IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676, p-ISSN: 2320-3331, Volume 17, Issue 1 Ser. I (Jan. – Feb. 2022), PP 55-60
www.iosrjournals.org

The Study of Internet of Things (IOT)

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

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

Abstract
The number of connected devices and services continues to grow. The very cheap price of sensors is supercharging the expansion of the Internet of Things. Many sectors are making increasing use of this technology, including healthcare, construction, agriculture, and transportation. Concerns about the Internet of Things' future development center on security and privacy issues. Most Internet-connected "things" are very basic devices with limited hardware capabilities, making it extremely difficult to secure them using conventional methods. In this chapter, we'll go over why it's crucial to protect IoT networks, what problems arise when trying to do so, and what solutions have been proposed elsewhere.

Keywords-*Internet of Things (IoT); security; privacy; IoT architecture*

I. INTRODUCTION

The Internet of Things (IoT) ushers in a revolutionary improvement in people's standard of living by facilitating unprecedented access to a wealth of fresh data and specialized services in a variety of fields, such as education, security, healthcare, and transportation. On the other hand, it will be crucial in boosting businesses' output thanks to the widespread availability of a locally intelligent network of smart devices and innovative services that can be tailored to individual customers' preferences. The Internet of Things (IoT) has several potential advantages, including better asset and product management, increased data volume, and the potential for optimized machinery and reduced resource use. Additionally, it allows for the development of novel intelligent interconnected devices and the investigation of novel business models.

Internet of Things (IoT) security refers to the technological subfield concerned with protecting IoT nodes and their associated networks. Adding internet connection to a network of interconnected computers, mechanical and digital machinery, items, animals, and/or humans is what the Internet of Things is all about. Every "thing" is assigned a number and given the capacity to communicate with one another and share information in an automated fashion. If necessary, precautions are not taken, allowing a device to connect to the internet exposes it to a wide variety of threats.

The importance of Internet of Things (IoT) security has been brought to light by a series of high-profile events in which a common IoT device was exploited to access and attack the wider network. It's essential for protecting networks that host Internet of Things gadgets. As the number of connected devices in contemporary enterprises continues to grow, so does the need for preventative measures to keep them secure.

The term "IoT security" describes the measures used to safeguard gadgets that operate via a network or the internet. The Internet of Things (IoT) refers to a wide range of interconnected computing devices and services, and its scope is expanding as new technologies emerge. Almost every modern electronic item, from wristwatches to thermostats to gaming consoles, may communicate with the web or other electronic gadgets.

IoT security refers to the methods, procedures, and resources that keep these gadgets safe from hackers. The irony is that the intrinsic connectedness of IoT devices renders them more susceptible to hackers.

Understanding IoT is crucial before delving into the challenges of privacy and security it presents. IoT, in its broadest meaning, is the worldwide web of interconnected gadgets that exchange data via the web. The gadgets exchange information with one another and generate and gather data to guarantee optimal performance.

In reality, IoT devices capture data about individual users, which may include very confidential and sensitive information. In addition, by 2022, the Internet of Things industry is expected to be worth more than $500 billion. Security and privacy issues have arisen as a result of the expanding Internet of Things (IoT).

II. LITERATURE AND REVIEW

Abeer Hassan Assiri (2018) The Internet of Things (IoT) is a vision of the future in which everyday things are embedded with electronics that allow them to link to one another and the internet to form a self-configuring, self-learning system. While the Internet of Things (IoT) has many potential advantages, concerns have been raised about its security and privacy, which are seen as major obstacles to the architecture's adaptation

and development. The biggest problem with the IoT is that security and privacy concerns have not been adequately addressed at any of the several layers. Many studies have proposed strategies for improving security. To keep IoT safe, you need a comprehensive security architecture that addresses problems at every level of the IoT stack. In this article, we examine some of the main concerns and difficulties related to IoT security and privacy. Security concerns specific to the IoT context were also highlighted, along with some potential solutions.

Vishal Sharma et al (2017) The Internet of Things (IoT) has attracted the attention of businesses and researchers worldwide due to the breadth of its potential uses. By connecting any devices with processing power to the internet, IoT makes it easier to run businesses. As wireless technology has advanced, attention has switched from basic IoT to M-IoT devices and platforms, which may provide low-complexity, low-cost, and efficient computing through sensors, machines, and even crowdsourcing. The term "M-IoT" may be used to describe all of these interconnected gadgets. While the positive impact on applications has been substantial, security, privacy, and trust remain the top concerns for these types of networks, and the introduction of even minor threats to M-IoT devices and platforms is a result of inadequate enforcement of these requirements. Therefore, it is crucial to learn about the various options for supplying a safe, private, and reliable mechanism for M-IoT. To our knowledge, there has been no comprehensive study conducted on the topic of M-IoT security, privacy, trust, secure protocols, physical layer security, or handover safeguards. The needs for security, privacy, and trust in smart and linked M-IoT networks are discussed, and a comparison of state-of-the-art solutions for IoT is presented. This article also discusses a variety of other topics related to security, privacy, and trust, including problems, applications, benefits, technology, standards, open issues, and a roadmap.

Kaushik Ragothaman et al (2023) The Internet of Things (IoT) is useful in many different settings, including the home and the workplace. When an Internet of Things (IoT) device is linked to a network, access control plays a critical role in deciding which users and devices have permission to access the data and services provided by the network. The features of the IoT provide several obstacles in building and implementing an appropriate access control solution for the IoT, such as the diversity of IoT devices, resource limits on IoT devices, and the heterogeneous nature of the IoT. In this study, we provide a systematic review of the literature on access control in the Internet of Things (IoT), including topics such as needs, authorization architecture, models, policies, research problems, and potential future developments. Important needs for security in the Internet of Things are highlighted. The article then assesses the feasibility of currently available access control strategies in meeting those needs. Decisions about who has access to what are based on these rules. We take a look at the many methods that have been proposed for specifying dynamic policies. The problems encountered by the currently available approaches to policy definition are emphasized. The study concludes by outlining the difficulties and potential future directions of access control in the IoT. Access control in the IoT is complicated since there is no universal solution to accommodate the wide range of IoT use cases. To protect the IoT, it would be ideal to have an access control solution that satisfies all the needs listed, notwithstanding the difficulties in developing and implementing the access control in the IoT.

Joseph Henry Anajemba et al (2020) There are many different communication technologies that make up the IoT, but the most pressing concern right now is security and privacy at the physical (PHY) layer, especially in light of the advent of the fifth-generation (5G) cellular network. The inability of the authentic source and destination (transmitter/receiver) nodes in the network to get information from the passive eavesdropper is the greatest practical difficulty in maintaining PHY security. It is difficult to optimize the transmitting settings without this knowledge. To address this issue and strengthen the physical layer (PHY) security in a three-node wireless communication network, we present a sequential convex estimation optimization (SCEO) technique in this study. Based on our experimental findings, we can conclude that transmission performance is maximized and convergence is improved by using the SCEO algorithm. We extended our study to create a fast privacy rate optimization algorithm for a multiple-input, multiple-output, multiple-eavesdropper (MIMOME) scenario, as it is relevant to security in IoT and 5G technologies, because of the potential security challenges envisioned when a multiple eavesdropper is active in a network. Compared to running with non optimal settings, the results of the study demonstrate that the algorithm executes substantially while maintaining a low level of complexity. When compared to earlier research, our method's performance stands out because we used rate constraint in conjunction with self-interference of the full-duplex transmission at the receiving node.

Jee Young Lee et al (2021) Hyper connectivity, hyper intelligence, and hyper convergence are the hallmarks of the fourth industrial revolution, which is ushered in by the smart mobile IoT network. Smart mobile IoT network security is becoming more important as this revolution gathers steam. The purpose of this research was to provide in-depth knowledge about IoT safety. We did a literature review and mapping exercise to help us spot developing themes related to IoT security and zero in on potential study areas. We looked at articles published between January 2009 and August 2020 to find leading scholars and emerging keyword trends. We also used structural topic modeling to estimate topic trends in order to determine which areas of study are currently active and likely to provide the most fruitful results. Future research directions were developed based on our synthesis and interpretation of the systematic mapping study's findings. The study's findings may help us better comprehend

emerging tendencies in IoT security and inform future IoT security studies and developments.

IOT SECURITY ISSUES AND CHALLENGES

The more channels via which devices may communicate with one another, the more opportunities there are for malicious actors to snoop on them. IoT devices depend on channels that hackers may intercept, such as HTTP (Hypertext Transfer Protocol) and API (Application Programming Interface).

Devices that don't have an internet connection might nonetheless fall under the IoT umbrella. Bluetooth-enabled home appliances fall within the umbrella of Internet of Things devices and need IoT security as well. The current increase in IoT-related data breaches may be traced in part to oversights like this one.

Here are a few Internet of Things security issues that continue to endanger people's and businesses' money:

1. Remote exposure

Due to their internet connection, IoT devices provide a greater attack surface than conventional technologies. While this convenience is invaluable, it also allows malicious actors to remotely access and manipulate devices. This is why phishing and other hacking tactics are so successful. In order to keep assets safe, IoT security, like cloud security, must take into consideration a wide variety of potential avenues of access.

2. Lack of industry foresight

Certain markets and their wares have undergone a digital transformation alongside their respective companies. Many sectors, including automotive and healthcare, have increased their use of IoT devices in order to boost output and cut costs. However, this increased reliance on technology is a downside of the digital revolution.

While this wouldn't normally be a problem, if a data breach were to occur, the effects would be magnified due to the reliance on technology. The fact that these sectors are becoming dependent on something that is fundamentally less secure, namely IoT devices, is cause for alarm. Moreover, many hospitals and car manufacturers were not willing to spend the money and time necessary to properly secure these devices.

Due to this lack of forethought, many businesses and manufacturers are more vulnerable to cyber attacks than they need to be.

3. Resource constraints

However, this is not the only issue with Internet of Things (IoT) security that newly digitized industries face. The limited hardware and software capabilities of many IoT devices also pose serious security concerns.

Not all IoT gadgets have the processing capacity to include comprehensive antivirus protection. Some of them can not even communicate with one another. Many Bluetooth-enabled Internet of Things (IoT) devices have recently been the target of hackers. One of the most hit industries is the car sector once again.

In 2020, a cyber security expert exploited a severe Bluetooth flaw to hijack a Tesla Model X in about 90 seconds. There have been similar assaults on other vehicles whose keyless entry and ignition systems use FOB (wireless) keys. To steal automobiles without setting off an alarm, criminals have figured out how to scan and duplicate the interface on these FOB-style keys.

If cutting-edge equipment like a Tesla can be breached through the Internet of Things (IoT), then any connected gadget may.

HOW TO PROTECT IOT SYSTEMS AND DEVICES

The following are a few Internet of Things security methods that businesses may use to strengthen their current data protection procedures:

1. Introduce IoT security during the design phase

Most of the stated IoT security challenges are solvable with adequate planning, especially at the outset of the R&D process for any consumer, commercial, or industrial IoT device. Enabling security by default, offering up-to-date operating systems, and using secure hardware are all vital.

However, it's important for IoT developers to keep cyber security in mind not just during design, but at every step of the process. To prevent a vehicle key hack, for instance, one may store the FOB in a metal box or move it away from potential entry points like windows and doorways.

2. PKI and digital certificates

PKI is a fantastic method of securing client-server communications over a network. PKI makes it possible to encrypt and decode private communications and data using digital certificates and a two-key asymmetric cryptosystem. Users' sensitive, clear-text information entered onto websites for the purpose of conducting private transactions is protected by these technologies. Without the reliability of PKI, electronic commerce would cease to function.

3. Network security

The potential for threat actors to take control of other people's IoT devices across networks is enormous. On-premises IoT security must take into account both digital and physical entry points since networks consist of both. Using antimalware, firewalls, intrusion detection systems/intrusion prevention systems; blocking unauthorized IP (Internet Protocol) addresses; and making sure systems are patched and up to date are all ways to protect an IoT network.

4. API security

Most modern websites wouldn't function without APIs. As an example, they facilitate the consolidation of flight details from many airlines into a single area for use by travel companies. API security is essential for ensuring that only authorized devices, developers, and applications connect with APIs and preserving the integrity of data being transferred from IoT devices to back-end systems. The data breach experienced by T-Mobile in 2018 is a prime illustration of the consequences of insufficient API protection. Due to a "leaky API," the mobile giant exposed the personal information of over 2 million users, including billing ZIP codes, phone numbers, and account numbers.

ADDITIONAL IOT SECURITY METHODS

Other ways to implement IoT security include:

Internet security: The network access controller (NAC) may assist discover and catalog IoT gadgets on a network. This will provide a standard for monitoring and tracking equipment.

Segmentation: Devices in the Internet of Things (IoT) that need an external internet connection should be isolated from the main company network. Abnormal network activity should be monitored so that corrective measures may be implemented if necessary.

Safe entry points: Security gateways, which act as a go-between for the Internet of Things and the network, are equipped with greater processing power, memory, and other resources than the IoT devices themselves, allowing them to install security measures like firewalls to protect the connected devices from intrusion.

Management of software patches and regular updates: It is essential to offer mechanisms for remotely and automatically upgrading hardware and software through networks. Devices should be updated as quickly as feasible, hence a coordinated disclosure of vulnerabilities is essential. Don't forget about planning for death.

Training: Many current security teams lack experience with Internet of Things (IoT) and operating system security. Security personnel must be prepared for new security issues by staying current with new or unfamiliar systems and by learning new architectures and programming languages. Cybersecurity training for executives and their teams is essential for them to stay abreast of emerging threats and effective countermeasures.

Teamwork that works: In addition to training, it might be helpful to bring together teams who are traditionally separated. Having programmers and security experts collaborate throughout development may help guarantee that enough safeguards are included into gadgets.

Instruction for Buyers: Consumers need to be educated on the risks posed by IoT devices and given tools to protect themselves, such as instructions on how to change the default passwords and install security patches. Consumers may play a part in ensuring the security of their gadgets by demanding that manufacturers produce only products that fulfill stringent security requirements and rejecting those that don't.

Which industries are most vulnerable to IoT security threats?

Any facility, from a smart home to a factory to a connected car, is at risk for an Internet of Things security breach. The extent of the damage will vary widely depending on the specific system, the data gathered, and/or the information stored.

Attacks that disable the brakes of a connected automobile or that hack a connected health equipment like an insulin pump to deliver too much medicine to a patient are two examples of such attacks that might have fatal consequences. Medicine that is stored in a refrigerator and whose temperature is monitored by an Internet of Things device is also at risk if the temperature suddenly changes. Equally devastating would be an assault on oil fields, power plants, or water treatment facilities.

The danger posed by such assaults, however, must not be dismissed. A thief may, for instance, gain access to a residence using a smart door lock that has been compromised. Another kind of security breach is when an attacker uses malware to harvest sensitive information from a networked computer.

Notable IoT security breaches and IoT hacks

Since the inception of the IoT concept in the late 1990s, security experts have voiced concerns about the potential dangers posed by a large number of unprotected devices connected to the internet. There have been a number of high-profile hacks since then, including spam sent through refrigerators and televisions and hackers

communicating with children via their infiltration of baby monitors. Some attacks on the Internet of Things don't even directly target the gadgets themselves; rather, they use the IoT to get access to other networks.

For instance, in 2010, scientists disclosed that the Stuxnet virus had been used to cause physical harm to Iranian centrifuges, with assaults beginning in 2006 and peaking in 2009. One of the early instances of an Internet of Things (IoT) attack, Stuxnet infected instructions issued by programmable logic controllers (PLCs) to compromise industrial control systems (ICS) supervisory control and data acquisition (SCADA) systems.

Malware like Crash Override/Industroyer, Triton, and VPN Filter, all of which target insecure operational technology (OT) and industrial IoT (IIoT) systems, have only increased their attacks on industrial networks.

The first IoT botnet was uncovered in December 2013 by a researcher at corporate security company Proofpoint Inc. The researcher found that more than 25% of the botnet was comprised of non-computer devices such as smart TVs, baby monitors, and domestic appliances.

In 2015, Charlie Miller and Chris Valasek of the security firm Black Hat changed the radio station on a Jeep's media center through wireless hack, activated the air conditioning and windshield wipers, and disabled the accelerator. They also claimed they could turn off the vehicle's engine, apply the brakes, and lock them in place. Miller and Valasek were able to hack into the car's network via Uconnect, Chrysler's in-car networking technology.

One of the biggest IoT botnets to date, Mirai, launched simultaneous assaults on the websites of journalist Brian Krebs and French web server OVH in September 2016 with throughputs of 630 Gbps and 1.1 Tbps, respectively. The following month, a cyberattack on the network of domain name system (DNS) provider Dyn rendered several popular websites inaccessible for many hours. Consumer IoT devices like IP cameras and routers were used as entry points into the network.

Numerous Mirai forks have appeared in the years since the initial outbreak, with names like Hajime, Hide 'N Seek, Masuta, Pure Masuta, Wicked botnet, and Okiru.

The FDA issued a warning in January 2017 that security vulnerabilities may exist in the embedded systems of some St. Jude Medical implanted cardiac devices that use radio frequency, such as pacemakers, defibrillators, and resynchronization devices.

To aid in delivering malicious payloads to unprotected Big-IP boxes, Trend Micro uncovered a Mirai botnet downloader for IoT devices in July 2020. Recent vulnerabilities in widely used IoT devices and software were observed to be exploited by the samples found.

A gang of Swiss hackers compromised 150,000 live-feed cameras belonging to security camera firm Verkada in March 2021. Institutions including schools, jails, hospitals, and even private businesses like Tesla have their activities watched by these cameras.

III. CONCLUSION

The Internet of Things (IoT) is responsible for several technical advancements that have improved the quality of our everyday lives in numerous ways. Internet of Things applications have limitless potential for improving every industry. The potential for the Internet of Things to improve social and economic conditions in the global South cannot be overstated. This encompasses several disciplines, such as ecological farming, medical care, industrial ecology, and environmental administration. Therefore, the Internet of Things (IoT) shows promise as a means to accomplish the Sustainable Development Goals set forth by the United Nations. However, the potential benefits to individuals, society, and the economy cannot be realized without first addressing the issues and challenges associated with IoT.

REFERENCE:

[1]. Assiri, Abeer & Almagwashi, Haya. (2018). IoT Security and Privacy Issues. 1-5. 10.1109/CAIS.2018.8442002.

[2]. Vishal Sharma, Ilsun You, Karl Andersson , Francesco Palmieri, Mubashir Husain Rehmani, and Jaedeok Lim (2017) Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey. Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. Digital Object Identifier 10.1109/Access.2017.DOI

[3]. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. Sensors **2023**, 23, 1805. https://doi.org/10.3390/s23041805

[4]. Anajemba, J.H.; Tang, Y.; Iwendi, C.; Ohwoekevwo, A.; Srivastava, G.; Jo, O. Realizing Efficient Security and Privacy in IoT Networks. Sensors **2020**, 20, 2609. https://doi.org/10.3390/s20092609

[5]. Jee Young Lee, Jungwoo Lee, "Current Research Trends in IoT Security: A Systematic Mapping Study", Mobile Information Systems, vol. 2021, Article ID 8847099, 25 pages, 2021. https://doi.org/10.1155/2021/8847099

[6]. Gaona-Garcia, P., Montenegro-Marin, C.E., Prieto, J.D., Nieto, Y.V. (2017) Analysis of Security Mechanisms Based on Clusters IoT Environments. International Journal of Interactive Multimedia and Artificial Intelligence, 4, 55-60.

[7]. Zhou, J., Cap, Z., Dong, X. and Vasilakos, A.V. (2017) Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications Magazine, 55, 26-33. https://doi.org/10.1109/MCOM.2017.1600363CM

[8]. Alavi, A.H., Jiao, P., Buttlar, W.G. and Lajnef, N. (2018) Internet of Things-Enabled Smart Cities: State-of-the-Art and Future Trends. Measurement, 129, 589-606. https://doi.org/10.1016/j.measurement.2018.07.067

[9]. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorgi, M. (2014) Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1, 22-32.

[10]. Khajenasiri, I., Estebsari, A., Verhelst, M. and Gielen, G. (2017) A Review on Inter-net of Things for Intelligent Energy Control in

Buildings for Smart City Applica-tions. Energy Procedia, 111, 770-779.
[11]. Liu, T., Yuan, R. and Chang, H. (2012) Research on the Internet of Things in the Automotive Industry. ICMeCG 2012, Beijing, 20-21 October 2012, 2-13. https://doi.org/10.1109/ICMeCG.2012.80
[12]. Yan, Z., Zhang, P. and Vasilakos, A.V. (2014) A Survey on Trust Management for Internet of Things. Journal of Network and Computer Applications, 42, 120-134. https://doi.org/10.1016/j.jnca.2014.01.014
[13]. Pei, M., Cook, N., Yoo, M., Atyeo, A. and Tschofenig, H. (2016) The Open Trust Protocol (OTrP). IETF.
[14]. Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. and Ladid, L. (2016) Internet of Things in the 5G Era: Enablers, Architecture and Business Models. IEEE Journal on Selected Areas in Communications, 34, 510-527.
[15]. Clausen, T., Herberg, U. and Philipp, M. (2011) A Critical Evaluation of the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL). IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Shanghai, 10-12 October 2011, 1-11.