ISSN 2347 - 3983
Volume 9. No. 4, April 2021
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter28942021.pdf
https://doi.org/10.30534/ijeter/2021/28942021

A Review Of The Issues And Challenges In IoT Security Using Machine Learning Techniques

Liberty Adams Omonkhoa, DrAbullahi Abdu Ibrahim
Altinbas University, Department of Electrical & Computer Engineering
Mahmutbey, Dilmenler Cd. No:26, 34217 Bağcılar/İstanbul, Turkey
adamsliberty88@gmail.com

Abstract
In a typical IoT network, a sensor connects to a controller using a wireless connection. Controllers collect data from sensors and sends the data for storage and analysis[1]. These controllers work with actuators that translate an electrical input to a physical action. The internet of things (IoT), have found application in different areas of human endeavor including healthcare, government, supply chain, cities, manufacturing, etc. and it is estimated that the number of connected devices will reach 50 billion by 2020[2] With the increasing number of devices comes an increase in the the varying number of security threats to the IoT network [3]. To contain these threats, a secure-by-design approach should be adopted as this will help the IoT devices to anticipate and neutralize the ever changing nature of the threats as against older systems where security was handled as it presents itself [2] This paper x-rays the security challenges in IoT networks and the application of machine learning (Supervised learning, Unsupervised learning and Reinforcement learning) in tackling the security challenges.

Key words: IoT, IoT security challenges, machine learning.

1. INTRODUCTION

The internet of things (IoT) is the interconnection of devices and solutions that enables the connection of millions of devices and sensors to the internet by means of machine-to-machine communication. i.e. without human interference. The configuration of IoT includes devices and sensors, cloud service and the eventual end-user. To gather data, a sensor is incorporated in an object, this happens to be the “Thing “in the IoT acronym [4] The data from the sensor is transferred to a controller via a wireless network. With the help of a controller, actuators convert electrical signal input into a physical action. As an example, actuator helps in opening and shutting the locks on doors. Below is a diagram showing the basic IoT architecture.

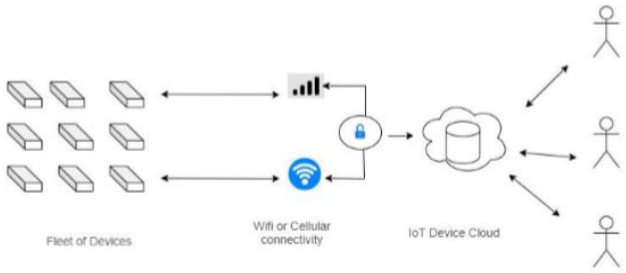

Figure 1: IoT Architecture. Source [4]

Figure 1 shows the basic architecture of an IoT network consisting of a fleet of devices, Wi-Fi or cellular connectivity and the IoT device. The Internet of Things or IoT is no longer a technological promise. The machine-to-machine connection on a large scale is already a reality in more advanced economies and its expansion occurs at an astonishing speed. Data from Horwitz[5] and Cisco Company [6] indicates that IoT will focus on health and safety equipment monitoring in 2021, There will be many companies that supply this *software* and *hardware* in the IoT and the final consumers will be the biggest holders of this type of technology.

IoT is an emerging computing paradigm that integrates the “things” of the real world into the technological world. It is a concept in which our everyday devices and objects are equipped with sensors capable of communicating with each other intelligently without the need for explicit human intervention. A “thing”, in the context of IoT, is a connected object that can be, for example, a person with a heart monitor, an industrial tank with level sensors, a car with sensors that warn tire pressure, a light bulb, public lighting of a city, a home outlet, or any other natural or man-made object.

There are many advantages and opportunities that the IoT can offer, however, there is a point that still raises many doubts and concerns both suppliers and consumers: how will the security and privacy of the data be guaranteed?

In a report published by HP [7], 70 % of IoT devices have serious security flaws and are quite susceptible to unauthorized attacks. About 80% of the devices raised privacy concerns. This large percentage is due to the fact

that the devices collect some type of personal information, such as name, address, date of birth, health information and even credit card numbers, being even more worrying because these devices are based on applications mobile or cloud services. The study (Figure 2) analysed the ten most common types of IoT devices, including televisions, webcams, home alarms, home thermostats, among others, all connected to some type of cloud computing, as well as mobile applications that allow their remote control. An average of 25 vulnerabilities were found on each device, totalling 250 vulnerabilities. In total, there are privacy flaws, lack of information transport encryption, insecure Web interface, insufficient authorization, insecure firmware authorization mechanisms and inadequate software protection.

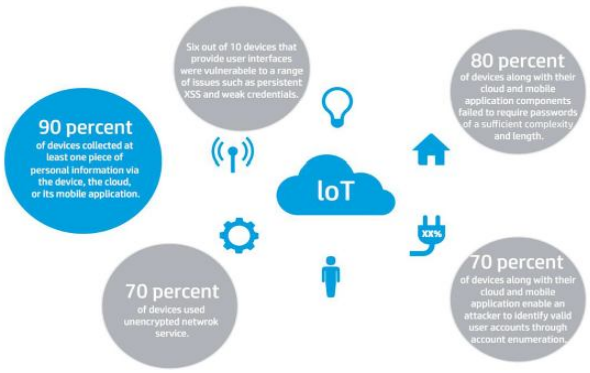

Figure 2: Results of the HP study on IoT. Source[7]

That said, IoT vendor organizations need to substantially improve their security policies and barriers, so that consumers feel that their personal data is secure, and that they only benefit from using IoT.

For Alecrim (2016), the IoT industry needs to define and follow criteria that guarantee the availability of services (including rapid recovery in cases of failures or attacks), protection of communications (which, in corporate applications, must include strict protocols and audit processes), setting standards for data privacy and confidentiality (no one can access data without proper authorization), integrity (ensuring that data will not be unduly modified), among others. Considering all these aspects is far from a trivial task. In addition to the technological challenges themselves, the industry needs to address each point taking into account global conventions and the legislation of each country. Several market segments already deal with such issues, but this is a work in constant development.

Faced with this reality, HP decided to create the project [8] (*Open Web Application Security Project*), a non-profit and internationally recognized entity that contributes to improving the security of IoT device *software*, gathering important information that allows assess security risks and combat forms of attacks over the internet.

1.1 Issues and Challenges

IoT is an increasingly present future. As a result of the connection between devices, IoT can make people's lives more comfortable and rational. However, in spite of all the benefits that IoT can bring, it still shows a great concern on the part of its users: How will the security and privacy of the data be guaranteed? This is probably the most difficult challenge for IoT.

Suddenly, everything from refrigerators to doors is connected, and while these devices make life easier and people's time management much more effective, they also create new attack vectors for *hackers*. Day-to-day devices and the connection between them will become even more common than *Smartphones* are today, and will have access to very sensitive personal data, such as credit cards or personal identification numbers. As the number of IoTdevices increases, so do concerns about data privacy and security.

According to a survey by Thomson [9], 20 % of mobile applications used to control IoT devices do not have data encryption. In addition, none of the applications that have been analysed have mutual authentication between the client and the server, which poses great risks to the user.

The [9] report tested 15 *interfaces*. Of these, 10 showed vulnerabilities that could, among other situations, allow an attacker to remotely unlock the user's home. For Symantec, *hackers* who gain access to the home network, for example, breaking into a weakly encrypted *Wi-Fi* connection, have more attack vectors at their disposal.

For Hernández [10], many other serious situations can occur due to the lack of privacy and security that the IoT presents. An example of the need for security and data privacy in the IoT happens in *Smart homes*, or *smart houses*: A network of sensors for domestic lights, if read by *hackers* can inform some personal aspects of the lives of the people who live in that house. Information such as how often a room is occupied, times when people are at home and when the house is empty. Temperature sensors can create an identical mapping of personal life by informing the time when a person usually takes a shower. The very nature of these devices makes them vulnerable.

Hernandéz[10] also states that IoT devices do not have the security features of traditional information technology (IT) equipment (servers, routers, etc.). The deoxyribonucleic acid (DNA) of current IoT devices is linked to a critical factor: it is essential to guarantee a competitive and low cost for products that are, after all, for the mass market. This is a challenge, as the information generated by the IoT is essential to bring better services and better management of the devices.

There has been vast application of IoT to improve various spheres of our human life due to the ever growing advancement in IoT technology and computing. IoT like other systems however comes with its issues some of which include those of connectivity due to limited coverage in most places and non-uniformity of technologies. There is also the issue of compatibility and interoperability between sensors and devices. Another common issue is that of integration

between products and IoT platforms. However, the most disturbing of all these challenges is that of security because [5] the huge amount of user data that IoT handles makes its users prone to risks in the event of a breach [5] [4] More worrisome is the fact that IoT devices can be remotely controlled across the network [2] and as such, users data are vulnerable when designs are not sophisticated [4].

Analysing the Nature & Types of Security Threats InIoT

As earlier stated, IoT is basically divided in three layers viz: *Perception layer, Network layer and application layer.* In order to fully understand the scope of the security threats in IoT, it is vital to study these threats in their different domains of the IoT. In a broad sense, these issues can be classified as low level, intermediate level and high level. We will understudy them in the table below:

As earlier stated, IoT is basically divided in three layers viz: Perception layer, Network layer and application layer. In order to fully understand the scope of the security threats in IoT, it is vital to study these threats in their different domains of the IoT. In a broad sense,

these issues can be classified as low level, intermediate level and high level.

The attacks at the low level are usually in the form of jamming attacks(DoS) which operates by attempting to obstruct traffic on the network by continuously sending RF signal to interrupt the traffic. There is also the insecure initialization, low level Sybil attack, which is common in the peer-to-peer networks and attacks the Sybil nodes by intercepting data meant for it. There is also the spoofing attack which is present in the link layer and finally the sleep deprivation attack. At the intermediate level there are attacks in the pattern of fragmentation caused by replay, this modifies the data between the sender and the destination node by tweaking the datagram receipt. There is also the buffer reservation attack that occupies space in the receiving node thereby making the target node to discard useful packages. Insecure neighbour discovery is another common attack, this duplicates address info and poses as a legitimate route. There is the sink-hole and black-hole attack, wormhole and rushing attack, RPL routing attack, Sybil attacks and verification secure communication.

2. THE IDEA OF MACHINE LEARNING

"Machine learning is an effective approach to find hidden insight through iteratively learning from data without being explicitly programmed" [8]. It involves making the computer learn algorithms and improve on them over time in a self-determining way. This is accomplished after the computer detects a pattern from a huge chunk of data it has studied then it learns from it and can possibly make predictions about what it has learnt. Machine learning can be classified into three types viz- supervised learning, unsupervised learning and reinforcement learning as seen in figure (3)

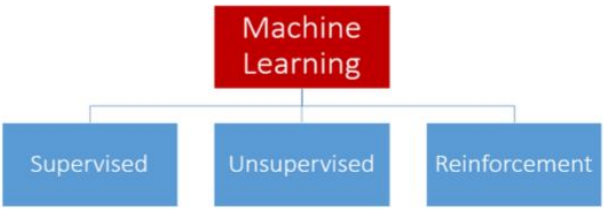

Figure 3:Classification of machine learning. Source [4]

In *supervised learning*, the algorithm is trained on labelled data with the input and output clearly labelled. Data is not labelled in *unsupervised learning*. However, patterns in the database are studied and the machine learns from them. Reinforcement learning in recent times have been touted as the most popular type of machine learning. This is so because it learns and improves on itself using a trial and error pattern, it reinforces and encourages useful outputs thereby making the system more efficient.

Machine learning has a wide range of application across various disciplines including but not limited to cognitive science and artificial intelligence. Machine learning techniques are mostly used in situations with limited human expertise, robotics is a good example, It is also very useful in situations where the threats or problems is dynamic in nature hence it can learn and make informed decisions to tackle the threats. Google for example utilizes machine learning algorithms in its security framework to monitor threats in android applications and mobile endpoint.

With the increasing deployment of IoT and the huge amount of data that it handles, it is impracticable to rely on traditional means of securing the network where security is mostly considered after design. Figure4 illustrates the threat model in IoT) Hence, machine learning techniques are best suited to enable IoT systems make intelligent decisions in key areas of privacy attack detection, security and malware detection.Figure4 illustrates the threat model in IoT.

Machine learning techniques are applied in areas like authentication, access control, secure off-loading and malware detection to improve network security.

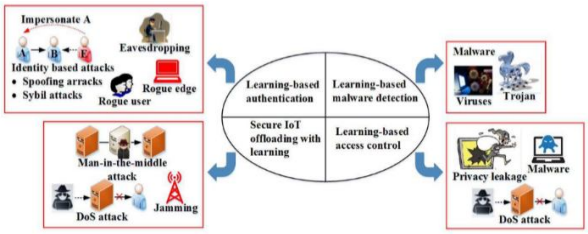

Fig. 4 Illustration of the threat model in Internet of Things. Source [12]

Machine Learning Based IoT Authentication: Limitations with IoT devices (including battery, limited computation and memory resources) makes it difficult to apply long-established authentication methods in checking identity based attacked such as spoofing and sybil attacks. [12]

However, PHY-layer authentication could be deployed to create hypothesis to liken the PHY feature of the data that is being tested. IoT authentication assumes a Markov Decision Process(MDP)therefore it can apply reinforcement methods to determine the test threshold which is an important authentication variable. It can achieve this without being aware of the network model. [12]

Access Control: With multiple data sources and nodes in IoT networks, it is usually difficult to design access control that can optimally handle the heterogeneity. [12]. However, some machine learning methods like SVM, K-NN and neural that are able to extract geometric correlations from the signals in the network can be used to detect a DoS attack. [12]

Secure IoT Off-loading with Learning: The IoT device isn't dependent on the off-loading or actions of the previous state to address actions in the present time interval. Reinforcement techniques which assume the Markov Decision Process can be applied to enhance the of-loading scheme in the ever changing environment. This can be used to address attacks such as jamming, man-in-the-middle, eavesdropping and similar attacks that are usually found in the PHY layer. [12]

Learning Based IoT Malware Detection: To build malware detection schemes, IoT uses supervised learning methods like K-NN and random forest classifiers, these could analyse the runtime characteristics of applications. [12]

3.CONCLUSION

This paper has been able to identify and analyse the nature and scope of the security threats in IoT in their different domains and how some IoT vendors are addressing the issues of privacy and security barriers on their devices.
The application of Machine learning in solving these issues was discussed extensively and it is hoped that further research will be made in the area of comparison in the approach of IoT vendors as regards data privacy in their products with the view of analysts and consultants for the same topic.

REFERENCES

[1] B. J. S. G. P. H. A. M. A.-M. GODFREY ANUGA AKPAKWU, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," in *IEEE Access*, South Africa, Nigeria, 2018.

[2] S. D. T. M. Francesco Restuccia, "Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking," *IEEE INTERNET OF THINGS JOURNAL*, vol. 1, no. 1, p. 14, 2018.

[3] R. R. P. J. Kazi Masum Sadique*, "Towards Security on Internet of Things: Applications and Challenges in Technology," in *The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks*, Stockholm, 2018.

[4] N. S. G. Amit Sagu, "Machine Learning Techniques for Securing IoT Environment," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* , vol. 9, no. 4, p. 6, 2020.

[5] L. Horwitz, "IoT Trends 2012:A focus on fundamentals, Not NIce-to-Haves," 2012.

[6] N. Gagliordi, "IoT to drive growth in connected devices through 2022," https://www.zdnet.com/article/iot-to-drive-growth-in-connected-devices-through-2022-cisco/., 2018.

[7] HP, "Hp study rveals 70 percent of internet of things devices vulnerable to attack," https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.YA1dvOhKjIU., 2014 (Cited 2021).

[8] OWASP, "Welcome to OWASP," https://www.owasp.org/index.php/Main_Page, 22016 (Cited 24th January 2021).

[9] D. Thompson, "State of Privacy rport," https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf. , 2015 (Accessed on MArch 18, 2016).

[10] R. Hernandez, "F-Secure - INternet of Things Promises many Benefits, but Privacy is Still a Point of Concern," http://www.consultcorp.com.br/noticias/126-f-secure-internet-das-coisas-promete-muitos-beneficios-mas-privacidade-ainda-e-um-ponto-a-se-preocupa., 2015 (Cited 2021 24th January).

[11] S. R. Himanshi Babbar, "Integration of WSN and IoT for smart cities," *EAI/Springer Innovations in Communication*, p. 211, 13 August 2020.

[12] X. W. X. L. Z. D. W. Liang Xiao∗†, "IoT Security Techniques Based on Machine Learning," in *Dept. of Communication Engineering, Xiamen University, Xiamen, China. Email: lxiao@xmu.edu.cn , National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, WINLAB, Rutgers University, North Brunswick, NJ, USA. Email: yyzhang@*, China, 2018.

[13] M. R. K. Shridevi Jeevan Kamble a*, "Machine Learning Approach on Traffic Congestion Monitoring System in Internet of Vehicles," in *Machine Learning Approach on Traffic Congestion Monitoring*, India, 2020.