Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778474

A CERTAINTY ON AI AND ML ALGORITHMS AS PREVENTIVE MEASURES FOR CYBER ATTACKS ON THE INTERNET OF THINGS

***Asha M., and Sheetalrani R Kawale**
Department of Computer Science, Karnataka State Akkamahadevi Women`s University, Vijayapura - 586108, Karnataka, India
*Corresponding author: **Asha M.,** Email: ashamugati@gmail.com

ABSTARCT
The fourth industrial revolution (Industry 4.0), which began in recent years, is marked by the exponential growth of the Internet of Things (IoTs), fog computing, computer security, and cyberattacks. IoT networks and devices are rapidly evolving, producing massive volumes of data that require rigorous authentication and security. One of the most promising approaches for combating cybersecurity risks and providing security is machine learning and artificial intelligence (AI). We categorise, map, and survey the available literature on ML and AI technologies used to detect cybersecurity assaults in the IoT context in this work. This is known as a systematic literature review (SLR).This SLR's scope covers a thorough analysis of the majority of ML and AI trending methodologies in cybersecurity and cutting-edge solutions. The usefulness of machine learning (ML) techniques employed in IoT security and their application to attack detection have been examined in this research. To address the current security and privacy issues, various research have suggested using intelligent architectural frameworks and smart intrusion detection systems (IDS) with AI.

Keywords: internet of things; artificial intelligence; machine learning; Artificial intelligence; cybersecurity; cyberattacks

INTRODUCTION

IoT is viewed as a distributed, interconnected network of embedded systems that communicate via wired or wireless methods [1]. It can also be described as a network of physical objects or things that are embedded with electronics (like sensors and actuators), software, and network connectivity that allow them to gather, occasionally process, and exchange data. These objects also have limited computation, storage, and communication capabilities.The term "things" refers to a variety of everyday items from smart home appliances like smart bulbs, smart adapters, smart metres, smart refrigerators, smart ovens, air conditioners, temperature sensors, smoke detectors, and IP cameras to more advanced gadgets like Radio Frequency IDentification (RFID) devices, heartbeat detectors, accelerometers, parking lot sensors, and a variety of other sensors in cars, among others [2]. The IoT offers a wide range of services and applications, including those for critical infrastructure, agriculture, the military, household appliances, and personal healthcare [3].The term "things" refers to a variety of everyday items from smart home appliances like smart bulbs, smart adapters, smart metres, smart refrigerators, smart ovens, air conditioners, temperature sensors, smoke detectors, and IP cameras to more advanced gadgets like Radio Frequency IDentification (RFID) devices, heartbeat detectors, accelerometers, parking lot sensors, and a variety of other sensors in cars, among others [2]. The IoT offers a wide range of services and applications, including those for critical infrastructure, agriculture, the military, household appliances, and personal healthcare

[3[However, user happiness and the assurance of security and privacy are the cornerstones of the commercialization of IoT technology. The threat environment for attackers is significantly expanded by IoT's use of enabling technologies like Software Defined Networking (SDN), Cloud Computing (CC), and fog computing.

Because the amount of data generated by IoT devices is so large, conventional methods for data collecting, storage, and processing could not be effective in this situation. The sheer volume of data can also be used to identify trends, behaviours, make predictions, and perform assessments. The heterogeneity of the data created by IoT also opens up a new avenue for the methods used today to process data. New processes are therefore required to fully utilise the value of the data supplied by the IoT. Machine Learning (ML) is regarded as one of the computational paradigms that is best suited in this situation to provide embedded intelligence in the IoT devices [4].ML can assist intelligent machines and devices in drawing conclusions about the world that are beneficial. It may also be described as a smart device's capacity to alter or automate a circumstance or behaviour based on knowledge, which is seen as a crucial component of an IoT solution[5]. In applications including classification, regression, and density estimation, ML approaches have been applied. ML algorithms and techniques are used in a wide range of applications, including computer vision, fraud detection, bioinformatics, virus detection, authentication, and speech recognition. IoT can also use ML to provide intelligent services in a similar way. But in this research, we emphasise how ML may be used to give IoT networks security and privacy services[6].

Characteristics of IoT Networks:

In the following we discuss some unique characteristics of IoT networks.

Heterogeneity: In an IoT network, a wide range of various devices that have various capabilities, traits, and communication protocols interact with one another. To put it more precisely, the devices may employ various standards, communication paradigms (such as cellular or Ethernet), and hardware resource limits.

Massive scale deployment: According to speculation, the capabilities of the current Internet will likely be surpassed by the billions of gadgets connected to it and each other online. IoT deployment on a grand scale is not without its difficulties. The design of smart device networking and storage architecture, effective data transfer protocols, proactive detection and defence of IoT from malicious assaults, standardisation of technologies, and device and application interfaces are a few of these problems [7], [8]. etc.

Inter-connectivity: IoT devices are anticipated to be linked to the world's information and communication infrastructure and accessible at all times and from any location. The type of service and application offered by the IoT service provider determines the connectivity (s). The connectivity may be local in some circumstances (such as with connected automobile technology or a swarm of sensors) but global in others, such as with access to smart homes via mobile infrastructure and critical infrastructure management.

Communication in close proximity: Another noteworthy aspect of IoT is the ability to communicate locally without using base stations or other central authority. Device-to-Device (D2D) communication makes use of the advantages of point-to-point technologies like Dedicated Short Range Communication (DSRC) and comparable ones. The architecture of the conventional Internet is primarily geared toward network-centric communication, but recently,

networks and services have been decoupled to also enable device- and content-centric connection, enhancing the range of IoT services.

Ultra-Reliable and Low Latency Communication (URLLC): In crucial real-time applications like industrial process automation, remote surgery, and intelligent traffic transport systems, where delay and dependability are the two main performance constraints, this characteristic of IoT networks is necessary.

Low-power and low-cost communication: Massive IoT device connectivity necessitates ultra low-power and affordable solutions for effective network operations.

Self-organization and self-healing characteristics: For urgent and modern IoT communication, including in emergency or disaster scenarios, these are necessary. Because relying on the network infrastructure in these circumstances is not an option, self-organizing networks should be implemented.

Dynamic changes in the network: IoT comprises of a vast array of devices that must be efficiently controlled. These devices will function dynamically; for instance, the application will determine when a device goes to sleep or wakes up, when it uses the internet and when it communicates directly, and so on. The IoT networks must also take these qualities into account.

Safety: In addition to other qualities, safety is crucial for the efficient operation of IoT networks. Due to the enormous number of IoT devices connected to the Internet, there is concern for both consumer and device safety. This is because these devices may put the personal data shared through them at risk. Furthermore, a crucial element is the device's security and privacy.

Intelligence: The intelligence that enables swift and well-informed decision-making is one of the most exciting features of IoT. IoT device data should be processed such that it can really be understood and that actions can be taken as a result of decisions based on the processed data.

Security Challenges in IoT Deployment

Two of the most important elements in the commercialization of IoT services and apps are security and privacy. The current Internet is a seductive playground for security attacks, from straightforward hacks to corporate-level, well-coordinated security breaches that have negatively impacted a variety of industries, including commerce and health care. For the security of both apps and devices, IoT device limits and the environment they operate in present new difficulties. To date, security and privacy issues have been extensively researched in the IoT domain from different perspectives such as communication security, data security, privacy, architectural security, identity management, malware analysis, and so on [10,11,12].

Gaps in the Existing Security Solution for IoT Networks

It's crucial to examine the causes of the security and privacy problems if the Internet of Things is to be implemented successfully. It is crucial to understand whether the security concerns in IoT are new or a rehash of the inheritance from the old technologies because the name IoT has been specifically discarded from the existing technologies. Fernandes et al. concentrated on the similarities and contrasts between the security challenges in traditional IT devices and the Internet of Things. They also concentrated on privacy-related problems. Software, hardware, networks, and applications are the primary motivating elements in comparisons of similarities and differences. These classifications show that there are significant parallels between typical IT security challenges and IoT security issues. The IoT's main problem, however, is with the resource limitations that prevent the application of advanced security solutions that are already

on the market in IoT networks. Furthermore, cross-layer architecture and optimised algorithms are needed to address the security and privacy problems in IoT. For example, IoT devices may require a new breed of optimised cryptography and other algorithms to handle security and privacy due to computing limits. On the other side, the sheer volume of IoT devices presents new difficulties for the security protocols.

The majority of security issues are complex, making discrete solutions impossible. For instance, there is a chance that false positives will occur while dealing with security issues like DDoS or infiltration, making the remedies useless against these attacks. Additionally, it will erode consumer confidence, diminishing the efficacy of these solutions. In order to handle security issues in IoT, a comprehensive security and privacy approach will draw on both existing security solutions and the creation of new intelligent, reliable, evolutionary, and scalable methods.

Machine Learning: A Solution to IoT Security Challenges

Machine learning is the term for intelligent techniques that employ example data or prior experiences to maximise performance criteria. More specifically, ML algorithms use mathematical approaches on big data sets to create models of behaviours. For smart devices, ML also makes it possible for them to learn without explicit programming. Based on the recently added data, future projections are made using these models as a foundation. ML is interdisciplinary by nature and draws inspiration from many branches of research and engineering, including, but not limited to, cognitive science, information theory, optimization theory, and artificial intelligence.

When human expertise is either lacking or unable to be applied, such as when traversing a hazardous environment or when robots, speech recognition, etc., machine learning is used. It is also used when the course of solving a particular issue varies over time (routing in a computer network or finding malicious code in a software or application). Additionally, it is employed in real-world intelligent systems. For instance, Google employs ML to assess dangers to Android-based mobile endpoints and applications. Additionally, it is utilised to locate and get rid of malware from infected mobile devices. Similarly, Amazon has introduced a tool called Macie that sorts and categorises data saved in its cloud storage service using machine learning. There is a danger of false positives and genuine negatives even though ML approaches excel in many domains. Therefore, if an incorrect prediction is made, ML approaches require coaching and model adjustment. The model can decide the prediction accuracy on its own in Deep Learning (DL), a new breed of ML. Self-service DL models are better suited for classification and prediction tasks in creative IoT applications with contextual and tailored support because to their self-service nature. The massive scale deployment of IoT, however, advocates for intelligent, robust, and reliable techniques. Traditional approaches are still frequently used for various IoT aspects (e.g., applications, services, architectures, protocols, data aggregation, resource allocation, clustering, and analytics). This includes security. To this aim, ML and DL are promising techniques for IoT networks for a number of reasons, including the vast volume of data produced by IoT networks, which ML and DL approaches need in order to add intelligence to the systems. Additionally, the ML and DL algorithms enable IoT systems to make wise and educated judgements, maximising the utility of the data supplied by the IoT. Security, privacy, attack detection, and malware analysis are major uses for ML and DL.

The implementation of new applications and services that take into account real-time interactions between people, smart devices, and the physical environment can be made possible by the employment of DL techniques in IoT devices to carry out complicated sensing and recognition tasks.

Some of the security related real-world applications of ML are as follows:

- Face recognition for forensics: pose, lighting, occlusion (glasses, beard), make-up, hair style, etc.
- Character recognition for security encryption: different handwriting styles.
- Malicious code identification: identifying malicious code in applications and software.
- Distributed Denial of Service (DDoS) detection: detecting DDoS attacks on infrastructure through behaviour analysis. Using ML and DL techniques in IoT applications on the other hand bring along new challenges.

These difficulties come in many forms. For instance, creating a model that is appropriate for processing data from various IoT applications is difficult. Effective input data labelling is also a time-consuming operation. Using little marked data in the learning process presents another difficulty. Other difficulties are caused by the deployment of these models on IoT devices with limited resources, where it is crucial to minimise the processing and storage overhead. Similar to this, real-time applications and essential infrastructure cannot survive the abnormalities brought about by ML or DL algorithms. In the aforementioned scenario, it is crucial to thoroughly examine the IoT security solutions that make use of ML and DL.

What Are the Available Practices to Reduce Cyber security Attacks for IoT Using AI Approaches?

We discovered that numerous AI strategies have been put forth by researchers as ways to address and lessen cyber security threats on IoT systems. Intelligent architecture frameworks, anomaly detection techniques, and smart intrusion detection systems are some of the available approaches. By creating new autonomous DL classification systems utilising CNN, an effective DL-based classification and approach has been applied to find cyber-attacks in IoT network traffic. AI-based data encryption improves IoT networks' intermediary nodes. Additionally, AI techniques investigate the extraction of IoT data characteristics and offer feature extractions for smart city intrusion detection systems based on deep migration learning models. The present AI methods do, however, have several drawbacks, including lengthy training times brought on by enormous input datasets and significant computing complexity. Additionally, we recommend combining models for improved performance and high detection strategies to increase the efficiency of AI models.

Artificial Intelligence Roadmap In this section, we provide an AI roadmap with brief overview of its development in detecting cyber security attacks within IoT systems. The methods have been categorized based on the cyber security threats they identify such as Probe, U2R, R2L

and DoS as shown in the below Figure

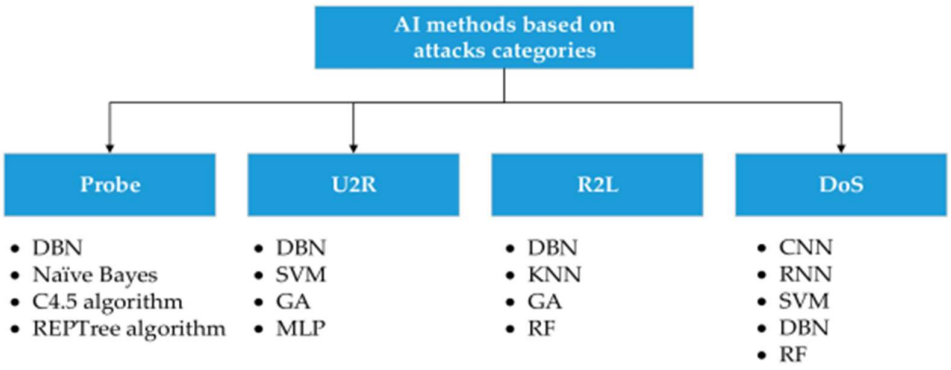

Figure: Illustrate of artificial intelligence methods based on attacks categories

AI for Detecting Probe Attack

Attacks known as probes seek information from specific external network sources like port sweep and IP sweep. Data within peer networks becomes accessible as a result of probe assaults, giving an attacker the opportunity to spy, get access to, or gather information. AI-based methods can be used to find this attack. To obtain a high detection rate in IoT systems, for instance, Zhang et al. [13] presented an IDS model based on genetic algorithms (GA) and deep belief networks (DBN). In addition, a fast intrusion detection system was proposed using hybrid AI techniques such as RF, Naïve Bayes, C4.5, REPTree algorithm to detect attacks [13].

AI for Detecting U2R Attack

User to root (U2R) attacks, such as those using perl and xterm, try to gain access to computers as regular users. U2R attacks can manipulate, spy on, or interfere with typical system activity. A novel SVM model was put up by Bagaa et al. [14] based on a security framework to enable mitigating various vulnerabilities, such as U2R in IoT systems. A GA has also been suggested for developing criteria to identify U2R threats [15].

AI for Detecting R2L Attack

When a user transmits packets to a system to which they do not have authorised access, such as xclock and guest password, this is known as a remote to user (R2U) attack. Attacks using R2L take use of system privileges. R2L assaults can be detected using AI using the Chatterjee and Hanawal methodology [16]. In order to centralise IoT security, a probabilistic hybrid ensemble classifier (PHEC) employing KNN and RF was developed in the article as the foundation for a federated learning IDS. Additionally, a GA was suggested for developing guidelines to recognise R2L assaults [17].

AI for Detecting DoS Attack

Due to its simplicity of execution, denial of service (DoS) attacks are among the most frequent. It can be carried out using DDoS attacks and UDP storms to disrupt network traffic. DoS attacks have the effect of keeping system resources too busy to handle legitimate networking requests. To detect DoS attacks in IoT Botnets datasets, an AI detection model has been suggested employing several ML/DL approaches, including CNN, RNN, and SVM [18].

CONCLUSION

IoT security and privacy are of utmost importance and are crucial to the development of the IoT market. The dynamic nature of IoT networks presents a variety of challenges for traditional

security and privacy solutions. The IoT devices can be made to adapt to their dynamic surroundings by using ML, and more specifically, DL and DRL approaches. By analysing statistical data from the environment, these learning techniques can enhance the performance of the entire system and support self-organizing operation (e.g. human users and IoT devices). These learning strategies don't need centralised communication between the device and controller because they are scattered by nature. The lack of available datasets for ML and AI algorithms makes it challenging to benchmark the effectiveness of ML and AI-based security solutions. In this article, we looked at the IoT's use of ML and AI from the perspectives of security and privacy. Attack vectors, security needs, and IoT security concerns have all been covered. We've discussed various ML and AI methods and how they apply to IoT security. In this article, we give a thorough analysis of cyber security detection assaults in the Internet of Things utilising AI techniques.

CONFLICT OF INTEREST

None

REFERENCES

[1] O. Novo, N. Beijar, and M. Ocak, “Capillary Networks - Bridging the Cellular and loTWorlds ,” IEEE World Forum on Internet of Things (WF-IoT), vol. 1, pp. 571–578, December 2015.

[2] F. Hussain, Internet of Things; Building Blocks and Business Modles, Springer, 2017.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys Tutorials, vol. 17, pp. 2347–2376, Fourth quarter 2015.

[4] J. Granjal, E. Monteiro, and J. S. Silva, “Security for the internet of things: A survey of existing protocols and open research issues,” IEEE Communications Surveys Tutorials, vol. 17, pp. 1294–1312, third quarter 2015.

[5] A. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Transactions on Emerging Topics in Computing, vol. 5, pp. 586–602, Oct 2017.

[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4, pp. 1125–1142, Oct 2017.

[7] M. Ammar, G. Russello, and B. Crispo, “Internet of things: A survey on the security of iot frameworks,” Journal of Information Security and Applications, vol. 38, pp. 8 – 27, 2018.

[8] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” IEEE Communications Surveys Tutorials, vol. 20, pp. 3453–3495, Fourth quarter 2018.

[9] F. Restuccia, S. DOro, and T. Melodia, “Securing the internet of things in the age of machine learning and software-defined networking,” IEEE Internet of Things Journal, vol. 5, pp. 4829–4842, Dec 2018.

[10] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, “Internet of things: A survey on machine learning based intrusion detection approaches,” Computer Networks, vol. 151, pp. 147 – 157, 2019.

[11] J. Hou, L. Qu, and W. Shi, “A survey on internet of things security from data perspectives,” Computer Networks, vol. 148, pp. 295 – 306, 2019.

[12] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199 – 221, 2018.
[13]. Zhang, Y.; Li, P.; Wang, X. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access 2019, 7, 31711–31722.
[14]. Ait Tchakoucht, T.; Ezziyyani, M. Building a fast intrusion detection system for high-speed-networks: Probe and dos attacks detection. Procedia Comput. Sci. 2018, 127, 521–530.
[15]. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A Machine Learning Security Framework for Iot Systems. IEEE Access 2020, 8, 114066–114077.
[16]. Paliwal, S.; Gupta, R. Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm. Int. J. Comput. Appl. 2012, 60, 57–62.
[17]. Chatterjee, S.; Hanawal, M.K. Federated Learning for Intrusion Detection in IoT Security: A Hybrid Ensemble Approach. arXiv 2021, arXiv:2106.15349.
[18]. Kim, J.; Shim, M.; Hong, S.; Shin, Y.; Choi, E. Intelligent detection of iot botnets using machine learning and deep learning. Appl. Sci. 2020, 10, 7009.