Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

A new model for security analysis of network anomalies for IoT devices

Mohammad Al Rawajbeh[a*], Wael Alzyadat[a], Khalid Kaabneh[b], Suha Afaneh[c], Dima Farhan Al-rwashdeh[d], Hamdah Samih Albayaydah[e] and Issam Hamad AlHadid[d]

[a]*Faculty of Science and Information Technology, Al Zaytoonah University of Jordan, Amman, Jordan*
[b]*Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan*
[c]*Faculty of Information Technology, Zarka University, Zarka, Jordan*
[d]*Faculty of Information Technology and Systems, University of Jordan, Aqaba, Jordan*
[e]*MIS, Faculty of MIS. Aqaba University of Technology, Aqaba, Jordan*

C H R O N I C L E

Article history:
Received: December 25, 2022
Received in revised format: March 2, 2023
Accepted: April 30, 2023
Available online: April 30, 2023

Keywords:
Internet of Things
Technology
Security Analysis
Anomaly detection system
Cybersecurity

A B S T R A C T

In the era of IoT gaining traction, attacks on IoT-enabled devices are the order of the day that emanates the need for more protected IoT networks. IoT's key feature deals with massive amounts of data sensed by numerous heterogeneous IoT devices. Numerous machine learning techniques are used to collect data from different types of sensors on the objects and transform them into information relevant to the application. Furthermore, business and data analytics algorithms help in event prediction based on observed behavior and information. Routing information securely over the internet with limited resources in IoT applications is a key problem. The study proposes a model for detecting network anomalies in IoT devices to enhance the security of the devices. The study employed the IoT Botnet dataset, and K-fold cross-validation tests were used for validating the values of evaluation metrics. The average values of Accuracy, Precision, Recall, and F Score was 97.4.

1. Introduction

The creation of the Internet of Things (IoT) is taking over an important place in our daily life. Various devices in our routine activities are interconnected with each other, at the same time they are connected to the Internet (Mohammadzadeh et al., 2018). Recently, the emergence of a new type of networking paradigm that enables physical objects to communicate with the Internet, known as the Internet of Things (IoT), has caught the attention of many research communities and the information and communication technology (ICT) industry. The amount of data generated by devices is increasing on the Internet of Things; According to a forecast, the IoT may have many billions of connected devices during the upcoming years (Shanmugam & Azam, 2023). Similarly, according to the International Data Corporation (IDC), data generated by things (devices in IoT) will reach 4.4 Zettabytes by 2020 (Rydning et al., 2018). Given the rapid growth of the IoT idea in recent years, it is easy to infer that the forecasts from the literature were accurate. A whole new virtual world is created with >50 billion devices that have internet connections, resulting in continuous growth and expansion of connection, healthcare and medical, transportation and logistics, smart cities, education, home and living environment, agriculture, infrastructure, industries, and government have benefited from the IoT (Kavyashree et al., 2018; Balaji et al., 2019; Sheng et al., 2015; Al Rawajbeh, 2017). In addition to these domains, the IoT idea is the backbone of the fourth industrial revolution, indicating a new degree of organization and management of the whole value creation chain (Balaji et al., 2019). The expansion of IoT is associated with an increase in

* Corresponding author.
E-mail address: m.rawajbeh@zuj.edu.jo (M. Al Rawajbeh)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.5.001

various challenges. Most of these challenges often occur in the form of network anomalies that are deviations from the normal traffic flow. These anomalies can be related to security or performance according to Hawkins's definition (Hawkins, 1980). Another forecast has estimated that 50 billion IoT devices will be in use around the world by 2030 (Statista, 2022). The potential for threats, attacks, and risks in smart devices will increase with the number of devices. Inadequate security can lead to serious threats, increased vulnerabilities, and cyber-attacks. This potentially increases users' security and privacy concerns via IoT devices and thus may reduce the radical growth of IoT. In (Mohammad et al., 2019), Authors proposed the IoT security issue as the main challenge that faces the growth of using IoT devices that are constrained in their computational capability, network bandwidth, packet size, and memory such as sensor nodes.

IoT networks are subject to various attacks such as denial of service (DoS), Man-in-the-Middle (MTM), eavesdropping, sniffing, etc. Several cyberattacks have caused major disruptions to IoT systems. Furthermore, a few of the IoT network attacks are inherited from Wireless Sensor Networks (WSNs). Mostly, secure routing in the distributed environment and the highly dynamic Internet of Things remains a challenge because of the heterogeneity of smart devices. Currently, IoT applications are an important sector that requires data and information protection. There are additional options for hackers to launch attacks on the data utilized by applications (Kouicem et al., 2018; Rawajbeh et al., 2021). As a result, IoT security is the most critical and pressing necessity for IoT developers. There are several major concerns about the use of existing authentication mechanisms (hashing algorithms, standard message digest, and Hash-based Message Authentication Code) and encryption mechanisms (Data Encryption Standard, Rivest, Shamir, and Adelman, and Advanced Encryption Standard) (Turner & Chen, 2011). Previously, IoT dealt with bytes and bytes of data sent over the network every second. Second, IoT devices have limited memory and storage capacity, making them more vulnerable to security threats when exchanging information among users (Lin et al., 2017; Yang et al., 2017). Simulation tools platforms were not mentioned in most of the published survey articles. Some investigations have also been conducted on secure routing algorithms used in IoT systems. This study aims to propose an IDS system to detect anomalies in IoT devices to improve their security. Only if we have confidence in the data the Internet of Things gives about the outside world will we be able to realize all this potential, therefore security is ultimately necessary. The Internet has a long history of stunning security flaws and has never been a safe place. The most serious ones have resulted in the loss of a significant amount of personal data, the compromise of many computers, or the inaccessibility of network services (Adhikary et al., 2020).

Many IDS solutions are designed to prevent cybercriminals from using IoT devices. These security solutions can be divided into preventive and corrective measures. A proactive approach can protect the IoT from external threats. However, because IoT is connected to the global internet, there is a great risk of intrusion from outsiders who can evade proactive security measures. As a secondary defense, an intrusion detection system (IDS) can stop many cyberattacks. Researchers and companies in the IoT field have paid attention to IDS solutions, and many IDS solutions have been released. IDS solutions can be classified into three groups based on detection method: signature, anomaly, and hybrid IDS models (Alsoufi et al., 2021). Consequently, the low computational power of IoT gateways, which complicates the operation of full-fledged IDSs, is the most difficult technical barrier to overcome when dealing with IDSs deployed on these devices. Therefore, many strategies have recently been proposed to run IDS on IoT devices to solve this problem (Eskandari et al., 2020).

2. Related Works

IoT refers to items or devices that are uniquely connected to the physical world and gather real-time data transfers, retrieve, and respond intelligently to action over the internet. The various IoT devices can be run and executed with minimal human interaction. Authors in (Mourtzis et al., 2016; Al Rawajbeh & Haboush,2015), stated that the number of IoT devices is expected to reach more than 20 billion, with more than 40 petabytes of data exchange potential over the Internet in the coming years. The adoption of IoT applications requires consideration of several factors, including connectivity, security, privacy, and the standardization of IoT networks. Security is the most critical characteristic on which researchers are focusing on each tier of IoT design. The effective deployment of an IoT system will be achievable if it is built with security in mind. As a result, security must be considered at the design stage of the application to control and maintain IoT networks. For IoT applications, security measures such as access control and authentication have been proposed (Alaba et al, 2017; Sfar et al, 2018). However, other security problems were not addressed. The surveys provided by (Tewari & Gupta, 2020; Sha et al, 2018; Hassan, 2019) include trust management and the latest trends in IoT security approaches.

Based on the findings of a decade's worth of study on IoT security, it has been determined that the most frequently utilized tools are NS2, Cooja, and MATLAB. These tools are useful for the performance evaluation of IoT protocols. Cooja is a network emulator that runs on the Contiki OS, which is a network-centric embedded operating system that focuses on IoT sensor networks (Velinov & Mileva, 2016). It is used to evaluate the performance of Internet of Things applications, protocols, and networks. The Cooja network simulator makes the building and testing of IoT applications easier and faster. Contiki is a C-based operating system that was created specifically for sensor nodes with limited resources. The Contiki-NG simulator is the next version, featuring support for a real-time application interface using Raspberry Pi sensor motes and the ability to simulate Bluetooth connections (Oikonomou et al., 2022). Cooja, a GUI-based simulator, makes it easy for users to create simulation applications as shown in Fig. 1.

Without deploying any hardware, the version 2 network simulator may be used to study the parameters of complicated network scenarios. In a dynamic IoT network, this simulator operates in both wired and wireless modes. NS2 can examine network metrics such as packet delay, throughput, packet loss, latency, and packet delivery ratio (TutorialsWeb, 2023). For network simulation, this simulator employs scripting languages such as C++, Otcl, and Tcl. In the context of the development of IoT applications, NS2 supports several networks, such as WSN, MANET, and RFID. However, the university no longer provides active support for NS2, but NS version 3 is well supported. NS3 is incompatible with NS2. In the simulation process, Network Animation (NAM) is utilized to visualize the network performance.

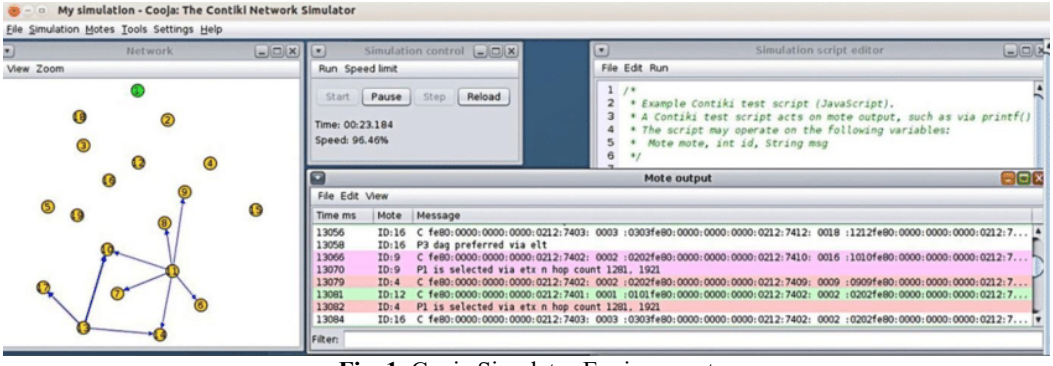

Fig. 1. Cooja Simulator Environment

MATLAB is considered a high-performance language that combines programming, calculation, and visualization (Zhang et al., 2012). C libraries will be supported to script the language. MATLAB is used to collect and analyze real-time IoT- data. The IoT facilitates the connection of embedded devices over the Internet, allowing them to communicate with each other while storing data in the cloud. IoT applications can be integrated with MATLAB analytics and a specific Simulink package to simulate virtual environments using C/C++, NET, PLC, and GPU. The data stream is interfaced to the cloud using the Thing-Speak platform. Furthermore, it works with large data, which is backed up by time-stamped and unstructured data from cloud storage. Furthermore, MATLAB has several functionalities for developing IoT applications, such as prediction, signal and image processing, optimization, and machine learning. The tools in Table 1 can all be distributed over networks with various waves of networks and protocols, which is a milestone for the IOT idea.

Table 1
Relevant tools

Tools	Purpose	Evaluation	Platform	Source
Cooja	Deployed using available hardware and software. networks of IoT motes to be simulated	single threaded	InstantContiki	(Bagula & Erasmus, 2015)
NS2	events network detect information	Efficiency network traffic	C++ and OTcl	((NSF), 2011)
QualNet	heterogeneous networks nodes exchanging different types of traffic Extensibility	Performance (real-time) Scalable Network	Visual Studio	(Siraj et al., 2012)
NetSim	Cyber-Physical Systems LowPAN Gateway	Model Predict Validate	Cross platforms	(Wahid-Ul-Ashraf et al., 2018)

Using this mechanism, they can be adopted in cloud architecture across the levels of infrastructure, user, services, and application (Al Rawajbeh, 2012; Mumtaz et al, 2022). An intelligent intrusion detection system (IDS) that can protect IoT devices directly connected to it. The peculiarity of the proposed solution is that it can be implemented directly on very low-cost IoT gateways (e.g., single-board PCs which currently cost tens of dollars), taking full advantage of the edge computing paradigm to detect cyber threats closer to the relevant data sources. We will try to answer the question of whether we can detect different types of attacks with very low false positive rates.

3. Methodology

This research is focused on detecting flow-based intrusion to increase the security of IP networks. Intrusion detection systems use network streams to evaluate network traffic and malicious activity. A flow-based intrusion detection system (IDS) is enabled to inspect the operation of a packet header, thus contributing to detecting flow-based anomalies and protocol examination. This paper proposes an anomalous activity detection model. In this research, the IoT Botnet dataset was used. Attacks on IoT networks are common. However, 15 attacks are severe and erupted due to inadequate security layers in IoT devices used in smart infrastructure. The network communication layer works to diversify the flow of the network. First, the IDS detects irregular activities with the help of local parameters. After detecting an anomaly, it is transferred to a level-two model for identifying the nature of the attack.

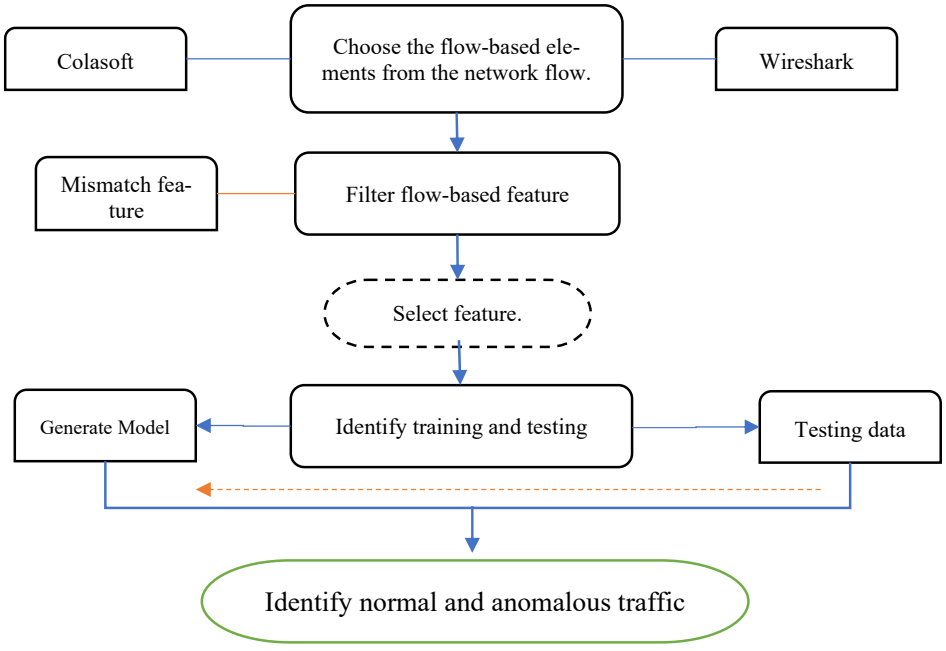

Fig. 2. Anomalous Activity Detection model

This study will follow the following steps to propose a model for detecting anomalies in IoT devices. Fig. 1 demonstrates the steps involved and Fig. 2 depicts the proposed model. The anomalous activity detection system as shown in Fig. 2 consists of five stages. All these steps are sequential flows where each step depends on the previous step. The first stage considers the capture of the flow according to the flow of the network, the second stage manages the data captured by the filter. Test mechanism and finally find out the normal and abnormal traffic.

3.1 Data collection stage

This stage is related to the primary process to use the performance diagnostics and analysis tools Colasoft Capsa and Wireshark offer to both experienced and inexperienced users a robust and all-encompassing packet capture and analysis solution with an intuitive user interface that enables network security and monitoring in a crucial business setting. The main purpose of this research is to choose the flow-based elements from the network flow of an IoT device based on a cloud platform, as shown in Fig. 3.

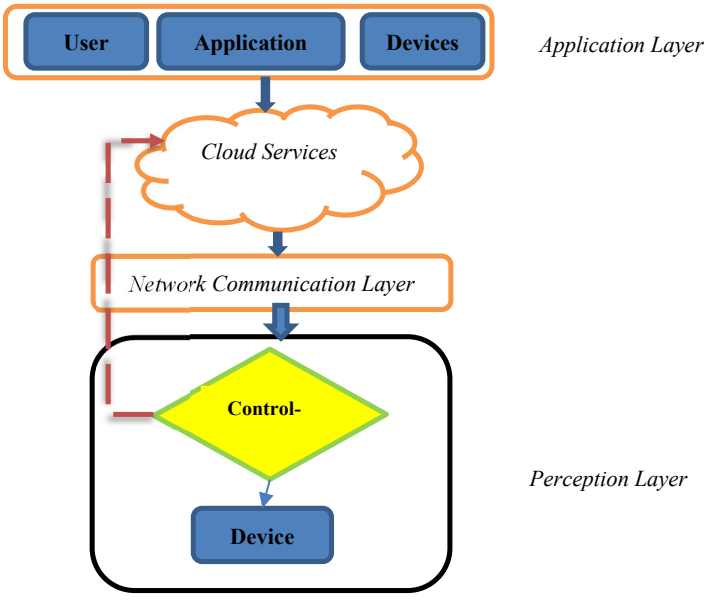

Fig. 3. IoT flow-based IDS

In this research, we will use the dataset named BoT-IoT dataset, which considers both regular and unusual traffic. The Ostinato tool and Node-red were used to create simulated network traffic (for non-IoT, and IoT respectively). The data structure is divided into four parts, the first part is ARGUS (DDoS, DDoS_HTTP. DDoS_TCP, DDoS_UDP, DoS, DoS_HTTP, DoS_TCP, DoS_UDP), the second part Scan (OS: 1:2: 3: 4), the third part is Theft (Data Exfiltration, Keylogging), the fourth part is services.

3.2 Filter flow-based feature stage

The data collected contains the missing and incomplete value which the filter will clean up vertically to provide the feature selection, meanwhile the filter technique is positively impacted to meaningful data and ignores the ambiguity. Especially, through the devices and interlink with the cloud platform including electrostatic attraction, inertial collision, direct interception or exclusion of dimensions, and diffusion interception. The removal of impurities from the air filter is made possible by the combination of all these methods. The time scale is a milestone for capturing and generating data in scope, IOT, and cloud platform in a multidimensional format measurement over different time periods. The multidimensional format represents the different attributes of a data set that make up a complete data set. Time series data also falls under panel data. The data set that contains the main data element that occurs frequently in each time series is worth studying. A balanced panel is a panel in which the panel data is observed continuously at each time interval where the matching data are adopted for feature selection.

3.3 Identify Training and testing

The support vector machine-supervised learning models with associated learning algorithms for transformation may be nonlinear and the transformed space high-dimensional (features); although the classifier is a hyperplane in the transformed feature space, it may be nonlinear in the original input space, the detection process will occur through a one-class support vector machine (SVM). Any malicious flow is carried forward to organize all malicious activities into a group to form clusters. The study used Src IP, Flow IAT, Dst Port, Flow duration, Flow Byts/s Dst Port, Flow IAT Std, Flow Pkts/s, Subflow Fwd Byts, Subflow Fwd Pkts, Cat, label, Flow Duration, Subflow Bwd Byts flow datasets that have been used for evaluation.

4. Experimentation

In the process of designing a computational model to detect intrusions in the system, the IoT Botnet dataset will be used in this proposed model. Before adoption, non-numeric functions will be changed into numeric features by using the method of column normalization:

$$\text{Column Normalization} = \frac{\text{X}-\text{Xmin}}{\text{Xmax}-\text{Xmin}} \tag{1}$$

The column normalization creates a relational database with an array-based structure and entails building tables and establishing linkages between those tables in accordance with guidelines intended to preserve the data as well as increase the database's flexibility by removing redundant and erroneous dependencies.

$$\text{Recall} = \frac{TP}{TP+FN} \tag{2}$$

Recall (sensitivity) is the percentage of important features that were successfully recovered. It can be viewed as the likelihood that the query will return relevant data.

$$\text{Precision} = \frac{TP}{TP-FP} \tag{3}$$

Precision, the goal of assessing a model's success is the accuracy of the measuring elements with relation to each other, the accuracy takes into consideration all retrieved data as illustrated in Eq. (4), but can also be evaluated against a specific limit, taking only the best results given by the system.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{4}$$

Here, TP denotes True Positive, TN True Negative, False Positive, and False Negative. In addition to this, Xmin and Xmax are the maximum and minimum values in the column. To measure the success rate of the proposed model, accuracy, precision, F score, and recall features were used. Generally, accuracy measures the correctness of predictions, precision is used to examine network intrusions, and a high value of precision denotes a low false positive indication. At the same time, all projected

intrusions are contrasted by the recall. F score represents IDS correctness that is calculated through the harmonic mean of recall and precision. Furthermore, the Python Skearn package was used in this study as a machine-learning library.

$$\text{F Score}=\frac{2(Precision*Recall)}{Precision+Recall} \quad (5)$$

Rely on Eq. (5) Precision, recall, precision, and F score were 100%. For DoS, it was 98.60, and for theft, it was 95.90. For DDoS, it was calculated as 97.80, as shown in Table 2. The mean value of Accuracy, Precision, and Recall and F score value of 97.4 was obtained.

Table 2
Mean values of accuracy precision, recall, and F Score

Attack Type	Accuracy	Precision	Recall	F Score
Normal	100	100	100	100
DoS	98.70	97.6	97.50	98.60
DDoS	97.60	95.40	97.60	97.80
Theft	96.40	93.80	97.30	95.90
Average	97.5	95.6	97.4	97.4

Table 3 presents a comparative analysis of the intrusion system in IoT networks. Numerous studies have employed CI-CIDS2017, UNSW-NB15, and KDD datasets to measure their models. Nevertheless, this study employed a ten-flow and botnet dataset to cross-check the detection capabilities of the proposed model.

Table 3
IDS networks and their success rates

Attack Type	Dataset	Accuracy	Precision	Recall	F-Score	References
Blackhole	Generated	-	97.2	-	97	(Thamilarasu & Chawla, 2019)
Multi	UNSW-NB15	-	89	87	88	(Mohamed et al., 2018)
-	WiLab	97.95	-	-	-	(Kumar et al., 2020)
Sybil	-	95	93.5	90.1	97	(Murali, & Jamalipour, 2019)
Multi	NSL-KDD	98.19	-	-	-	(Li et al., 2020)
Multi	CICIDS2017	99.80	98.68	92.76	95.04	(Lee & Park, .2021).
Multi	BoT-IoT	97.5	95.6	97.4	97.4	Proposed

5. Discussion

Fig. 4 presents a comparative analysis of the intrusion system in IoT networks. Numerous studies have used CICIDS2017 and UNSW-NB15 datasets to measure their models. However, this study used a ten-flow and botnet dataset to cross-check the detection capabilities of the proposed model.

This study only evaluated the general categories of attacks but did not include the subcategories of attacks on IoT devices. Moreover, the values of accuracy, precision, recall, and F-Score of this proposed model are not 100%. The accuracy of identifying attacks can be augmented by generating more flow-based systems and selecting an algorithm to filter the most relevant elements of the dataset. Subsequently, it will enhance the model's ability to detect attacks.

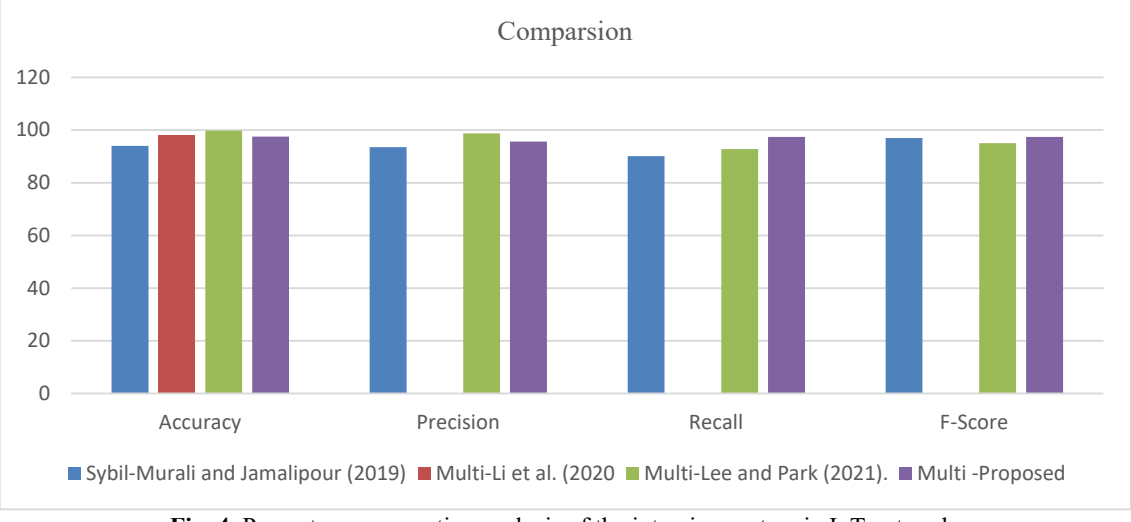

Fig. 4. Presents a comparative analysis of the intrusion system in IoT networks

5. Conclusion

The IoT last year gained a significant role in improving our life. On the other side, the giant amount of data which is produced by IoT networks faces numerous challenges in many areas including security and privacy issues. The study proposes a model for detecting network anomalies in IoT devices to enhance the security of the devices. The study employed the IoT Botnet dataset, and K-folds cross-validation tests were used for validating the values of evaluation metrics. The study evaluated a ten-flow and botnet dataset and their values for Accuracy, Precision, Recall, and F Scores. However, the study obtained a mean value of 97.4 percent through K-fold cross-validation. For future research, the subcategories of intrusion attacks in the IoT devices along with 100 mean values of Accuracy, Precision, Recall, and F Score of the proposed model.

Acknowledgment

The authors are very thankful to the Al Zaytoonah University of Jordan, for supporting this research. Also, the authors are very thankful to all the associated personnel in any reference that contributed in/for the purpose of this research.

References

Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Evaluating the Impact of DDoS Attacks in Vehicular Ad-Hoc Networks. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)*, *12*(4), 1-18.

Al Rawajbeh, M. (2017). Low cost design and implementation for HAS using multifunctional WI-FI. *International Journal of Computer Networks & Communications (IJCNC)*, *9*(3), 105-116.

Al Rawajbeh, M. (2019). Performance evaluation of a computer network in a cloud computing environment. ICIC Express Letters, *13,* 719-727.

Al Rawajbeh, M., & Haboush, A. (2015). Advanced object monitoring using wireless sensors network. *Procedia Computer Science*, *65*, 17-24.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10-28.

Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in IOT using deep learning: A systematic literature review. *Applied sciences*, *11*(18), 8383.

Bagula, B. A., & Erasmus, Z. (2015, March). Iot emulation with cooja. In *ICTP-IoT workshop* (p. 99).

Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT technology, applications and challenges: a contemporary survey. *Wireless personal communications*, *108*, 363-388.

Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*, *7*(8), 6882-6897.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks, 148*, 283-294.

Hawkins, D. M. (1980). *Identification of outliers* (Vol. 11). London: Chapman and Hall.

Kavyashree, E. D., Vidyashree, H. D., & Kumar, B. A. (2018). A survey of internet of things (IoT)-applications, merits, demerits & challenges. *International Journal of Innovative Research in Computer and Communication Engineering*, *6*(2), 903-907.

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 141*, 199-221.

Kumar, R., Venkanna, U., & Tiwari, V. (2020, January). A binary classification approach for time granular traffic in SDWMN based IoT networks. *In 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS) (pp. 531-534). IEEE.*

Lee, J., & Park, K. (2021). GAN-based imbalanced data intrusion detection system. *Personal and Ubiquitous Computing, 25*, 121-128.

Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., ... & Cui, L. (2020). Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement, 154*, 107450.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, *4*(5), 1125-1142.

Mohamed, T., Otsuka, T., & Ito, T. (2018). Towards machine learning based IoT intrusion detection service. In Recent Trends and Future Technology in Applied Intelligence: 31st International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE 2018, Montreal, QC, Canada, June 25-28, 2018, Proceedings 31 (pp. 580-585). Springer International Publishing.

Mohammad, Z., Abusukhon, A., & Qattam, T. A. (2019, April). A survey of authenticated Key Agreement Protocols for securing IoT. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 425-430). IEEE.

Mohammadzadeh, A. K., Ghafoori, S., Mohammadian, A., Mohammadkazemi, R., Mahbanooei, B., & Ghasemi, R. (2018). A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran. *Technology in Society*, *53*, 124-134.

Mourtzis, D., Vlachou, E., & Milas, N. (2016). Industrial big data as a result of IoT adoption in manufacturing. *Procedia cirp, 55,* 290-295.

Mumtaz, R., Samawi, V., Alhroob, A., Alzyadat, W., & Almukahel, I. (2022). PDIS: A Service Layer for Privacy and Detecting Intrusions in Cloud Computing. *International Journal of Advanced Software Computer Applications, 14*(2).

Murali, S., & Jamalipour, A. (2019). A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things. *IEEE Internet of Things Journal, 7*(1), 379-388.

NSF, N. S. F. (2011). The Network Simulator - ns-2. https://nsnam.sourceforge.net/wiki/index.php/User_Information#The_Network_Simulator_-_ns-2

Oikonomou, G., Duquennoy, S., Elsts, A., Eriksson, J., Tanaka, Y., & Tsiftes, N. (2022). The Contiki-NG open source operating system for next generation IoT devices. *SoftwareX, 18*, 101089.

Rawajbeh, M. A., Sayenko, V. I., Alhadid, I. H., Al-Turjman, F., & Ramasamy, L. K. (2021). Evaluation of functional maturity for a network information service-design and case analysis. *International Journal of Ad Hoc and Ubiquitous Computing*, *38*(1-3), 3-16.

Rydning, D. R. J. G. J., Reinsel, J., & Gantz, J. (2018). The digitization of the world from edge to core. *Framingham: International Data Corporation*, *16*.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks, 4*(2), 118-137.

Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future generation computer systems, 83*, 326-337.

Shanmugam, B., & Azam, S. (2023). Risk Assessment of Heterogeneous IoMT Devices: A Review. *Technologies*, *11*(1), 31.

Sheng, Z., Mahapatra, C., Zhu, C., & Leung, V. C. (2015). Recent advances in industrial wireless sensor networks toward efficient management in IoT. *IEEE access*, *3*, 622-637.

Siraj, S., Gupta, A., & Badgujar, R. (2012). Network simulation tools survey. *International Journal of Advanced Research in Computer and Communication Engineering, 1*(4), 199-206.

Statista, "Number of connected devices worldwide 2030 | Statista," Statista Research Department, 2020. [Online]. Available:https://www.statista.com/statistics/802690/worldwide-connecteddevices-by-access-technology/. [Accessed: 26-May-2022].

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future generation computer systems*, *108*, 909-920.

Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors, 19*(9), 1977.

things challenges in Iran. *Technology in Society*, *53*, 124-134.

Turner, S., & Chen, L. (2011). *Updated security considerations for the MD5 message-digest and the HMAC-MD5 algorithms* (No. rfc6151).

TutorialsWeb. (2023). Network Simulator 2 (NS2) : Features & Basic Architecture Of NS2. https://www.tutorialsweb.com/ns2/NS2-1.htm

Velinov, A., & Mileva, A. (2016). Running and testing applications for Contiki OS using Cooja simulator.

Wahid-Ul-Ashraf, A., Budka, M., & Musial, K. (2018). Netsim–the framework for complex network generator. *Procedia Computer Science, 126*, 547-556.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258.

Zhang, Y., An, J. P., & Chen, P. (2012). Research of Hybrid Programming with C#. net and Matlab. *Physics Procedia*, *24*, 1677-1681.