International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
Volume 9, Issue-3 May-June - 2022
Email: editor@ijermt.org www.ijermt.org

ANALYSIS OF APPLICATIONS, CHALLENGES, AND FUTURE DIRECTIONS OF MACHINE AND DEEP LEARNING FOR IoT SECURITY AND PRIVACY

Badde. Hari Babu, Dr. Vikas Kumar

CSE Department, CMJ University, Meghalaya

Abstract: A number of intelligent gadgets that can communicate with each other with minimal human intervention are connected to the Internet of Things (IoT). IoT is rapidly making its place in the field of computer science. However, the transdisciplinary elements involved in implementing such plans and the cross-cutting design of IoT systems present significant security challenges. The use of security protocols such as application security, authentication, encryption, and access networks is ineffective for Internet of Things (IoT) systems and their fundamental security flaws. Effective security of the IoT environment can also be achieved by improving current security technologies. Deep learning (DL) and machine learning (ML) have made great strides in many important applications in recent years. As a result, DL/ML techniques are essential to transform the security of IoT systems from simply allowing secure communications between intelligent systems to security between IoT systems. This review aims to provide better strategies for securing IoT devices by thoroughly examining the latest advances in ML systems and DL techniques. However, several recent developments in deep learning and machine learning for IoT securities show how they can support further study. Future IoT device attacks and the potential threats associated with each surface are identified, as well as IoT security concerns related to emerging or critical threats. Next, we examine DL and ML IoT security strategies in-depth and outline the advantages, capabilities, and shortcomings of each strategy. This review covers a number of potential difficulties and restrictions.

Keywords: *DL, ML, IoT, Intelligent gadgets, Techniques etc.*

Introduction

The Internet of Things (IoT) has emerged as a transformative technology paradigm, connecting a vast array of devices and sensors to enable seamless communication and data exchange across various domains, including healthcare, transportation, smart cities, and industrial automation. Is. However, the widespread deployment of IoT systems presents significant security and privacy concerns, as the interconnected nature of IoT devices creates vulnerabilities that can be exploited by malicious actors. In this context, the application of machine learning (ML) and deep learning (DL) techniques provides innovative solutions to enhance IoT security and privacy.

Securing IoT systems against cyber threats and preserving user privacy are paramount objectives in ensuring the reliability and trustworthiness of IoT deployments. ML and DL approaches have shown promising results in addressing these challenges by enabling intelligent threat detection, anomaly detection, and privacy-preserving mechanisms tailored for IoT environments. By analyzing large amounts of IoT data and identifying patterns indicative of security breaches or privacy violations, ML and DL algorithms can increase the resilience of IoT systems against a wide range of threats.

However, despite the potential benefits, the application of ML and DL to IoT security and privacy presents several challenges that need to be addressed. These challenges include the resource constraints of IoT devices, the need for robust and interpretable ML models, the vulnerability of ML algorithms to adversarial attacks, and the ethical implications of collecting and analyzing sensitive IoT data. Overcoming these challenges requires interdisciplinary research efforts that integrate expertise from domains such as cybersecurity, machine learning, cryptography, and ethics.

In this paper, we analyze the applications, challenges, and future directions of machine learning and deep learning for IoT security and privacy. We review recent advances in ML and DL techniques designed for IoT

environments, examine the challenges associated with their deployment in real-world IoT systems, and discuss potential strategies to overcome these challenges. . Additionally, we explore emerging research directions and opportunities to leverage ML and DL to enhance the security, privacy, and resilience of the IoT ecosystem.
Through comprehensive analysis and discussion, this paper aims to contribute to ongoing efforts to secure IoT systems and preserve user privacy in an increasingly connected world. By examining the applications, challenges, and future directions of ML and DL for IoT security and privacy, we provide insight into the potential benefits and limitations of these technologies and opportunities for further research and development in this rapidly evolving area. Let's identify. The phrase “Internet of Things” (IoT) refers to the concept of interconnectivity between various objects, such as mechanical systems, industrial systems, intelligent sensors, autonomous vehicles, mechanisms and terminals, etc. [1, 2]. Another way to describe it is as a network of physically connected objects or things, with limited computational, communication and storage capabilities, based on software, network connectivity, embedded electronics (such as sensors and actuators) and data. Are combined with the ability to exchange and collect. 3]. The Internet of Things (IoT) is pervasive in our daily lives and includes more sophisticated gadgets ranging from smart meters, IP cameras, smoke detectors, smart adapters, smart refrigerators, smart lights, smart air conditioning units and temperature sensors in the home. Accelerometers, radiofrequency identification (RFID) devices, heartbeat detectors, IoT in cars and sensors in rooms. Military, home appliances, critical agricultural infrastructure, and personal healthcare are among the industries seeing growth in IoT-related services and applications [1]. The sheer scope of Internet of Things networks brings with it new challenges, such as managing these devices, handling the entire volume of data, communication, processing, storage and so on among other things. Many elements of the Internet of Things, including architecture, communications, apps, protocols, security, and privacy, have been the subject of extensive research. The cornerstone of commercialization of IoT technology is the assurance of security, privacy, and user happiness. Attackers face greater risks as the Internet of Things (IoT) leverages powerful technologies such as edge computing, software-defined networking (SDN), and cloud computing (CC). As a result, monitoring security has now become difficult and complex as IoT infrastructure evolves. Comprehensive solutions are needed to address security challenges [5]. In contrast, IoT solutions are often deployed without preparation. Therefore, a fraudster can physically access sensitive data by connecting to an Internet of Things device over a wireless network. IoT systems are characterized by their complexity and integrated arrangements. It can be challenging to meet the constantly changing security requirements for the Internet of Things given the widespread use of linked devices. Solutions that provide the required level of security must take into account the entire system. However, most IoT devices are capable of working without human input. Thus, these gadgets can be physically accessible to anyone without authorization [6-8].

Inspiration and Scope

Deep Learning (DL) and Machine Learning (ML) are effective methods for learning how IoT devices and devices interact with each other in an IoT environment, as well as data analysis for “abnormal” and “normal” behavior. . It is related to [14]. Data input from IoT systems can be analyzed and aggregated to identify patterns in interactions, so malicious behavior can be detected at an early stage. Moreover, deep learning/machine learning is very important in identifying new threats that constantly replace existing threats, as they can detect the first threats that know the future by learning from past challenges. Therefore, IoT systems must be able to transform from security-based intelligence and secure communication between devices to security and value through ML/DL technology. The following articles discuss various specific aspects of IoT networks.
Heterogeneity: Each activity in the IoT network has unique characteristics, communication protocols, and collaboration capabilities. Devices may use different communications networks and protocols (such as Ethernet or cellular) and have different hardware.

Close to Communication: Additionally, IoT devices can communicate with each other without needing a resource such as a base station, which is also important. It uses device-to-device communication (D2D), short-circuit communication (DSRC), and other point-to-point communication technologies.
Mass deployment: Mass deployment must exceed the capacity of the existing Internet by millions of devices connected to the Internet. Deploying large-scale IoT is not without challenges.
Low-cost and low-power communications: To achieve high performance in the network, most connected IoT devices must use low-cost and low-power solutions.
Low Latency and Ultra-Reliable Communications (LLURC): Remote surgery, intelligent transportation, and business process automation all rely on the ability of IoT networks to provide high reliability and rapid response to urgent needs.
Security: Due to the number of IoT devices connected to the Internet, personal data exchanged by these devices may be at risk. Privacy and device security are also important considerations.
Dynamically changing networks: Large numbers of IoT devices require proper management. These devices can operate dynamically.

Contribution

The main impact of this project is as follows:
Comprehensive review of the latest advances in machine learning and network learning Comprehensive IoT protection: Examined deep learning and machine learning algorithms for the most effective IoT security solutions, Advantages, disadvantages and applications of Security IoT systems argues. There is also a comparison table and explanation of deep learning and machine learning for education.
- Describes many of the most advanced applications of deep learning and machine learning in IoT security and privacy.
- We offer a variety of innovative IoT privacy and security solutions based on deep learning and machine learning technologies. The new understanding of ML and DL in IoT security is also explained.
â highlights the limitations, challenges, future directions of DL and ML, and suggestions for how they can aid current and future research.

Internet of Things Threats

Multiple heterogeneous sensing systems communicating with each other through a local area network (LAN) called the Internet of Things [4]. The risks of the Internet of Things differ from those identified by traditional networks, mainly due to the tasks of accessing end devices [7]. While the traditional Internet relies on powerful and efficient computers and servers, the Internet of Things relies on memoryless devices and computing power. Therefore, in the real world, IoT devices cannot continue to use multiple authentications and dynamic processes like normal networks. Wireless protocols used by IoT devices, such as ZigBee and LoRa, are less secure than the protocols used by traditional networks. The absence of operating systems and specific functions in IoT applications leads to the creation of a large number of data points and structures throughout the system, making it difficult to develop a security system [8].

Privacy threats

In addition to security risks, there is also a privacy threat to IoT data and users, such as anonymization, guessing, and sniffing. In all cases, whether the data is in use or in force is relevant to the personal data.

Security Threats

Denial of Service (DoS) is the most common threat compared to other types of threats. The simplest application. Additionally, as the number of IoT devices with weak security features continues to grow, DoS attacks have become a favorite tool for attackers. The main goal of a DoS attack is to flood the IoT network with illegal requests and network resources, including bandwidth. Therefore legitimate customers cannot access the service.

Other Threats to Safety and Security

There are two types of threats to security: physical threats and cyber threats.

IoT Security Applications

Security is extremely important in almost all IoT applications currently in use or under development. IoT applications are growing rapidly and being integrated into most existing industries. Although operators use up-to-date technologies to support these applications, some IoT applications require strict security support from the IoT-based technologies they use. This section introduces several important IoT applications.

Home Automation

The Internet of Things has many applications, including home automation. This category includes applications that remotely control devices to save energy, devices installed on doors and windows to prevent access, etc. Contains. Monitor electricity and water usage using monitoring tools and offer customers suggestions to save resources and money.

Smart City

Smart city uses the latest computer and communication technologies to improve people's lives[19]. Smart services such as smart cities, smart transportation and smart services are included. Governments around the world are encouraging the creation of smart cities with various incentives [20]. Although smart applications are designed to improve people's quality of life, they pose a threat to personal privacy.

Smart Retail

IoT application is widely used in retail. Many applications have been developed to track the temperature and humidity of the product as it moves through equipment. Additionally, IoT can further improve product performance by tracking the movement of products. For example, smart stores continue to be developed to serve customers based on their preferences, behaviors and understanding of certain products. This application is under development. Additionally, an augmented reality system was developed to offer online shopping opportunities. IoT applications are available and used by retail companies that have security issues.

Livestock and Smart Agriculture

Monitoring soil moisture, controlling water selection in arid regions, and controlling microclimate conditions such as temperature and humidity are some of the smart agricultural applications. Using hillsides in agriculture can be profitable and help keep farmers from losing money. In addition, fungal diseases and other microbial diseases can be prevented by carefully monitoring and controlling humidity and temperature during the production of various vegetables and grains.

Smart grid and smart metering

Management, monitoring and metering can all be done with smart meters. It is the most frequently used smart meter to track and measure energy consumption in smart projects. Smart metering systems can be used to prevent electricity theft. Tank monitoring and reservoir monitoring are two applications for smart meters.

Smart Environment

IoT can be used to detect forest fires, monitor snow slopes, prevent earthquakes, detect earthquakes early, monitor pollution and much more. There is a close relationship between human and animal life and the use of IoT applications in these areas. The data obtained from these IoT applications will also be used by government agencies operating in these areas.

Deep Learning and Machine Learning for IoT

Security and privacy are interconnected. One can imagine a place that is safe but does not provide privacy. It may seem that a house with windows is made special, but this is not always a protection against intruders. Although it is impossible to achieve privacy without compromising the level of security, the opposite is not true. Privacy is always compromised when security is inadequate or compromised. In this section, we describe the best-known ML and DL models used to classify IoT security features. Machine learning techniques refer to both unsupervised and supervised learning. The tracking method is divided into Naive Bayes (NB), Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbor (KNN), Decision Making (DT), Integrated Learning (EL) and Association Rules (AR). . disappeared. Moreover, the neglect method refers to only two methods: principal

component analysis (PCA) and k-means. Deep learning methods are similarly divided into unsupervised, supervised, and hybrid methods.

Using deep learning or machine learning algorithms to solve IoT threats

Privacy and security concerns can be mitigated in many ways. In Section 3, we explain the different types of threats in IoT. There are no solutions or discussions on how to ensure the security or privacy of IoT systems. Therefore, in this section, we focus on recent research on privacy and security protection for IoT. We define the solutions suggested by deep learning or machine learning algorithms as tools that ensure privacy and security.

A security plan is a set of policies and procedures designed to protect an organization's information and most valuable assets. It does not focus on people's personal details, only statistics and other facts. On the other hand, passwords, logins and other sensitive information are the main purpose of privacy.

Protecting confidentiality, protecting the integrity of data and information and facilitating access are the cornerstones of our security. The right to privacy of your own and your employer's personal information is the foundation of privacy. Security measures can help provide a level of privacy, and confidentiality of credentials and access to information is critical to security.

Machine Learning (ML) is a data processing tool used in data processing pipelines on any basis. For example, machine learning models can measure the flow of information across a network to determine deadlines. Both the underlying IoT node and the data input from the IoT node to the ML model are subject to poisoning or detection attacks. Reversibility and direct resistance at the output are possible [25]. Therefore, the confidentiality and security of the system cannot be compromised at the same time.

Challenges, limitations and future directions

Machine and deep learning algorithms have been developed recently and are not suitable for cryptographic applications. For example, two previous studies [13, 14] have shown that ML can be used to hack sample attacks using SVM and cryptographic models. Similarly, the developers of [12] introduced deep learning to decrypt encrypted frames and concluded that deep learning can do this. Machine learning (SVM and RF) and statistical algorithms are more efficient than CNN and AE algorithms. It has previously been shown that RNNs can learn decoding. Examining the internal success of this cipher can also be used to determine the mechanism of combining RNNs with 3000 units of LSTM; results also show that deep learning algorithms such as RNNs can capture and process multiple password table algorithms for cryptanalysis [13]. Machine learning/deep learning has the potential to drive advances in the Internet of Things.

Limitations of Machine Learning in IoT

The disadvantage of the basic machine learning method is that large amounts of data are required for model testing. Learning models are used to predict or classify the results of real-world applications. However, it should be noted that not all methods cover all equipment and features. In this case, deep learning is used to eliminate the shortcomings of machine learning techniques. Because deep learning can process a lot of data and its algorithms can adapt as more data is added, it is suitable for testing models and can improve the accuracy of predictions. Higher functions and variables are derived dynamically and hierarchically from the data entered by the DL. Many IoT applications produce unregistered or partially registered results. Deep learning can use anonymized data in an unsupervised way to uncover useful information.

Limitations of deep learning in IoT

We conducted a qualitative analysis and the results show that existing work needs to be modified to meet higher security requirements in the IoT field. Security issues are important because authorization, portal security, data security, data integrity, access to search tools, and packet capture play a role in identifying the suspect. Security issues are serious. Customized IDS algorithms, data prioritization, extraction processes, and best-in-class tools are all required for deep learning-based malware detection. Flexibility and planning are also issues with deep learning. The authors of [16] studied different DNN models and found that small accuracy takes a long time to improve. Additionally, since the number of layers and accuracy are linearly related, setting the parameters is also

an important issue. If you want to optimize a deep learning algorithm that is sensitive to data structure and size, you need a large number of hyperparameters. Research challenges in deep learning-based IoT security environment include:

(i) End-to-end security (integrity, access control, authentication, confidentiality, and access to search system);

(ii) Data preprocessing, optimization function selection, and removal.

Challenges of Machine Learning

As discussed below, inadequate data collection is one of the reasons for using data in machine learning and deep learning.

(i) No test data: Data can be exploited using deep learning and computing solutions. Real data from the real physical world is used to validate and evaluate the results of various deep learning and reinforcement learning algorithms. This information includes sensitive personal information that differentiates not only people but also their behavior and lifestyle. For example, data generated by BANs and other health apps can affect consumers' security, while data from smart homes can also affect their lifestyles and behavior. Therefore, it is important not to compromise customer security when using machine learning and deep learning. Various anonymization methods are used to keep data anonymous until it is used for analysis; However, research shows that this process can be hacked and the model can be misused by adding false information.

(ii) Inconsistency of data: When attacks are rare in the IoT environment, data obtained through machine learning or deep learning will often be inconsistent. The dependency of the attack on the attack and the detection of penetration will be related to these different information.

(iii) Data fusion: Data from different IoT devices and connected models should be combined to create machine learning and deep learning models. This can be difficult as data from different sources can have different structure and content, complexity and uncertainty.

DL Challenges

ML is a technique for extracting information from results and has been used for both malicious and malicious purposes. It turns out that in the future, competitors can use advanced learning algorithms based on machine learning and deep learning to solve hidden problems. For example, the authors use neural networks to reverse cryptanalysis. Additionally, incorrect data entered into machine learning algorithms can cause inefficiency in the entire learning-based learning process. Oversampling, insufficient test data, and throughput are issues that must be considered when applying knowledge in smart ecosystems.

The Future of Machine Learning

Artificial intelligence and machine learning have significantly contributed to the advancement of computer security. We also use IoT devices, smart homes, smart cars, etc. to improve our daily lives. they use. An advanced security framework cannot be considered successful unless it uses artificial intelligence and machine learning. Artificial intelligence and machine learning solutions can often help identify similarities between past attacks and receive alerts if similar threats are found. The most important feature of AI/ML is the ability to understand users' behavior on a regular basis, changing usage patterns, and many other things [13, 17]. One of our evaluation recommendations that security experts agree with is to create easy-to-use data from machine learning solutions to support decision making and data interpretation.

Future Directions of Interactive Learning

Building a modern IoT network using security techniques such as authentication, access control, privacy, and venous sensing is a good solution for ultimate security. New IoT architectures should prioritize quality of service over performance and include emerging models such as SDN and atomized IoT. Optimization algorithms such as Genetic Algorithm (GA), Bacterial Forage Optimization (BFO), Particle Swarm Optimization (PSO), as well as extraction and selection methods and transformations can also be used. Hybrid deep learning can be used to improve performance without increasing computation time. Blockchain technology using deep learning can also

be used to increase IoT security. Blockchain technology is a new solution to ensure the privacy and security of decentralized information.

Conclusion

Modern security and privacy strategies still face many problems arising from the complexity of IoT networks. Deep learning and machine learning can be used to adapt IoT devices to our real life. This review covers various IoT threats. Deep learning and machine learning are considered as many ways to secure IoT. Various deep learning and machine learning models and their applications in IoT security are described. This review discusses cutting-edge IoT privacy and security solutions that use deep learning and machine learning and their integration. While we examine the privacy and security of machine learning, we also try to analyze IoT threats using previous deep learning and machine learning studies. The focus is on new problems and insights from machine learning and deep learning in IoT security. Also included are future directions, security issues, limitations, and recommendations for supporting future technologies.

References

[1]. 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, no. 4, pp. 2347-2376, 2015.

[2]. A. Sharma, P. K. Singh, and Y. Kumar, "An integrated fire detection system using IoT and image processing technique for smart cities," Sustainable Cities and Society, vol. 61, p. 102332, 2020.

[3]. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," IEEE Communications Surveys & Tutorials, 2020.

[4]. [4] F. Hussain, Internet of things: Building blocks and business models. Springer, 2017.

[5]. 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, no. 4, pp. 2347-2376, 2015.

[6]. A. Sharma, P. K. Singh, and Y. Kumar, "An integrated fire detection system using IoT and image processing technique for smart cities," Sustainable Cities and Society, vol. 61, p. 102332, 2020.

[7]. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," IEEE Communications Surveys & Tutorials, 2020.

[8]. [4] F. Hussain, Internet of things: Building blocks and business models. Springer, 2017.

[9]. 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, no. 5, pp. 1125-1142, 2017.

[10]. M. Abomhara, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65-88, 2015.

[11]. S. Ray, Y. Jin, and A. Raychowdhury, "The changing computing paradigm with internet of things: A tutorial introduction," IEEE Design & Test, vol. 33, no. 2, pp. 76-96, 2016.

[12]. [8] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," 2010, pp. 731-736: IEEE.

[13]. E. Bertino and N. Islam, "Botnets and internet of things security," Computer, vol. 50, no. 2, pp. 76-79, 2017.

[14]. S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad hoc networks, vol. 11, no. 8, pp. 2661-2674, 2013.

[15]. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80-84, 2017.

[16]. M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "Corrauc: a malicious bot-iot traffic detection method in iot network using machine learning techniques," IEEE Internet of Things Journal, 2020.

[17]. H. Li, K. Ota, and M. Dong, "Learning IoT in edge: Deep learning for the Internet of Things with edge computing," IEEE network, vol. 32, no. 1, pp. 96-101, 2018.
[18]. E. Fernandes, A. Rahmati, K. Eykholt, and A. Prakash, "Internet of things security research: A rehash of old ideas or new intellectual challenges?," IEEE Security & Privacy, vol. 15, no. 4, pp. 79-84, 2017.
[19]. J. Qiu, Q. Wu, G. Ding, Y. Xu, and S. Feng, "A survey of machine learning for big data processing," EURASIP Journal on Advances in Signal Processing, vol. 2016, no. 1, pp. 1-16, 2016.
[20]. S. Yao et al., "Deep learning for the internet of things," Computer, vol. 51, no. 5, pp. 32-41, 2018.
[21]. A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, vol. 4, no. 2, pp. 118-137, 2018.
[22]. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer networks, vol. 76, pp. 146-164, 2015.
[23]. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10-28, 2017.
[24]. P. Podder, M. R. H. Mondal, B. Bharati, and P. K. Paul, "Review on the security threats of internet of things," Int. J. Comput. Appl, vol. 176, no. 41, pp. 37-45, 2020.
[25]. S. Bharati, P. Podder, M. R. H. Mondal, and P. K. Paul, "Applications and Challenges of Cloud Integrated IoMT," in Cognitive Internet of Medical Things for Smart Healthcare: Springer, 2021, pp. 67-85.
[26]. D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199-221, 2018.