IoT Security Techniques Based On Machine Learning: How IoT Devices use AI to Enhance Security

Lakshmisri Surya

Sr. Data Scientist & Department of Information Technology USA

Abstract

The internet of things (IoT) integrates various devices within the network to come up with intelligent and advanced services that help protect the privacy of the user and attacks, which includes eavesdropping, jamming, denial of service (DOS) attacks, and spoofing attacks. This research paper investigates the model used by IoT systems in cooperation with AI to enhance devices' security. The report also reviews IoT security solutions focused on machine learning technology, which includes reinforcement of learning, unsupervised learning, and supervised learning. The article also focuses on IoT malware detection, secure offloading, access control, and authentication techniques based on machine learning, which is AI. Additionally, the paper addresses the challenges which need to be investigated and addressed when implementing these machine learning schemes of security in IoT systems practically. IoT celebrated as the next technological revolution's enabler would involve easy accessibility across extreme security, complex service mobility and context-aware, and cellular network networks. Thus, AI can play a significant role in the technology of the network infrastructure. However, by using the principles, instruments, and technologies of AI in cellular connections used by IoT, a range of problems will surface. The fundamental issues in using AI in wireless information systems that enable end-to-end IoT connectivity with possible comprehensive future research directions and solutions are addressed in this paper.

Keywords - *Machine learning, Artificial Intelligence, Cloud Computing, Cyber threats, and IoT security.*

Introduction

Through the widespread introduction of sensors in the real world, to accomplish knowledge exchange, growing physical entities are linked to the IoT by sensors, which aids information sharing. IoT technology has been broadly used in diverse fields, including environmental perception, wearable medical, smart home, and smart city. IoT-interconnected sensors and computers need to send data to cloud servers to perform computational activities in a standard IoT service. The processed data would be transmitted to the IoT devices after the tasks are done (Osuwa et al., 2017). While the cloud lowers the processing burden of sensors and computers, it is impossible to disregard the immense overhead delivery of data. However, the current expansion of network capacity is far behind the pace of growth of data, and the dynamic network climate significantly hinders latency reduction. For conventional IoT networks, network latency has been the critical bottleneck that should be overcome.

Many security approaches and algorithms are presented to compensate for the safety risks created by edge computing dynamics. Many modern protection systems are based on models and algorithms that adapt a single pattern to detect intrusions, protect privacy, or manage access. Orthodox defensive strategies are also rapidly replaced with the relentless update of assault tactics and processes. It is fascinating, though, that the advent and growth of AI provide new alternatives to privacy and security problems. These issues include access control, which occurs due to multiple devices operating together within the same environment in which access control becomes the main issue. Privacy preservation is another issue since IoT devices revolve around almost all the aspects of our lives and hold privacy-sensitive information. Intrusion detection is another issue whereby the primary attacks that are intrusive are and distributed denial of service (DDoS) and denial of service (DoS) attacks (Xiao et al., 2018). As AI inquiries continue to progress, several areas of edge defense have increasingly been added to AI. For example, for the training efficacy of ML, vast quantities of transparent data are necessary. Still, adequate data assume that the device has encountered mass attacks and can reliably recognize these malicious activities. In the meantime, the threats against the training set still need to be careful, reducing the model's efficiency by tampering with the parameters (Lu et al., 2017). Because of the limited computational resources and storage, a compact AI algorithm is still required. While several experiments on the configuration of AI have been undertaken, there is very little debate and examination of AI to protect devices based on IoT. A systematic analysis based on state-of-the-art technologies and accomplishments in the area alluded to is therefore addressed in this paper.

Literature Review

How AI Enhances Security in IoT Devices

As the modern threat environment keeps growing, it is becoming paramount to develop and sustain an efficient defense framework to incorporate AI into a security plan. Network security players need to have the help and support of AI-based capabilities and machine learning, given the complexity and speed of modern cyber threats and the current shortage of cybersecurity skills (Rutledge et al., 2016). It comes as no surprise, though, that while companies are embracing AI to improve their defense efforts, malicious hackers are also embracing topics such as machine learning, automation, and agile product creation use AI themselves to potentially help detect network vulnerabilities and exploit them more rapidly (Canedo & Skjellum, 2016). Cybercriminals now have the potential and capacity to conduct swift, sophisticated attacks on these inherently insecure systems as entrances into enterprise networks because of the rising number and range of IoT and OT devices accessing network infrastructures. The future attack capabilities raised by AI would only further aggravate the risks to today's digitalization efforts.

AI can quickly have the means to successfully defend or target the IoT successfully, establishing an AI arms race between security researchers and cybercriminals. IT teams must consider recent developments in cybercriminal tactics, which might contribute to an AI-driven threat landscape within the next several years to preserve digital transitions and sustain a rigid security infrastructure (Sha et al., 2017). In order to retain a stable security infrastructure as their framework continues to grow and develop, they will need to realize which AI features they need to start integrating into their security stack now. Its adoption by malicious hackers is unavoidable as legal AI capabilities begin to expand in today's networks (Ren et al., 2017). Malicious hackers are facing their digital revolution, and, as a consequence, they are now using topics such as agile growth to speed up the development of ransomware to outperform manual vulnerability detection and effectively counter current defense strategies.

Proactive IT professionals have started redesigning their defense strategy to incorporate AI as part of an optimized and streamlined security fabric to effectively protect IoT and OT devices while minimizing the prevalent threats threatening them. Information security workers will now achieve an edge in the current cyberwar to safeguard the sustainability of their digitalization efforts, including the deployment of IoT, while preserving their network integrity, with AI serving as the workhorse of network protection (Calo et al., 2017). In specific, AI provides IT teams with a mix of classic fabric-based security with; Automated threat containment, unified threat analysis, and comprehensive device visibility.

Automated threat containment helps when a breach has successfully taken place within the network. IoT containment protocols can be streamlined with AI in operation, allowing contaminated computers to be correctly partitioned or taken offline until they can disperse to additional locations across the network (Yukitake, 2017). The unified threat analysis helps when threat detection and prevention activities across the network are becoming incredibly impossible to perform at a scale that will keep up with the technological cyber threats. Thus, AI provides IoT teams with the means to easily compile real-time threat intelligence information easily, find flaws inside their systems, and deploy defense strategies that prevent those threats (Canedo & Skjellum, 2016). The comprehensive device visibility ensures that security experts can gain direct insight into any computer accessing a network at any particular time by using AI-assisted network security. When equipped with linear device transparency at computer speeds, each device can be appropriately segmented, protected, tracked, and inventoried.

IoT Security Challenges

In many ways, the IoT is marvelous. However, technology has not effectively evolved and is not that safe. From suppliers to consumers, the entire IoT ecosystem still has several IoT security problems to address, such as user's knowledge and awareness, physical hardening, update management, and manufacturing standards. Also, various IoT security threats exist, which can be more serious threats to the devices (Abbasi et al., 2017). They include a lack of adequate consent on the IoT manufacturers' side, which means that since new devices are manufactured daily, most of them come along with undiscovered vulnerabilities. This is exactly one of the main IoT security problems. Although there are no standard IoT security specifications, developers will continue to manufacture poor security products (Sha et al., 2017). The concept of "security" as the key factor in their product development phase is not accessible to producers who have begun to increase the Internet connectivity to their products.

A lack of understanding and customer knowledge is the other problem. Internet users have worked out ways to avoid spyware or spam emails, run ransomware detects on their remote machines, and communicate on their wireless networks reinforced with a very strong password. However, IoT technology is a recent creation, and people don't know so much about its use (Yang et al., 2017). While much of the hazards associated with IoT security problems are always associated with the manufacturers, customers, and business activities can create more tremendous challenges. The misunderstanding and lack of understanding of IoT

technology among users have become key threats and challenges to IoT security. This, therefore, places us at risk of being exposed to threats (Lee & Kim, 2017). The management of system management is another problem. Updating the IoT devices is very key in preserving the level of security on IoT computers. It means that they should always be updated immediately after finding a new vulnerability within the devices. Compared to other devices that get updates automatically, even some IoT-connected devices still do without the key upgrades (Rehman et al., 2017). The other challenge is that, after updating, the device can send its backup to the servers within the cloud and experience a sudden outage. Therefore, it means that if the connection is unsecured and the updated files are not secured, private information is rendered vulnerable.

Another problem that may also trigger challenges with IoT security is the lack of physical hardening. Although these IoT devices must run independently without user intervention, they must be physically protected from alien attacks (Tripathy & Anuradha, 2017). Additionally, these IoT machines can also be located in remote places for a long time. The main problem with this is that these devices are particularly vulnerable to malicious attacks. It is because they have regular software modifications to the software within the computer. This makes it possible for them to transform into undead zombies and to deliver vast volumes of knowledge as weapons. A malware infected single IoT device poses no unique danger. Rather, it is a sequence of them that can bring down something (Banafa, 2017). By invading malware to undertake a botnet intrusion, the attacker comes up with an army of bots and directs them to send hundreds of requests now and then knock the target down.

Eavesdropping and industrial espionage is another challenge that is faced by IoT devices. When hackers control on-site monitoring by attacking IoT computers, spying has always not been the only option since they may also execute such attacks that include requesting ransom demand (Deshpande et al., 2016). Another popular IoT protection challenge is therefore violating privacy. Intruding and spying using IoT gadgets is a significant issue since it is easy to hack and manipulate various confidential data. The other challenges that IoT devices face include; crypto mining with IoT bots, having rogue IoT devices, risks of data integrity in healthcare, and hijacking the IoT devices.

Recommendations on How AI Can Enhance Security on IoT Devices

Technology updates to protection systems focused on AI and ML are needed to improve IoT devices' security. Since AI and ML require minimal human involvement, this will minimize downtime and increase organizational performance in detecting abnormal activities. The AI protection solution makes free detection of errors by using datasets, detecting abnormal behaviors, and analyzing security patterns. In order to interpret the results, it should gather data from all endpoints in the enterprise and run a statistical algorithm, enabling rational decision-making (Madakam & Date, 2016). With predictive analytics and effective risk management, early threat identification allows averting protection concerns while already in the earliest stage. This is forcing vendors of security measures to move from conventional solutions to ML-based integrated technology solutions. Over traditional security systems, identification and a real-time approach to an event should take precedence. Organizations can easily and reliably deter complex cyberattacks by implementing technology such as machine learning and AI. In the light of the change to protection, organizations will follow a robust technology architecture that incorporates risk and enforcement, privacy monitoring, and data security that are well served by analytics.

IoT vendors seek markets to expand their industries despite rapid technology developments, inventions, and improved connectivity. Connectivity firms of the next generation are searching for technologies that can integrate multiple players with internet infrastructure. In order to design new technologies and tap market prospects, cybersecurity enterprises should collaborate with AI-based service providers. With significant global technology giants and various AI- and IoT-focused startups, the AI-driven IoT security industry is fragmented (Yang et al., 2017). Soon, when well-established multinational giants are aggressively purchasing and collaborating with AI-based innovations, the industry is projected to consolidate steadily.

How the Research is Going to help the United States

This research on AI implementation in IoT leads to a wide variety of advantages for enterprises and clients within the U.S., such as smart automation, customized experience, and positive interference. Some of the most popular benefits of this research that involves the combination of disruptive technologies in the business sector within the United States include; elimination of downtimes that are costly and unplanned, increases the scalability of IoT, triggers enhanced and new services and products, offers a better risk management plan, and boost the efficiency of operation. Since the United States is leading to a significant number of players in the industry competing in domestic and foreign markets, AI in the IoT economy is extremely a competitive advantage for the country (Calo et al., 2017). The competition is fractured due to the rise in AI applications in the IoT industry. Major market players are implementing tactics such as product growth, collaboration, mergers, and acquisitions. Therefore, with research and further implementation

of technology like AI in IoT devices, the U.S. can effectively win through its operations.

Conclusion

We live in an age where much of the security protocols are advanced. The solution requires any AI to be a perfect solution. Machine Learning and Artificial Intelligence play a major role in strengthening conventional cybersecurity. Yet, via IoT computers, we also enhance the quality of our everyday lives, such as smart vehicles and smarter houses, among others. Safety experts also say that companies should draw a fine balance in reviewing whether or not to opt with a supervised or unsupervised approach. While ML and AI systems can function effectively without human control, it is always wise that a limited human involvement would make the system more efficient and successful. Security professionals' most basic suggestions are to streamline the available information and make it easier for ML-based technologies to decode the data and easily interpret it. Machine Learning-based systems can help counter any cyber-attacks once the data sets are standardized and specified.

REFERENCES

[1] Abbasi, M. A., Memon, Z. A., Memon, J., Syed, T. Q., & Alshboul, R. (2017). Addressing the future data management challenges in iot: A proposed framework. International Journal of Advanced Computer Science and Applications, 8(5), 197-207.

[2] Banafa, A. (2017). Three major challenges facing iot. IEEE Internet of things.

[3] Calo, S. B., Touna, M., Verma, D. C., & Cullen, A. (2017, December). Edge computing architecture for applying AI to IoT. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 3012-3016). IEEE.

[4] Canedo, J., & Skjellum, A. (2016, December). Using machine learning to secure IoT systems. In 2016 14th annual conference on privacy, security and trust (PST) (pp. 219-222). IEEE.

[5] Deshpande, A., Pitale, P., & Sanap, S. (2016). Industrial automation using Internet of Things (IOT). International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 5(2), 266-269.

[6] Lee, J. H., & Kim, H. (2017). Security and privacy challenges in the internet of things [security and privacy matters]. IEEE Consumer Electronics Magazine, 6(3), 134-136.

[7] Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. IEEE Access, 5, 3302-3312.

[8] Madakam, S., & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In Connectivity frameworks for smart devices (pp. 23-41). Springer, Cham.

[9] Osuwa, A. A., Ekhoragbon, E. B., & Fat, L. T. (2017, September). Application of artificial intelligence in Internet of Things. In 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 169-173). IEEE.

[10] Rehman, H. U., Asif, M., & Ahmad, M. (2017, December). Future applications and research challenges of IOT. In 2017 International conference on information and communication technologies (ICICT) (pp. 68-74). IEEE.

[11] Ren, Z., Liu, X., Ye, R., & Zhang, T. (2017, July). Security and privacy on internet of things. In 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC) (pp. 140-144). IEEE.

[12] Rutledge, R. L., Massey, A. K., & Antón, A. I. (2016, September). Privacy impacts of IoT devices: A SmartTV case study. In 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW) (pp. 261-270). IEEE.

[13] Sha, K., Errabelly, R., Wei, W., Yang, T. A., & Wang, Z. (2017, May). Edgesec: Design of an edge layer security service to enhance iot security. In 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC) (pp. 81-88). IEEE.

[14] Tripathy, B. K., & Anuradha, J. (Eds.). (2017). Internet of things (IoT): technologies, applications, challenges and solutions. CRC Press.

[15] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.

[16] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250-1258.

[17] Yukitake, T. (2017, June). Innovative solutions toward future society with AI, Robotics, and IoT. In 2017 Symposium on VLSI Circuits (pp. C16-C19). IEEE.