IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 1, Ser. I (Jan. – Feb. 2023), PP 69-74
www.iosrjournals.org

Safety in Next-Generation IoT Systems

Idrees Ahmad Thoker
Research Scholar, Information Technology, SunRise University, Alwar (Rajasthan)

Dr. Prasadu Peddi
Research Supervisor, Information Technology, SunRise University, Alwar (Rajasthan)

ABSTRACT
The field of study known as "the Internet of Things" (IoT) is vast and intricate. The hardware, software, and protocols used to build such systems are typically quite varied. As a result, and because of the rising volume of hastily developed Internet of Things solutions and services, the vast majority of these deployments are riddled with vulnerabilities. Recent events have shed even more emphasis on these security concerns.

Keywords: *Internet of Things, Security, privacy and trust, Wireless communications, Artificial intelligence, Decentralized architecture*

I. INTRODUCTION

The Internet of Things refers to a system in which many technological gadgets are linked together. In addition to making life more convenient, these gadgets make it easier to regulate a number of different types of automated tasks. According to IoT Analytics, a market research firm, by 2021, there will be 12.3 billion operational endpoints worldwide that are linked to the IoT. Future years will see this figure rise. Siri and Alexa are just two examples of virtual assistants that have helped level the playing field between humans and networked technology. If the Internet of Things business keeps advancing, linking smart cities together won't be science fiction. However, there is still work to be done to ensure the safety of IoT gadgets.

By 2030 (and beyond), it is expected that there will be more than a trillion sensors and associated devices in the Internet of Things (IoT) space. While this has the potential to bring about enormous economic opportunities, enhanced services, and even fundamental societal shifts, it also raises significant security concerns as these devices become more widely distributed. Several recent incidents have directly involved IoT systems or have used them as entry points into other networks.

Experts predict that the frequency and severity of such accidents will rise in the coming years. There is a growing concern that these issues will only become worse as new technologies, such as block chains, become more widely used and 'fog' and 'edge' computing become more commonplace. As was previously said, IoT systems create a large amount of data, necessitating security solutions that pay attention not only to the compute nodes but also to the network that transmits the data. There is also a need for novel methods that enable users and/or designers to verify the authenticity of the created data.

Increased network resilience (both locally and across greater distances) and the establishment of trust for the IoT system's compute nodes both contribute to higher confidence in the produced data. As a result, attempts to improve IoT security will need to come from a variety of directions, such as developing new theories for how to best use block chains and similar technologies for enhanced logging and monitoring and developing new authentication techniques for IoT devices. It is crucial to understand the dangers these systems confront in order to create countermeasures.

As was previously said, the number of connected devices and the breadth of IoT applications are both on the rise. Despite their promise, IoT technologies are still immature and face numerous obstacles. The most crucial of them is undoubtedly safety. Already there are millions of connected devices, and the number of sensors is in the billions. Each and every one of them requires safe and steady internet access. Therefore, businesses and organizations that want to take advantage of IoT technologies need to implement carefully thought-out security IoT architectures. The attack surface is enormous since every IoT device might be a potential target, and the number of threats in this space is constantly expanding. Physical access to certain IoT devices is possible for attackers, putting them in control of the device.

Many devices in the Internet of Things fail to implement basic security measures like least-privileged or role-based access. TVs, webcams, thermostats, remote power outlets, sprinkler controllers, home alarms, door locks, and garage door openers are all examples of smart-home IoT devices that communicate over the network without encryption and don't give the user the option to enable strong passwords. Devices used in the Internet of Things (IoT) must make do with limited resources, so they use minimal amounts of electricity while yet delivering all necessary features. Consequently, security is an afterthought, if even considered at all, during the development lifecycle.

II. LITERATURE AND REVIEW

Cheng, Peng & Chen, Youjia& Ding (2023) The proliferation of complex and varied IoT applications has placed a heavy burden on already overburdened communications and processing infrastructure. To meet this stringent requirement, it is necessary to build system-wide methods for highly flexible online resource allocation, which will streamline the functioning of existing networks. Effective online resource allocation is made possible by deep reinforcement learning (DRL), a technique that combines the strengths of RL and DL to address difficult decision-making issues. DRL combines the benefits of deep learning with those of reinforcement learning. We provide a DRL-based approach to allocating resources in this article. We begin by discussing the background of DRL and then moving on to some of the more current applications of this technique. Finally, we develop two new DRL algorithms that make it simpler to take use of DRL's potential and provide workable solutions to a broad range of resource allocation problems. The first deals with an optimization issue subject to a combination of discrete and continuous action spaces and a wide range of highly non-linear quality-of-service (QoS) constraints. The second one uses a novel semi-distributed architecture to transform the simpler single-agent DRL into the more challenging multi-agent DRL. Finally, we'll discuss the challenges of applying DRL to actual IoT networks, as well as the potential benefits that may result.

Aqeel, Muhammad & Ali, Fahad & Iqbal (2022) Use of the Internet of Things (IoT) in various applications has grown exponentially during the last two decades. There are around fifty billion internet-connected devices in use today. Because of their dependence on the Internet, IoT applications are always under attack from a wide range of traditional threats including malware, spyware, Trojan horses, injected malicious code, and backdoor exploits. Important services like as authentication, authorization, and accountability may be supplied by using conventional forms of violence. Authentication and authorization relate to the steps used to verify a person's claimed ownership of an object. When deciding whether or not to provide someone access to a resource, traditional authentication and authorization methods employ three separate factors to establish their identity. In addition, as this definition makes clear, computer viruses fall under the umbrella of malware. Software designed specifically to do harm to a computer system includes viruses, worms, Trojan horses, spyware, and ransom ware. High-frequency electromagnetic waves or a more advanced kind of malicious software pose a serious threat to Internet of Things (IoT) equipment. Committed to their work while retaining their own selves Internet of Things devices can operate efficiently even when faced with insufficient infrastructure. This makes it imperative to solve these security vulnerabilities, since relying on the status quo ante is not a viable option. These issues of security and confidentiality need immediate attention from the industry and the academic community. The most significant contribution of this work is that it draws attention to a gap in our understanding and the necessity for further investigation. The primary goal of this in-depth literature review is to start a discussion about the many threats that might affect IoT gadgets. The most important element of our objective is to understand how these threats function so that we may design a recovery mechanism to offset the damage they do. This research analyzes more than 170 scholarly works systematically to get a deeper familiarity with the issues surrounding security and privacy. In addition, a hierarchical organization of security threats and attacks is presented on a single platform, with an explanation of how and to what extent they affect the targeted Internet of Things (IoT) systems. This review paper organizes the security flaws in the IoT into categories and then analyzes them using a comparative research approach. In addition, the study's results highlight the need of investing in the research and development of cutting-edge technologies like block chain, machine learning, and artificial intelligence to guarantee the integrity of IoT infrastructures.

Alam, Tanweer & Gupta, Ruchi (2022) FL stands for "federated learning," and it's a novel approach to AI. It's a distributed system for problem solving that lets users hone their skills using massive datasets. Cutting-edge technology is used by a top-secret secrecy agency to store raw data. This state-of-the-art system simultaneously disconnects data connections and trains ML models. There is a rising demand for the development of systems and infrastructure that may boost the efficiency of advanced learning systems since experts in the area promote machine learning setups that involve a considerable amount of secret data. This study examines FL in depth, dissecting its components down to the level of the underlying application and system platforms, mechanisms, actual applications, and process settings. Because FL produces accurate classifiers without requiring the disclosure of any information, it effectively safeguards both privacy policies and access control rights. The first part of the article serves as an overview of FL. We will next examine the technical information available in FL, focusing on the ways in which this information facilitates innovation, contracts, and software. Our goal is to offer researchers with the resources they need to create the most successful privacy protection measures for Internet of Things devices by providing a more in-depth explanation of the best procedural systems and authentic FL software than has been provided in prior review publications. We also survey related scientific works and critically analyze the most pressing problems encountered by contemporary publications. Furthermore, we examine the pros and cons of FL and present numerous distribution scenarios to illustrate how particular FL models can be used to achieve the desired results.

Nalini, T. & Krishna, T. (2022) The Internet of Things, or IoT for short, is a technology that is becoming more commonplace as time goes on. Between 30 and 35 billion devices are expected to be linked to the internet of things by 2022. The growing number of internet users may be directly attributed to the widespread availability of low-cost internet service. Therefore, a tremendous amount of information is being produced by a vast network of interconnected electronic gadgets. As a consequence, safeguarding IoT devices and maintaining the privacy of data sent over the network have become two of the industry's biggest obstacles to date. Privacy, confidentiality, integrity, and reliability are only few of the security issues that must be addressed as a result of the widespread dissemination of users' private data across several devices. Companies of all stripes are cranking out IoT gadgets that conform to a wide range of specifications. The battery life of IoT devices may be shortened by an excessive volume of data flow through Internet Protocol, which might be the result of a poorly configured device or malfunctioning apps on a mobile device. Several topics, such as a review of existing studies on IoT security, are central to this investigation. This study also investigates how IoT devices and mobile applications communicate with one another, how vulnerable IoT technology is to cyber attacks, what kinds of IoT tools and manufacturers are available, and what kinds of simulators are now in use.

Abid, Muhammad (2022) As Internet of Things (IoT) use grows, so does the size of the attack surface, giving cybercriminals more opportunities than ever before. In the first part of this short essay, we'll learn about IoT and the security issues that surround it. Models and topologies for IoT layers, as well as related standardization efforts and protocols, will all be introduced here. We next go on to a discussion of the Internet of Things' vulnerabilities, followed by concrete suggestions for strengthening its defenses. This paper is intended for readers who have some experience with networking but are just getting started with the Internet of Things. It has been concluded that a lack of standards for the internet of things and resource constraints on devices are major obstacles. Research has the potential to develop lightweight, energy-efficient cryptographic solutions and effective intrusion detection systems (IDS) for the Internet of Things. It's obvious that we need standardized protocols and channel-based security solutions, and that these solutions need to be backed up by legislative mandates to ensure we get the quality we expect and prevent manufacturers from cutting shortcuts to save money.

BLOCKCHAINS FOR IOT SECURITY

In recent years, block chain technology has emerged as one of the most talked-about topics in distributed computing. The question of whether or not this technology will fulfill the criteria of a certain application is not always easy to answer. Block chains have been heralded as the answer to many issues, including that of IoT security, thanks to a speculative economy, anti-establishment feelings, and media and marketing reasoning. But should we believe this hype? Simply said, a block chain is a data structure made up of data blocks that are connected to one another by a hash of the preceding block's data. Additionally, this data structure is typically dispersed across a group of nodes to form a distributed database. The primary advantage of this database over more conventional ones is that it ensures no data will be changed by insufficiently represented parties.

The security of the Internet of Things may benefit from the implementation of many different types of such storage systems. Example uses for block chains include security monitoring and the equitable distribution of system resources by recording device behavior over time. The second car in a platoon often speeds up much faster than the first while driving in a group. In order to ensure that the system is fair, it is helpful to have a worldwide database of vehicle behavior. Device status tracking is another exciting use case for block chains. The device's firmware version, current configuration settings, and activity levels over time may all be utilized to identify problems with the device's functionality.

What, therefore, prevents block chains from being universally accepted as a foundational IoT technology and, maybe, for security in such systems? Managing the block chain’s block generation (often incorrectly called a consensus layer) is a significant obstacle to block chain deployment in the context of Internet of Things (IoT) devices. Proof-of-work (PoW), proof-of-stake (PoS), and permissioned systems are the three primary methods developed so far to address this issue. There is a wide variety of these methods, each with its own temporal performance, scalability, resource efficiency, and architectural prerequisites. PoW is obviously impractical for IoT devices due to its excessive resource requirements. PoS is best suited for monetary applications and has limited use in many IoT settings.

TRUSTWORTHY SENSOR DATA

Verifying the authenticity of edge-generated sensor data is a significant problem for IoT security. In order to identify or avoid sensor attacks, data integrity is essential. Due to their inherent differences in design patterns from general-purpose computers, IoT applications make it difficult to secure the integrity of sensors in the IoT. Cryptographic integrity, Byzantine agreement, and data provenance are the three standard methods for ensuring the trustworthiness of sensor data. There are advantages and disadvantages to each strategy. Digital signatures and cryptographic hash functions are two common applications of cryptographic integrity in general-purpose computing. Unfortunately, cryptographic algorithms typically have high time, space, and power consumption.

Traditional cryptography is difficult to implement on IoT devices due to their limited resources. Lightweight cryptography is a hot topic in the quest to solve this problem. To reach consensus in a distributed system among honest nodes despite a fractional number of Byzantine nodes is the Byzantine Generals Problem, and Byzantine agreement is a solution to this problem. However, these solutions are designed for large-scale distributed systems and are not appropriate for resource-constrained IoT edge devices, even though Byzantine fault tolerant systems can tolerate up to one-third of nodes acting arbitrarily (malicious). Appropriate Byzantine agreement methods, which result when consensus guarantees are loosened, have potential for use in Internet of Things sensor fusion.

MAIN TRENDS IN THE NEXT GENERATION IOT SECURITY

The state of the most important areas of IoT security has been taken into account. Here, we'll take a look at where security for the Internet of Things (IoT) is headed. After a quick examination of the overall trends, we'll give some thought to a few upcoming technologies that have the potential to improve the security of the next generation of IoT. Then, we'll zero in on recent advances in the three most important areas of IoT security: trust, data confidentiality, and privacy. We'll talk about the future security measures and tools that will be needed to overcome these deficiencies.

The security of future Internet of Things (IoT) systems must be comprehensive, protecting the system throughout its entire lifetime and all of its parts. To identify and stop such assaults, new forms of analytics, risk management, and self-healing mechanisms must be developed. New federated identity and access management solutions will be required to collect, integrate, and interpret heterogeneous data from disparate sensors, devices, and systems. Responding rapidly and properly to threats and assaults, incorporating and learning new threat information, and developing and enforcing thread mitigation measures are all necessary capabilities for future IoT systems.19 It is also necessary to have the capacity for collaborative issue diagnosis and the implementation of security strategies for the system's many subsystems, which may be controlled by different parties.

In addition, future IoT systems will need to guarantee granular data ownership across organizational boundaries. novel data analytics algorithms and novel cryptographic approaches, such as homomorphic or searchable encryption, are required to protect the privacy of consumers and/or businesses while processing massive amounts of data. The cooperative security measures made possible by the sharing of threat intelligence information by various systems allow for a more unified understanding of both existing and prospective assaults.

New technologies are needed to gather and analyze security-related data and to conduct dynamic and online threat analyses in order to develop risk assessment and risk management approaches for the whole lifespan of complex IoT systems. Real-time threat analytics requires novel strategies built on machine learning techniques. The unique threat analytics algorithms needed to meet this challenge must provide alerts with a high degree of precision and a low false positive rate. Additionally, they need to be resistant to adversarial attacks that willfully compromise and subvert learning data to manipulate the performance of machine learning algorithms. In order to implement early warning in future IoT systems, new cooperative risk management systems and security protocols will need to be developed.

The dynamic evaluation of real-time IoT security levels will need the development of test-based and monitoring-based continuous security audit approaches. These continuous audit techniques must be versatile enough to evaluate the security of platforms and edge components, as well as the components of a wide variety of heterogeneous IoT devices, with varying degrees of intrusiveness and weight.

Future IoT systems will have new features for keeping tabs on data ownership and enforcing data access regulations. Different anonymization algorithms will function on data at different levels, and as more data processing moves to the edge, more data anonymization capabilities should be available at the edge. Anomaly detection at the edge, and the capacity to conduct it, becomes more crucial.

NEXT GENERATION IOT SECURITY: DATA CONFIDENTIALITY

Homomorphic Encryption

It is feasible to conduct arithmetic operations on ciphertexts using homomorphic encryption techniques. Thus, it is possible to perform data analytics or searches on encrypted data using fully homomorphic encryption (FHE) without revealing search patterns or access to the original data. With FHE, data owners may rest easy while their private healthcare IoT data is analyzed for insight into the opioid issue.

Searchable Encryption

Storage providers may examine encrypted data for certain keywords or patterns with the use of searchable encryption techniques. Although it is possible to conduct keyword searches, neither the encrypted data nor the plaintext it conceals can be accessed in any way.

NEXT GENERATION IOT SECURITY: TRUST

Trust Establishment

Most Internet of Things use cases need an ad hoc, hands-off trust establishment process between devices that have never met each other before. This necessitates the development of novel, efficient methods for establishing confidence. Trust in public keys and the distribution of such keys to users is the primary emphasis of existing technologies for creating trust. Trust in transactions and agreements, as well as device and platform integrity, will be necessary for future IoT solutions.

Block chain and IoT: Trust in Transactions

The growing popularity of block chain-based protocols offers a potential solution to the problem of trust establishment. Smart contracts based on block chains are essential for business-critical interaction between devices without human intervention and hence may become an important part of future IoT trust infrastructures. However, block chains have a high bandwidth overhead and require a lot of computational resources. This restricts their use in IoT, necessitating the development of new, lightweight block chain-based systems.

Trust in Platforms

Hardware and software remote attestation are two methods that may be used to create confidence in distant platforms automatically. Due to the high price of specialized hardware modules like HSMs required for hardware remote attestation, it may not be feasible to utilize on low-cost sensor gear. On top of that, many battery-operated gadgets cannot afford the extra resources that such hardware requires. While remote software attestation can theoretically guarantee an adequate level of security for most applications, this is not the case in practice. Comprehensive software-only remote attestations may be possible in the future thanks to advances in code obfuscation, white-box cryptography, and control-flow integrity technologies.

Identity Management

We analyzed current identity and access management solutions, all of which provide for the safe, unified administration of data from a variety of sources. Advanced security and trust management technologies, such as use control, are anticipated to be used in the future to regulate autonomous data flows between various organizations.

NEXT GENERATION IOT SECURITY: PRIVACY

Privacy through Data Usage Control

Managing how data is used is an expansion of the idea of access control. In the future, data use control solutions will go beyond the scope of standard access control principles to monitor and label information at every stage of its processing lifecycle. In order to ensure that massive data sets maintain their privacy features while being used for learning algorithms and analytics, they will create fine-grained use limitations.

The primary benefit of data use control is that it gives people agency over how their data is used, even when it's being handled by a third party. This will aid in conforming to the laws of various countries (such as the EU's General Data Protection Regulation [GDPR]). Implementations of future IoT systems will need end-to-end privacy assurances, as well as the ability to locally regulate data exposure and interact with a wide range of other systems.

Privacy in Multifaceted and Dynamic Contexts

Additional attack surfaces for user data confidentiality breaches result when services from a utility company, device manufacturer, or application provider access the data. Consensually-accessible services are nonetheless possible threats from the perspective of the data owner. Future IoT platforms will need more sophisticated services and technologies to enforce proper access controls as more data is stored, transported, and processed over shared infrastructure.

III. CONCLUSION

In this post, we'll take a look at the state of Internet of Things (IoT) security and discuss some of the biggest concerns, as well as some potential solutions. It demonstrates the critical role that security plays in creating successful IoT systems. If you're looking to use safe IoT solutions in your business, I hope this article is helpful.

REFERENCES

[1]. Cheng, Peng & Chen, Youjia & Ding, Ming & Chen, Zhuo & Liu, Sige & Chen, Yi-Ping. (2023). Deep Reinforcement Learning for Online Resource Allocation in IoT networks: Technology, Development, and Future Challenges. IEEE Communications Magazine.

[2]. Aqeel, Muhammad & Ali, Fahad & Iqbal, Muhammad waseem& Rana, Toqir& Arif, Muhammad &Auwul, Md. (2022). A Review of Security and Privacy Concerns in the Internet of Things (IoT). Journal of Sensors. 2022. 1-20. 10.1155/2022/5724168.

[3]. Alam, Tanweer & Gupta, Ruchi. (2022). Federated Learning and Its Role in the Privacy Preservation of IoT Devices. Future Internet. 14. 246. 10.3390/fi14090246.

[4]. Nalini, T. & Krishna, T. (2022). Analysis on Security in IoT Devices—An Overview. 10.1002/9781119769026.ch2.

[5]. Abid, Muhammad. (2022). IoT Security Challenges and Mitigations: An Introduction.

[6]. J. Voas. Networks of ‘Things.’ NIST Special Publication800-183.2016.

[7]. IERC Cluster SRIA 2014 –Internet of Things.

[8]. http://www.openfogconsortium.org;Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Cisco White Paper, 2015.

[9]. H. Suo, J. Wan, C. Zou, and J. Liu, Security in the internet of things: are view. In Computer Science and Electronics Engineering (ICCSEE),p.648,2012.

[10]. 10. International Telecommunication Union – Telecommunication Sector, Series Y: Global Information Infrastructure, Internet Protocol Aspects and next Generation Networks -Frameworks and functional architecture models - Overview of the Internet of things, Y. 2060", June2012.

[11]. O. Vermesan and P. Friess, Eds. ERC Cluster SRIA 2014 – Internet of Things – From Research and Innovation to Market Deployment. River Publishers Series in Communication, 2014.

[12]. The Internet of Things Reference Model. Cisco, June2014.

[13]. K. Laeeq and J. A. Shamsi. A Study of Security Issues, Vulnerabilities, and Challengesin the Internet of Things. In Securing Cyber-Physical Systems. Taylor and Francis. Oct 2015.

[14]. N. Jeyanthi. Internet of Things (IoT) as Interconnection of Threats (IoT). In: Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. Fei Hu(Ed).CRCPress,2016.

[15]. Driss, Maha & Hasan, Daniah & Boulila, Wadii& Ahmad, Jawad. (2021). Microservices in IoT Security: Current Solutions, Research Challenges, and Future Directions