Advanced Production and Industrial Engineering
R.M. Singari and P.K. Kankar (Eds.)

doi:10.3233/ATDE220798

A Review on Machine Learning Techniques on IOT Based Privacy Preserving Network

ANKIT AGGARWAL
Bachelors of Technology, Department of Chemical Engineering, Manipal Institute of Technology, Karnataka, India
ankit.acoolguy@gmail.com
SNEHA ARORA
PhD Scholar, Department of Electronics and Communication, Lovely Professional University, Punjab, India
snehaarora56@gmail.com

Abstract

Expanded data collection and processing at greater rates have come from a growth in the number of devices connected to the internet, which is especially important now that the requirement for real-time action has increased significantly in recent years. It is becoming more difficult to finish data processing within an acceptable time frame as the variety and validity of data continues to grow in volume and quality. Because the data generated is supplied to a variety of different cloud data centres located all over the world, the current cloud architecture is a sub-optimal choice in these situations, according to the researchers. In this approach, implementing machine learning technologies into the present cloud environment may improve the overall efficiency and effectiveness of the cloud environment. In this article, works on machine learning and security in the Internet of Things platform are evaluated.

Keywords- machine learning, encryption, security, IOT

Introduction

The Internet of Medical Things (IoMTs) is gradually overtaking the traditional healthcare system in terms of usage and acceptance, as stated by the World Health Organization (WHO). However, when it comes to the design of devices and systems that are connected to the Internet of Things (IoT), inadequate thought has been given to the requirements for the devices' and systems' respective levels of security. It is quite likely that one of the primary contributing factors to this predicament is the challenges that are connected with adapting conventional security solutions to the context of IoMT. In the last several years, machine learning (ML) has shown to be a highly successful technique in the detection and mitigation of cyberattacks, notably in the defence sector. In addition, ML has also showed promise in the prevention of cybercrime. Advanced machine learning algorithms have the potential to be a viable option in order to solve the present and future security and privacy challenges linked with the Internet of Things (IoT). Methodologies of machine learning that are at the cutting edge It is necessary to understand how these techniques can be effectively implemented in the IoMT system given the current challenges faced by the IoMT system in order to effectively implement these techniques in order to meet the security and privacy requirements of the IoMT system without sacrificing the quality, services, or device lifetime of the IoMT system. This is necessary in order to effectively implement these techniques in order to meet the security and privacy requirements of the IoMT system. Aside from that,

there is a massive amount of data that is stored on the cloud, and this data may be utilised as an input by machine learning algorithms. [3] It's possible to organise and combine various data sets by using a fundamental technique from the field of machine learning called clustering. After that, you have the option of using extra cognitive and predictive algorithms in order to improve the results. Cloud computing is a practise that has recently gained favour among data scientists due to its ability to allow for more effective computing via the use of a range of machine learning and artificial intelligence technologies. This practise is known as cloud computing (examples include Amazon Web Services with Keras, IBM Watson, and Microsoft Cognitive AI). [...] Aside from that, in this day and age, which is characterised by the Internet of Things, Big Data Analytics, and Blockchain, almost all of the data is processed in the cloud, and machine learning and artificial intelligence are essential in order to meet the growing demand for effective and efficient computing resources. Deep learning is considered to be a new frontier in the field of machine learning. However, it is also considered to be an important subset of artificial intelligence since it is expected to represent a large subset of AI. A technique known as deep learning, which is also considered to be an innovative problem in the field of artificial intelligence, is one that learns not only from new experiences but also from those that have come before (AI). The term "deep learning" has been defined in a myriad of various ways throughout the course of human history; nevertheless, the definition that is presented in this article is the most comprehensive of the many possibilities that are available. The following is an explanation of what is meant by the term "deep learning": Deep learning is a set of techniques that are used in the area of machine learning to increase accuracy. These methodologies are based on artificial neural networks that have multiple layers [7], and deep learning is a subfield of machine learning. Deep learning is a subset of machine learning approaches that are now being used in a variety of different software programmes. When they published their results on the subject in the journal Nature in the 1940s, they were the pioneers who gave the scientific community its first exposure to the idea of artificial neural networks. The biological brain systems were the first to be discovered, and they served as the foundation for the fundamental idea of using neural networks for the processing of information [9], which was then refined further. This article takes a comprehensive look at a number of other publications and approaches that focus on applying machine learning to the Internet of Things.

Literature Review

P. C. Arachchige, amongst a number of others, and a number of other people. The significant risk of privacy leakage that is posed by machine learning models is a significant barrier to their full participation in the Fourth Industrial Revolution. This barrier is a direct result of the significant danger that these models pose to the confidentiality of the data on which they are based. Using the PriModChain architecture, which is comprised of differential privacy, federated machine learning, the Ethereum blockchain, and smart contracts, data privacy and trustworthiness are enforced as part of the Internet of Things (IoT). This is accomplished by utilising the PriModChain architecture. The Internet of Things is made up of this particular architectural framework (IoT). An investigation into the viability of PriModChain is carried out by employing Python-based socket programming simulators on a general-purpose computer. The goal of this investigation is to establish whether or not PriModChain meets the criteria for privacy, security, reliability, safety, and robustness. The results are presented in this article together with its other content.[1-2] Chamikara and a few more folks in addition to them Industry 4.0, also known as the Industrial Internet of Things (IIoT), is in the process of transforming several important industries, including those dealing with energy, agriculture, mining, transportation, and healthcare, amongst others. This transformation is taking place in several different countries around the world. The Internet of Things (IoT), which makes considerable use of machine learning (ML), is a primary factor behind the development of Industry 4.0. This is due to the fact that ML is required in order to make use of the vast volumes of data produced by IIoT as well as the huge interconnections that they create. The use of machine learning models that are produced from sensitive data puts that data at danger of being targeted by adversaries, which in turn restricts the potential of Industry 4.0. The author of this piece proposes the creation of a system known as PriModChain that would make use of differential privacy, federated machine learning, the blockchain technology used by Ethereum, and smart contracts. This solution would guarantee that the data provided by IIoT devices could be trusted while also protecting the privacy of the data that is created by such devices.[3] Hussain and the other members of the Internet of Things (IoT) of the future will have a significant impact on many facets of our society, such as the economics, the corporate world, and social life. Hackers see the nodes that make up Internet of Things networks as possible targets for their attacks since these nodes often have restricted access to the resources that make up such networks. The inherent privacy and security problems of IoT networks have been the topic of extensive research and development efforts, with the bulk of these efforts focused on the use of standard cryptographic processes. This has resulted in tremendous progress being made in this area. On the other

hand, standard solutions are unable to fulfil the whole security spectrum associated with Internet of Things (IoT) networks due to the unique characteristics of IoT nodes. This is the case because IoT nodes are distributed throughout the network. Using Machine Learning (ML) and Deep Learning (DL) strategies, both of which are capable of embedding intelligence in the devices and networks that make up the Internet of Things, it is possible to handle a variety of different security issues. This is something that is both feasible and highly desirable (IoT).[4] Parikshit N. Mahalle and a lot of other academics have come to the conclusion that... The Internet of Things (IoT) is a massive network of interconnected electronic devices that are able to communicate with one another and work together to provide a variety of services at any time, from any location, and in any way that can be imagined. These devices are able to communicate with one another and work together thanks to the Internet of Things (IoT). One of the most fundamental issues associated with identity management is ensuring that access control, authentication, and device management are always brought up to date. This problem develops when different devices interact with one other, with different services, and with people. Managing one's identities in today's age of contemporary technology and online communication involves a variety of obstacles that need to be solved. Due to the infinite number of linked devices and the coming limits that will emerge as a direct result of their being a limited quantity of accessible resources, these problems are made significantly worse by the Internet of Things (IoT). Modern identity management systems have a significant focus on identifying end users and services within the context of a networked environment as their primary mission. This stands in stark contrast to the identification of organisations, which is a lower priority than it formerly was. F. Restuccia et al. [5] The Internet of Things, also known as "IoT," is the realisation of a vision in which billions of networked devices are placed almost everywhere, ranging from the author's own body to some of the most remote locations in the world. This vision was originally referred to as the "Internet of Everything." Originally, this concept was referred to as the "Internet of Everything." Because the Internet of Things will eventually permeate every part of day-to-day life and will be available to everyone, it is more important than ever to find solutions to major security challenges related with the Internet of Things as soon as it logistically viable to do so. There is a possibility that the protection provided by traditional security measures, such as adding security after the fact and as a "patch" for known flaws, is insufficient. Audits of the security system are another example. [6] B. Niu and a few more individuals in addition Because of the mismatch between the limiting capacity of local devices and the rising complexity of DNN models, offloading computationally heavy operations to a distant server, such as the cloud, is a realistic alternative. This is because of the mismatch between the two factors. However, in order to train neural networks and infer outcomes, the untrusted server will require all of the user data. This will result in the loss of the local's assets as well as serious privacy issues about the sensitive data of the user. The author presents a fundamental framework that may concurrently strike a balance between user privacy, model correctness, and training efficiency in contexts that include machine learning as a service in order to find a solution to this problem. This framework is provided in order to find a solution to this problem. M. Bagaa et al. [7] Both educational and business-related organisations are finding that ensuring the safety of the Internet of Things is becoming an increasingly important priority (IoT). When a device is linked to the Internet of Things (IoT), it opens itself up to a broad variety of security concerns. Some examples of these risks include denial-of-service attacks, network infiltration, and data loss. This study introduces a novel, machine learning (ML)-based security architecture that can automatically adjust to the growing number of threats posed by the Internet of Things (IoT). This design makes use of enablers for both software-defined networking (SDN) and network function virtualization (NFV), in addition to other types of technologies, in order to guard against a broad variety of threats. This was done in order to keep the network safe. When it comes to conducting network pattern analysis and anomaly-based intrusion detection in Internet of Things (IoT) systems, our artificial intelligence framework makes use of machine learning models in both the monitoring agent and the AI-based reaction agent. Both of these agents are responsible for artificial intelligence. Because of this, our framework is able to provide a complete solution by integrating a monitoring agent and an AI-based response agent. [8] N. Chaabouni together with a great many other individuals. The Internet of Things (IoT) is quickly gaining popularity in countries all over the world. As a consequence of assaults such as the Dyn botnet assault that took place in 2016, it has become clear that intelligent networks are susceptible to a wide variety of threats, some of which are very severe. The Internet of Things (IoT) has very lately emerged as a key cause for concern in the public eye. In addition, the danger presented by infected Internet-connected things has an impact not just on the safety of the internet, but also on the ecosystem that makes up the internet. Botnets are networks of insecure Things (smart devices) that have been programmed to carry out harmful actions. This eco-system has the potential to be abused by botnets, which are networks of vulnerable Things (smart devices). Because of many distributed denial-of-service attacks, the Internet was taken down as a result of the Mirai virus, which was responsible for the compromising of video surveillance equipment. Over the course of the last several years, there has been a growth not just in the sophistication of security attack vectors but also in the variety of security attack vectors. The former has gotten more complex, while the latter has expanded its range of options. It is essential to conduct strategy reviews within the framework of the Internet of Things in order to identify

existing threats and either eliminate them or come up with new ones (IoT). This research classifies the hazards and concerns about the security of IoT networks by doing an analysis of the defensive techniques that are currently in place and finding new risks and problems. In addition, this study identifies potential new threats and challenges. [9] Chaabouni, in addition to a few other people The Internet of Things (IoT) is quickly gaining popularity in countries all over the world. As a consequence of assaults such as the Dyn botnet assault that took place in 2016, it has become clear that intelligent networks are susceptible to a wide variety of threats, some of which are very severe. Significant strides have been made in the protection of devices that are linked to the Internet of Things (IoT), which stands for the Internet of Things. Infected devices that are linked to the internet represent a danger not just to the safety of the internet as a whole, but also to the ecosystem that makes up the internet. This ecosystem is susceptible to being abused by botnets, which are networks of weak items (such as smart devices) that are used to launch attacks on other botnets. Not only does this danger have an effect on the safety of the internet, but it also has an effect on the internet as a whole. The distributed denial-of-service assaults that resulted in the loss of Internet access and the infection of video surveillance equipment were triggered by the computer virus known as Mirai (DDoS). Over the course of the last several years, there has been a growth not just in the sophistication of security attack vectors but also in the variety of security attack vectors. The former has gotten more complex, while the latter has expanded its range of options. It is essential to conduct strategy reviews within the framework of the Internet of Things in order to identify existing threats and either eliminate them or come up with new ones (IoT). The study classifies the dangers that face the security of the Internet of Things as well as the challenges that it creates for the networks that make up the IoT. The classifications are based on an analysis of the different defence mechanisms that are now in operation. As a direct result of this, the study that is being conducted explores the presently available network intrusion detection system (NIDS) implementation tools and datasets, in addition to free and open-source network sniffer software. The topic of intrusion detection systems is studied in great detail in this work (NIDS). This research then investigates, evaluates, and compares the existing NIDS concepts for usage in the Internet of Things in terms of architecture, detection approach, validation procedures, threats addressed, and algorithm implementations. [10] F. Hussain in addition to a number of other individuals. The Internet of Things (IoT) of the future will have a significant impact on many facets of our society, such as the corporate world, the economics, and our everyday social interactions. Hackers see the nodes that make up Internet of Things networks as possible targets for their attacks since these nodes often have restricted access to the resources that make up such networks. The inherent privacy and security problems of IoT networks have been the topic of extensive research and development efforts, with the bulk of these efforts focused on the use of standard cryptographic processes. This has resulted in tremendous progress being made in this area. On the other hand, standard solutions are unable to fulfil the whole security spectrum associated with Internet of Things (IoT) networks due to the unique characteristics of IoT nodes. This is the case because IoT nodes are distributed throughout the network. Using Machine Learning (ML) and Deep Learning (DL) strategies, both of which are capable of embedding intelligence in the devices and networks that make up the Internet of Things, it is possible to handle a variety of different security issues. This is something that is both feasible and highly desirable (IoT). The purpose of this piece is to provide the reader with an in-depth analysis of the security needs, possible points of attack, and solutions that are presently available for IoT networks. The author continued their research on the flaws that are inherent in security solutions that need the use of methodologies such as machine learning and deep learning. [11] O. Salman in addition to a number of other individuals. As a consequence of the expansion of data that is connected to the Internet and the incorporation of apps made by third parties, the administration of access control has become more complicated. This is particularly the case for sensitive data. A security model is required since this is a direct consequence of the situation. The widespread adoption of "softwarization" and network "virtualization" ushered in a new network management paradigm and paved the way for the development of a global network operating system a few years ago. These developments occurred as a result of the invasion of new technologies. The term "softwarization" is used to refer to the first tendency, whereas "virtualization" is used to refer to the second trend. The author of this post is going to talk about the challenges that the Internet of Things presents in terms of the need for privacy and protection of personal information. In addition, the authors provide a software-defined architecture as a method for guaranteeing the security of devices that are connected to the Internet of Things. [12]Li and his associates.This article will concentrate on security solutions for a number of enabling technologies and the consequences those solutions have on a few distinct applications in order to give a complete examination of the security issues and concerns related to the Internet of Things (IoT) (IoT). The approach and the methodology (the design, the methodology, and the approach) – The methodology and the approach The four-layer framework that is used as a lens to analyse the security demands of the Internet of Things and possible solutions consists of a sensing layer, a network layer, a service layer, and an application layer. This framework is used as a lens since it is comprised of four different layers. After we finish talking about the cross-layer threats, we will move on to an investigation of the safety of the underlying technologies. These supporting technologies include identifying and tracking technologies, wireless sensor

networks and radio frequency identification (RFID), communication, network management, and service management, amongst others. However, this list is not exhaustive and does not include all of these technologies. The findings suggest that a new security framework, one that is based on current technology needs, is necessary for devices that are linked to the Internet of Things. Consequently, brand new security architectures for the Internet of Things (IoT) need to include these modernised conditions in order to be effective. Security is necessary not only on the level of the physical device but also on the level of the service-application in order for the Internet of Things to operate effectively and fulfil its intended purposes. [13] Khattab and the remaining members of the The environment of the information and communication technology business is undergoing a profound transformation as a direct result of the alarmingly rapid growth in the number of smart devices that are capable of running complex applications. This shift is directly attributable to the fact that smart devices are becoming more and more affordable. The Internet of Things (IoT) is gaining popularity and relevance in the everyday activities that modern man partakes in at this point in time. On the other hand, as the Internet of Things develops, the difficulties that it brings with it will become an increasingly significant cause for worry. Creating new applications for the Internet of Things and making sure it stays current with technological advances is becoming an increasingly vital goal. In recent years, machine learning algorithms have been applied into Internet of Things devices in order to maximise the capabilities of these devices. This has been done in order to maximise the capabilities of these devices. In this chapter, we will be discussing how machine learning algorithms may be used to various platforms that are associated with the Internet of Things. [14] J. Caedo and co. The Internet of Things (IoT) refers to a vast collection of individual devices that are connected to one another via the use of a single network. These devices might feature either sensors or actuators, and they could communicate with one another via either wired or wireless networks. Over the last decade, the Internet of Things (IoT) has seen amazing development, and it is expected that more than 25 billion devices will be linked to the network by the year 2020. Over the course of the development of the Internet of Things, security has consistently been ranked among its most vulnerable building blocks. When attempting to implement security in a network that is linked to the Internet of Things, there are a number of problems that must be overcome. Two of these issues are the heterogeneity of the system and the sheer number of devices that must be monitored. The author advocates integrating machine learning into an Internet of Things gateway as a method to improve overall system security and find a solution to the difficulties associated with protecting devices that are linked to the Internet of Things (IoT).

M. Al-Rubaie et al. [15] In order to address privacy issues in machine learning (ML) systems in an appropriate manner, there has to be a narrowing of the knowledge gap that exists between the ML community and the privacy community. This article's goal is to provide a broad overview of the junction of these two fields, with a particular emphasis on the information security techniques that are now in use. [16] R. Shokri in addition to a number of other individuals. Deep learning is a technique that is gaining in popularity for modelling, categorising, and recognising complex data kinds such as photos, audio, and text. This approach is made feasible by artificial intelligence, which is the driving force behind its development. Artificial neural networks, which are instruments for the processing of data and are known for their high level of effectiveness, form the basis of the deep learning methodology. ştiinştiinştiin Deep learning strategies have been more popular in recent years as the basis for a broad range of brand new artificial intelligence (AI) applications that can be accessible over the internet. This is mostly due to the exceptional accuracy that these strategies provide. Companies in the business world that collect vast amounts of user data have reaped the most benefits from this trend since the effectiveness of deep learning techniques is highly connected to the quantity of accessible training data. Due to the fact that deep learning necessitates the collecting of enormous amounts of data, there is a substantial danger posed to the privacy of people as a consequence of this need. Companies that ask their customers to provide information that can be used to personally identify them and that is also considered to be extremely sensitive, such as images and voice recordings, save this data on their systems indefinitely. Examples of this type of information include photographs and audio recordings. It is impossible to erase it, and the user has no influence over how it may be used in the future.[17] Tanuwidjaja, H. C. et al. The exponential development of big data and deep learning has resulted in an increase in the amount of data that is supplied by society, which in turn has led to a rise in the number of data users. The application known as Machine Learning as a Service (MLaaS), which improves decision-making by using deep learning algorithms for predictive analytics in order to do so, has witnessed an increase in the degree of popularity it has received. On the other hand, using MLaaS presents challenges in terms of data privacy for those who are in possession of the data as well as challenges in terms of security for those who are in possession of deep learning models, as will be elaborated upon in more depth below.

Clients are concerned about the safety and confidentiality of their data when it is stored on machine learning platforms, while the owners of these platforms are concerned that competitors will steal their models by posing as customers on these platforms. Customers are concerned about the safety and confidentiality of their data when it is stored on machine learning platforms. As a direct consequence of this fact, a method that has

been given the name Privacy-Preserving Deep Learning (PPDL) has been proposed as a potential answer to the problem. In recent years, a number of articles that examine the use of PPDL for MLaaS have been published in publications that need prior approval from qualified industry experts. On the other hand, to the best of the author's knowledge, no previous study has sought to synthesise the existing research on PPDL and its specific relevance to the MLaaS scenario. This is something that the author believes should be done. The author believes that this is a significant hole in the existing knowledge in the field. Beginning with more conventional approaches and progressing all the way to well-known applications of deep learning and beyond, the authors of this paper provide a comprehensive analysis of solutions that preserve the privacy of users. In addition, a comprehensive description of PPDL is provided, and the paper also contains a discussion over whether or not PPDL should be used for MLaaS. [18] M. Zolanvari, along with a number of other individuals. It has been shown that methods integrating machine learning are suitable for the task of protecting platforms for information technology systems. [Citation needed] [Citation needed] Because of the fundamental differences between traditional information technology networks and the industrial internet of things (IIoT), it is essential to conduct a separate performance evaluation for each type of network. This is because conventional information technology networks are more widely used. It is vital to apply a broad range of risk management techniques in order to comply with the severe rules that are linked with IIoT systems. These systems come with their own set of inherent dangers. The authors of this work investigate the reasons why machine learning need to be included into the security processes of the Internet of Things, in addition to the areas in which it does not deliver sufficient performance. As part of the design process for their experiment, the authors undertake an investigation of the complexity and challenges that develop in the real world that are associated with this subject. In order for the author to provide proof of concept, he built a testbed for the Industrial Internet of Things (IIoT) that is designed to resemble a facility that would be found in a real-world industrial setting. [19] Mohanta, along with the others During the course of the last ten years, the Internet of Things (IoT) has seen expansion at a rate that is close to exponential development. On Earth, the total number of connected smart devices has already surpassed the number of humans currently inhabiting the globe. [Citation needed] These gadgets generate a very significant quantity of data. Users of a variety of applications, such as smart monitoring, healthcare systems, and smart homes, communicate private information with one another via the Internet of Things (IoT). When it comes to the applications of the Internet of Things, ensuring security and protecting users' privacy are two of the most difficult challenges to surmount. Researchers are taking a look at some tried-and-true cryptography and security practises in the hopes of finding a solution to some of the problems that have arisen inside the Internet of Things system. Devices that are linked to the Internet of Things are more susceptible to attacks from the outside world since there are less resources available to support them. The design of applications that use the Internet of Things presents a difficulty that is always there, and that issue is the processing and computation of sensitive data. A potential vulnerability in the Internet of Things (IoT) technology is examined in this piece of writing as a potential threat to network safety. With the assistance of later-discovered machine learning techniques, it is possible that some of the security problems that were found in Internet of Things apps might be rectified. The authors of the research came to the conclusion that using machine learning to improve the security of Internet of Things (IoT) systems and the efficiency with which they handle data might be accomplished via the use of machine learning algorithms. This was one of the conclusions reached by the research.

[20] Ahmad and the others As the Internet of Things (IoT) continues to develop and grow, the number of attacks against IoT applications as well as their frequency and level of complexity are increasing. This systematic literature review (SLR) was created with the intention of offering academics a research resource on current developments in Internet of Things (IoT) security research. The author listed six research concerns related to the security of internet of things devices and machine learning in his SLR article, which served as the motivation for the study. This in-depth analysis of recent research on the topic of Internet of Things security uncovered a number of significant research trends that are going to have a significant impact on the direction of future study in this field. It is vital to create models that integrate cutting-edge big data and machine learning techniques and technologies in light of the growing frequency of large-scale Internet of Things risks in recent years. This is because the frequency of these threats has been rising in recent years. According to the findings of the study, two essential characteristics of quality are the accuracy and effectiveness of the algorithms and models that are used to identify Internet of Things risks in real time or near real time.

Conclusion

This paper evaluates a large number of works on machine learning, and it comes to the conclusion that high-security and high-speed encryption and decryption techniques are necessary. If almost any physical or logical

entity or object can be assigned a unique identification number, and it has the ability to communicate autonomously over the Internet or other similar networks, information security in the Internet of Things refers to the additional safeguards that must be put in place to prevent personal information from being exposed in such an IoT environment.

References

[1] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe and M. Atiquzzaman, "A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems," in IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6092-6102, Sept. 2020, doi: 10.1109/TII.2020.2974555

[2] Chamikara, M.A.P. & Bertok, Peter & Khalil, Ibrahim & Liu, Dongxi & Camtepe, Seyit & Atiquzzaman, Mohammed. (2020). A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Transactions on Industrial Informatics. PP. 1-1. 10.1109/TII.2020.2974555.

[3] Hussain, Fatima & Hussain, Rasheed & Hassan, Syed & Hossain, Ekram. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2020.2986444.

[4] Parikshit N. Mahalle; Poonam N. Railkar, "Identity Management for Internet of Things," in Identity Management for Internet of Things , River Publishers, 2015, pp.i-xx.

[5] F. Restuccia, S. D'Oro and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4829-4842, Dec. 2018, doi: 10.1109/JIOT.2018.2846040.

[6] Niu, Ben & Zhang, Likun & Chen, Yahong & Li, Ang & Du, Wei & Cao, Jin & Li, Fenghua. (2020). A Framework to Preserve User Privacy for Machine Learning as a Service. 1-6. 10.1109/GLOBECOM42002.2020.9322322.

[7] Bagaa, Miloud & Taleb, Tarik & Bernal Bernabe, Jorge & Skarmeta, Antonio. (2020). A Machine Learning Security Framework for IoT Systems. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2996214.

[8] [8] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019, doi: 10.1109/COMST.2019.2896380.

[9] Chaabouni, Nadia & Mosbah, Mohamed & Zemmari, Akka & Sauvignac, Cyrille & Faruki, Parvez. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2019.2896380.

[10] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi 10.1109/COMST.2020.2986444.

[11] O. Salman, I. Elhajj, A. Chehab and A. Kayssi, "Software Defined IoT security framework," 2017 Fourth International Conference on Software Defined Systems (SDS), 2017, pp. 75-80, doi: 10.1109/SDS.2017.7939144.

[12] Li, Shancang & Tryfonas, Theo & Li, Honglei. (2016). The Internet of Things: a security point of view. Internet Research. 26. 337-359. 10.1108/IntR-07-2014-0173.

[13] Khattab, Ahmed & Youssry, Nouran. (2020). Machine Learning for IoT Systems. 10.1007/978-3-030-37468-6_6.

[14] J. Cañedo and A. Skjellum, "Using machine learning to secure IoT systems," 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016, pp. 219-222, doi: 10.1109/PST.2016.7906930.

[15] M. Al-Rubaie and J. M. Chang, "Privacy-Preserving Machine Learning: Threats and Solutions," in IEEE Security & Privacy, vol. 17, no. 2, pp. 49-58, March-April 2019, doi: 10.1109/MSEC.2018.2888775.

[16] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2015, pp. 909-910, doi: 10.1109/ALLERTON.2015.7447103.

[17] H. C. Tanuwidjaja, R. Choi, S. Baek and K. Kim, "Privacy-Preserving Deep Learning on Machine Learning as a Service—a Comprehensive Survey," in IEEE Access, vol. 8, pp. 167425-167447, 2020, doi: 10.1109/ACCESS.2020.3023084.

[18] M. Zolanvari, M. A. Teixeira and R. Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), 2018, pp. 112-117, doi: 10.1109/ISI.2018.8587389.

[19] Mohanta, Bhabendu & Jena, Debasish. (2021). Internet of Things Security Using Machine Learning. 10.1007/978-981-15-5243-4_11.

[20] Ahmad, Rasheed & Alsmadi, Izzat. (2021). Machine Learning Approaches to IoT Security: A Systematic Literature Review. Internet of Things. 14. 100365. 10.1016/j.iot.2021.100365.