Signature-Based Intrusion Detection System for IoT

Chapter · November 2023

DOI: 10.1201/9781003404361-8

4 authors, including:

Usman Haider
Kadir Has University

Inam Ullah Khan
Multimedia University

Muhammad Fayaz
Kohat University of Science and Technology

CRC Press
Taylor & Francis Group

Signature-Based Intrusion Detection System for IoT

Bakhtawar Nawaal[1], Usman Haider[2], Inam Ullah Khan[3], Muhammad Fayaz[4]

[1]University of Engineering and Technology Taxila, Pakistan, (Email: bakhtawarnawaal@gmail.com)

[2]National University of Computer and Emerging Sciences Islamabad, Pakistan, (Email: usmanhaider@ieee.org, ORCID: https://orcid.org/0000-0002-1086-4510)

[3]Isra University Islamabad Campus, Pakistan, (Email: inamullahkhan05@gmail.com, ORCID: https://orcid.org/0000-0003-3637-6977)

[4]University of Central Asia Naryn, Kyrgyzstan, (Email: muhammad.fayaz@ucentralasia.org)

DOI: 10.1201/9781003404361-8

Abstract

Security has become a factor of key importance since recent advancements in technology and in the domain of Internet of Things (IoT). All researchers have agreed to this point that not a single system can be worth deploying without a proper solution for its security. So, the significance of cybersecurity cannot be neglected anymore. An Intrusion Detection System (IDS) monitors the network traffic and warns in case of possible threats. Three types of IDS are being used i.e., Anomaly-based, Signature-based and Hybrid-based. Signature-based IDS matches threats with cyberattack signatures from databases and alerts in reference to that. Researchers have proposed various kinds of approaches for signature-based IDS using pattern-matching approach, Machine learning (ML) and Deep Learning (DL) Algorithms. This paper exhibits a detailed survey on Signature-based IDS for IoT environments.

Keywords

Cyber Security, IoT, IDS, ML.

1. Introduction

Internet of Things (IoT) is a network of devices that communicates over internet and distributes information among themselves and external environment. The term IoT was first used by Kevin Ashton in 1998 when he mentioned that IoT has the potential to change the entire world. It has improved people's lifestyle by adding intelligent systems to our environments. Evolution in IoT has added billions of IoT devices to Internet. Its applications have progressed in diverse streams including fitness, health, automation and smart societies [1]. With IoT technologies, cities have become more efficient. Traffic is managed smartly using sensors. Smart parking has saved fuel and time for drivers by providing data on available slots. Smart waste management, street lights, water supply, environment etc. have effectively enhanced lifestyle of citizens. Smart farming has helped thousands of farmers in managing the requirements of water, fertilizer and manure for plants. Quality of human life has improved too with effective healthcare systems which monitor patient's health and track changes [2].

Increasing demand for devices has provided space for various attacks from worms, viruses, trojan horses, malware etc. [3]. With time devices have become more vulnerable to security attacks. Commonly encountered attack includes DoS and DDoS. A Denial-of-Service (DoS) Attack tends to shut down network resources for the host [4]. In Distributed Denial-of-Service (DDoS) attack, the attacker utilizes resources from multiple locations to affect the network. According to Cisco White Paper, DDoS attacks will reach up to 15 million by 2023 while in 2018 they were 7 million [5]. IoT Botnets have caused much danger to IoT devices. The most common examples of Botnets include Linux/Hydra, Psyb0t, Linuz Darlloz, Spike (Dofloo), BASHLITE and Mirai etc. [6]. Other types of attacks include Brute Force Attacks, Rolling Code attacks, ClueBorne attacks, Sybil attacks, and buffer overflow attacks which affect IoT components. Sybil attacks use fabricated devices to hinder the performance of network devices and create traffic junctions [7]. BlueBorne virus attacks the device via Bluetooth and involves no human interaction [8]. List of attacks keeps on increasing with the addition of devices on internet.

Ultimately these consequences of cyberattacks have led to the major development of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). An IDS provides extensive surveillance which detects unusual or malicious traffic entering the network [9]. Three basic genres of IDS are;

- Signature-Based IDS
- Anomaly-Based IDS
- Hybrid-Based IDS

Signature-based IDS consists of existing patterns of malicious codes which are utilized in identifying attacks. This IDS is easy to use. Anomaly-based IDS compares data patterns with already created data of normal behavior of packets to detect abnormality [10]. Hybrid-based IDS in the union of both of the later types, hence it lowers the error rate. It can detect multiple categories of attacks from a variety of reckoning environments. An overview of signature-based intrusion detection is shown in Figure 1.

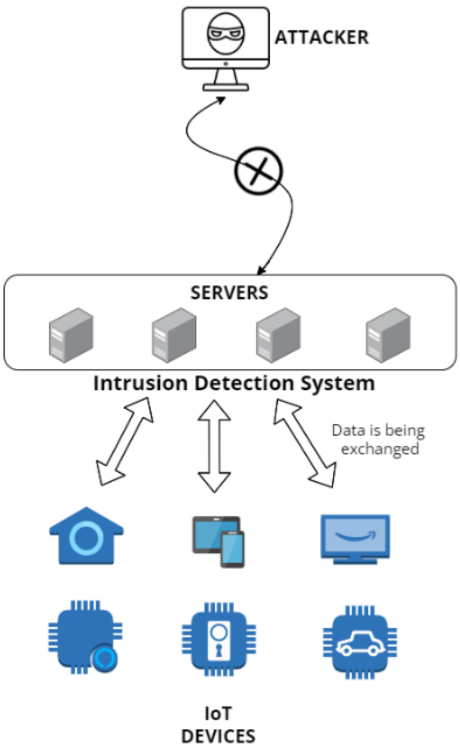

Figure 1: Overview of Signature-based IDS

Signature-based ID systems depend upon previously defined attacks and is better than anomaly-based in certain ways. It is simple and operates online in real-time [11]. They observe certain patterns and events and match them with signatures of attacks on a predefined list of known indicators of compromise (IOCs). 80% of incidents in any cyber-physical system are easily marked and detected using signature-based methodologies [12].

2. Literature Study

This section discusses the recent work performed to extract limitations related to Intrusion detection systems using various techniques, as illustrated below:

Intrusion detection systems functions on a certain algorithm. There has been plenty of work related to various IDS previously which helped in delivering important outcomes. To identify selective forwarding black hole attacks, Hidoussi et al. [13] presented a signature-based IDS. It was meant for wireless sensor networks (WSNs) that are cluster-based. Another signature-based IDS was proposed by Patel SK et al. [14] to identify port scan attacks via (EPSDR) which is port scan detection rule. Mehare et al. [15] designed an IoT-based IDS which depended on location and neighborhood information of the nodes which attacked. This paper covered only the DoS attack whereas they did not evaluate the proposed model in paper. Krimmling et al. [16] suggested signature-based IDS that lean on ML algorithms. The system uses a lightweight algorithm and is applied to CoAP applications. Liu et al. [17] established an artificial immune IDS for an IoT environment. The IDS could learn new attacks which are based on ML and signature-based models.

A Unified Intrusion detection system (UIDS) was suggested by Kumar et al. [18] for IoT-based networks. The model was analyzed on upgraded data set UNSW-NB15. An analysis of UNSW-NB15 [19] dataset was directed by Moustafa et al. [14]. They compared the operation of this dataset with KDD99 [20] using machine learning. Koroniotis et al. [21] have also conducted an analysis of various ML techniques using the UNSW-NB15 dataset to check how it detects intrusions in the network. Garcia-Font et al. [22] suggested an IDS for Wireless Sensor Networks (WSNs) using signature-based approach and ML techniques. They improved the detection rate and FPR by using a signature and anomaly-based detection engines. The main goal of the system is to identify malicious codes in WSNs in various smart city environments and was also applicable to large city environments.

Various types of IDSs have certain limitations. Anomaly-Based IDSs depend upon statistical features of normal traffic. They can identify unknown attacks. Major issues encountered by these systems are the high false-positive ratio when it comes to unpredictable traffics [23]. It also causes problems while processing and analyzing big data [24]. Utilization of outdated data sets has also caused hindrances in evaluating the performance of IDS [25]. Labelling of Data Sets is another hurdle faced if not done rightly. Correct labelling of data sets makes the IDS reliable by defining all attacks [26]. Moreover, labelling improves the accuracy of detection by making use of supervised Learning algorithms [27].

Signature-based IDS also encounters problems in detecting polymorphic worms and Metamorphic malware because of the rewriting process in every iteration. Polymorphic worms are the greatest challenge for Signatures-Based IDS as they modify and replicate themselves to fool the system. However, Y-Tang and S. Chen proposed an Intrusion Detection System which could detect polymorphic worms via Position Aware Distributions Signatures. (PADS) [24]. A Signature-based IDS detects already known attacks through a database of patterns [28]. Some of its disadvantages include false alarms, overloading of network packets and high cost of signature matching [29]. Memory constraints also pose some disadvantages to the signature-base system by making it less performant due to storage of huge databases [30]. Pattern databases in signature-based IDS need to be consistently changed. These IDSs detect intrusions based on previous knowledge. Table 1 shows the limitations of various types of IDS.

Table 1: Limitations of IDSs

Reference	**Type of IDS**	**Technique Used**	**Behavior**	**Description**	**Limitations**
[31]	Signature -based	Pattern Matching Approach	Depends on pre-existing patterns of malicious codes	This proposed a pattern-matching IDS for embedded security systems. It uses an auxiliary skipping (AS) algorithm which helps in reducing the number of matching operations. This IDS applies to smart objects that have confined memory size.	Do not allow finding higher-order pattern malware
[32]	Anomaly -Based	Machine Learning	Compares normal traffic with current incoming data packets	IDS uses a mathematical algorithm to train itself on normal dataset. It learns characteristics and then detects the malicious codes.	Takes long time in training data and identify threats from alerts
[33]	Anomaly -Based	Machine Learning	The IDS captures human activity or inactivity through IoT device sensors placed in the simulated smart environment.	This IDS uses machine learning technique which is based on artificial immune system. It is a behavior modelling IDS which decides if the behavior is acceptable or not	Vague warning leads to the provision of unclear information to the administrator
[34]	Hybrid-Based	DT, SVM Algorithms	The ensemble approach gave better results	This work presented the use of machine learning through Decision Tree (DT) and Support Vector Machine (SVM) techniques for efficient IDS.	SVM does not satisfy in case of larger datasets.

[35]	Hybrid-Based	Deep Neural Network (DNN)	Significantly flexible on commodity hardware server.	This paper proposed the use of deep learning to counter the problems of high false alarm rate, single dataset usage, and modern huge network obstinacy.	The details regarding the malware cannot be acquired using this model.
[36]	Anomaly-Based	Naïve Bayes (NB)	A threshold is defined to differentiate between the normal and attack records.	This work presented an IDS based on Bayesian Probability using KDD dataset and NB classifier.	The NB classifier has limited functionality in real-time.
[37]	Hybrid-Based	Convolutional Neural Network (CNN)	The model works in four-stages i.e., data collection, pre-processing, training and detection	This paper proposed an IDS based on CNN for IoT environment and network is divided into various layers i.e., convolutional, input and hidden layer.	CNN model is comparatively slower.
[38]	Signature-based	Hybrid Placement Strategy	The proposed used an IDS border router (BR) and various detectors in IoT network.	This research suggested a new signature-based IDS for IoT framework. It incriminates centralized and distributed IDS modules.	Zero-Day exploit remains unattended
[39]	Signature-based	Collaborative Blockchain Technology	The model is divided in various nodes and IDS nodes exchange data with each other.	The work suggested a blockchain-based IDS, CBSigIDS for IoT habitat by integrating the blockchains with distributed signature-based IDS.	The system's accuracy needs improvement and blockchain technology can be vulnerable to various attacks.

3. SECURITY CHALLENGES & CYBER ATTACKS IN IoT NETWORK

All devices in an IoT system communicate wirelessly and therefore they are exposed to several vulnerabilities that bridge all layers of the IoT architecture. It must be prevented from threats [40]. Compatibility and complexity are the two most significant challenges that IoT-based environments face. They are mostly affected by Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), SQL Injection Attacks, Ping of Death (PoD) Attacks , Sinkhole Attacks etc. [41]. A sinkhole attack is launched by an inside attacker whereas a DoS attack makes the network unavailable to the users. IoT systems face four types of security issues;

i. Validation and Vulnerabilities
ii. Confidentiality Compromises
iii. Data Integrity Inconsistencies
iv. Privacy Violations

Table 2 describes the cyber issues that are commonly raised in different IoT layers [42].

Table 2: Categories of Security Challenges Faced by IoT Systems

Sr. No.	Categories	Detail
1	Validation and Vulnerabilities	Mostly precepted by sensors as they are open to physical attacks.
2	Confidentiality Compromises	Occurs in between network layer and gateways
3	Data Integrity Inconsistencies	This issue arises during applications and service of IT systems, when IoT System is affected by noise or attack.
4	Privacy Violations	Data privacy is the most important challenge that is faced by IoT systems.

The utilization of various technologies and products in IoT framework poses threats to the security of smart environments. This is due to lack of standardization. Moreover, penetration of a single-end device also causes harm to the whole network [43].

4. Intrusion Detection System for IoT Networks

An intrusion detection system working in an IoT system protects the network from intrusions and threats. It maintains the integrity, availability and confidentiality of the network [44]. IDS detects the network condition and it alerts in the form of alarms. There are four situations of IDS alerts i.e., true positive, true negative, false positive and false negative pointing to real threat, normal scenario, false alert and misdetection respectively [45], [46]. Figure 2 explains the classification of threat alerts in IDS.

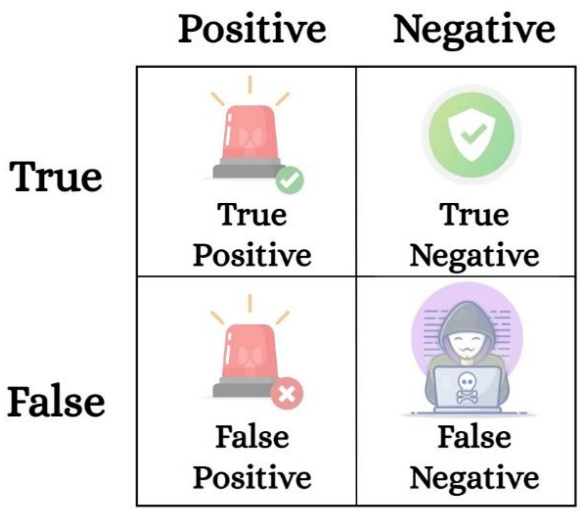

Figure 2: Classification of Threat Alerts

Two main types of IDSs can be implemented in the system i.e., Host-Based Intrusion Detection System (HIDS) and Network-Based Intrusion Detection System (NIDS). HIDS is deployed on a single system and uses the metrics of the host environment to detect attacks [47]. Whereas, a NIDS senses intrusions from network data packets [48]. Figure 3 shows the overview and placement of HIDS and NIDS. These two types of IDSs are further classified on the bases of their detection techniques among anomaly-based detection, signature-based detection and hybrid-based detection.

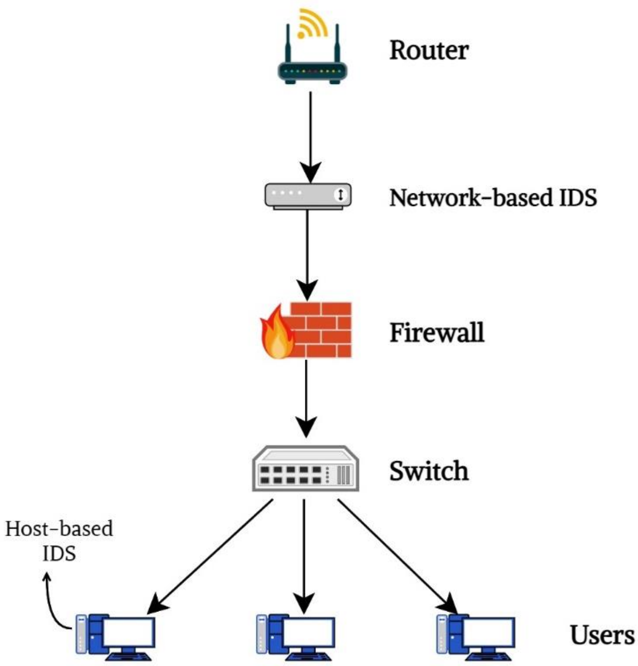

Figure 3: Overview and Placement of HIDS and NIDS

4.1. Signature-Based IDS for IoT

A signature-based technique uses patterns and signatures of known malicious codes to detect attacks [54]. It uses previous knowledge to detect these attacks. Hence, databases of patterns and signatures need to be updated. Writing signatures require expertise as new types of attacks are continuously being discovered. For this, we need to have enough data for analysis purposes and a good understanding of the behavior of signatures [55]. Signature-based technique minimizes false alarms providing accuracy. Hence, many commercial systems are installed with signature-based detection due to the production of fewer false alarms [56]. However, advancement in technology has hindered the efficiency of Signature-based IDSs as the number of signatures would also be increased with technologies such as encrypted data channels, nop generators, and payload encoders [57]. Figure 4 explains the concept of Signature-based IDS.

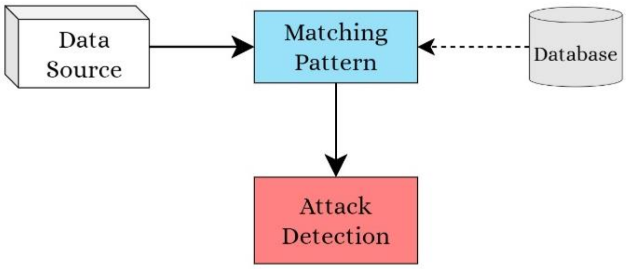

Figure 4: Concept of Signature-based IDS

4.2. Hybrid-Based IDS for IoT

In Hybrid Intrusion Detection technique, the concept of both HIDS and NIDS is used. It collects data from the host as well as from network and then analyses it for intrusions. The analysis is held based on anomaly detection or a database of signature-based patterns [58]. Hybrid Intrusion Detection includes two steps. In the first step, anomaly detection part of HIDS functions to identify abnormalities using a particular approach. In case of any malicious code identification, its pattern is stored in signature database to protect the IoT system from similar attacks. This process is executed in second stage [59]. The hybrid-based IDS accomplishes the targets of a high alarm probability and low false positives [60].

5. Machine Learning Based Signature-IDS Solutions for IoT

Signature-based IDS can be implemented using various machine learning (ML) techniques. The machine learning technique consists of training and testing stages [61]. During training of a dataset, algorithms use data at normal state as information source to train themselves on the features of IoT network. After that classification is performed in testing stage [62]. Below listed are some of the ML techniques that can be used to implement Signature-based IDS for IoT;

In Supervised learning, classification model is created by using the characteristics of training datasets. This is the learning phase of the model [63]. Whereas, unsupervised Learning model doesn't use clustered training data.

Naive Bayes algorithm can be used for probability calculations, using network traffic characteristics in signature-IDS based on an IoT system [64]. Naive Bayes requires less amount of data in characterization cycle to find the estimated boundaries. It performs well on KDD CUP 1999+NSL, UNSW-NB15 datasets and helps in detecting DDoS, DoS, Code injection etc. [65].

Decision Tree (DT) classifier facilitates decision making by using the techniques of Information gain and genii index. Data can be manipulated and missing values can be found by using this algorithm [66]. Decision trees are easy to use and can be implemented to CICIDS 2017, BOT-IoT, KDDS99, NSL-KDD datasets in identifying attacks such as Sybil, flooding, spyware etc. [67].

K-Nearest Neighbor (KNN) calculates the distance between the neighbors using Euclidean distance [68]. KNN categorizes the new occurrence based on maximum number of nearest neighbors. It can be implemented on datasets such as DS2OS, UNSW-NB15 etc. [69].

Support Vector Machine (SVM) is another ML technique that helps in real-time detection of both known and unknown attacks [70]. SVM classifies linearly separable data into two-dimensional planes. The kernel function in SVM converts non-linear data into linear form for attack detection. The performance of SVM depends upon the data set and its environment [71]. Datasets such as UNSW-NB15, KDDCUP99, NSL-KDD, and NOT-IoT can be used for SVM in detecting attacks like Man-in-the-Middle attacks, DoS, DDoS, tempering etc. [72].

6. Deep Learning Based Signature-IDS Solutions for IoT

We apply deep learning (DL) techniques while dealing with larger datasets rather than machine learning-based solutions. These methodologies are widely applied in IDSs. Deep learning is the domain of ML that consists of neural networks which help in finding high-level features of data through layers of modification [73]. In an intrusion detection system, the hidden layers of the neural network help in identifying the best features for pattern selection. It contains an input layer, hidden layer(s) and an output layer. Specific weights are associated with every input of the network which are adjusted to get the best output via backpropagation method [74]. Deep learning detection techniques are classified into three main streams, that is, supervised learning, unsupervised learning techniques and Hybrid methods [75].

Some of the famous DL techniques like Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) etc. are included in Supervised Learning methods. These methods provide high accuracy. Deep Neural Networks (DNN) contains numerous hidden layers which aid in feature extraction. Complex functions with fewer parameters can be expressed through these hidden layers. Tang et al. [76] designed a simple DNN which performed flow-based detection. Convolutional Neural Network (CNN) performs convolution, pooling, full connection with the dataset input. CNN involves less preprocessing. Kolosnjaji et al. [77] designed a model to detect malware by proposing CNN with recursive network layers. Recurrent Neural Network (RNN) comprises of a memory function that stores previous data. It efficiently deals with time series information. C. Yin et al. [78] evaluated RNN with binary classification and multiclass classification.

Unsupervised learning techniques include Generative Adversarial Networks (GANs), Autoencoder (AE), Deep Belief Networks (DBN) etc. These methods are low in performance as insufficient knowledge is available from labelled data. Gao et al. [79] tried various DBN models to construct IDS. The best performance was acquired on KDDCup 99 dataset. Generative Adversarial Network (GAN) is a type of unsupervised learning that help to process, scrutinize, and capture data. It consists of a generator and discriminator which helps in identifying real images from fake ones. Erpek et al. [80] designed a jamming attacks detection model-based d on generative adversarial network. It consists of Transmitter, Receiver, Jammer. Autoencoder is a data compression algorithm used for reducing dimensions and detecting of outliers. It uses feature space for compressing the input. Zhang et al. [81] proposed an IDS by involving dilated convolutional AE (DCAEs) to extract useful features from original data traffic of network.

Hybrid methods result in high performance and a smaller number of training samples but computing time is high because of the complex structure. Li et al. [82] used a hybrid deep learning technique that implemented Autoencoder and Deep neural network for anomaly detection. AE was used to reduce the dimensions of data.

7. Signature-Based Intrusion Detection System Architecture

The researchers have used various kinds of IDS depending upon framework of the network as well as per requirements. Sourour et al. [83] suggested a two-layered IDS address the security concerns related to Network Address Translation (NAT). Layer 1 monitors the network entities and layer 2 is deployed using three modules i.e., alert consolidation, alert classification and alert correlation, to lower the number of alerts and to pin down false alarms. Zhang, Yichi, et al. [84] introduces a dispersive kind of IDS for the smart grid having multi-layered architecture using SVM for Classification of attack and Clonal Selection Classification (CSC) Algorithm for Attack Detection. Modular Deep Learning (MDL) Model is also suggested to deploy in an IDS as it has a multi-architectural topology inspired by human brain but this concept is still newborn [85]. The Application Layer is vulnerable to various kinds of attacks, so for cloud security, a signature-based cloud IDS is an efficient approach thus securing the application layer along with rest of the layers [86], [87]. The common organisation and threat detection phenomenon of signature-based IDS is shown in figure 5.

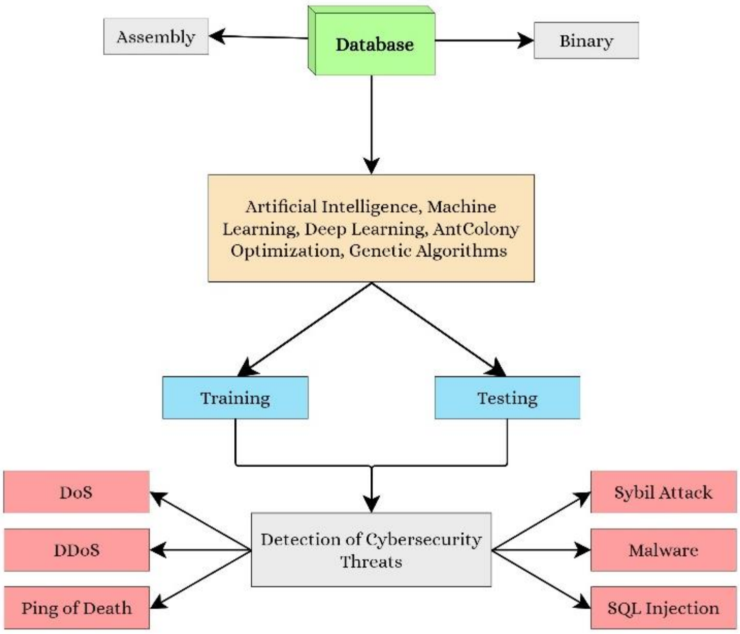

Figure 5: Threat Detection using Signature-based IDS

8. Limitations in Signature-Based Intrusion Detection System

Signature-based technique for IDS is a widely used approach because it usually has low false alarm rate and very efficient results. But this technique has some limitations that need to be addressed with proper solutions. Signature-based IDS can only identify the threats whose attack-signatures are been saved already thus it fails to detect anything absent from the database [88] thus Zero-Day-Exploit remains unattended [89], [90]. Sometimes it causes network packet overload and it has a huge false alarm rate when operated in a large-scale network environment [91]. Each packet in signature-based approach needs to be match examined, in case of large incoming traffic anomalies occur. In most cases, the following scenario leads to packet drop when IDS can't handle the traffic leaving chance to miss potential threats [92]. Thus, these limitations are termed as design or implementation flaws of the signature-based technique [93].

9. Discussion & Future Directions

Advancements in technology and the Internet of Things have caused much vulnerability to the security of data [94], [95]. Signature-based IDS are one of the widely installed IDSs in commercial sector networks because of their pattern-based anomaly detection capability. These systems are improving every day to meet the complexity of new threat variants. A detailed survey of signature-based IDS along with various implementation techniques is discussed in this research paper. Future work can be performed on it by implementing signature-IDS with specific techniques which makes it threat prone and performant. Software such as SNORT and WINPCAP etc. can be focused on real-time detection and efficiency [96]. Markov distribution also helps in packet filtering in IDS [97]. Furthermore, various DL algorithms can be used to reduce to computational complexity of the IDS as there is huge scope for this and enormous work can be done in this field.

10. Conclusion

Security has no longer been a choice in IT infrastructure; it is an utter compulsion to be focused on. The mushroom growth of IoT devices has raised challenge of security in the IoT environment. Signature-based IDS is an excellent approach to counter security threats. Many solutions using signature-based detection techniques have been suggested by different researchers using different methodologies. Pattern matching approach has been the identification of this type of detection but it has some limitations leading to false negative conditions and potential danger. Machine Learning and Deep Learning algorithm counters the limitation of signature-based detection by implying the training over various datasets thus decreasing the False detection rate and improving the accuracy. This work offers a detailed survey of a variety of signature-based IDS and the techniques deployed to them by different researchers.

References

[1] B. Alqahtani and B. AlNajrani, ‘‘A study of Internet of Things protocols and communication,’’ in Proc. 2nd Int. Conf. Comput. Inf. Sci. (ICCIS), Oct. 2020, pp. 1–6, doi: 10.1109/ICCIS49240.2020.9257652.

[2] Naveen, Soumyalatha. (2016). Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges.

[3] N. Abdalgawad, A. Sajun, Y. Kaddoura, I. A. Zualkernan and F. Aloul, "Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset," in IEEE Access, vol. 10, pp. 6430-6441, 2022, doi: 10.1109/ACCESS.2021.3140015.

[4] Mann, P., Tyagi, N., Gautam, S., & Rana, A. (2020). Classification of Various Types of Attacks in IoT Environment. 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN).

[5] Cisco Annual Internet Report—Cisco Annual Internet Report (2018-2023) White Paper. Accessed: May 31, 2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executiveperspectives/annual-internet-report/white-paper-c11-741490.html

[6] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, “Novel deep learning- enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 4507

[7] Archana M B , Harshitha B N , Prajakta M “A technique to safeguard cluster-based Wireless Sensor Networks against Sybil Attack”. International Journal of Recent Trends in Engineering and Research”, Vol. 3(4), pp. 370–373, 2017. doi: 10.23883/ijrter.2017.3159.jsizq

[8] Wang, W., He, S., Sun, L., Jiang, T., & Zhang, Q. (2019). CrossTechnology Communications for Heterogeneous IoT Devices Through Artificial Doppler Shifts. IEEE Transactions on Wireless Communications, 18(2), 796–806. doi: 10.1109/twc.2018.2883443

[9] Kumar, Vinod. (2012). Signature Based Intrusion Detection System Using SNORT. International Journal of Computer Applications & Information Technology. 1. 7.

[10] Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: Methods, systems and tools. IEEE Commun Surv Tutor 16(1):303–336

[11] Y. Tang and S. Chen, "An Automated Signature-Based Approach against Polymorphic Internet Worms," in IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 7, pp. 879-892, July 2007, doi: 10.1109/TPDS.2007.1050.

[12] Snehi, Jyoti. (2020). Diverse Methods for Signature-based Intrusion Detection Schemes Adopted.

[13] Hidoussi F, Toral-Cruz H, Boubiche DE, Lakhtaria K, Mihovska A, Voznak M (2015) Centralized IDS based on misuse detection for cluster-based wireless sensors networks. Wireless Pers Commun 85(1):207–224

[14] Patel SK, Sonker A (2016) Rule-based network intrusion detection system for port scanning with efficient port scan detection rules using snort. International Journal of Future Generation Communication and Networking 9(6):339–350

[15] Mehare TM, Bhosale S (2017) Design and development of intrusion detection system for internet of things. Int J Innov Res Comput Commun Eng 5(7):13469–13475

[16] Krimmling J, Peter S (2014) Integration and evaluation of intrusion detection for CoAP in smart city applications. In: 2014 IEEE Conference on Communications and Network Security. IEEE, San Francisco. pp 73–78

[17] Liu C, Yang J, Chen R, Zhang Y, Zeng J (2011) Research on immunity-based intrusion detection technology for the internet of things. In: 2011 Seventh International Conference on Natural Computation, vol. 1. IEEE, Shanghai. pp 212–216

[18] Kumar, V., Das, A.K. & Sinha, D. UIDS: a unified intrusion detection system for IoT environment. Evol. Intel. 14, 47–59 (2021). https://doi.org/10.1007/s12065-019-00291-w

[19] Mohammadi M, Akbari A, Raahemi B, Nassersharif B, Asgharian H (2014) A fast anomaly detection system using probabilistic artificial immune algorithm capable of learning new attacks. Evolut Intel 6(3):135–156

[20] Jha J, Ragha L (2013) Intrusion detection system using support vector machine. In: International Journal of Applied Information Systems: Proceedings on International Conference and workshop on Advanced Computing ICWAC, vol 3, Foundation of Computer Science, New York, USA, pp 25–30

[21] Koroniotis N, Moustafa N, Sitnikova E, Slay J (2017) Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In international conference on mobile networks and management, Springer Cham:30–44

[22] Garcia-Font V, Garrigues C, Rifà-Pous H (2017) Attack classification schema for smart city WSNs. Sensors 17(4):1–24

[23] Mitchell R, Chen I-R (2014) A survey of intrusion detection in wireless network applications. Comput Commun 42:1–23

[24] Y. Tang and S. Chen, "An Automated Signature-Based Approach against Polymorphic Internet Worms," in IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 7, pp. 879-892, July 2007,doi: 10.1109/TPDS.2007.1050.

[25] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), Canberra, ACT, Australia, 2015, pp. 1–6

[26] P. Gogoi, M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Packet and flow based network intrusion dataset,” in Contemporary Computing, M. Parashar, D. Kaushik, O. F. Rana, R. Samtaney, Y. Yang, and A. Zomaya, Eds. Heidelberg, Germany: Springer, 2012, pp. 322–334.

[27] P. Laskov, P. Düssel, C. Schäfer, and K. Rieck, “Learning intrusion detection: Supervised or unsupervised?” in Image Analysis and Processing (ICIAP), F. Roli and S. Vitulano, Eds. Heidelberg, Germany: Springer, 2005, pp. 50–57.

[28] Bul’ajoul W, James A, Pannu M (2015) Improving network intrusion detection system performance through quality-of-service configuration and parallel technology. J Comput Syst Sci 81(6):981–999

[29] Meng W, Li W, Kwok L-F (2014) Efm: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. Comput Secur 43:189–204

[30] Abduvaliyev A, Pathan ASK, Zhou J, Roman R, Wong WC (2013) On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Commun Surv Tutor 15(3):1223–1237

[31] Oh D, Kim D, Ro WW (2014) A malicious pattern detection engine for embedded security systems in the internet of things. Sensors 14(12):24188–24211

[32] Elrawy, M., Awad, A. & Hamed, H. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comp 7, 21 (2018). https://doi.org/10.1186/s13677-018-0123-

[33] Arrington B, Barnett L, Rufus R, Esterline A (2016) Behavioral modeling intrusion detection system (BMIDS) using internet of things (IoT) behavior-based anomaly detection via immunity-inspired algorithms. In: 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa. pp 1–6

[34] Peddabachigari, Sandhya, et al. "Modeling intrusion detection system using hybrid intelligent systems." Journal of network and computer applications 30.1 (2007): 114-132.

[35] Vinayakumar, Ravi, et al. "Deep learning approach for intelligent intrusion detection system." Ieee Access 7 (2019): 41525-41550.

[36] Altwaijry, Hesham. "Bayesian based intrusion detection system." IAENG Transactions on Engineering Technologies: Special Edition of the World Congress on Engineering and Computer Science 2011. Springer Netherlands, 2013.

[37] Smys, S., Abul Basar, and Haoxiang Wang. "Hybrid intrusion detection system for internet of things (IoT)." Journal of ISMAC 2.04 (2020): 190-199.

[38] Ioulianou, Philokypros, et al. "A signature-based intrusion detection system for the internet of things." Information and Communication Technology Form (2018).

[39] Li, Wenjuan, et al. "Designing collaborative blockchained signature-based intrusion detection in IoT environments." Future Generation Computer Systems 96 (2019): 481-489.

[40] Bandyopadhyay D, Sen J (2011) Internet of things: Applications and challenges in technology and standardization. Wirel Pers Commun 58(1):49–69.

[41] Abdollahi, A., Fathi, M. An Intrusion Detection System on Ping of Death Attacks in IoT Networks. Wireless Pers Commun 112, 2057–2070 (2020). https://doi.org/10.1007/s11277-020-07139-y

[42] Khan, Y.; Su’ud, M.B.M.; Alam, M.M.; Ahmad, S.F.; Salim, N.A.; Khan, N. Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. Electronics 2023, 12, 88. https://doi.org/10.3390/electronics12010088

[43] Forsström S, Butun I, Eldefrawy M, Jennehag U, Gidlund M (2018) Challenges of securing the industrial internet of things value chain In: 2018 Workshop on Metrology for Industry 4.0 and IoT, 218–223.. IEEE, Brescia.

[44] Ghorbani AA, Lu W, Tavallaee M (2010) Network Intrusion Detection and Prevention, Advances in Information Security, vol. 47. Springer, US.

[45] Spathoulas, Georgios P., and Sokratis K. Katsikas. "Reducing false positives in intrusion detection systems." computers & security 29.1 (2010): 35-44.

[46] Concha, Astrid, et al. "Using sniffing behavior to differentiate true negative from false negative responses in trained scent-detection dogs." Chemical senses 39.9 (2014): 749-754.

[47] Kumar S, Gautam, Om H (2016) Computational neural network regression model for host based intrusion detection system. Perspect Sci 8:93–95.

[48] Macia-Perez F, Mora-Gimeno FJ, Marcos-Jorquera D, Gil-Martinez-Abarca JA, Ramos-Morillo H, Lorenzo-Fonseca I (2011) Network intrusion detection system embedded on a smart sensor. IEEE Trans Ind Electron 58(3):722–732.

[49] Hong J, Liu C, Govindarasu M (2014) Integrated anomaly detection for cyber security of the substations. IEEE Trans Smart Grid 5(4):1643–1653.

[50] Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: Methods, systems and tools. IEEE Commun Surv Tutor 16(1):303–336.

[51] Mishra P, Pilli ES, Varadharajan V, Tupakula U (2017) Intrusion detection techniques in cloud environment: A survey. J Netw Comput Appl 77:18–47.

[52] Duque S, bin Omar MN (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). Procedia Comput Sci 61:46–51.

[53] Amin SO, Siddiqui MS, Hong CS, Lee S (2009) RIDES: Robust intrusion detection system for ip-based ubiquitous sensor networks. Sensors 9(5):3447.

[54] Bul'ajoul W, James A, Pannu M (2015) Improving network intrusion detection system performance through quality of service configuration and parallel technology. J Comput Syst Sci 81(6):981–999.

[55] Neminath Hubballi, Vinoth Suryanarayanan,False alarm minimization techniques in signature-based intrusion detection systems: A survey,Computer Communications,Volume 49,2014,Pages 1-17,ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2014.04.012.

[56] Christopher Kruegel, Thomas Toth, Recent Advances in Intrusion Detection, 2003, Volume 2820, ISBN : 978-3-540-40878-9

[57] Veeramreddy, Jyothsna & Prasad, V. & Prasad, Koneti. (2011). A Review of Anomaly based Intrusion Detection Systems. International Journal of Computer Applications. 28. 26-35. 10.5120/3399-4730.

[58] Chauhan, Pavitra & Chandra, Nidhi. (2013). A Review on Hybrid Intrusion Detection System using Artificial Immune System Approaches. International Journal of Computer Applications. 68. 22-27. 10.5120/11695-6499.

[59] Khraisat A, Gondal I, Vamplew P, Kamruzzaman J, Alazab A. A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. Electronics. 2019; 8(11):1210. https://doi.org/10.3390/electronics8111210

[60] Yassine Maleh, Abdellah Ezzati, Youssef Qasmaoui, Mohamed Mbida,A Global Hybrid Intrusion Detection System for Wireless Sensor Networks,Procedia Computer Science,Volume 52,2015,Pages 1047-1052,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2015.05.108.

[61] Tsai JJP, Yu PS (eds)2009. Machine Learning in Cyber Trust: Security, Privacy, and Reliability. First edn. Springer US, Springer-Verlag US. pp 1–362.

[62] Nishani L, Biba M (2016) Machine learning for intrusion detection in MANET: a state-of-the-art survey. J Intell Inf Syst 46(2):391–407.

[63] Namdev N, Agrawal S, Silkari S (2015) Recent advancement in machine learning based internet traffic classification. Procedia Comput Sci 60:784–791.Return to ref 71 in article

[64] Olufowobi H, Young C, Zambreno J, Bloom G (2019) Saiducant: Specification-based automotive intrusion detection using controller area network (can) timing. IEEE Trans Vehicular Technol 69:1484–1494

[65] Eskandari M, Janjua ZH, Vecchio M, Antonelli F (2020) Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE internet of things J 7:6882–6897. https://doi.org/10.1109/JIOT.2020.2970501

[66] Kumar V, Das AK, Sinha D (2020) Statistical analysis of the UNSW-NB15 dataset for intrusion detection. Computational intelligence in pattern recognition. Springer, Singapore, pp 279–294

[67] Mehmood A, Khanan A, Umar MM, Abdullah S, Ariffin KAZ, Song H (2017) Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. IEEE Access 6:5688–5694
[68] Sabeel U, Chandra N (2013) Categorized security threats in the wireless sensor networks. Countermeas Security Manag Schem 64:19–28
[69] Hummen R, Hiller J, Wirtz H, Henze M, Shafagh H, Wehrle K (2013) 6LoWPAN fragmentation attacks and mitigation mechanisms. In: Proc 6th ACM Conf Secur Privacy Wirel Mobile Netw, pp. 55–66
[70] Kasinathan P, Pastrone C, Spirito MA, Vinkovits M (2013) Denial-of-service detection in 6LoWPAN based internet of things. In: 2013 IEEE 9th Int Conf Wirel Mobile Comput, Netw Commun (WiMob), pp. 600–607
[71] Kasinathan P, Costamagna G, Khaleel H, Pastrone C, Spirito MA (2013) An IDS framework for Internet of Things empowered by 6LoWPAN. In Proc 2013 ACM SIGSAC Conf Comput Commun Secur, pp. 1337–1340
[72] Scarfone K, Mell P (2007) Guide to intrusion detection and prevention systems (IDPS). NIST Spec Publ 800:94
[73] H. Yar, T. Hussain, Z. A. Khan, D. Koundal, M. Y. Lee, and S. W. Baik, "Vision sensor-based real-time fire detection in resource-constrained IoT environments," Computational Intelligence and Neuroscience, vol. 2021, Article ID 5195508, 15 pages, 2021.
[74] N. Islam, M. Altamimi, K. Haseeb, and M. Siraj, "Secure and sustainable predictive framework for IoT-based multimedia services using machine learning," Sustainability, vol. 13, no. 23, Article ID 13128, 2021.
[75] Yirui Wu, Dabao Wei, Jun Feng, "Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey", Security and Communication Networks, vol. 2020, Article ID 8872923, 17 pages, 2020. https://doi.org/10.1155/2020/8872923
[76] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proceedings of 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 258–263, IEEE, Reims, France, October 2016.
[77] B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep learning for classification of malware system call sequences," in Proceedings of Australasian Joint Conference on Artificial Intelligence, pp. 137–149, Springer, Hobart, Australia, December 2016.
[78] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.
[79] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in Proceedings of 2014 Second International Conference on Advanced Cloud and Big Data, pp. 247–252, IEEE, Huangshan, China, November 2014.
[80] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 1, pp. 2–14, 2018.
[81] Y. Yu, J. Long, and Z. Cai, "Network intrusion detection through stacking dilated convolutional autoencoders," Security and Communication Networks, vol. 2017, Article ID 4184196, 10 pages, 2017.
[82] Y. Li, R. Ma, and R. Jiao, "A hybrid malicious code detection method based on deep learning," International Journal of Security and Its Applications, vol. 9, no. 5, pp. 205–216, 2015.
[83] Sourour, Meharouech, Bouhoula Adel, and Abbes Tarek. "Network security alerts management architecture for signature-based intrusions detection systems within a NAT environment." Journal of Network and Systems Management 19.4 (2011): 472-495.
[84] Zhang, Yichi, et al. "Distributed intrusion detection system in a multi-layer network architecture of smart grids." IEEE Transactions on Smart Grid 2.4 (2011): 796-808.

[85] Atefinia, Ramin, and Mahmood Ahmadi. "Network intrusion detection using multi-architectural modular deep neural network." The Journal of Supercomputing 77 (2021): 3571-3593.
[86] Sangeetha, S., et al. "Signature based semantic intrusion detection system on cloud." Information Systems Design and Intelligent Applications: Proceedings of Second International Conference INDIA 2015, Volume 1. Springer India, 2015.
[87] Hamdi, Omessaad, Maïssa Mbaye, and Francine Krief. "A cloud-based architecture for network attack signature learning." 2015 7th international conference on new technologies, mobility and security (nTMS). IEEE, 2015.
[88] Otoum, Yazan, and Amiya Nayak. "As-ids: Anomaly and signature based ids for the internet of things." Journal of Network and Systems Management 29 (2021): 1-26.
[89] Jyothsna, V. V. R. P. V., Rama Prasad, and K. Munivara Prasad. "A review of anomaly-based intrusion detection systems." International Journal of Computer Applications 28.7 (2011): 26-35.
[90] Khan, Saba, and Dilip Motwani. "Implementation of IDS for web application attack using evolutionary algorithm." 2017 International Conference on Intelligent Computing and Control (I2C2). IEEE, 2017.
[91] Meng, Weizhi, Wenjuan Li, and Lam-For Kwok. "EFM: enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism." computers & security 43 (2014): 189-204.
[92] Uddin, Mueen, and Azizah Abdul Rahman. "Dynamic multi layer signature-based intrusion detection system using mobile agents." arXiv preprint arXiv:1010.5036 (2010).
[93] Bronte, Robert, Hossain Shahriar, and Hisham M. Haddad. "A signature-based intrusion detection system for web applications based on genetic algorithm." Proceedings of the 9th International Conference on Security of Information and Networks. 2016.
[94] Khan, Inam & Hassan, Muhammad & Aziz, Muhammad. (2021). Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETS. Computers, Materials and Continua. vol.70. 3654-3665. 10.32604/cmc.2022.020697.
[95] Inam Ullah Khan, Muhammad Abul Hassan, Mohammad Dahman Alshehri, Mohammed Abdulaziz Ikram, Hasan J. Alyamani, Ryan Alturki, Vinh Truong Hoang, "Monitoring System-Based Flying IoT in Public Health and Sports Using Ant-Enabled Energy-Aware Routing", Journal of Healthcare Engineering, vol. 2021, Article ID 1686946, 11 pages, 2021. https://doi.org/10.1155/2021/1686946
[96] Shah, Sagar N., and Ms Purnima Singh. "Signature-based network intrusion detection system using SNORT and WINPCAP." International Journal of Engineering Research & Technology (IJERT) 1.10 (2012): 1-7.
[97] Inam Ullah Khan, Asrin Abdollahi, Ryan Alturki, Mohammad Dahman Alshehri, Mohammed Abdulaziz Ikram, Hasan J. Alyamani, Shahzad Khan, "Intelligent Detection System Enabled Attack Probability Using Markov Chain in Aerial Networks", Wireless Communications and Mobile Computing, vol. 2021, Article ID 1542657, 9 pages, 2021. https://doi.org/10.1155/2021/1542657