Universe International Journal of Interdisciplinary Research
(Peer Reviewed Refereed Journal)

© UIJIR | ISSN (O) – 2582-6417
DECEMBER 2022 | Vol. 3 Issue 7
www.uijir.com

APPLICATIONS OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THE SECURITY OF IOT DEVICES

Author's name: [1]Ashadul Haque, [2] Debajit Sensarma

Affiliation: [1]Assistant Professor, Dept. of Computer Science, Vivekananda Mission Mahavidyalaya, West Bengal, India

[2]Assistant Professor, Dept. of Computer Science, Vivekananda Mission Mahavidyalaya, West Bengal, India

DOI No. – **08.2020-25662434**

Abstract

Any device connected to the internet is called the Internet of Things (IoT). There are more than 20 billion IoT devices present in 2021 and it is expected to increase to 50 billion in 2050. IoT devices have a tremendous effect in various fields like automated devices, medical care, agriculture, traffic system, smart cities, finance, manufacturing and many more. It is very challenging to secure IoT devices from intruders, vulnerable attacks etc as IoT devices have different sizes, power consumption, hardware, software, and configuration and may have operated in real-time or dynamic in nature. In this paper, the authors discuss different parts of IoT devices, the challenges to securing IoT devices and how Artificial Intelligence or Machine Learning (AI/ML) help t secure IoT devices. The authors also discuss related work to secure IoT devices.

Keywords: *IoT, security, AI, ML, Classification*

INTRODUCTION

The Internet helps us to share information or talk to people miles away. IoT helps to improve or automate and increases performance in agriculture, finance, manufacturing, medical care, emergency services, traffic system, gas supply, fire protection, electricity etc. The application of the internet is now changing rapidly using Artificial Intelligence (AI) and Machine Learning (ML). Internet of thing (IoT) is one of them where machines or devices gather information using sensors then process the information and perform some action using actuators. There are few examples of sensors are given below:

- Accelerometer: Movement of IoT devices measure using Accelerometer.
- Magnetometer: Detect magnetic fields
- Gyroscope: Changes occur IoT device's orientation.

Examples of actuators are given below:

- Mechanical actuator
- Pneumatic actuators use to control air pressure
- Hydraulic actuators use to control fluid pressure
- Electrical actuator

IoT helps to automate devices, predict trends, connect the unconnected, smart cities, manage resources efficiently etc. AI and ML can also help to defend the security of Internet of Things (IoT) devices from continuous attacks from cyber. Traditional security system becomes a failure in front of more advanced and sophisticated hacker as they keep improving and building new methods to hack the different system. It is estimated that nearly 20.4 billion devices with internet connectivity are there in 2021, out of which 7.5 billion devices are to be used by different organizations. It is also expected that in 2025 there will be 50 billion devices with internet connectivity. IoT devices are revolutionizing our life and society in many ways. It has effects from social networks to healthcare, consumer electronics devices, transport and many

more. AI and ML can help the system minimize security breaches and increase its efficiency of the system.

CHALLENGES IN IOT SECURITY

There are many challenges in IoT Security. They are

- There are already 20.4 billion devices with internet connectivity and it is expected to grow exponentially.
- IoT devices are mostly operated in real-time and are dynamic in nature as connected to the internet.
- IoT devices are coming in different sizes, configurations, costs, power consumption, hardware and software.
- Personal information is required in many IoT devices. There is much information stored like contact numbers, personal pictures, communication with others, fingerprint, bank details etc. It can be easily accessible by some intruders as many devices don't have proper protection. So, this data has to be secure from an intruder or unauthorized persons.
- Many IoT devices don't have enough storage or power consumption to run security solution software or threat detection signature.

IMPACT OF ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

AI/ ML help to

- Adapt IoT devices to change their configuration in a dynamic and real-time environment to secure the devices.
- Bio-metric, facial, handwritten or finger-print based ML authentication help to secure IoT device from an intruder or unauthorized person.
- As many IoT devices have limited storage or power consumption, ML helps to secure IoT devices through a lightweight end-point protection system.
- As AI/ML help to predict different threat based on previous data or experiences without human interaction and take action accordingly. So, it helps the company to save lots of money by hiring a huge number of security experts.
- Self-healing of IoT devices, machines or any kind of node or grid in a network is an active research area where AI or ML can take a huge role.
- IoT device store our personal data, search history, and various other activities. AI can secure data from malicious programs and unauthorised users.
- IoT devices connected to the internet have various software installed in them and some software may be malicious or affected by some malicious software. AI/ML can help to detect this malicious software.

First, for a machine learning model, samples are used to train and test a model and gave some accuracy based on model performance. For a Covid patient identification model, CT scan data are used to train and test the model and a covid patient is positive or negative classified based on the doctor's input of the patient's CT scans.

RELATED WORK

home where different appliances Nagaraja Seshadri et al. [1] briefly describe a smart like fans, CCTV, air conditioning, lights, power, water supply, geysers, door, cars, or garages are remotely monitored using a smartphone application.

IoT devices become a part of our daily lives. Medical IoT devices help to identify Covid using patients' CT

scans and X-ray images. IoT devices also help to measure body temperature using a thermal camera, social distance identification using face detection method etc. At the time of Covid-19, we see healthcare employees use IoT devices using the DL algorithm to track covid patients as it spreads rapidly due to contact with another covid patient. Md. Abdur Rahman et. al. [2] built six applications of the DL model to identify wear a mask or not using live camera feed, maintain DL-based QR codes as immunization certificates, classified COVID patients based on their CT Scan or X-ray images etc.

It is very difficult to secure the data from an intruder at times of interaction between devices as the Internet of Things connects billions of devices and shares a large amount of data without human supervision. There are various Encryption Algorithms present but it is very difficult to find the best algorithm for a specific application. Arslan Shafique et. al. present a novel technique to select the best Encryption algorithm using pattern recognition and machine learning techniques[3].

Industrial Control System (ICS) helps to supervise and monitor industrial critical systems. Industrial Internet of Things (IIoT) is to take advantage of the Internet of Things (IoT) system and the Inclusion of IoT in ICS help enhance the system to collect real-time data, interact between devices, analysis of the data and network intelligence etc. Maede Zolanvari et. al. [4] present common IIoT protocols to secure the system and also present their associated vulnerabilities. In [4], the author runs a machine-learning algorithm to counter different vulnerabilities.

It is a challenge to built an IoT device with highly efficient, reliable, secure and also consume less power. Muhammad Shafique et al. discuss the emerging trend to design highly efficient, reliable, secure, scalable IoT devices using machine learning [5]. In [5], the authors also discuss the challenges faced to build scalable, reliable, efficient IoT devices.

Sometimes Cloud Computing environment needed to store the data and process the data which is generated from IoT devices. AI or ML is used to analyse the store data and processed data. Temechu G. Zewdie et. al. proposed a hybrid detection model using AI or ML to combat and mitigate vulnerability and security issues in cloud-based IoT devices [6].

In [7] the authors look at how machine learning methods could improve the security of IoT devices. They concentrate on the use of reinforcement learning, supervised and unsupervised learning techniques, and host-based and network-based security solutions in the IoT context. Finally, they go over some of the issues that need to be resolved in order to use machine learning techniques successfully and improve IoT device security.

The study in [8] suggests using the Internet of Things with an Artificial Intelligence System (IoT-AIS) to secure the delivery of healthcare. IoT technology is used to construct wireless sensor networks. The IoT network connects the digital and physical worlds. IoT-AIS is used to encrypt and monitor patient data. To keep the patient data current and allow for distant access, the encrypted data are kept on the cloud. Individual patients can keep their information independently with single-user access using the IoT-AIS dashboard's personalised user interface. The simulation study in the proposed research demonstrated that the patient record for medical treatment might be encrypted and offer customised access. When compared to other techniques, the experimental results of IoT-AIS show the highest data transmission rate of 98.14%, the highest delivery rate of (98.90%), a long period of standard responses (93.79%), less delay estimation (10.76%), improved throughput (98.23%), effective bandwidth monitoring (83.14%), low energy usage (8.56%), and the highest performance rate (98.4%).

Cloud-based machine learning models make it possible for devices with limited resources to connect and improve performance. Instead of decreasing dangers to privacy and security, the new data gathering and gadget designs aim to save energy. As a result, security and privacy issues still exist since intelligent city networks do more than only gather data from vulnerable heterogeneous nodes. The authors of [9] discuss security concerns in applications for smart cities and the accompanying solutions utilising AI and machine learning. Then, several solutions for smart energy, smart transportation, and smart health are provided in an effort to overcome these protection and privacy issues.

In [10], several classification models, notably logistic regression, artificial neural networks, decision trees, K-nearest neighbors, and random forest, are implemented to predict accident severity. All models have been validated and experimental results show that these classification models achieved considerable accuracy. The paper also described a secure communication architecture model for securely exchanging information between all ITS-connected components. Finally, a web-based paper message alert system was implemented. It is used to alert users via smart IoT devices.

CONCLUSION

Internet of Things (IoT) devices are being widely integrated and deployed within organizations because of the promise that more data leads to better decisions. However, such devices are rarely implemented with security concerns in mind. Moreover, even when such measures are implemented, there are clear limitations to the rules and signatures that can be used to identify potential adversaries. In this article, we examined some existing work looking at securing his IoT using artificial intelligence and machine learning techniques. We also highlighted the capabilities and limitations of machine learning algorithms due to the unique characteristics of IoT devices and their environments.

REFERENCES

1. Nagaraja Seshadri, Sivakumar Dhakshinamoorthy. Internet of things (IoT) and Security. Vol. 8, Issue 15, *NCAIT-2020 Conference Proceedings, International Journal of Engineering Research & Technology (IJERT)*.
2. Rahman, A., Hossain, M. S., Alrajeh, N. A., & Alsolami, F. (2020). Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices. *IEEE Internet of Things Journal*, *8*(12), 9603-9610..
3. Shafique, A., Mehmood, A., Alawida, M., Khan, A. N., & Khan, A. U. R. (2022). A novel machine learning technique for selecting suitable image encryption algorithms for IoT applications. *Wireless Communications and Mobile Computing*, *2022*.
4. Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), 6822-6834.
5. Shafique, M., Theocharides, T., Bouganis, C. S., Hanif, M. A., Khalid, F., Hafiz, R., & Rehman, S. (2018, March). An overview of next-generation architectures for machine learning: Roadmap, opportunities and challenges in the IoT era. In *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 827-832). IEEE.
6. EMERGING CYBER THREATS IN CLOUD COMPUTING ENVIRONMENT. *Issues in Information Systems*, *21*(4).
7. Zeadally, S., & Tsikerdekis, M. (2020). Securing Internet of Things (IoT) with machine learning. *International Journal of Communication Systems*, *33*(1), e4169.
8. Ghazal, T. M. (2021). Internet of things with artificial intelligence for health care security. *Arabian*

Journal for Science and Engineering.

9. Ahmed, S., Hossain, M., Kaiser, M. S., Noor, M. B. T., Mahmud, M., & Chakraborty, C. (2021). Artificial intelligence and machine learning for ensuring security in smart cities. In *Data-driven mining, learning and analytics for secured smart cities* (pp. 23-47). Springer, Cham.
10. Mohanta, B. K., Jena, D., Mohapatra, N., Ramasubbareddy, S., & Rawal, B. S. (2022). Macinhe learning based accident prediction in secure iot enable transportation system. *Journal of Intelligent & Fuzzy Systems*, *42*(2), 713-725.