International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 12 | December - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Analysis on Intrusion Detection Systems to Secure IoT Networks

Pranjali Shah, Anika Bisht, Rudrendra Bahadur Singh, Ravikant Tiwari, Ram Ishwar

Abstract: The amalgamation of physical objects and the internet constitutes the Internet of things(IoT). In the subsequent times, more such physical objects will be connected to the internet and this will lead to the escalation in the attacks carried out on IoT devices and network. This is mainly due to the less memory and lack in built-in security controls. This has made IoT Security, the most researched topic in the past decade. Thus to protect IoT nodes and networks, a security mechanism called Intrusion Detection System(IDS) is brought in use.The advent of Internet of things has played a crucial role in making the lives of the people more easier and comfortable. It has improved the lives of the people in terms of several aspects like comfort and efficiency. This has overall consequently lead to what is called smart environments. When the case of real world smart environment is discussed, both security and privacy comes into play in being the key issues to be considered. But the need demands for the Intrusion Detection Systems (IDSs) to be designed for the IoT networks or environments to mitigate attack related issues. These are the attacks that exploits the vulnerabilities present in the network. The work here demonstrates the need of the fact that despite having previous technologies, we still lack a secure system that could safeguard IoT networks.

In this paper, a detailed analysis is provided on IoT, security attacks in IoT, IDS, types of IDS, Machine learning and Deep learning techniques and algorithms used with IDS in IoT and current trends and research on use of IDS in securing Internet of Things is discussed. Lastly future research based on the current analysis is also examined.

Keywords: IoT, IDS, Network, Security, Machine Learning,
Deep Learning

1. Introduction

Internet of Things or IoT, an evolving paradigm that facilitates connection and exchange of data among other devices on the internet and other communication networks has become crucial in all aspects of human life. With the technical, economical, social and scientific implications of the IoT, the risk of cybersecurity attacks is increased. The reason behind the large number of easily exploitable vulnerabilities in IoT is its resource-constrained features. Multiple such unsecured connected devices on the global network are increasing gradually. The problem with the IoT devices arises as they are developed without keeping note of the basic security needs. Researchers and scholars usually focus on authentication mechanisms and encryption methods for securing IoT devices. The wider attack surface area in IoT makes it more probable for security attacks. Some solutions for improving IoT security were developed but even after that IoT networks are still vulnerable. So the need of the hour is to develop security tools which are particular to IoT and thus emanates the concept of Intrusion Detection Systems.

The act of monitoring and preventing the network traffic from the malicious activities of the intruders is called Intrusion Detection System. In case if any such thing happens, the IDS reports this act of intrusion by generating an alert. To protect the networks from malicious traffic, IDS works as a software or a combination of hardware and software. IDS observes all kind of activities in the network and issues alarms in case of any suspicious traffic or activity. The five main functionalities of IDS include analyzing, assessing, monitoring, acting and tracking. The IDS analyzes by looking into system configuration, vulnerabilities, anomalies and attack patterns. It assesses for system integrity and file integrity. System activity and file activity is monitored. It tracks the user and the system for policy violations. IDS functionality also includes acting by generating alerts and mitigating attacks.

Since there are a large number of IoT constraints, the need is to model a lightweight IDS that is adaptable to all these constraints. In this paper, the objective is to inspect all the suitable IDS available to protect the IoT networks. For this, the major aim is to understand the need for Intrusion Detection Systems in securing IoT networks. Here we will explore different types of IDS already existing for IoT networks and challenges and issues that come and results in need for future research.

Past few years have witnessed progress in Artificial Intelligence that includes machine learning and deep learning techniques. These techniques have been used to improve Intrusion Detection Systems. Various research studies applied machine learning and deep learning techniques on different datasets. Various types of datasets This paper provides an analytical review of different machine learning and deep learning techniques which are used in building IDS for IoT networks. The fundamental security properties that should be considered while building an enthralling security model for IoT includes confidentiality, integrity, authentication, authorization and availability. Security threats can be both virtual and real. Cyber threats constitute both active threats and passive threats. Three layers which compose the architecture of IoT are application layer, network layer and perception layer. The layer implemented at the bottom of the IoT architecture is known as perceptron layer or sensor layer. Transmission Layer or network layer is implemented in the middle of the IoT architecture. Business layer or application layer is the top layer in IoT architecture.

The common attack surface areas in IoT is listed by Open Web Application Security Project (OWASP). Researchers, developers, manufacturers and companies who want IoT deployment in their organization should understand these attack surface areas in order to save their IoT networks from attack. Common IoT technologies includes application protocols and infrastructure protocols. The following sections deal with all the aspects of IDS and IDS in IoT.

2. Related Work

Huge developments has been witnessed in the domain of telecommunications networks which has eventually led to the birth of Internet of Things. This IoT is responsible for the creation of smart environments or in other words, IoT networks which is constituted by wireless sensors, wireless communication techniques etc.A network intrusion detection system is a security mechanism that is concerned with the network layer of the IoT System. The IDS should be such that it could analyze the packets of data present in the traffic across the network and categorize it as malicious or non- malicious. These responses should be generated in real time as they are dealing with real time smart environment.

Susilo, Bambang & Sari, Riri. (2020). Intrusion Detection in IoT Networks Using Deep Learning Algorithm. Information. 11.279.10.3390/info11050279. They have explained in their paper how internet and internet

related devices i.e. IoT's is surrounding us now a days and their main or the key problem which they have observed is revolving around Distributed Denial of Service Attacks (DDoS) particularly Mirai. As, far as solution is concern the authors of the given paper use Deep learning techniques and for the implementation of the Deep learning model the author took very well processed and discovered dataset developed by the University of New South Wales (UNSW) Canberra Cyber center as NSL-KDD. They have implemented the solution using Convolution Neural Network method; multi-layer perceptron: MLP. They have proposed the result to be used in a network based intrusion detection system (NIDS)

Tanzila Saba, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, Saeed Ali Bahaj, Anomaly-based intrusion detection system for IoT networks through deep learning model, Computers and Electrical Engineering, Volume 99, 2022, 107810, ISSN 0045-7906.This paper presents a CNN-based approach for anomaly-based intrusion detection systems (IDS) that takes advantage of IoT's power, providing qualities to efficiently examine whole traffic across the IoT. The proposed model shows ability to detect any possible intrusion and abnormal traffic behavior. The model is trained and tested using the NID Dataset and BoT-IoT datasets and achieved an accuracy of 99.51% and 92.85%, respectively.

Elrawy, M., Awad, A. & Hamed, H. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comp 7, 21 (2018).This paper revolves around key considerations for the development of such IDSs are introduced as a future outlook at the end of this survey. This paper also covers some of the prominent attacks on the network of IoT devices such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks and deals with the impact of such attacks on the device. This article focuses on the important factors that consumption, processing time, and performance overhead.

Khraisat, A., Alazab, A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecur 4, 18 (2021).This article propose the aspect of numerous IoT intrusion detection systems have been proposed in the literature to tackle attacks on the Iot ecosystem, which can broadly classified based on the detection technique, validation strategy, and development strategy. This survey paper presents a comprehensive review of contemporary IoT IDS and an overview of the techniques, deployment Strategy, validation strategy and datasets that are commonly applied for building IDS. The main solution provided by this is article is signature based intrusion

detection system (SIDS) which involves detection of the malicious activity based only on the data provided and if any anomaly arises it will fail to detect.

Sherasiya, Tariqahmad, Hardik Upadhyay, and Hiren B. Patel."A survey: Intrusion detection system for internet of things." International Journal of Computer Science and Engineering (IJCSE) 5.2 (2016): 91-98.his article briefly discuss about Intrusion Detection System (IDS) is used to monitor the particular node and network. This article mainly deals with the different types of intrusion detection system such as Signature based IDS, Anomaly based IDS, and a third type of IDS system as Specification Based IDS. Specification based IDS is somewhat similar to anomaly detection technique. In this technique, the normal behavior of the network is defined by manually, so it gives less incorrect positives rate. This technique attempts to excerpt best between signature-based and anomaly based detection approaches by trying to clarify deviations from normal behavioral patterns that are created neither by the training data nor by the machine learning method.

M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.This article not only deals with the intrusion detection system within the IoT devices but also with the cyber-threats available on the forefront of today's world full of gadgets and internet enable devices. This article deals with the problem of intrusion detection in IoT in slightly peculiar form such that by using a device Passban an intelligent intrusion detection system (IDS) able to protect IoT devices that are directly connected to it. The device used in this article takes full advantage of the edge computing paradigm to detect cyber threats as close as possible to the corresponding data sources.

The idea behind this paper is evaluation of performance of the Raspberry Pi, one of the most used commodity single-board computers, while running Snort, a widely known, open source Intrusion Detection System (IDS). The experiment within the article propose architecture based on resource constrained devices such as the asp erry i can effectively serve as I in a distri uted syste as IoT. . forzin . . r ol M. Conti and J. -M. Bohli, "RPiDS: Raspberry Pi IDS — A Fruitful Intrusion Detection System for IoT," 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016, pp. 440- 448, doi: 10.1109/UIC-ATC- ScalCom-CBDCom-IoP-SmartWorld.2016.0080.

This paper investigate the prospects of using machine learning classification algorithms for securing IoT against DoS attacks. This article is a short of a review article with uses popular datasets CIDDS-001, UNSW-NB15, and NSL-KDD for performance assessment of classifiers is done in terms in prominent metrics and validation methods. Raspberry Pi is used to evaluate the response time of the classifiers on IoT specific hardware. Verma, A., Ranga, V. Machine Learning Based Intrusion Detection Systems for IoT Applications. Wireless Pers Commun 111, 287-2310(2020) .

This paper mainly deals with the threats which are mainly in most of the Machine to Machine (M2M) communication.This paper also deals with efficient and effective solutions. Solution here mention is Software-defined IDS based distributed cloud architecture, that provides as secure IoT environment. Experiment evaluation of architecture, that provides a secure IoT environment. Park, Jong Hyuk (Dept. of Computer Science and Engineering, Seoul National University of Science & Technology (SeoulTech)), Received : 2020.05.05, Accepted : 2020.07.01, Published : 2020.08.31

This article explains various types of attacks such as sinkhole attack, eavesdropping, denial of service attacks, etc. And proposed solution for the above attacks such as Intrusion detection system can be used to detect such attacks when the network security is breached. This paper also deals with the convolutional neural network model. The paper's key focus is on wormhole attack in which the target node is attacked or breached from two different directions. The proposed model alters the network administrator. Identifying the neighborhood nodes and extracting the

impact of the threats. Journal of ISMAC (2020) Vol.02/ No.04 Pages: 190-199 http://irojournals.com/iroismac/ DOI: https://doi.org/10.36548/jismac.2020.4.002.

3. Security Attacks in IoT

Multiple techniques are implemented by the attackers to target IoT devices and networks. In this section, we will discuss OWASP Top 10 IoT Threats, OWASP IoT attack surface areas, IoT Vulnerabilities and IoT attacks.

3.1 OWASP Top 10 IoT Threats

Open Web Application Security Project has given top 10 IoT threats. These include Weak, Guessable or Hardcoded Passwords, Insecure Network Services, Insecure Ecosystem Interfaces, Lack of Secure Update Mechanisms, Use of Insecure or Outdated Components, Insufficient Privacy Protection, Insecure Data Transfer and Storage, Lack of Device Management, Insecure Default Settings and Lack of Physical Hardening.[18]

3.2 OWASP IoT Attack Surface Areas

Ecosystem as an attack surface area includes vulnerabilities like Interoperability standards, data governance, system-wide failure, individual stakeholder risks, implicit trust between components, enrollment security and decommissioning system.[19]

Device Memory as an attack surface includes vulnerabilities like sensitive data such as cleartext usernames, encryption keys and clear passwords.

Device Physical Interfaces as an attack surface area includes vulnerabilities like firmware extraction, user CLI, admin CLI and tamper resistance.

3.3 IoT Vulnerabilities

Some of the OWASP IoT vulnerabilities include username enumeration, weak passwords, account lockout and unencrypted services. Denial of Service, Two-factor authentication and removal of storage media.

3.4 IoT Attacks

Some types of IoT attacks are DDoS Attack, Rolling code attack, BlueBorne Attack, jamming attack, exploit kits, replay attacks, sybil attack, side-channel attack, ransomware attack, sql injection attack, fault injection attack and DNS Rebinding Attack.[17]

4. Intrusion Detection in the Internet of things

In this section, insights are provided on the basis of research on Intrusion Detection System for IoT networks. All the existing research on IDS for IoT is presented in detail. The research carried out is categorized on the basis of characteristics such as placement strategy of IDS and detection method. In each of these further categorization is done.[1] Placement Strategy of IDS is categorized into distributed, centralized and hybrid. Detection Method is divided into signature based, anomaly based and hybrid. In this paper, we will discuss all these methods in detail.

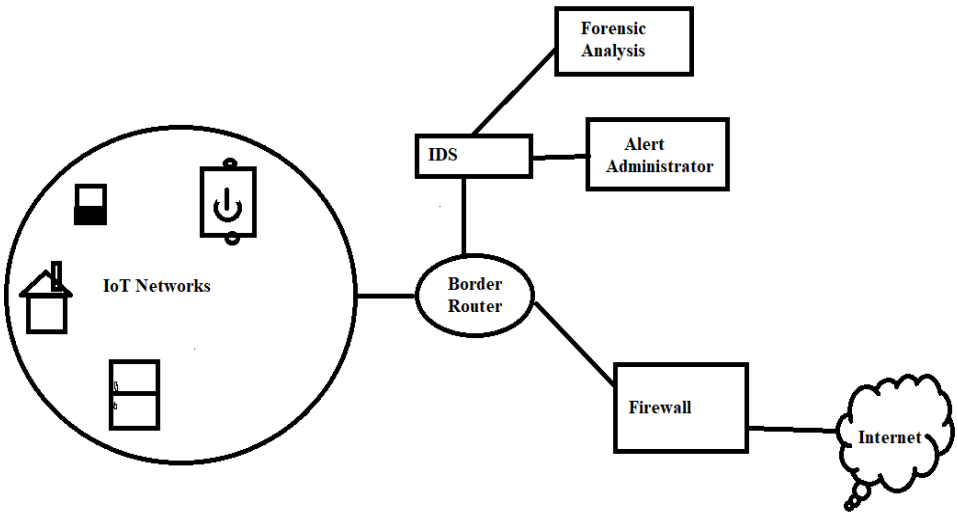

Fig. 1 (IDS integrated at Border Router)

4.1 Types of IDS based on its position or placement in the Network

4.1.1 Centralized IDS: In this method, installation of IDS is done on a centralized router or a dedicated server. Implementation of centralized IDS is very simple. It's because of the centralized edge node which connects the IoT network to the internet.

4.1.2 Distributed IDS: In this strategy, monitoring and detecting attacks is done by each node present in the network. So IDS is installed on all the nodes in the network.

4.1.3 Hybrid IDS : This is the one which includes strengths of centralized and distributed IDS and excludes drawbacks of them.

4.2 Types of IDS based on the Detection method

4.2.1 Signature-Based IDS: Also known as misuse-based IDS in which all the attack patterns possible are stored in the database of the IDS. The generated information is analyzed and matched with the known attack.

4.2.2 Anomaly-Based IDS : In this, classification of the system behavior is done as abnormal or anomalous. Any activity that violates normal behavior is regarded as an attack.

4.2.3 Hybrid IDS : The combination of any of the above mentioned IDS is called hybrid based IDS.

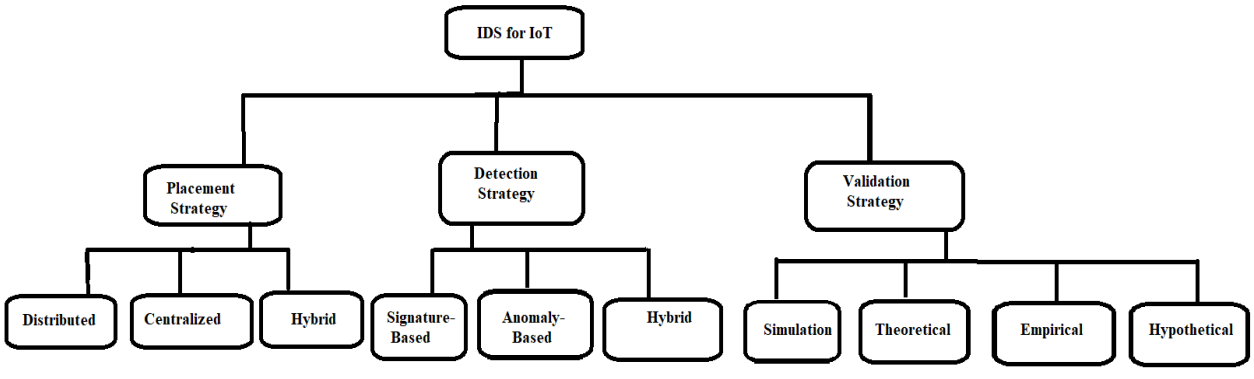

Fig. 2 (Types of IDS and their sub types).

4.3 Techniques for implementing Anomaly Intrusion Detection System

The techniques for implementing anomaly based intrusion detection systems are categorized into four groups: Supervised Learning, Unsupervised Learning, Reinforcement Learning and Deep Learning.[2] The process of examining and collecting every input and output variable so as to approximate the mapping function so that it can predict output for any new input record is called supervised learning.[3] But when we have only input variables and no output variables, unsupervised learning comes into play. In reinforcement learning, we aim for maximizing the total reward of the agent.

Supervised learning includes algorithms like decision tree classification, naive bayes, genetic algorithm, artificial neural network, fuzzy logic, support vector machine and hidden markov model.[15] Unsupervised Learning includes algorithms like k-means clustering, probabilistic clustering, independent component analysis and hierarchical clustering. The main aim of using machine learning methods is to create IDS that requires less human knowledge and improve accuracy.[16]

Related works	Corresponding IDS	Used Tools	Attack Detection	Required measures
Ioulianou et al.[3]	Hybrid	Cooja Simulator, Pattern Matching Algoritm	DoS	IDS functionalities are not considered
Raza et al. [4]	Hybrid	SVELTE	Sink-hole attacks	Additional control overhead due to 6Mapper module

Shreenivas et al. [5]	Hybrid	Extension to SVELTE using ETX metric, the geographical detection algorithm	ETX and Rank attack	Maximum 8 nodes only used.
Amaral et al.[6]	Hybrid	Watchdogs	Routing attacks based on a different set of rules	Requires optimization in enforcing and storing new security rules.
Eskandari et al.[7]	Centralized	Passban IDS, iForest	Port Scanning, Brute force, flooding attack	Not considered the attacks in the training phase, flooding attack reduces the detection rate.
Midi et al.[8]	Centralized	KALIS	DoS, Routing attacks	Complex functionalities
Kumar et al. [9]	Centralized	Decision Tree	Exploit, DoS, Probe, Generic	Requires refinement for detecting new attacks.

Mbarek et al. [10]	Centralized	ENIDS protocol	Clone attacks	Consumes more energy in normal scenario
Lee et al.[11]	Distributed	Auxiliary Shifting, early decision	Conventional attacks using signatures	Single device only
Parra et al.[12]	Distributed	Deep Learning	Phishing, DDoS, Botnet	More training time
Alkadi et al [13]	Distributed	Blockchain, Bidirectional Long Short-Term Memory(BiLSTM)	DoS, DDoS, Port Scanning, OS Scan etc.	Need futher refinement for real-time implementation
Sforzin and Conti [14]	Distributed	Snort tool	Conventional Attacks	Single Node is considered

Table 1. Analysis on Intrusion Detection Systems to secure IoT Networks.

5. Conclusion

IoT networks forms the foundation of smart environments. Thus if there is any insufficiency in the security of these networks, it will directly impact the smart environments. A tremendous increase of IoT users, services and applications have been witnessed. This clearly depicts the expansion of IoT networks. Thus lot of contemplation and rumination is required on the security issue associated with these networks. An IDS is one possible thing which could be done. Various studies and research work is being carried out on various security issues. The current trend observes that there will be more shift towards the IoT in the near future. This will also lead to the escalation of the associated risks with the security of these devices and network.

References

[1]. Susilo, Bambang & Sari, Riri. (2020). Intrusion Detection in IoT Networks Using Deep Learning Algorithms. Information. 11.279.10.3390/info11050279.

[2]. Tanzila Saba, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, Saeed Ali Bahaj, Anomaly- based intrusion detection system for IoT networks through deep learning model, Computers and Electrical Engineering, Volume 99, 2022, 107810, ISSN 0045-7906.

[3]. P. P. Ioulianou, V. G. Vassilakis, I.D. Moscholios and M. D. Logothetis, "A Signature-based Intrusion Detection System for the Internet of Things", International Conference on Information and Communication Technology Forum (ICTF-2018) ,Graz, Austria, 2018, https://www.researchgate.net/publication/ 326376629.

[4]. S. Raza, L. Wallgren and T. Voigt, "SVELTE: real-time intrusion detection in the Internet of Things", Ad Hoc Network, 11(8), ISSN: 2661-2674, 2013, DOI:10.1016/j.adhoc.2013.04.014.

[5]. D. Shreenivas, S. Raza and T. Voigt, "Intrusion Detection in the RPL connected 6LoWPAN Networks", Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, IOTPTS'17, Abu Dhabi, United Arab Emirates, 2017.

[6]. J. Amaral, L. Oliveira, J. Rodrigues, G. Han and L. Shu, "Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks", IEEE International Conference on Communications (ICC-2014), pp. 1796–1801, 2014.

[7]. M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonell, "Passban IDS: An Intelligent Anomaly Based Intrusion Detection System for IoT Edge Devices", IEEE Internet of Things Journal, pp. (99):1-1, 2020, DOI: 10.1109/JIOT.2020.2970501.

[8]. D. Midi, A. Rullo, A. Mudgerikar and E. Bertino, "KALIS: A system for knowledge-driven adaptable intrusion detection for the Internet of Things", Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS'17), 2017.

[9]. V. Kumar, A. K. Das and D. Sinha, "UIDS: A Unified Intrusion Detection System for IoT Environment", Evolutionary Intelligence, 14, pp. 47–59, 2021, DOI: 10.1007/s12065-019-00291-w.

[10]. B. Mbarek, M. Ge and T. Pitner, "Enhanced Network Intrusion Detection System Protocol for Internet of Things", Proceedings of ACM SAC Conference (SAC'20), ACM, New York, Article 4, 2020, DOI: 10.1145/3341105.3373867.

[11]. T. H. Lee, T. H. Wen, L. H. Chang, H. S. Chiang and M.C. Hsieh, "A lightweight Intrusion Detection Scheme based on Energy Consumption Analysis in 6LowPAN", Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Lecture Notes in Electrical Engineering 260, Springer Netherlands, pp. 1205–1213, 2014.

[12]. G. D. L. T. Parra, P. Rad, K. R. Choo and N. Beebe, "Detecting Internet of Things Attacks using Distributed Deep Learning", Journal of Network and Computer Applications, 163(102662), ScienceDirect, 2020, DOI: 10.1016/j.jnca.2020.102662.

[13]. O. Alkadi, N. Moustafa, B. Turnbull and K. R. Choo, "A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks", IEEE Internet of Things Journal, 2020, DOI:10.1109/JIOT.2020.2996590.

[14]. A. Sforzin and M. Conti, "RpiDS: Raspberry Pi IDS-A fruitful Intrusion Detection System for IoT", International IEEE Conference on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart World Congress, 2016, DOI:10.1109/UIC-ATC-Scalcom-CBDCom-IOP-SmartWorld.2016.114.

[15]. Khraisat, A., Alazab, A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecur 4, 18 (2021). https://doi.org/10.1186/s42400-021-00077-7.

[16]. Sherasiya, Tariqahmad, Hardik Upadhyay, and Hiren B. Patel. "A survey: Intrusion detection system for internet of things." International Journal of Computer Science and Engineering (IJCSE) 5.2 (2016): 91-98.

[17]. M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.

[18]. Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016, pp. 440-448, doi: 10.1109/UIC ATCScalCom-CBDCom-IoP-SmartWorld.2016.0080.

[19]. Verma, A., Ranga, V. Machine Learning Based Intrusion Detection Systems for IoT Applications. Wireless Pers Commun 111, 2287–2310 (2020).