IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Security with Machine Learning for IoT Intrusion Detection Systems

Gaurav Mehta
ECE Deptt, UIE Chandigarh University Mohali, India

***Abstract*— The Internet of Things (IoT) has seen rapid growth, connecting millions of devices across various sectors, from healthcare to smart homes. However, this expansion has introduced significant security vulnerabilities, making IoT systems prime targets for cyberattacks. Traditional security mechanisms often struggle to cope with the dynamic nature and scale of IoT networks, necessitating more sophisticated and adaptive solutions. This paper presents an improved security framework for IoT environments through the integration of Machine Learning (ML) techniques for Intrusion Detection Systems (IDS). By leveraging supervised and unsupervised learning models, the proposed approach enhances the detection accuracy and response times to potential threats, while adapting to evolving attack patterns. The system analyzes network traffic, device behavior, and system logs to identify abnormal activities and potential intrusions in real-time. Key ML algorithms, such as Decision Trees, Random Forest, and Neural Networks, are evaluated for their effectiveness in distinguishing between normal and malicious activities. The results demonstrate that the ML-based IDS significantly outperforms traditional signature-based methods, offering higher detection rates and reduced false positive rates. This work contributes to the advancement of IoT security by providing a scalable, adaptive, and efficient solution to safeguard IoT ecosystems against emerging threats.**

***Keywords*— *Machine learning Internet of things Security Intrusion detection Classification algorithm*.**

I. INTRODUCTION

The Internet of Things (IoT) has transformed how we interact with the world, enabling a vast network of interconnected devices that streamline processes, enhance convenience, and improve efficiency in industries such as healthcare, transportation, manufacturing, and smart homes. However, as the number of IoT devices continues to grow, so does the risk of security vulnerabilities. These devices, often limited in processing power and security features, present attractive targets for cyberattacks. Traditional security measures, such as firewalls and signature-based Intrusion Detection Systems (IDS), often fail to address the unique challenges posed by IoT networks, such as the sheer scale of devices, dynamic environments, and diverse communication protocols.

This paper proposes an improved security framework for IoT networks by integrating Machine Learning into the Intrusion Detection System. The goal is to enhance the detection and mitigation of malicious activities within IoT ecosystems, while minimizing false positives and maintaining low latency. Through the use of various ML algorithms, such as Decision Trees, Random Forests, and Neural Networks, the proposed system can effectively identify abnormal behaviors and potential intrusions based on network traffic, device interactions, and historical data. By utilizing ML techniques, the IDS can continuously learn from new data, improve over time, and offer a scalable and robust

solution to the growing security concerns of IoT networks. This approach aims to overcome the limitations of traditional security measures and provide a more efficient, proactive defense against a wide range of cyber threats in the rapidly evolving landscape of IoT.

There are numerous of products around us to make our life simpler and easier, which as like virtual companion. Trending usage of Internet of Things in the era of Information and Communication Technology is accelerating in drastic way to connect with numerous of gadgets [1]. Recently, there has been a growing interest in exploring the potential of machine learning technologies to improve on the electronic gadgets around in everyday activities on its security. This scenario powered the huge amount of data proliferate the intelligence to mitigate threats. Applying the intelligence to Internet of things by the artificial approach, is one of the methods to minimize the intensive job request for every process [2].

As prototype, Internet of Things gadgets can be used for various purposes and install at various places based on the use cases. These gadgets size may vary from tiny to huge on deployment, which carries most crucial and sensitive information through all the sensory mode of daily life activities [3].

2. Machine learning for IoT applications

Machine Learning (ML) is becoming a key enabler for the Internet of Things (IoT) due to its ability to enhance the intelligence, efficiency, and security of IoT systems. IoT refers to a network of interconnected devices, sensors, and systems that communicate and exchange data. As IoT ecosystems grow in complexity, traditional methods for processing and managing data become insufficient. This is where ML plays a pivotal role by providing automated data analysis, predictive capabilities, and decision-making processes that are essential for IoT applications.

In this aspect not only having current data, along with past data accumulation an enormous amount of data applied to comparison with machine automated learning algorithms defines accurate results [4].

There are more applications for machine learning in all domains because it has many benefits in the Internet of Things, including cost savings, and machine learning is essential to the industry's applications. The more accurate predictive measure on typical examples of large machinery with sensors that allow the machine learning algorithm to identify defects with high accuracy, lower maintenance costs, and carry over on time

World popular part of machine learning is shaping the future based on the recommendation, where consist of numerous examples like Amazon, YouTube, Netflix etc., having greater significant in the business not limited to the extent [5]. Threat has prone to economic instability when the system was connected with net- work. If the data accumulation gadgets of Internet of Things were more vulnerable in these aspects of security and privacy in order to maintain growth of the business [6]. In Fig. 1, has the data to

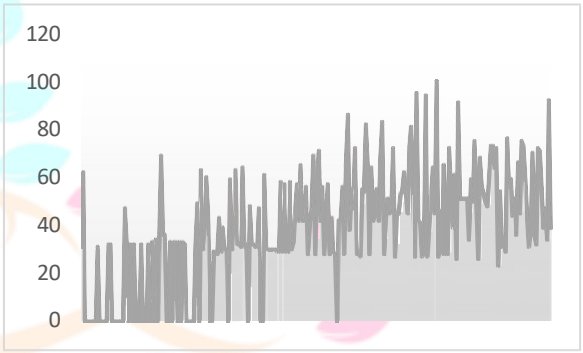


Fig. 1. Use of IoT machine learning (Google Trends).

1. It shows the trending of interlinkage with Internet of Things and Machine Learning over the worldwide projection over past five years.
2. Anything that is linked to the internet is vulnerable to security and privacy risks (e.g., power failure on functional gadgets, physical harm to devices, privacy on sensed data). Machine Learning enables the optimized method to identify the unusual behavior in sensors or other smart devices in an effective technology [7]. Sensors on monitoring and actuators on reacting agents of an Artificial Intelligence architecture provides the abnormal behavior intrusion detection on analysis of network connected Internet of Things gadgets. The categories of Machine Learning techniques were differed from the utilization of computational power and efficiency while producing output [8].

Unsupervised machine learning techniques use less computing power during the training phase than during the implementation phase, whereas supervised machine learning techniques use greater computational resources during the training phase.

With machine learning technique has the optimized datasets paved to increase the

security on networks on Internet of Things allows to protect the infrastructure, when connected in traditional topology [9].

When IoT devices prone to attack, then it has a high chance on information leakage. This kind of loss on information may interrupt working process leads to quality negotiation, probably Inter- net of Things consist of heterogeneity gadgets into a system, which need to overcome the issue by using the method of infusing a software into the network [10]. Installing software on a network is a common practice in the telecom sector, where cloud computing technologies are used to provide network services using software approach. Threats to the security of IoT smart devices vary depending on the features that were included. In order to improve the security, target the approaches apply on the terminal either at host-based method or network- based method; that enabling efficient and effective on security for IoT using Machine Learning techniques [11]. Machine learning-based security for an Internet of Things domain makes the automated approach possible within its framework.
Networks connected to the Internet of Things are susceptible to several types of assaults. This session includes a thorough explanation of attacks, including sur-face attacks, their impacts, and the types of attacks that can occur in the Internet of Things. It is imperative that makers and developers of gadgets around the world exercise greater caution. in Fig. 2.

a. Types of attack: further divided into physical and cyberattacks; a cyberattack will cost the IoT system's connection, which is most likely wireless.

b.

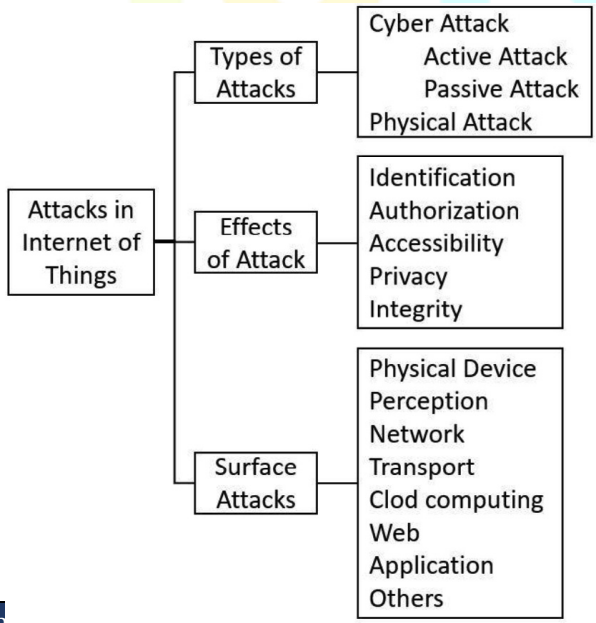


Fig. 2. Categories of attacks in internet of things.

In this scenario, the hacker attempts to use the sensors to steal, erase, alter, or destroy data. Whereas cyberattacks are divided into active and passive phases, physical attacks harm hardware and disrupt the services offered by IoT devices[12]. In order to alter the system configuration and disrupt services in various ways, an active assault gains access to the network system. In a passive attack, information is manipulated from multiple sources and the private data collected by IoT devices is decrypted to allow for misuse or to cause the devices to get inaccurate information due to misconfigured settings[13].

c. Identity, authorization, accessibility, privacy, and integrity are further categories of attack impacts that were susceptible to threads of security and privacy of personal information.

[14]. In order to prevent various types of network security eavesdropping attacks, users must first register in order to consent over transfers based on their identification. This ensures the IoT system's robustness.
[15]. In order to ensure that only humans can access the platform and that other devices can access the system, authorization ensures that users can access the network with permission based on the accuracy of their credentials. Therefore, a secured environment is necessary when it grows too big, it's hard to keep[16].

The internet of things system's accessibility will enable trustworthy users to obtain information, and preventing needless requests that keep the system busy is vital for the protocol to access IoT devices without interruption.
[17]. The most crucial component of IoT system security for user data is privacy. When personal data is stored or transferred across a network from various IoT devices, it can be accessed by unauthorized individuals, which can result in a threat for user data. Integrity guarantees that the registered user can change data on the Internet of Things system over the network for communication, and that other harmful attacks may also take place while the data is being stored.
[18]. Describe the surface assault on the layers of the IoT architecture. Physical device and perception surfaces, network and transportation surfaces, application and online services, cloud computing services, and other surfaces are

the categories under which these attacks fall.

Perception and the physical device the physical layer utilized for identification and information exchange is readily accessible through a surface known as a "direct attack" on the IoT system's surface, which compromises private and sensitive data. Therefore, physical devices are more likely to assault on the face

[19]. Transportation and the network Strong security protocols are necessary to prevent surface attacks via wired or wireless networks of the Internet of Things. Otherwise, the vast system of IoT would be vulnerable to such attacks. Surface attacks on cloud computing have the capacity to remotely share information and gain access to data stored on cloud storage without the IoT system's security. Web and attack applications in the digital age of smart technology, where one can access the control of the smart gadget remotely and change it using a miss configural technique

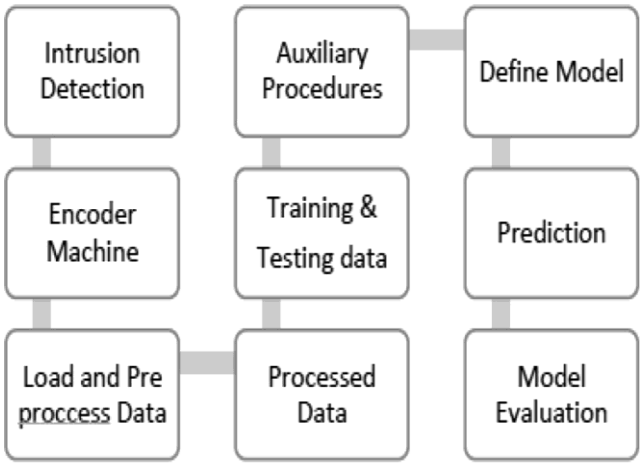
[20]. Other attacks are also being launched in this network when the system is connected to other systems independently. Some of these attacks involve illegally obtaining information about social media users on the Internet of Things system. Intrusion detection, which falls into three primary categories based on the signature model, anomaly model, and specification model, was the identification of anomalous behavior that occurred in the network.

[21]. Finding patterns in a connected network that resemble those in the current signatures database is the goal of the signature model intrusion detection system. An alarm is always triggered if any patterns are found via the network; however, it is ineffective to do so if a new pattern emerges that is not found in the database. [22].

In the specification model, the intrusion detection system compares network traffic behavior to the predefined criteria on the specification, which were established to identify anomalous network activity. The specification process was manually defined by a security expert.

The anomaly model of an intrusion detection system, as opposed to the signature and specification model, allows for continuous network traffic monitoring for any deviation from the standard network communication process[23]. If there is a variance that is significant enough to cause an alarm, then toast it for attack detection. Machine learning algorithms fully trained and tested the aforementioned standard network procedure. Accordingly, the anomaly model of an intrusion detection system is more effective than the other model at detecting new network traffic attacks; nonetheless, in terms of detection, only the limit determines the alarm trigger rate[24]. Based on the quality of patterns found in the network traffic (data set), which was used to train the model based on trained direction process, the anomaly model intrusion detection system's efficient behavior and effective performance have the potential to identify new network attacks. The machine learning algorithm is entirely dependent on acquired datasets[25]. The Internet of Things' intrusion detection system model uses binary classification on networks to identify if network traffic is in normal or attack mode. This classification should have a greater accuracy and a lower false rate. Together with training and testing data sets, the classification algorithm bears full responsibility for defining performance in terms of accuracy and fewest false positives[26]. The intrusion detection method will be used to identify network attacks when the machine learning algorithm is applied to the internet of things network system. Using a threshold limit, this detection technique applies a machine learning algorithm throughout the network to classify attacks as either normal or anomalous[27]. The methodical process, which is started by the intrusion detection, forwards the strategy to the encoder machine, encrypts the data from the data sets, loads and preprocesses the data model, which helps the data in the anticipated way by removing unnecessary data, incorrect data, and noise[28].

This pre-processing technique is crucial for the data set that will determine the prediction accuracy. The processed data has defined two



distinct training and testing data sets, respectively, and has made it possible for the subsequent auxiliary procedures to manipulate the data effectively for the machine learning model.

Fig. 3. Model of applying machine learning for intrusion detection system.

It will make predictions based on the classification of TCP packets as normal or anomalous, and at the end, the model will be tested using training and testing data sets to determine how accurate and effective it is at identifying network attacks, as shown in Fig. 3: Model of applying machine learning for intrusion detection system[29]. The information was gathered via the internet of things during the TCP/IP local area network environment through the defense network simulation procedure. Multiple attacks on the network system were launched in order to manipulate the LAN network[30].

Allow TCP data packets to be transferred over a network connection for a specific amount of time in order for the packets to flow from source to destination according to a clearly specified protocol method. Additionally, training data that has been identified as normal or anomalous with a particular type of attack through detection, such as for each type of 800-bit sample. About 40 categories were identified from the datasets to determine if the network was normal or abnormal[31].

Result

As a result, that result identifies anomaly detection in the network of IoT devices for 500 epochs of each variety with 800 bits of data transfer. To determine whether a TCP packet is an anomalous or normal transaction, a threshold limit of 0.499 is noted for intrusion detection in Fig. 4, and the green horizontal line indicates whether the attack was normal or anomalous. Outliers were present in this instance, thus the machine learning technique was used to identify the maximum number of points that constituted an anomaly in order to improve the TCP packet categorization with high accuracy on the intrusion detection system. [32].

In order to classify anomalous and typical attacks of the TCP packets that were obtained, a model was applied to the datasets using a machine learning technique (Table1). The classification model's accuracy rate is 94.57 percent. Based on the average macro and average weight of the TCP packets, the detailed classification report provides a classification based on precision, recall, and F1-score over the result that falls between 0 and 1. The model is applied to train by dataset, and the test dataset yields a much more accurate result. In addition to optimizing anomaly detection, threshold point selection should be accurate for the dataset. The model accuracy employing machine learning across the Internet of Things network along with a comprehensive categorization chart based on values gathered by the intrusion detection system[33].

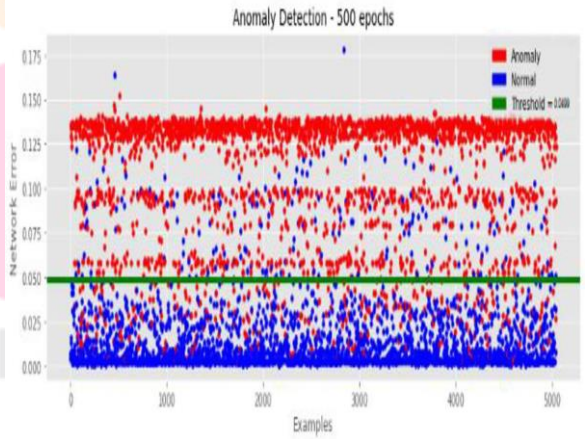


Fig. 4. Anomaly detection using 500 epochs with threshold as 0.499.

3. Conclusion

Machine learning applications are endless and serve as a universal process for a wide range of industrial and technological streams using Internet of Things systems. This

encourages study, and the firm will advance with precise choices and a well-defined analytical action plan. The Internet of Things connects all of the gadgets and equipment into a unified system, making it possible to access information securely and conveniently from anywhere at any time. Because there are many different approaches for innovative solutions, machine learning can be used to solve security and privacy issues more effectively. Although the use of cutting-edge technologies to prevent assaults on the Internet of Things network is not always possible[34]. In light of the preceding two years' study on machine learning and the internet of things, numerous action plans have been implemented to address numerous security concerns; yet, even with new strategies, new attack patterns cannot be defeated. Additionally, a machine learning algorithm illuminates the way for future researchers to achieve the goal in the most straightforward manner of large attacks on wide area internet of things networks, which is a novel technique necessary to alleviate concerns. Credit authorship contribution statement

K. Mandal: Conceptualization, Data curation. M. Rajkumar: Formal analysis, Methodology. P. Ezhumalai: Project administration, Writing - original draft. D. Jayakumar: Supervision, Validation, Funding acquisition. R. Yuvarani: Writing - review & editing, Formal analysis.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Amiri-Zarandi, R.A. Dara, E. Fraser, A survey of machine learning-based solutions to protect privacy in the internet of things, Comput. Security 101921 (2020).

[2] M.F. Mridha, M.A. Hamid, M. Asaduzzaman, ‘‘Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm”. In Proceedings of International Joint Conference on Computational Intelligence, (2020)395-406). Springer, Singapore.

[3] M. Amiri-Zarandi, R.A. Dara, E. Fraser, A survey of machine learning-based solutions to protect privacy in the internet of things, Comput. Security 101921 (2020).

[4] M.F. Mridha, M.A. Hamid, M. Asaduzzaman, ‘‘Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm”. In Proceedings of International Joint Conference on Computational Intelligence, (2020)395-406). Springer, Singapore.

[5] S. Zeadally, M. Tsikerdekis, ‘‘Securing Internet of Things (IoT) with machine learning”. International J. Commun. Syst., 33(1)(2020) e4169.

[6] A. Verma, V. Ranga, Machine learning based intrusion detection systems for IoT applications, Wireless Pers. Commun. 111 (4) (2020) 2287–2310.

[7] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, ‘‘Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study”. arXiv preprint arXiv:2006.15340, 2020.

[8] S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, J. Netw. Comput. Appl. 102630 (2020).

[9] F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: current solutions and future challenges, IEEE Commun. Surv. Tutorials (2020).

[10] M. Bagaa, T. Taleb, J.B. Bernabe, A. Skarmeta, A machine learning security framework for IoT systems, IEEE Access (2020).

[11] M. Amiri-Zarandi, R.A. Dara, E. Fraser, A survey of machine learning-based solutions to protect privacy in the internet of things, Comput. Security 101921 (2020).

[12] M.F. Mridha, M.A. Hamid, M. Asaduzzaman, ‘‘Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm”. In Proceedings of International Joint Conference on Computational Intelligence, (2020)395-406). Springer, Singapore.

[13] S. Zeadally, M. Tsikerdekis, ‘‘Securing Internet of Things (IoT) with

machine learning". International J. Commun. Syst., 33(1)(2020) e4169.

[14] A. Verma, V. Ranga, Machine learning based intrusion detection systems for IoT applications, Wireless Pers. Commun. 111 (4) (2020) 2287–2310.

[15] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, ''Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study". arXiv preprint arXiv:2006.15340, 2020.

[16] S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, J. Netw. Comput. Appl. 102630 (2020).

[17] F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: current solutions and future challenges, IEEE Commun. Surv. Tutorials (2020).

[18] M. Bagaa, T. Taleb, J.B. Bernabe, A. Skarmeta, A machine learning security framework for IoT systems, IEEE Access (2020).

[19] M. Amiri-Zarandi, R.A. Dara, E. Fraser, A survey of machine learning-based solutions to protect privacy in the internet of things, Comput. Security 101921 (2020).

[20] M.F. Mridha, M.A. Hamid, M. Asaduzzaman, ''Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm". In Proceedings of International Joint Conference on Computational Intelligence, (2020)395-406). Springer, Singapore.

[21] S. Zeadally, M. Tsikerdekis, ''Securing Internet of Things (IoT) with machine learning". International J. Commun. Syst., 33(1)(2020) e4169.

[22] A. Verma, V. Ranga, Machine learning based intrusion detection systems for IoT applications, Wireless Pers. Commun. 111 (4) (2020) 2287–2310.

[23] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, ''Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study". arXiv preprint arXiv:2006.15340, 2020.

[24] S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, J. Netw. Comput. Appl. 102630 (2020).

[25] F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: current solutions and future challenges, IEEE Commun. Surv. Tutorials (2020).

[26] M. Bagaa, T. Taleb, J.B. Bernabe, A. Skarmeta, A machine learning security framework for IoT systems, IEEE Access (2020).

[27] F. Zantalis, G. Koulouras, S. Karabetsos, D. Kandris, A review of machine learning and IoT in smart transportation, Future Internet 11 (4) (2019) 94.

[28] C. Shetty, B.J. Sowmya, S. Seema, K.G. Srinivasa, ''Air pollution control model using machine learning and IoT techniques", In Advances in Computers, 117(1) (2020)187-218). Elsevier.

[29] B.K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, ''Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology", Internet of Things, (2020)100227.

[30] J. Fürst, M.F. Argerich, B. Cheng, E. Kovacs, Towards knowledge infusion for robust and transferable machine learning in IoT, Open J. Internet of Things (OJIOT) 6 (1) (2020) 24–34.

[31] M. Amiri-Zarandi, R.A. Dara, E. Fraser, A survey of machine learning-based solutions to protect privacy in the internet of things, Comput. Security 101921 (2020).

[32] M.F. Mridha, M.A. Hamid, M. Asaduzzaman, ''Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm". In Proceedings of International Joint Conference on Computational Intelligence, (2020)395-406). Springer, Singapore.

[33] S. Zeadally, M. Tsikerdekis, ''Securing Internet of Things (IoT) with machine learning". International J. Commun. Syst., 33(1)(2020) e4169.

[34]A. Verma, V. Ranga, Machine learning based intrusion detection systems for IoT applications, Wireless Pers. Commun. 111 (4) (2020) 2287–2310.

[35]H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, ''Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study". arXiv preprint arXiv:2006.15340, 2020.

[36]S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, J. Netw. Comput. Appl. 102630 (2020).

[36]F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: current solutions and future challenges, IEEE Commun. Surv. Tutorials (2020).

[37] M. Bagaa, T. Taleb, J.B. Bernabe, A. Skarmeta, A machine learning security framework for IoT systems, IEEE Access (2020).

[38] F. Zantalis, G. Koulouras, S. Karabetsos, D. Kandris, A review of machine learning and IoT in smart transportation, Future Internet 11 (4) (2019) 94.

[39] C. Shetty, B.J. Sowmya, S. Seema, K.G. Srinivasa, ‘‘Air pollution control model using machine learning and IoT techniques”, In Advances in Computers, 117(1) (2020)187-218). Elsevier.

[40] B.K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, ‘‘Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology”, Internet of Things, (2020)100227.

[41] J. Fürst, M.F. Argerich, B. Cheng, E. Kovacs, Towards knowledge infusion for robust and transferable machine learning in IoT, Open J. Internet of Things (OJIOT) 6 (1) (2020) 24–34.

[42] A. Hussain, U. Draz, T. Ali, S. Tariq, M. Irfan, A. Glowacz, A.J.A. Daviu, S. Yasin, S. Rahman, Waste management and prediction of air pollutants using IoT and machine learning approach, Energies 13 (15) (2020) 3930.

[43] T.A. Khoa, C.H. Phuc, P.D. Lam, L.M.B. Nhu, N.M. Trong, N.T.H. Phuong, N.V.
Dung, Y, N.Tan, H.N. Nguyen, D.N.M. Duc, Waste management system using IoT-based machine learning in University. Wireless Communications and Mobile Computing, 2020.

[44] S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, Journal of Network and Computer Applications 161 (2020).

[45] B.B. Zarpelao, R.S. Miani, C.T. Kawakani, S.C.D. Alvarenga, A survey of intrusion detection in internet of things, J. Netw. Comput. Appl. 84 (2017) 25–37.

[46] M.B.M. Noor, W.H. Hassan, Current research on internet of things (iot) security: A survey, Comput. Netw. 148 (2019) 283–294.

[47] K.T. Nguyen, M. Laurent, N. Oualha, ‘‘Survey on secure communication protocols for the internet of things,” Ad Hoc Networks, 32(2015) 17 – 31. Internet of Things security and privacy: design methods and optimization.

[48] K. Sha, W. Wei, T.A. Yang, Z. Wang, W. Shi, On security challenges and open issues in internet of things, Future Generat. Comput. Syst. 83 (2018) 326–337.

[49] M. Tao, K. Ota, M. Dong, Z. Qian, Accessauth: Capacity-aware security access authentication in federated-iot-enabled v2g networks, J. Parallel Distrib. Comput. 118 (2018) 107–117.

[50] S.B. Baker, W. Xiang, I. Atkinson, Internet of things for smart healthcare: Technologies, challenges, and opportunities, IEEE Access 5 (2017) 26521–26544.

[51] F. Javed, M.K. Afzal, M. Sharif, B. Kim, ‘‘Internet of things (IOT) operating systems support, networking technologies, applications, and challenges: A comparative review,” IEEE Communications Surveys Tutorials, 20(third quarter 2018) 2062–2100.

[52] A. Colakovi˘c, M. Had´ ziali˘c, ‘‘Internet of things (iot): A review of ´ enabling technologies, challenges, and open research issues,” Comput. Netw., 144(2018) 17 – 39.

[53] M. Mohammadi, A. Al-Fuqaha, S. Sorour, M. Guizani, ‘‘Deep learning for IOT big data and streaming analytics: A survey,” IEEE Communications Surveys Tutorials, 20 (Fourth quarter 2018) 2923–2960.