Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

A Comparative Approach on Network Tools for Analysing Suspicious Behaviour in Network Streaming Data

[1]Mr. B. Senthil Kumar, [2]Dr. M. S. Josephine, [3]Dr. V. Jeyabalaraja

[1]Research Scholar, Bharathiar University, Coimbatore
[2]Professor, Dr.MGR Educational and Research Institute
[3]Professor, Velammal Engineering College

E-mail: [1] senthilkumar32@yahoo.com, [2] josejbr@yahoo.com, [3] jeyabalaraja@gmail.com

Abstract: Cyber threats and intelligence are facing massive challenges in present world. Computers connected to the network get compromised routinely due to various cyber-attacks over the network, which lead to financial damages, loss of important data and disclosure of secrets to be revealed in the public world. Even though cyber intelligence plays a vital role in combatting against the network attacks, AI powered malwares and its behaviours are very difficult to analyse. Malicious network data obviously bypass the security systems installed in the computer and compromise the entire system within a less time span. So, cyber professionals need the automated tools for analysing and detecting the suspicious behaviour in the network. In this paper, we study the various existing cyber analytics tools used for detecting the suspicious network activity in the data streaming network and compare the efficiency of the tools using some key performance indicators by generating real time attacks artificially in the live monitor mode. The results obtained in this study are combined with cyber intelligence platform for visualising the suspicious activities. It is a real research challenge, to address this challenge, the obtained results are utilized as real time case studies. With these case studies, we suggest some modifications which need to be carried out in large network operational centres and also this paper discusses the work flow of large network operational centres and the changes required to do in their work flows are addressed.

1. Introduction

Networking resources are regularly undermined, coming about in the exfiltration of protected innovation, the divulgence of characterized data, and enormous monetary harms. In spite of crafted by digital security specialists, these trade-offs happen routinely and the effects are faltering. The Centre for Strategic and International Studies assessed the worldwide expense of digital wrongdoing at $445 billion every year; in the US, these misfortunes address 0.6% of GDP and in Germany 1.6%. While reports referring to such enormous numbers may be viewed as self-serving, different impacts of digital wrongdoing are considerably more basic. Complex assault bunches at the country state level continually grow new organization entrance strategies that current advances can't distinguish. The 2016 US races, with charges of Russian hacking, are a calming token of the earnestness and worldwide effect of cyber-attacks.The most regularly conveyed measures for recognizing attacks on organizations and frameworks are interruption recognition/avoidance frameworks and antivirus programming. These frameworks ordinarily work dependent on marks, which use design coordinating to recognize malignant action. Despite the fact that viable at recognizing known assaults, these frameworks can't distinguish novel assaults or varieties.

Trojan horse attack:

Trojan horse is kind of malware, it is a type of social engineering attack. It can be performed on email attachments. If the user clicks or view the attachments the malware triggered itself to gather the user information and send the information to the attackers end. To prevent these kind of attack by using the IDS software called as Back Orifice, TFN2K master-to-zombie, etc. to prevent the system from any kind Trojan horse attacks.

Surveillance attack:

This attack can performed via TCP ports to collect the information of the user. This attack will be analyze and attack the TCP 3 way handshake technique and collect the user data and encrypt the data send to

attacker system. These attacks can be prevented by using some of the IDS software likes Nmap and Whisker to scan the network port vulnerability and intimate to the user.

Phishing attack

Phishing is an attacking strategy to collect the user personal information for various attacking reasons. Those collected data may include the username, password, credit details, email charts, call logs, etc. Some of the phishing attacks are spear phishing, whaling phishing, smishing & vishing phishing, and email phishing.

IDS

An intrusion detection system (IDS) is a hardware or software that classifies and detects cyber-attacks at the network and host level, allowing an administrator or centrally deployed security management systems to provide reports (SIEM). This system collects data from multiple sources and employs an alert filtering mechanism to distinguish between malicious and false alarms. The intrusion detection system (IDS) is used to detect intrusions in single computers to big computer networks. Network Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDSS) are the most widely utilized IDS technologies (HIDS). NIDS systems collect data from a variety of networking devices, including routers, bridges, switches, and networking taps. Misuse detection, anomaly detection, and state-full protocol analysis are used to analyze network traffic. Misuse detection detects attacks using signatures; it collects human digital signatures and updates databases on a regular basis to detect attacks.Anomaly detection employs a heuristic approach to detect malicious attacks, but it frequently produces false results. In this case, the organization employs both the misuse and anomaly methods to effectively detect the malicious attack. In comparison to the other two procedures, state full analysis is the most successful. This approach keeps track of the application, transport, and network layers.

Host Intrusion Detection System (HIDS):

Host based intrusion detection is a type IDS, which is a device with capable of analysis the entire parts of the computer system or network. This device can able to analyze a particular part or protocol in the computer network. HIDS basically used for analyze the dynamic behavior of the system because of the network. It will checks the system behavior and log file for preventing the HIDS attacks, and also monitoring the system server protocol such as DNS, web servers, mails, etc. It works in various attacking situation such as improper client-server request and file permission change attack. It will monitor the database in usual manner and checks if any change occurs in the system and generate the report about the HIDS attacks to the administrator to prevent the loss of data and run the antivirus software to protect the system from various attacks in the networks.

This system will monitor both internal and external system behavior and also checks the system activities from the begging of the system. For example, the HIDS application runs on the server side, it will analyze the network packets and its behavior through the network firewall. If any changes in the packet flow in the network it will generate the report from the attackers traces in the network, during the attack the attacker leaves her identity in the network. From that logging information the HIDS device identify the attacker scope and who is the attacker. Once the system administrator gets the report, they will able to change the system security. They also check the trusted application from the network to comprise the HIDS application.

Protocol Intrusion Detection System

Protocol based intrusion detection system is a type specification IDS. This is installed in the webservers to monitor the protocol in the network systems. PIDS also checks the topology based attacks in the network and it will monitoring the http or https protocol for checking security threads. This is a frontend based web server implementation techniques to protect the computer from threads. This generates the report based on the anonym's activity in the http protocol because this protocol is responsible for client and server request and responses. This protecting technic cost based to provide more security to the system and it's responsible for packet filtering and IP filtering of the network.

This PIDS further more implemented in specific application based. It also known as Application Protocol Intrusion Detection System (APIDS) these can also implemented in web servers. It monitoring the dynamic behavior of the system in the web server view through the APIDS application installed in the webserver at frontend client observations. APIDS typically monitoring the system between web server and data base management systems. For example, the client requests the server for access the data base to store the

private data of the organization. If the attacker can able to send the fake request get the data from same request id stole the data from the data base. In this case if the APIDS installed in the web server they take responsible for identify the true and false rate of request and response to authorized client and also report the attack to server administrator and update the fire wall automatically to protect the system from future attacks.

Hybrid Intrusion Detection System (Hybrid IDS)

Hybrid IDS is the combination of the Packet Header Anomaly Detection (PHAD) and Network Traffic Anomaly Detection (NETAD), this combination will give the more system security and protect system from unauthorized user. It is also called as improved intrusion detection system. This system will used in various real time application like wireless network, software defined network and organization based computer networks. Hybrid IDS increase the detection rate and reduce the false positive rate in the system. This ids can used in both anomaly detection and signature based attacks in the system and result the more accurate possibility of the attacks to administrator of the network.

Signature Based Detection:

The observed signatures are compared to the signatures in the database using this process. This collection is made up of a list of known attack signatures. The system monitored the packet and its surroundings by extracting features from any signature pattern. If a signature matches in the database, it will be flagged as a security policy violation. Because this approach has some computing and preparation overhead, it does not monitor all network traffic behaviour. Instead, it just examines the database or file for recognised signatures. The signature-based technique also looks for known threat payloads in system calls. This approach is successful against known attacks or violations, but it is ineffective at detecting new ones until fresh signatures are added. Attackers with knowledge of the alteration and a target system that hasn't been updated with fresh signatures can simply evade this system.

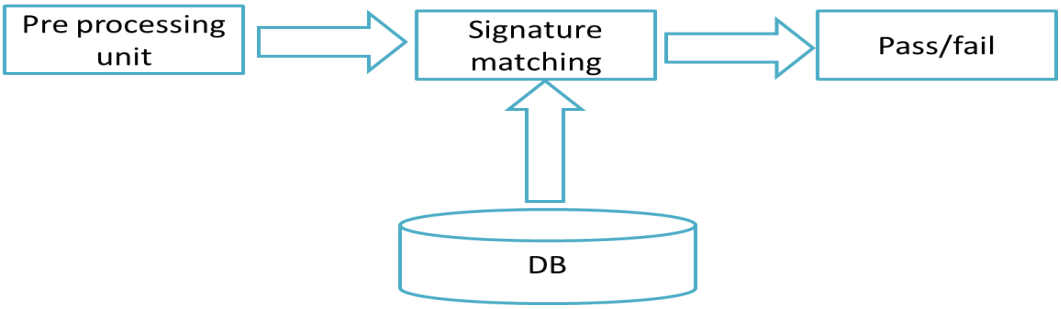

Fig 1: Signature based detection

Anomaly Based Detection:

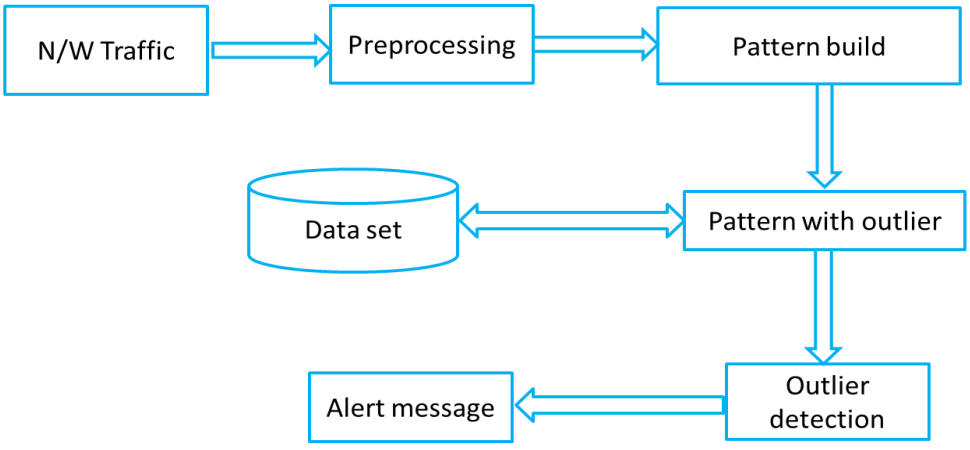

Fig 2: anomaly based detection

Network IDS behaviors model systems are used to detect this detection, which is also known as "Behavior-Based Detection." It monitors network traffic and alerts the administrator if there is any deviation from normal behavior. Anomaly detection is a technique for detecting new or possible assaults. It relies on the notion of distance measurement, which involves creating profiles that approximate usual usage and then comparing them to the data's current behavior to see if there is a mismatch. Anomaly-based detection identifies any traffic, new or unusual, and is effective at detecting sweeps and probes directed at network hardware. These systems are capable of quickly detecting web anomalies, port anomalies, and misfired attacks in which the URL has been mistyped. If there are any misclassifications, a large number of false positive alarms are generated.

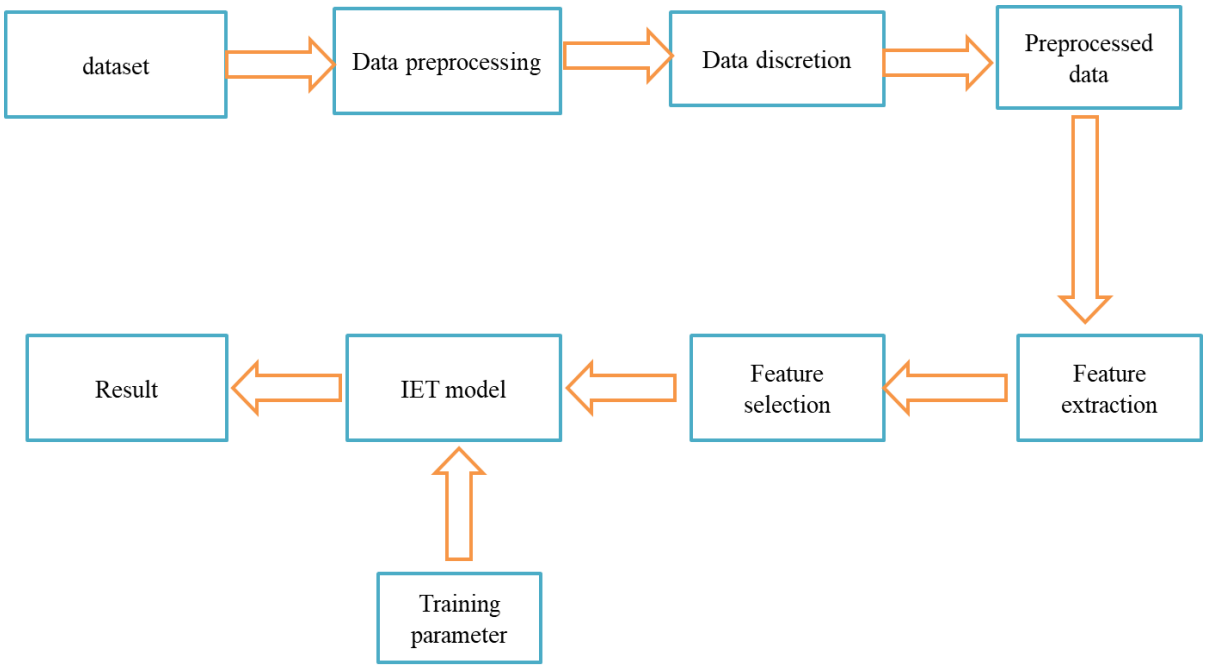

Fig 3: System Architecture

Unauthorized user attacks:

The 3rd party users access the resources without the admin permission. These attacks are comes under the central control of the network. These attacks caused by using the central computer as a major role in sharing resources to entire networks. The entire work load can be handled by the centralized computer. So that the attacker can access the resources by attacking the centralized computer

Traffic diversion attacks:

This attack can be performed by attacker to redirecting the data packets because of traffics in the networks, they can easily penetrate into the system with duplicate packets and they are stolen original data packets.

ARP snooping attack:

The man-in- the-middle attack also called as ARP snooping. The hacker uses ARP snooping, they inflated into the networks they can monitor the traffic, modify it, change the packets delivery speed and stole the packets also.

Password guessing /brute force attack:

It happen on a Network service with password guessing /brute force, an unauthorized user gain access to penetrate through the SDN networks.

Phishing attack

Phishing is an attacking strategy to collect the user personal information for various attacking reasons. Those collected data may include the username, password, credit details, email charts, call logs, etc. Some of the phishing attacks are spear phishing, whaling phishing, smishing & vishing phishing, and email phishing.

Spear phishing

This phishing attack is targeted on particular user information not on group attacking strategy. The attacker collects the particular user information on social media network and other browsing sites. This is a first step to attack the organization to particular or targeted system.

Whaling phishing

The attacker can attack the organization head like ceo or founder of the company is called whaling phishing attack. This is long term process to collect the user information and wait for correct chance to get login details to stole the high level business information of the company by this attack.

Email phishing

It is widely used phishing method to send the malicious email to the individual or company. This method spots the organization domain name and snoop them to send the email, for instance name@domainname.com to bypass the company security. The attacker attach the malicious code to get the user information.

Smishing and vishing

Smishing is the type of attack to send the text message to victim to gather information. And vishing is the method to attacking by telephone conversion. The attacker sends text message or calling to gather the user bank details and credit card information to transfer money to attacker account form victim account. Those accounts are unauthorized or criminal accounts.

2. Related Work

Zeinab Movahedi, et al. presented the survey on the promising trust management. They monitor the various attacks in the mobile ad-hoc attacks in the network. They also compare the different distortion resistant frameworks to identify the open issue in the ad-hoc network [1].Weidong fang et al. proposed the efficient trust management scheme for IoT network. The authors proposed the model to detect and solve the network attacks in the IoT device [2]. This model increase the security level in the IP networks and remove the malicious node from the networks. They analysis the latency and mobility of the 5G networks to improve the connectivity and communication of the IoT devices. Wenzhen wang et al. proposed the model to detect the sequential attacks. Authors use the image inpainting algorithms to detect the defects in the computer vision [3]. They build a model in image fabric pattern to identify the defects in the product to improve the quality inspection.Jinyong Chang et al. proposed the model to detect pollution attacks in the networks. Authors use the kept encoding method to detect the pollution attacks [4]. This model increases the data integrity and queried data structure. Marija Furdek et al. proposed the machine learning model to monitor the optical network security. The authors use machine learning model and SSL based learning methodology to improve the monitoring efficiency of the optical network security [5]. Ojo S et al. proposed the model to predict the stock market behaviour by machine learning mechanism. The authors design the model using the stacked LSTM networks to predict the stock market behavior using the machine learning data sets [6]. Aidan et al. proposed the survey on petya ransomware attack detection. The authors describe the recent ransomware attacks and detection and prevention technics. They also analysis the detection possibilities of the petya ransomware attacks and prevention technics from cyber ransomware attacks [7].

Bahrani & Bidgly et al. proposed the ransomware detection technics using the mining algorithms. The authors implement the software based ransomware detection model to identify the ransomware detection and classify the ransomware by its behavior. They use system logs to identify theransomware attacks and model detects the almost 21 types of ransomware [8]. Wang et al. 2019 proposed the model to improve the QoS of the cloud services. The authors use POS based decision algorithm to allocate the memory in the cloud service. This helps the cloud self-management to improve the performance of the cloud computing service in advanced manner [9]. Liu, C *et al*. proposed the encryption algorithm for cloud computing to ensure the cloud security. The authors use k-means algorithm to ensure the cloud security. The proposed k-means improve the performance and throughput of the system [10].Shojafar et al. proposed the energy efficient model to manage

the resources in the vehicular cloud services. The authors use the TCP based connection to ensure the energy efficiency in the cloud environment. This system tested in the networked fog centers, TCP single hop mobile cloud centers, and scheduler based system with virtual environment.

Yi Yi Aung et al. proposed the collaborative model for intrusion detection system. Which uses the k-means algorithm to improve the detection accuracy and use the hybrid mining approach to detect the singleton attacks in the system. It results to reduce the time complexity between and single and multiple nodes in the system. Authors also describe the projective adaptive resonance model to improve the throughput of the system. As a result of this, the data mining method plays an important part in the IDS inters of time complexity [11]. The automated approach for hybrid intrusion detection was proposed by Shengyi Pan et al. With a 73 percent accuracy rate on a similar dataset, the authors' proposed system identifies infiltration from data logs. However, this strategy is not ideal for larger data sets; the issue is that capturing log files in the system is quite complex [12]. Saranya et al. proposed the model to equally divide the load balancing in the cloud environment. The author's analysis the various load balancing algorithms and develop the model to achieve the better performance in the cloud environment. They also use ant-colony optimization algorithm to implement model in real time environment to reach better performance load balancing algorithm in cloud computing based.

Jiadai Wang et al. proposed the topology-based model to detect the poising attacks in the SDN networks. They use the IoT devices to ingrate the data transferring between SDN controllers [13]. To monitor and improve the security in the controllers they use Edge computing and defined networking methodologies. Muhammad Imran et al. proposed SDN model to detect the malicious attacks in the network. This model monitors the network ports and host configuration in network [14]. This also detects the DoS attacks in the network system.

Sapkota et al. 2019 [21] proposed the spectral clustering approach to summarize the data set using the cluster and classification algorithms. The authors use the k-means algorithms to classify the data set and form the cluster to reduce the time. From this approach the clustering error of the dataset is reduced. Li, H & Lu, Q et al. proposed the SVM classification optimization mechanism to improve the forecast accuracy of the system. The authors use K-CV parameter optimization model to improve the SVM classification accuracy. S. Chandra and M. Kaur et al. 2015 [22] proposed the classification mechanism to enhance the accuracy of the classification algorithm. Authors developed model specifically used for the medical data classification and monitor the accuracy of the system. Okfalisa et al. 2017 [23] proposed the comparative analysis of the classification algorithms. The authors comparatively take the two classification algorithm for testing. They use k-nearest and modified k-nearest neighbor algorithm. It results modified k-nearest neighbor algorithm produce the result accuracy is better than the KNN. Pristyanto et al 2018 [24]proposed the balance distribution model for classify the education related data set. They use the OSS, SMOTE method to balancing the data set from the raw data. This classification improvises the balancing accuracy in the SVM classifications.

Basarslan, M. S., & Argun, I. D et al. 2018 [25] proposed the classification model for bank data classification. The authors use the UCI machine learning approach to classify the large data set in efficient accuracy. This model inherits the native bayes, KNN and decision algorithm behavior to classify the datasets. Baralis et al. 2008 [26] proposed the lazy model to improve the associative classification method accuracy. The authors use the SVM and decision tree algorithm for the lazy model to improve the classification accuracy of the system. Erol, H et al. 2018 proposed the classification method for data mining technics. The authors use the data mining clustering algorithms to classify the remotely sensed imaged data. This model clustering the sensed image into 6 part. Karamouzis and Vrettos et al. 2009 [27] proposed the ANN model to predict the student performance from the student profile. They trained the algorithm to cross validate the classified data set of the student profile.

Jiang Q et al. 2018 [28] proposed the model to improve the security in the mobile cloud environment. The authors discuss the distributed cloud computing and authentication mechanism of the cloud. This model improve the privacy policy of the cloud by the existing attacks and fingerprints of the attacking strategies in mobile cloud computing. Sekaran K et al. 2019 [29] proposed the model to improve the performance in M-learning based cloud computing environments. The authors use various query learning mechanism to demonstrate the load balancing techniques to improve the throughput of the cloud computing environment. Misra S et al. 2016 [30] proposed the model to improve the cloud based decision making system performance.

The authors utilize the existing the system model and improve the protocol by sensors. This model improves the reserving resource availability upto 25% from normal traffic without any compromise.

Taylor S et al. 2018 [31] proposed the solution to improve the experience in the cloud technology. The authors implement model in transAt CFD software to improve the local cluster performance. The model uses the fluid dynamic mechanism to reduce the complexity of the cloud service. Zhang H et al. 2015 [32] proposed the vehicle assisted computing smartphones based on the cloud environment. The authors use smartphone application to control the vehicle and improve the security level. This model monitors the vehicular cloud infrastructure to improve the response time and reduce the power consumption of the cloud to provide efficient and reliable service to the vendors. Dubey K et al. 2019 [33] proposed the model to improve the management community standards in the cloud computing. The authors use the MSMC virtual machine environment to ensure the security of the cloud environment. Model use the IDA algorithm to schedule the workflow of the processing the cloud data to it. They simulate the experiments with various cloud platforms improves the reserving resource availability.

Saranya et al. 2015 [34] proposed the model to equally divide the load balancing in the cloud environment. The author's analysis the various load balancing algorithms and develop the model to achieve the better performance in the cloud environment. They also use ant-colony optimization algorithm to implement model in real time environment to reach better performance load balancing algorithm in cloud computing based. Markandey et al. [35] 2018 proposed the model to improve data access security in cloud computing environment. The author's analysis various security threads in the cloud data accessing and minimise the hazards in the cloud. This model also improves the data transit and reset in the cloud security. Rindos & Wang et al. 2016 [36] proposed the model to improve the cloud computing performance in the parallel processing. The authors explore the dew computing feature to the cloud computing to improve the scalability of the system.

Mershad et al. 2017 [37] proposed the model to analysis the performance of the cloud data center servers. The authors describe the complexity of the cloud server performance and develop the model to increase the cloud performance by the middleware servers. They also implement FPGA technic to computing the cloud data in the efficient way. Zinno et al. 2015 & Visu et al 2023 [38,39] proposed the algorithm to improve the performance of the cloud environment. The authors describe the performance of the P-SBAS & ASR algorithm to improve the cloud computing performance. They tested the model in various cloud services and exploiting the performance feature of the cloud. Jalali et al. 2016 [40] proposed the model to save the energy in cloud computing. The authors use the fog computing services for the centralized data centers to reduce the consuming of the energy in the cloud. They use Nano technic in resource storage in data center to protect the cloud environment and energy consumption. Chi, F et al. 2015 [41] proposed the ad-hoc based cloud environment to improve the performance of the system. The authors use the mobile ad-hoc networks to allocating the dynamic storage for the gaming environment. The system utilized the resources of nearby data centers in the efficient to reduce the time complexity of the system.

3. Methodology

Experimentation

The experimentation is performed in HPz420 workstation with Intel Xeon processor and 28GB RAM in windows and Linux Operating System. The entire algorithm is implemented in python.

Data pre-processing

Data set for the experimentation is collected in real time. 10 GB of data is collected for more than 10 hours and the entire live traffic from the analyzer is pruned and structured to KDD data format. The experimental validation is categorized in (i) timely manner (ii) connection based feature (iii) content based feature.

Training

Using the tshark software, the incoming traffic is tapped and monitored. Every hour, the principal traffic flow Openflow stats reply is checked to confirm that the network is operational. The live training data is created using the KDD dataset, and the training data format is explained in the previous section. The testing data is collected on the fly from traffic generated by end hosts in the SDN and sent into the Intrusion detection model as a live feed. The CNN model extracts and classifies the characteristics from the testing data. The classifiers

seek for substantial differences in the characteristics and packet lost rate, as well as their deviation. If any of the characteristics, such as proto type and source IP address, are subject to change [15]. The originating IP address is then blocked in the flow table, and the flow table is otherwise modified.In order to present the proposal, three fold cross validation is done on the training data set.

Feature Dimensionality Reduction:

In this phase, the feature dimensionality reduction is performed. There are two process included in the conventional feature dimensionality reduction such as feature selection and feature transformation [16]. There are two types of feature selection method (i) scalar method (ii) vector method. Here we use vector method by getting the vectors of feature for normalization of data by using vectorization algorithm. Features are categorized and extracted using the transformation and selection method. It is a complex method which selects the subsets of features on the basis of mutual relationship. Three classification methods are used to classify the features that are obtained from feature dimensionality reduction method.

The DDoS attacks had been generated with live TCP Syn, experimental results have been taken in to two iterations, in the first iteration power consumption is taken into account and it has been added as a parameter when the attack is launched. From the figure 5, the experimental results clearly depicts abnormal traffic moment in the network and records the power fluctuation. The difference between normal and abnormal traffic generates in the network would be shown in figure 6. The above results proved that power consumption in network scenario can be controlled with network attacks.

4. Result Discussion

Here the proposed model is experimentally setup with the data sets collected from the three connected client and server machine. Machine 1, machine 2 and machine 3 are the three machines used for collecting the input parameters in the form of data sets. Simulation is carried on the r2013b and figures from 5 to 14 clearly denotes the implementation results of the proposed methodology. Here machine 1 acts as server for the covert communication, machine 2 and machine 3 acts as the client for back door (cover communication). The machine1, machine 3 runs on windows 7 and windows server 2012 but machine 2 runs on kali Linux. In back track running machine was initialized using the backdoor “Meterpreter” and machine 2 was initialized by timing channel based covert communication.

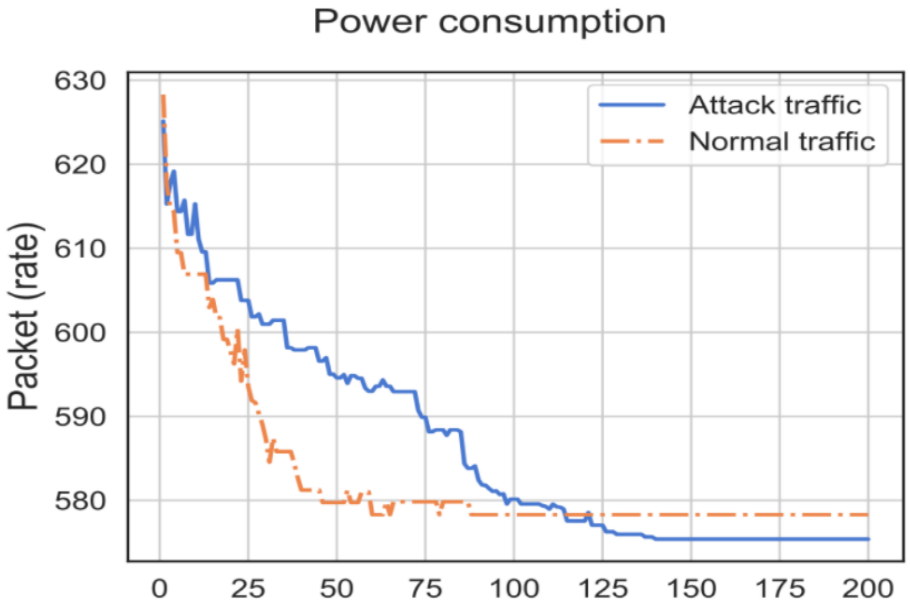

Fig 5: Power consumption in first phase (Normal vs. Attack traffic)

Figure 5 describes the attacking and normal traffic power consumption;it is clear that the attack traffic generated at the test host is comparatively high. Red colour defines the normal traffic whereas the blue colour shows the attack traffic generated in the system.

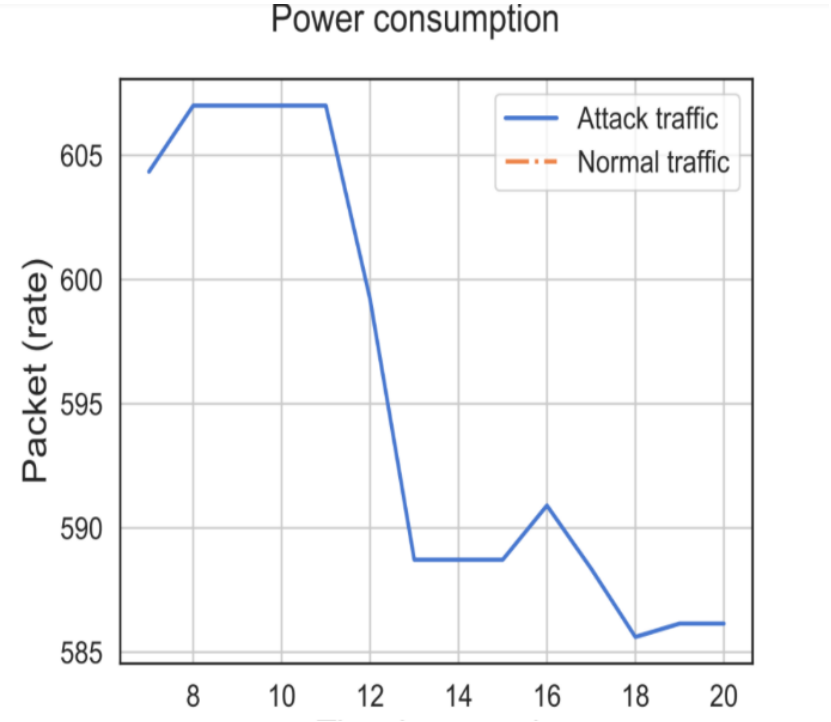

Fig 6: Power consumption in second phase (Normal vs. Attack traffic)

Figure 6 depicts the test host's health metric. The total number of incoming bytes (mb) is higher, indicating that the traffic is hitting the test host, as seen in the graph. Furthermore, the system memory and CPU use are at their highest levels..

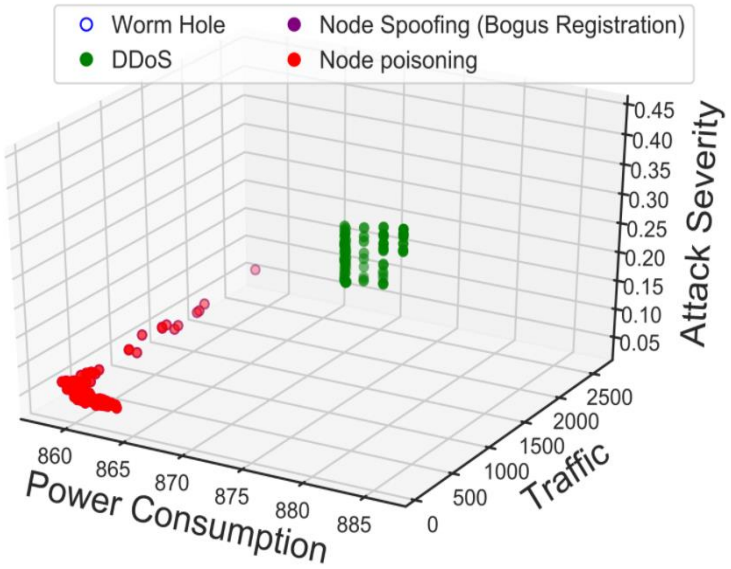

Fig 7: Attack analysis with power consumption (Normal vs. Attack traffic)

Figure 7 show the classification comparison of different attacks such as (DDoS, Worm Hole, Node Spoofing, node Poising) with power consumption, traffic and attack severity of the system.

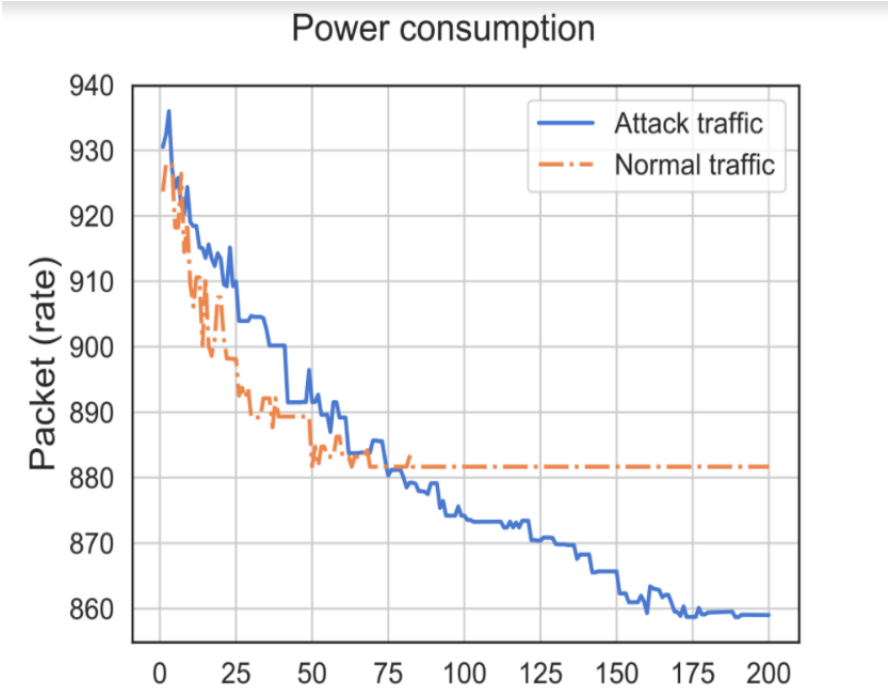

Fig 8

Figure 8 shows, the protocol grouping was finished by which hypertext move convention, secure attachment layer, straightforward mail move convention which bundles were arranged from the tapped parcels. Order of whole traffic was a perplexing cycle because of expansion in computational time.

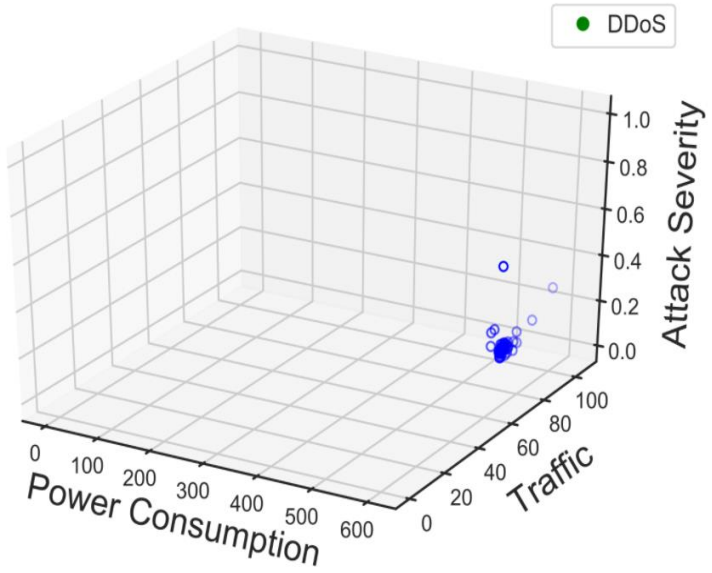

Fig 9: Attack severity analysis in

Figure 9 show the classification of DDoS with power consumption, traffic and attack severity of the system.

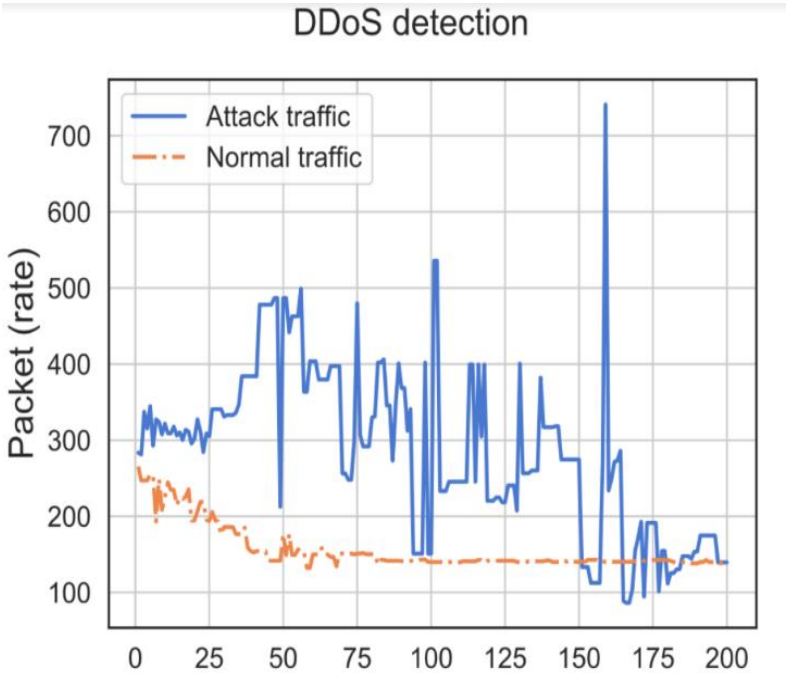

Fig 10: DDoS Detection in first phase of attack (Normal traffic vs. Abnormal Traffic)

Figure 10 show the classification of DDos with power consumption, attacking and normal traffic power consumption; it is clear that the attack traffic generated at the test host is comparatively high. Red colour defines the normal traffic whereas the blue colour shows the attack traffic generated in the system.

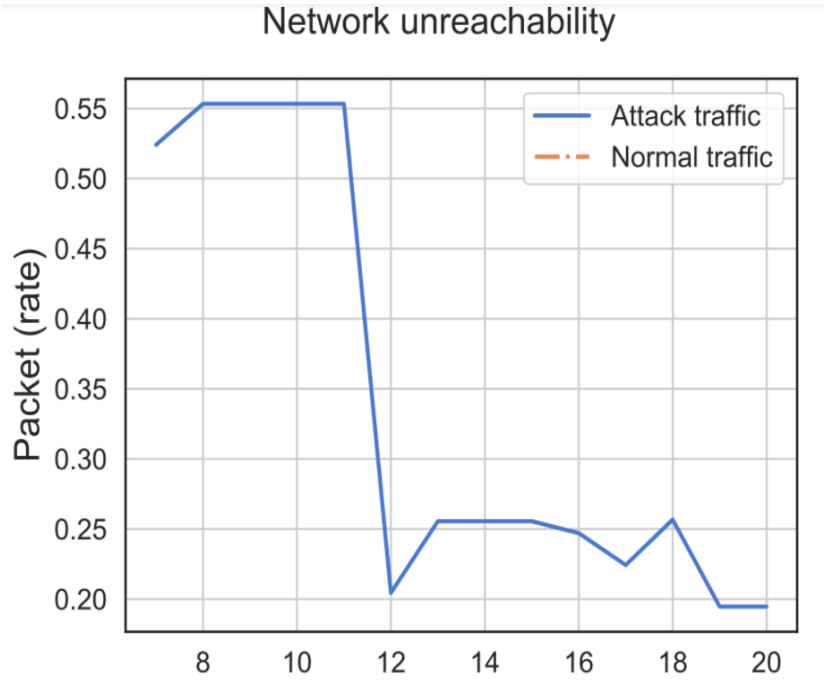

Fig 11: Network Unreachability in first phase (Normal traffic vs. Abnormal Traffic)

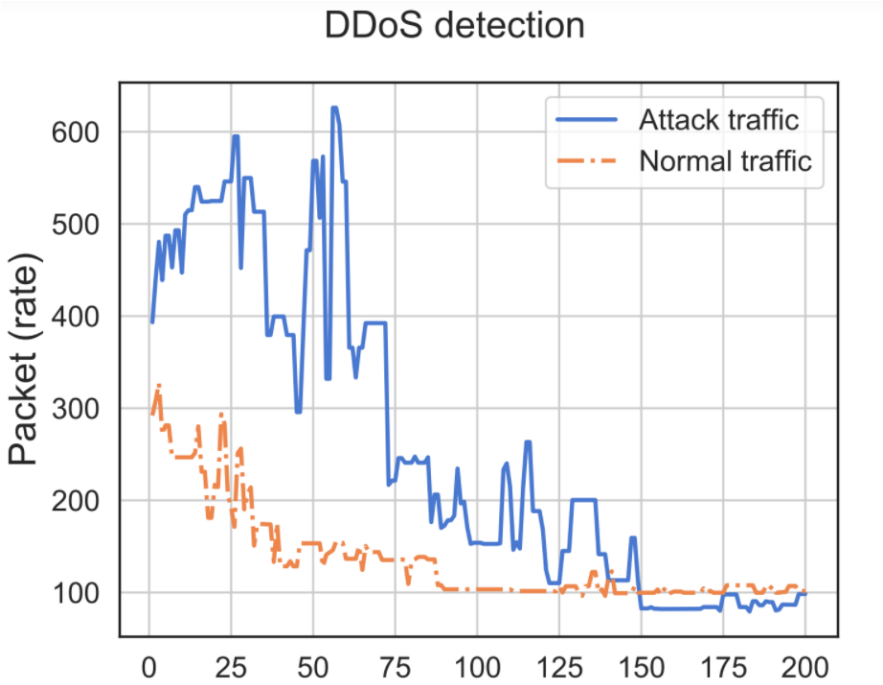

Fig 12: DDoS Detection in second phase(Normal traffic vs. Abnormal Traffic)

Figure 12 describes the DDoS detection rate in terms of accuracy and the packet flow of the attack traffic vs. normal traffic with respect to the efficiency of the system. Order of whole traffic was a perplexing cycle because of expansion in computational time.

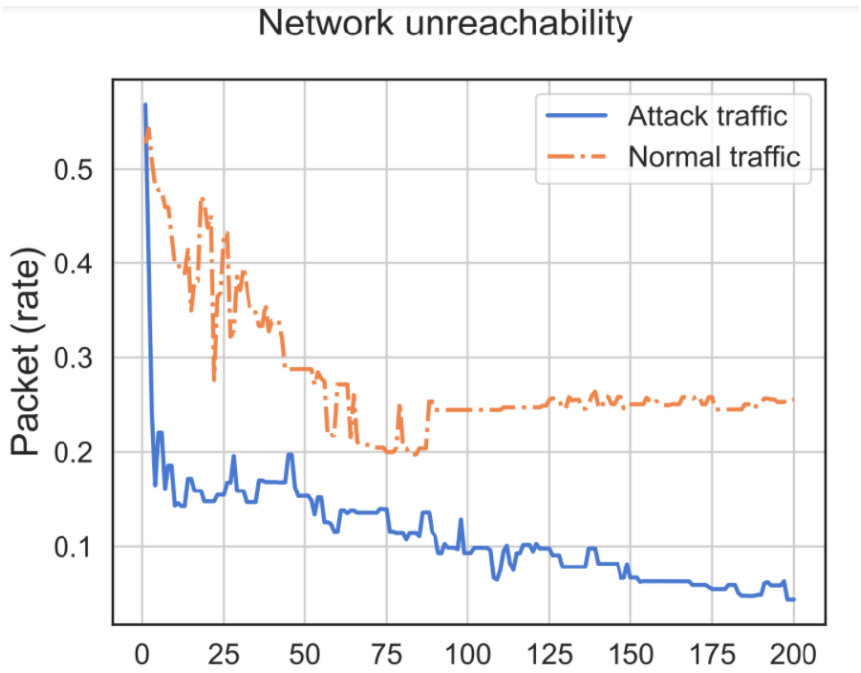

Fig 13: Network Unreachabilityin second phase (Normal traffic vs. Abnormal Traffic)

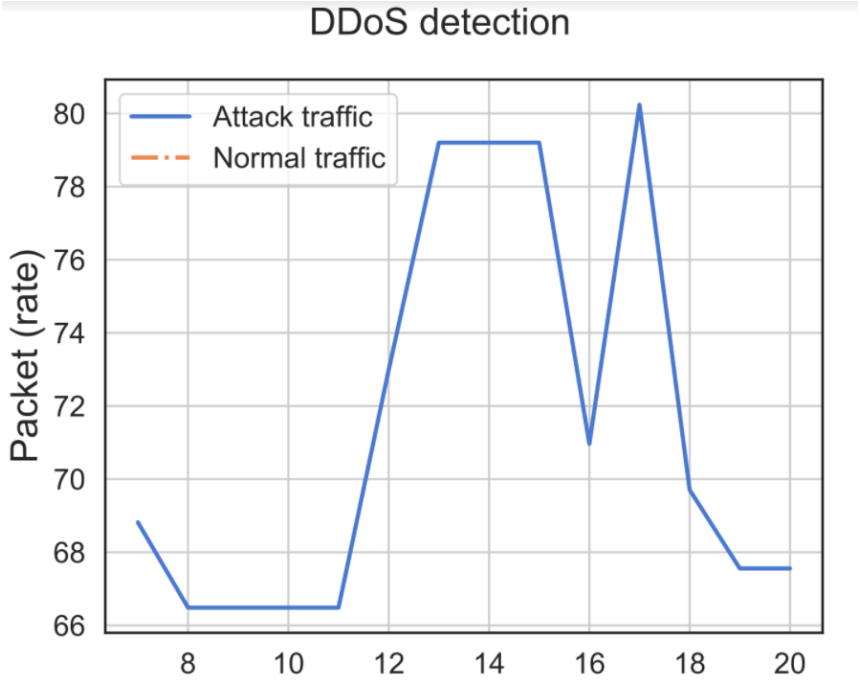

Fig 14: DDoS detection in third phase (Normal traffic vs. Abnormal Traffic)

Figure 11 and 13 show the network unreachability of the normal traffic and attack severity of the system. Figure 14 describes the DDos detection rate in terms of accuracy and the packet flow of the attack traffic.

5. Conclusion

Hence, we conclude this paper by proposing a robust anomaly detection approach to covert communication in the network. State of the art of our work is using Machine Learning in detection phase and to model all the hosts as states. The learning phase is used to learn the behaviour of the system and host with basic network parameters. The results illustrated in figures shows that the proposed model outperforms with higher accuracy in terms of prediction. The comparative approach of the various network tools to follow with absolute resulting values in terms of figures reveals the proposed model has better compatibility and high accuracy in detecting network attacks. The proposed model can be applied to any application tier protocol to detect covert communication.

Reference

[1] Z. Hosseini and Z. Movahedi, "A Green Trust Management Scheme to Mitigate Trust-Distortion Attacks on MANETs," 2016 Intl IEEE Conferences on(UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016, pp. 518-525, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0091.

[2] C. Tang et al., "A Mobile Cloud Based Scheduling Strategy for Industrial Internet of Things," in IEEE Access, vol. 6, pp. 7262-7275, 2018, doi: 10.1109/ACCESS.2018.2799548.

[3] W. Wang, N. Deng and B. Xin, "Sequential Detection of Image Defects for Patterned Fabrics," in IEEE Access, vol. 8, pp. 174751-174762, 2020, doi: 10.1109/ACCESS.2020.3024695.

[4] J. Chang, B. Shao, Y. Ji and G. Bian, "Comment on “A Tag Encoding Scheme Against Pollution Attack to Linear Network Coding”," in IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 11, pp. 2618-2619, 1 Nov. 2020, doi: 10.1109/TPDS.2020.2999523.

[5] M. Furdek and C. Natalino, "Machine Learning for Optical Network Security Management," 2020 Optical Fiber Communications Conference and Exhibition (OFC), 2020, pp. 1-3.

[6] J. A. Adisa, S. O. Ojo, P. A. Owolawi and A. B. Pretorius, "Financial Distress Prediction: Principle Component Analysis and Artificial Neural Networks," 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019, pp. 1-6, doi: 10.1109/IMITEC45504.2019.9015884.

[7] J. S. Aidan, H. K. Verma and L. K. Awasthi, "Comprehensive Survey on Petya Ransomware Attack," 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), 2017, pp. 122-125, doi: 10.1109/ICNGCIS.2017.30.

[8] A. Bahrani and A. J. Bidgly, "Ransomware detection using process mining and classification algorithms," 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), 2019, pp. 73-77, doi: 10.1109/ISCISC48546.2019.8985149.

[9] Y. Wang, J. -T. Zhou, Y. Jiao and X. Song, "Comparative Analysis of Evolutionary Algorithms Based on Swarm Intelligence for QoS Optimization of Cloud Services," 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2019, pp. 434-439, doi: 10.1109/CSCWD.2019.8791926.

[10] R. Li and A. X. Liu, "Adaptively Secure Conjunctive Query Processing over Encrypted Data for Cloud Computing," 2017 IEEE 33rd International Conference on Data Engineering (ICDE), 2017, pp. 697-708, doi: 10.1109/ICDE.2017.122.

[11] M. Shojafar, C. Canali, R. Lancellotti and J. Abawajy, "Adaptive Computing-Plus-Communication Optimization Framework for Multimedia Processing in Cloud Systems," in IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1162-1175, 1 Oct.-Dec. 2020, doi: 10.1109/TCC.2016.2617367.

[12] Y. Y. Aung and M. M. Min, "A collaborative intrusion detection based on K-means and projective adaptive resonance theory," 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 2017, pp. 1575-1579, doi: 10.1109/FSKD.2017.8393000.

[13] S. Pan, T. Morris and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems," in IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3104-3113, Nov. 2015, doi: 10.1109/TSG.2015.2409775.

[14] A. Saranya, R. Senthilkumaran and G. Nagarajan, "Enhancing network lifetime using tree based routing protocol in wireless sensor networks," 2015 2nd International Conference on Electronics and Communication Systems (ICECS), 2015, pp. 1392-1396, doi: 10.1109/ECS.2015.7124813.

[15] J. Wang, Y. Tan, J. Liu and Y. Zhang, "Topology Poisoning Attack in SDN-Enabled Vehicular Edge Network," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9563-9574, Oct. 2020, doi: 10.1109/JIOT.2020.2984088.

[16] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool and W. Dou, "Complementing IoT Services Through Software Defined Networking and Edge Computing: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1761-1804, thirdquarter 2020, doi: 10.1109/COMST.2020.2997475.

[17] H. Yuan, X. Zhan and Y. Yang, "Research on QoS Optimization Method of Wireless Access Network," 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), 2019, pp. 203-208, doi: 10.1109/ICCNEA.2019.00047.

[18] Y. Xiao, C. Xing, T. Zhang and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," in IEEE Access, vol. 7, pp. 42210-42219, 2019, doi: 10.1109/ACCESS.2019.2904620.

[19] R. Kumar and D. Sharma, "HyINT: Signature-Anomaly Intrusion Detection System," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-7, doi: 10.1109/ICCCNT.2018.8494088.

[20] M. H. Ali, M. Fadlizolkipi, A. Firdaus and N. Z. Khidzir, "A hybrid Particle swarm optimization - Extreme Learning Machine approach for Intrusion Detection System," 2018 IEEE Student Conference on Research and Development (SCOReD), 2018, pp. 1-4, doi: 10.1109/SCORED.2018.8711287.

[21] N. Sapkota, A. Alsadoon, P. W. C. Prasad, A. Elchouemi and A. K. Singh, "Data Summarization Using Clustering and Classification: Spectral Clustering Combined with k-Means Using NFPH," 2019

International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 146-151, doi: 10.1109/COMITCon.2019.8862218.

[22] S. Chandra and M. Kaur, "Creation of an Adaptive Classifier to enhance the classification accuracy of existing classification algorithms in the field of Medical Data Mining," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 376-381.

[23] Okfalisa, I. Gazalba, Mustakim and N. G. I. Reza, "Comparative analysis of k-nearest neighbor and modified k-nearest neighbor algorithm for data classification," 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017, pp. 294-298, doi: 10.1109/ICITISEE.2017.8285514.

[24] Y. Pristyanto, I. Pratama and A. F. Nugraha, "Data level approach for imbalanced class handling on educational data mining multiclass classification," 2018 International Conference on Information and Communications Technology (ICOIACT), 2018, pp. 310-314, doi: 10.1109/ICOIACT.2018.8350792.

[25] M. S. Başarslan and İ. D. Argun, "Classification Of a bank data set on various data mining platforms," 2018 Electric Electronics, Computer Science, Biomedical Engineerings' Meeting (EBBT), 2018, pp. 1-4, doi: 10.1109/EBBT.2018.8391441.

[26] D. Apiletti, E. Baralis, T. Cerquitelli and V. D'Elia, "Network Digest analysis by means of association rules," 2008 4th International IEEE Conference Intelligent Systems, 2008, pp. 11-32-11-37, doi: 10.1109/IS.2008.4670505.

[27] S. T. Karamouzis and A. Vrettos, "Sensitivity Analysis of Neural Network Parameters for Identifying the Factors for College Student Success," 2009 WRI World Congress on Computer Science and Information Engineering, 2009, pp. 671-675, doi: 10.1109/CSIE.2009.592.

[28] F. Wei, P. Vijayakumar, Q. Jiang and R. Zhang, "A Mobile Intelligent Terminal Based Anonymous Authenticated Key Exchange Protocol for Roaming Service in Global Mobility Networks," in IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 268-278, 1 April-June 2020, doi: 10.1109/TSUSC.2018.2817657.

[29] K. Sekaran, M. S. Khan, R. Patan, A. H. Gandomi, P. V. Krishna and S. Kallam, "Improving the Response Time of M-Learning and Cloud Computing Environments Using a Dominant Firefly Approach," in IEEE Access, vol. 7, pp. 30203-30212, 2019, doi: 10.1109/ACCESS.2019.2896253.

[30] N. Sharma, M. Singh and A. Misra, "Prevention against DDOS attack on cloud systems using triple filter: An algorithmic approach," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 560-565.

[31] E. Afgan, V. Jalili, N. Goonasekera, J. Taylor and J. Goecks, "Federated Galaxy: Biomedical Computing at the Frontier," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 871-874, doi: 10.1109/CLOUD.2018.00124.

[32] H. Zhang, G. Zhang and J. Wang, "State estimation for a four-wheel-independent-drive electric ground vehicle," 2015 34th Chinese Control Conference (CCC), 2015, pp. 8073-8078, doi: 10.1109/ChiCC.2015.7260924.

[33] K. Dubey, M. Y. Shams, S. C. Sharma, A. Alarifi, M. Amoon and A. A. Nasr, "A Management System for Servicing Multi-Organizations on Community Cloud Model in Secure Cloud Environment," in IEEE Access, vol. 7, pp. 159535-159546, 2019, doi: 10.1109/ACCESS.2019.2950110.

[34] B. Balamurugan, N. G. Shivitha, V. Monisha and V. Saranya, "A Honey Bee behaviour inspired novel Attribute-based access control using enhanced Bell-Lapadula model in cloud computing," International Confernce on Innovation Information in Computing Technologies, 2015, pp. 1-6, doi: 10.1109/ICIICT.2015.7396064.

[35] A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 633-636, doi: 10.1109/GUCON.2018.8675033.

[36] A. Rindos and Y. Wang, "Dew Computing: The Complementary Piece of Cloud Computing," 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom), 2016, pp. 15-20, doi: 10.1109/BDCloud-SocialCom-SustainCom.2016.14.

[37] K. Mershad, H. Artail, M. A. R. Saghir, H. Hajj and M. Awad, "A Study of the Performance of a Cloud Datacenter Server," in IEEE Transactions on Cloud Computing, vol. 5, no. 4, pp. 590-603, 1 Oct.-Dec. 2017, doi: 10.1109/TCC.2015.2415803.

[38] C. De Luca et al., "Unsupervised on-demand web service for DInSAR processing: The P-SBAS implementation within the ESA G-POD environment," 2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), 2015, pp. 2692-2695, doi: 10.1109/IGARSS.2015.7326368.

[39] P Visu, P.S.Smitha, V.Murugananthan, Mohd Wazih Ahmad “Enhanced EEG classification using adaptive DWT and heuristic-ICA algorithm” Automatika 64 (4), 827-836, 2023

[40] F. Jalali, A. Vishwanath, J. de Hoog and F. Suits, "Interconnecting Fog computing and microgrids for greening IoT," 2016 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia), 2016, pp. 693-698, doi: 10.1109/ISGT-Asia.2016.7796469.

[41] P. Raad, S. Secci, C. Phung and P. Gallard, "PACAO: A protocol architecture for cloud access optimization in distributed data center fabrics," Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft), 2015, pp. 1-9, doi: 10.1109/NETSOFT.2015.7116143.