In this instance, the technique and traffic from a backscatter dataset successfully detect the DDoS attempt. The investigation and results demonstrate that an anomaly exists when the expected and observed frequencies differ significantly. If the calculated result value in the chi-square test is higher than the tabular value, an anomaly has been found. The computed value is significantly higher in their results than the calculated value.

By exploiting the statistical features of the target graph-signal and modeling sensor measurements as the target graph-signal, **Hamidreza Sadreazami et al. (2018)** suggested a novel Distributed Blind Intrusion Detection (DBID) framework. Based on hypothesis testing and using the log-likelihood ratio criterion, it has been built using the Gaussian Markov random field distribution. The statistics test closed-form expression has been developed and empirically verified. The framework provides a detection performance that is superior to other current schemes, according to temporal study of the network behavior established in the research.

Ying Zhong et.al (2019) introduced a novel framework for anomaly identification. It is based on the organic integration of numerous Deep Learning (DL) algorithms. The first phase involves using the Damped Incremental Statistics method to extract characteristics from network traffic; the second phase involves training an auto-encoder with scant label data; the third phase relies on utilizing an auto-encoder to identify network traffic that is abnormal; the fourth phase consists of in utilizing labeled data to train an LSTM; and the final phase is using a weighted method to calculate the overall abnormal score.

3. Related Research Work

The techniques for detecting intrusions are divided into three categories: misuse, anomaly, and hybrid model [6, 11, 18, 19, 23, 25, 29, 32, 38, 41]. The misuse detection establishes patterns of illegal conduct, referred to as signatures, in particular to foresee and identify later attempts that would be similar. A hybrid technique has been proposed to improve the capabilities of current intrusion detection and prevention systems by merging these two methods of misuse and anomaly. The fundamental notion is that while anomaly identifies unknown attacks, misuse detects known assaults [5, 20, 24, 26, 33]. The goal of anomaly detection is to identify unusual patterns of behavior. Any deviations from the baseline of typical usage patterns that intrusion detection and prevention system establishes are marked as potential intrusions [12].

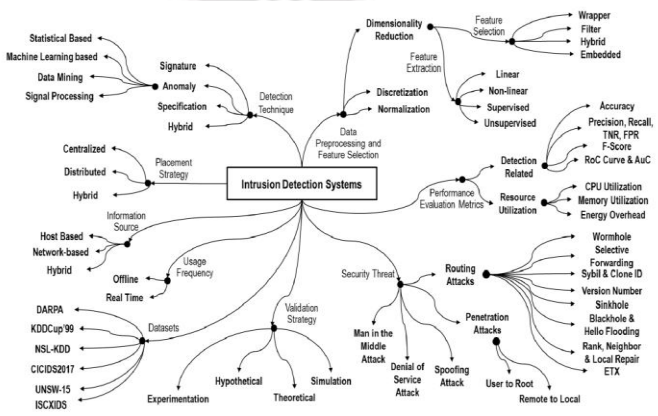

Figure 1: Taxonomy of Intrusion Detection System

Statistical: using a statistical method, the system tracks the behavior of various subjects, such as the utilization of CPU or the number of TCP connections, and creates profiles representing their characteristics. As a result,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

two profiles are created, one during the training phase and the second during the detection phase. The distinction between the profiles allows the detection of anomalies.

Machine learning (ML) based techniques have the ability to learn and improve their performance over time. They focus on developing a system that can adjust its execution plan in response to feedback and maximize its performance in a cycle.

Data mining-based: By uncovering patterns, associations, anomalies, changes, and significant events and structures in data, data mining techniques serve to improve the intrusion detection process. The intrusion detection and prevention system uses clustering, classification, outlier detection, and an association of rule discovery.

Intrusion prevention systems are divided into four categories. They are (i) By examining protocol behavior, a network-based intrusion prevention system scans the entire network for suspicious traffic. (ii) By examining the protocols, the Wireless Intrusion Prevention System (Wi-IPS) looks out for strange traffic in the wireless network. (iii) Network Behavior Analysis (NBA) examines network traffic to detect risks such as DDoS attacks, certain types of malware, and policy violations that lead to anomalous traffic patterns. (iv) A host-based intrusion prevention system analyzes events on a host to look for guarded activity.

The research objective is to identify intruders during communication in advanced computer networks using a behavioral profiling algorithm and to prevent intruders using a statistical model. To test the proposed model, 100 systems connected to a cloud network were selected. Files of different sizes were transferred between the systems. During the transformation, the number of data packets sent, received, and lost was dynamically stored and updated in the database with the system number at specific time intervals. The open source programming language PHP5.5 helps to determine the standard deviation, mean and variance. During the transformation, the system that loses more packets was marked as attacked system with the system number. Finally, the system number was transferred to the administrator to monitor and stop the processes running in the system and lock the system in the whole cloud network.

4. Proposed Model

Typically, IDS is a passive actor that issues alerts but does nothing to stop an attack or prevent it from being detected. In contrast, IPSs are considered extensions of IDS because they track system or network activity and attempt to prevent or block intruders. Unlike IDS, IPS is installed inline and has the ability to actively stop detected intruders. More specifically, IPS can, among other things, delete unnecessary network and transport layer options, remove malicious packets, generate alerts, reset the connection, fix transmission problems, etc. Essentially, behavior-based IDPSs build a data-driven model for good behavior. There are three main types of attributes that the data can often contain:

1) How many device resources are being used, e.g., CPU /memory consumption, battery life, incoming and outgoing network traffic, etc.

2) System calls made by various applications to the mobile OS kernel, e.g., the frequency with which a particular application makes calls to open, read, write, quit, etc,

3) Access to the permissions requested by an application, such as the ability to read and send SMS, as well as the camera, microphone, contact list, and location of the device. To achieve this goal, the following behavioral profiling algorithm and a statistical technique were used.

Proposed Behavior Profiling Algorithm:

Step 1: Logs entropy (or Information gain) from Server

Step 2: Identify the Process and respective PID (Process Identification Number)

Step 3: Identify the IP (Internet Protocol) Address for each Process using PID.

Step 4: Identify the TCP/ UDP transformation Process

Step 5: Identify the Active Time and Response time for each process.

Step 6: Identify the Data Packet transformation and Data Packet Loss

Step 7: Trace the IP Address and its behavior of Transformation

Step 8: Classify the Authorized and Unauthorized Transformation

Step 9: Make the Prevention from the Unauthorized Transformation

Statistical Techniques:

To determine if the current behavior is different from the expected behavior, statistical approaches use statistical features and tests. These techniques provide a role that maps the typical behavior of network traffic (in the absence of an attack). Then, the network is monitored, proles are formed periodically, and anomalies are found by comparing them to reference proles. These techniques can be time-series or event-based, multivariate or univariate.

To identify the standard deviation (σ) by using the number of packets (N) sent, received and loss of packets the following equation 1 has used. To implement the equation the sum ($\sum x$) and N the mean (μ) the standard deviation (σ) and the variance (σ^2) has derived.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

$\sigma = \sqrt{1/N \sum_{i=1}^{N} (xi - \mu)^2}$ ----------(1)

$$\sigma^2 = \frac{\Sigma(x_i - \mu)^2}{N}$$ ----------(2)

For testing the proposed model the 100 cloud network systems were taken and based on the loss of packets (in MB) ranges the samples were classified as 0-100, 101-200, 201-300, 301-400, 401-500, 501-600, 601-700 respectively. The found mean and variance has been tabulated in the following [Table 1]. From [Table 1], the range of data loss is assumed to be an interval of 100 Mbps.

It is assumed that the higher the data loss ranges, the more data is lost. The mean, variance, and standard deviation were calculated to verify the data loss ranges. The mean and variance of data loss in cloud networks are shown graphically in [Figure 2]. The variance measures how each number in the set deviates from the mean (average). The variance is represented by this symbol. The mean (average) of the data loss in the ranges 0-100 is 060.77 and the mean in the ranges 101-200 is 144.714 data losses, which gradually increases in proportion to the data loss ranges, and in the ranges 601-700 it is 665.769 data losses. The square root of the variance is the standard deviation. It measures the dispersion of a data set relative to its mean.

Data Loss Ranges (in MB)	Number of systems	Mean	Variance	Standard Deviation	Confidence Level (95%)
0-100	9	065.777	038.173	06.178	1.960
101-200	14	144.714	157.489	12.549	
201-300	16	241.250	240.813	15.518	
301-400	17	355.764	303.944	17.434	
401-500	18	455.888	608.320	24.664	
500-600	13	553.307	571.136	23.898	
601-700	13	665.769	890.024	29.833	

Table 1: Statistical Analysis of data loss ranges in cloud Network

Looking at the variance, in the ranges 0-100 it is small compared to the mean (average). In data ranges 101-200 and 201-300, the variance of data loss is relatively high, and in data range 301-400, the variance of data loss is low compared to the mean. However, in the 401-500, 501-600, and 601-700 data ranges, the variance of data loss is relatively high compared to the mean. The standard deviation shows that the data loss is higher when the standard deviation is higher, and the data loss is lower when the standard deviation is lower. It can be concluded that as the data ranges increase, the loss ranges also increase.

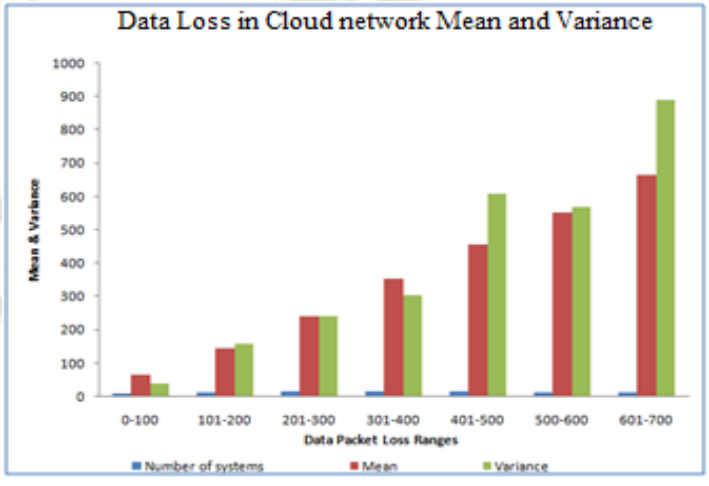

Figure 2: Graphical representation of Data lose in Cloud Network Mean and Variance

5. Result and Discussion

Cloud network users and their actions were tracked using the proposed approach. The received and sent details of the status of data packet transformation from the user to

the server and from the server to the user were studied. The packet conversion information in the cloud network is shown in [Table 1]. Using the log files, administrators were able to distinguish between allowed and unusual users. If the server's file system entry point has error information in its log files. This data was entered into the database and is known as the user's behavior profile. The activities of network users were also examined.

From the statistical approach model, the differences between mean and variance indicated that the intruder attacked the files during the data transformation in the network. Therefore, the administrator has to monitor the warning message from the proposed IPS model and get data packet losses in the transformation. If the frequency of data loss is low, the administrator can assume that the data flow is low due to network problems. On the other hand, if the frequency of data loss in the network system is high, he can block the transformation and protect the data file.

6. Conclusion

This paper concludes that the behavioral profiling algorithm combined with a statistical model achieves an efficiency of over 96% in wired networks, over 97.6% in wireless networks, and over 98.7% in cloud networks. This algorithm is the most effective in detecting intrusions. The performance analysis of the algorithm used to build the intrusion detection and prevention system using Big Data could be determined in future studies, whether it is a wired, wireless, or cloud network.

References

[1] Dorothy E. Denning, "An Intrusion Detection Model", IEEE Transactions on Software Engineering, Vol.SE.13, No.2, Feb 1987, PP: 222-232.

[2] Sathish Alampalayam P. Kumar, Anup Kumar, S.Srinivasan, "Statistical Based Intrusion Detection Framework using Six Sigma Technique", International Journal of Computer Science and Network Security, VOL.7 No.10, October 2007, PP:333-342.

[3] Mahboubian, Nor I. Udzir, "A Naturally Inspired Statistical Intrusion Detection Model", International Journal of Computer Theory and Engineering, Vol. 5, No. 3, June 2013, PP: 578-581.

[4] Waskita, Suhartanto, Persadha, Handoko, "A simple statistical analysis approach for Intrusion Detection System", 2014, PP: 1-5.

[5] Aneetha Avalappampatty Sivasamy and Bose Sundan, "A Dynamic Intrusion Detection System Based on Multivariate Hotelling's T^2 Statistics Approach for Network Environments", The Scientific World Journal, Vol. 2015,PP: 1-9.

[6] Luca Boero, Marco Cello, Mario Marchese, Enrico Mariconti, Talha Naqash, Sandro Zappatore, "Statistical fingerprint-based intrusion detection system (SF-IDS)", International Journal of Communication Systems, 2016, PP:1-11.

[7] Anup Ingle, Aditya Wagh, Rajneesh Sharma, Akshay Shikre, "Statistical Approaches for Network Anomaly Detection for UDP Spoofing", International Journal of Advanced Computational Engineering and Networking,Vol. 4, Iss. 7, Jul 2016, PP: 4-7.

[8] Rajvirkaur, Gauravdeep, "Statistical Approach for Detecting Distributed Denial of Service Attacks", Asian Journal of Computer Science And Information Technology, Vol. 7, Iss. 5, September 2017, PP: 85 - 89.

[9] Hamidreza Sadreazami, Arash Mohammadi, Amir Asif, Konstantinos Plataniotis, "Distributed-Graph-Based Statistical Approach for Intrusion Detection in Cyber-Physical Systems", IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS, Vol. 4, No. 1, MARCH 2018, PP:137-147.

[10] Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges", Cybersecurity, 2:20, 2019, PP: 1-22.

[11] Ying Zhong, Wenqi Chen, Zhiliang Wang, Yifan Chen, Kai Wang, Xia Yin, Xingang Shi, Jiahai Yang, Keqin Li, "HELAD: A novel network anomaly detection model based on heterogeneous ensemble learning", Computer Networks, 169, 2020, PP: 1-16.

[12] Roberto Magan Carrion, Jose Camacho, Gabriel Macia Fernandez, Angel Ruız Zafra, "Multivariate Statistical Network Monitoring–Sensor: An effective tool for real-time monitoring and anomaly detection in complex networks and systems", International Journal of Distributed Sensor Networks, Vol. 16(5), 2020, PP: 1-14.

[13] Waleed Bulajoul, Anne James, Siraj Shaikh, "A New Architecture for Network Intrusion Detection and Prevention", IEEE Access, Vol. 7, 2009, PP: 18558-18573.

[14] Paulo Freitas De Araujho Filho, Antonio J Pinheiro, Georges Kaddoum, Divanilson R Campelo, "An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks with a Low-Cost Platform", IEEE Access, Vol 9, 2021, PP: 166855-166869

[15] Jose Ribeiro, Firooz B. Saghezchi, Georgios Mantas, Jonathan Rodriguez, and Raed A. Abd Alhameed, "HIDROID: Prototying a Behavioral Host-Based Intrusion Detection and Prevention System for Android", IEEE Access, Vol 8, 2020, PP: 23154-23168

[16] Reza Parsamehr, Georgios Mantas, Jonathan Rodriguez, Jose Fernan Martinez Ortega, "IDLP: An Efficient Intrusion Detection and Location Aware Prevention Mechanism for Network Coding Enabled Mobile Small Cells", IEEE Access, Vol 8, 2020, PP: 43863-43875.

[17] Muhammad Nadeem, Ali Arshad, Saman Riaz, Shahab S Band, Amir Mosavi, "Intercept the Cloud Network from Brute Force and DDoS Attacks via Intrusion Detection and Prevention System", IEEE Access, Vol 9, 2021, PP: 152300-152309

[18] Jia Jingping, Chen Kehua, Chen Jia, Zhou Dengwen, and Ma Wei, "Detection and Recognition of Atomic Evasions

Against Network Intrusion Detection/ Prevention Systems", IEEE Access, Vol 7, 2019, PP: 87816-87826

[19] Jennifer Appiah Kubi and Chen Ching Liu, "Decentralized Intrusion Prevention Against Co-ordinated Cyberattacks on Distribution Automation Systems", IEEE Access Journal of Power and Energy, Vol 7, 2020, PP: 389-402.

[20] Iftikhar Ahmad, Mohammad Basheri, Muhammad Javed IQbal, Aneel Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection", IEEE Access Special Section on Survivability Strategies for Emerging Wireless Networks, Vol 6, 2018, PP: 33789-33795

[21] Amir Ali and Muhammad Murtaza Yousaf, "Novel Three-Tier Intrusion Detection and Prevention System in Software Defined Network", Vol 8, 2020, PP: 109662-109676

[22] Lampis Alevizos, Max Hashem Eiza, Vinh Thong Ta, Qi Shi, Janet Read, "Blockchain-enabled Intrusion Detection and Prevention System of APTs within Zero Trust Architecture", IEEE Access, 2022.

[23] Bruhan Ul Islam Khan, Farhat Anwar, Rashidah Funke Olanrewaju, Bisma Rasool Pampori and Roohie Naaz Mir, "A Novel Multi-Agent and Multilayered Game Formulation for Intrusion Detection in Internet of Things(IoT), IEEE Access, Vol 8, 2020, PP: 98481-98490

[24] Kamaldeep, Maitreyee Dutta, Jorge Granjal, "Towards a Secure Internet of Things A Comprehensive Study of Second Line Defense Mechanisms", Vol 8, 2020, PP: 127272-127312

[25] Seunghoon Yoo, Jaemin Jo, Bohyoung Kim, Jinwook Seo, "Hyperion: A Visual Analytics Tool for an Intrusion Detection and Prevention System", IEEE Access, Vol 8, 2020, PP: 133865-133881.

[26] Nivedita Mishra, Sharnil Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review", Vol 9, 2021, PP: 59353-59377

[27] Waleed Bulajoul, Anne James, Siraj Shaikh, "A New Architecture for Network Intrusion Detection and Prevention", IEEE Access, Vol 7, 2019, PP: 18558-18573

[28] Sydney Mambwe Kasongo, "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms", IEEE Access, Vol 9, 2021, PP: 113199-113212

[29] Wenjuan Wang, Xuehui Du, Na Wang, "Building a Cloud IDS Using an Efficient Feature Selection Method and SVM", IEEE Access, Vol 7, 2019, PP: 1345-1354

[30] Poongodi M, Mounir Hamdi, Ashutosh Sharma, Maode Ma, Pradeep Kumar Singh, "DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET", IEEE Access Special Section on Artificial Intelligence(AI)-Empowered Intelligent Transportation Systems, Vol 7, 2019, PP: 183532-183544

[31] Sibi Chakkaravarthy S, Sangeetha D, Meenalosini Vimal Cruz, Vaidehi V, Balasubramanian Raman, "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks", IEEE Access, Vol 8, 2020, PP: 169944-169956.

[32] Qaisar Shafi, Abdul Basit, Saad Qaisar, Abigail Koay, Ian Welch, "Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network", IEEE Access, Vol 6, 2018, PP: 73713-73723.

[33] Md Ali Reza Al Amin, Sachin Shetty, Laurent Njilla, Deepak K Tosh, Charles Kamhoua, "Hidden Markov Model and Cyber Deception for the Prevention of Adversarial Lateral Movement", Vol 9, 2021, PP: 49662-49682.

[34] Kishwar Sadaf, Jabeen Sultana, "Intrusion Detection Based on Autoencoder and Isolation Forest in Fog Computing", Vol 8, 2020, PP: 167059-167068.

[35] Hongsheng Yin, Mengyang Xue, Yuteng Xiao, Kaijian Xia, "Intrusion Detection Classification Model on an Improved K-Dependence Bayesian Network", IEEE Access, Vol 7, 2019, PP: 157555-157563.

[36] Abdallah R Gad, Ahmed A Nashat, Tamer M Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset", IEEE Access, Vol 9, 2021, PP: 142206-142217.

[37] Mehedi Hassan, Md Enamul Haque, Mehmet Engin Tozal, Vijay Raghavan, Rajeev Agrawal, "Intrusion Detection Using Payload Embeddings", IEEE Access, Vol 10, 2022, PP: 4015-4030.

[38] Poongodi M, Vijayakumar V, Fadi Al-Turjman, Mounir Hamdi, Maode Ma, "Intrusion Prevention System for DDoS Attack on VANET with reCAPTCHA Controller Using Information Based Metrics", IEEE Access Special Section on Secure Communication for the Next Generation 5G and IOT Networks, Vol 7, 2019, PP: 158481-158491.

[39] Abdulaziz Fatani, Mohamed Abd Elaziz, Abdelghani Dahou, Mohammed A Al-Qaness, Songfengu Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization", IEEE Access, Vol 9, 2021, PP: 123448-123464.

[40] Nikos Tsikoudis, Antonis Papadogiannakis, Evangelos P Markatos, "LEoNiDS: A Low-Latency and Energy-Efficient Network Level Intrusion Detection System", IEEE Transactions on Emerging Topics in computing, Vol 4, No 1, Mar 2016, PP: 142-155.

[41] Panagiotis Radoglou-Grammatikis, Konstantinos Rompolos, Ranagiotis Sarigiannidis, Vasileios Argyriou, Thomas Lagkas, Antonios Sarigiannidis, Sotirios Goudos, Shaohua Wan, "Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach", IEEE Transactions on Industrial Informatics, Vol 18, No 3, March 2022, PP: 2041-2052.

[42] Wooseok Seo, Wooguil Pak, "Real Time Network Intrusion Prevention System Based on Hybrid Machine Learning", IEEE Access, Vol 9, 2021, PP: 46386-46397.

[43] Fahad M Alotaibi, Vassilios G Vassilakis, "SDN Based Detection of Self Propagating Ransomware: The case of BadRabbit", IEEE Access, Vol 9, 2021, PP: 28039-28058.

[44] Panagiotis I Radoglou-Grammatikis, Panagiotis G Sarigiannidis, "Securing the Smart Grid: A Comprehensive

Compilation of Intrusion Detection and Prevention Systems", IEEE Access, Vol 7, 2019, PP: 46595-46620.

[45] Wael Said, Ayman Mohamed Mostafa, "Towards a Hybrid Immune Algorithm Based on Danger Theory for Database Security", IEEE Access, Vol 8, 2020, PP: 145332-145362.

[46] Smitha Rajagopal, Poornima Panduranga Kundapur, Hareesha K S, "Towards Effective Network Intrusion Detection From Concept to Creation on Azure Cloud", IEEE Access, Vol 9, 2021, PP: 19723-19742.