Sahel International Multidisciplinary Journal (SIMJ) Volume 6, Number 1.
e-ISSN: 2630-6611, p-ISSN: 2408-6118 (August, 2022)

Cybersecurity of Industrial Internet-Of-Things (IIOT) Systems and User Privacy

Akingbade, Luisa Osasere[1] Ahmed, Danasabe Suleiman[2]

[1]Department of Computer Engineering
Federal Polytechnic, Ilaro, Ogun State
Correspondence e-mail: luisa.akingbade@federalpolyilaro.edu.ng

Abstract

(Times New Roman 12p Itilized) Internet of Things is a computing emerging technology of monitoring and controlling physical objects known as dumb objects through Internet interface remotely by the user. A user can monitor and control physical objects like machines, systems, appliances, automobiles, or processes like production processes, supply chain processes, transportation processes both in consumer and industrial perspectives. Meanwhile, cybersecurity is the implementation of security techniques like security architectures while working on the internet. However, as this seminar topic will dive into the cybersecurity of IoT devices and the privacy of the user/operator in an industry, it is pertinent to take into adequate and proper consideration while majority both consumers and manufacturers/industries are clamouring for the IoT technology for better, efficient, real-time services and smart process monitoring, the equipment safety and user/operator privacy involved in the operation of the IoT technology. However, various researchers had established different methods like Edge-Computing, Fog-Computing, secure device architectural design, as well as various standards being set to improve the security level of devices, components, and the user privacy. This seminar's contribution is aim at focusing on creating the security awareness to both the IoT users and operators or employees, so as to foster the pre-established architectural layers for security enhancement, security infrastructures and measures, because despite various established IoT cybersecurity techniques being established, IoT devices and user privacy are not totally secured if users or operators are void of the understanding of vulnerabilities and how to apply required updates and patches as defence against unanticipated cyber-attacks.

Keywords: Computing, Cybersecurity, Internet of Things, Privacy, Technology

I. Introduction

Due to the technological advancement in recent years, especially in the world of computing, when conducting domestic, social, business, and educational activities, we have grown more entangled in and reliant upon international networks in our daily activities for easy, smart and better life experiences (Rachna, 2019). Since the whole world is fully harnessing the world of computing where information is digitised, stored and made accessible for monitoring, controlling and to perform proper and desired manipulation as well as global internetworking which has tremendously influence and used in almost every section of human life. Objects are now connected through the internet to communicate with each other without physical or direct interaction of human (Luigi,2010). This means that networked objects can be monitored and controlled by the user remotely through the internet. Hence, the user privacy and security of those networked objects or devices must be properly fostered effectively against any form of attack which normally endangers victims and devices i.e. user privacy as confidential information and data may be stolen and used for crime/illegal or fraud activities.

Cybersecurity

Cybersecurity is a coined technical computing term from “cyber” and “security” which means internet and safety respectively (Malik, 2019) Cybersecurity is thus the safety of every internet related activity. It evolved and continues to evolve as internet entrenches every aspect of human life activity, as various unauthorised persons steal the data or information being processed on the internet to the detriment of the owner. This, however, necessitates developing various techniques, architectures, designs, standards, and measures to mitigate internet attacks by internet criminals known as hackers or scammers (Sohal,2018).

II. The Concept of Internet-of-Things (IoT)

Internet of Things (IoT) is the network or connection of objects, devices, machines or processes so as to enable proper control and monitoring of the connected objects by human from a distance (i.e. remotely). The Internet of Things (IoT) refers to physical objects (or collections of such objects) that have sensors, processing power, software, and other technologies integrated into them that can connect to and exchange data with other systems and devices over the Internet or other communication networks 2019 (Mollah).

Internet of Things (IoT) according to Lee (2019), is an important technology in the world of computing (computer age) that guarantees a smart and easy-driven human life, by enabling real- communication between people, things, machines, processes, and everything else known as the user. The Internet of Things (IoT) is a system made up of physical objects and the sensors that are attached to them that are connected to the Internet through wired (guided) and wireless (unguided) networks. The figure 1gives the physical illustration of the concept of IoT.

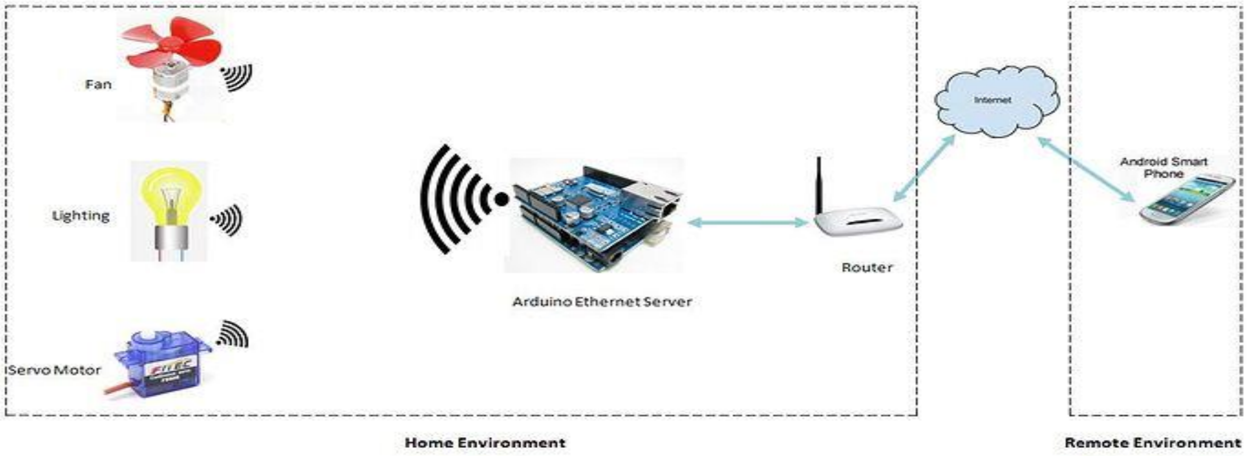

Figure 1: Communication interfaces of IoT

Cybersecurity of IoT

A number of security vulnerabilities on the Internet and in computer systems have been raised due to the growing use of computer networks, including, which springs another area of concern technically known as cybersecurity (Dhamdhere, 2008). Every business, regardless private or public, financial and non-financial, corporate and military, accesses their data online and stores data, programs, processes, and files on computers, clouds, and other devices. This highlights the importance of cyber security. And because these data are crucial and contain sensitive information that could be accessed by cybercriminals or cyber attackers (such as personal information, intellectual property, financial data, and unauthorized data), cyber security is crucial, and everybody needs to be aware of all the precautions that ought to be taken when using networks (Nadikattu, 2020).

The Concept of Industrial IoT

Industrial Internet of Things is known as IIoT. It is the internetworking of industrial machines, processes, and objects for efficient and optimized production services with less or no human rigorous intervention ((Hejazi, 2020). Millions of embedded devices are utilized in today's rapidly developing technology to ensure the safety and security of crucial applications including industrial control systems, contemporary automobiles, and vital infrastructure. The Industrial Internet of Things is the result of the recent convergence of traditional production engineering, automation, and intelligent computation technologies (IIoT). Increasingly more complex Cyber Physical Systems (CPS), which are embedded devices that may be freely programmed to control physical processes and machines, are replacing programmable logic controllers in industrial control systems, production systems, and factories. Although frequently connected via the Internet, CPS typically uses closed industrial communication networks for communication.

Architectural Layers in IoT Cybersecurity

Since each layer of the IoT architecture interacts with other layers and has specific security problems, Atzori (2010) argued that security measures should be considered for the entire design. We may gain a systematic and comprehensive understanding of IoT cybersecurity by conducting a literature evaluation of cybersecurity technologies via the lens of the IoT architecture. The following emphasizes on layer-level cybersecurity challenges and solutions and is based on Lee's five-layer business IoT architecture (Luigi, 2010).

III. Methodology

According to the literature that has already been evaluated, IoT cyber risk management has not received the required attention from the industry, leaving consumers and IoT devices open to assaults. The large range of linkages between the many devices and actors are too complex for the present risk assessment methods to handle (Neisse, 2019). We are motivated to build an IoT cyber risk management framework and architecture from each layer up that enhances the pre-existing frameworks and quantitative risk assessment methods because of our study of the earlier studies. The prevention-is-better-than-cure approach to IoT cyber risk management that is proposed by this study integrates the qualitative and quantitative approaches being established by early researchers and offers a crucial roadmap for efficient risk management and the necessary skills to avert IoT compromise and attacks. Using Cisco Packet Tracer, the figure 3.1 below was created to illustrate how the Industrial Internet of Things for a smart factory interconnect and interacts.

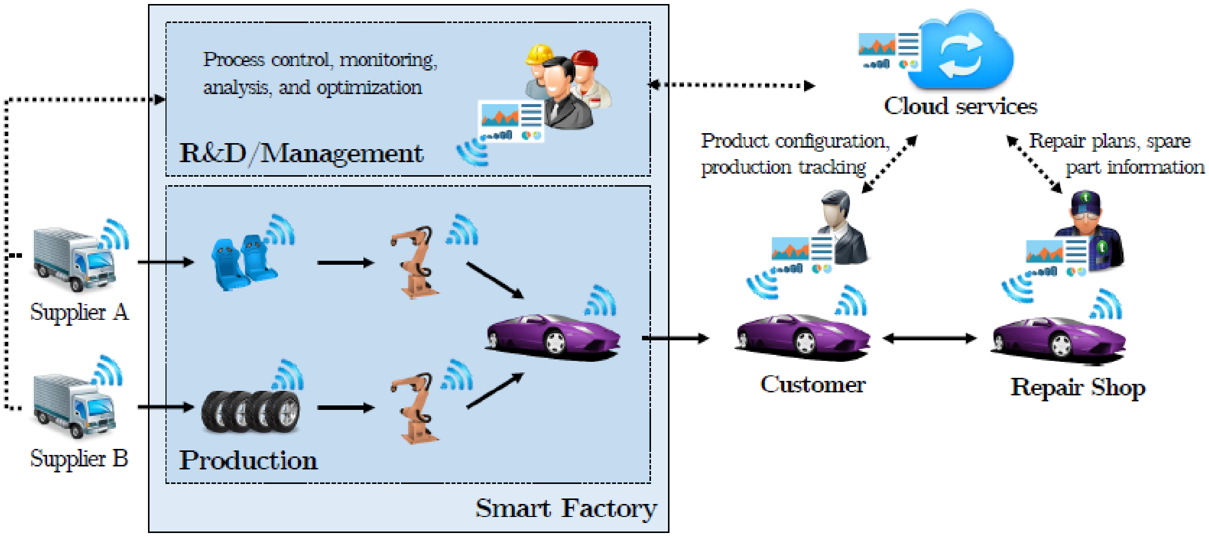
Process control, monitoring, analysis, and optimization
R&D/Management
Supplier A
Supplier B
Production
Smart Factory
Cloud services
Product configuration, production tracking
Repair plans, spare part information
Customer
Repair Shop

Figure 3.1: Communication between Industrial Internet of Things systems and devices

The following basic technical skills and cyber ethics was developed for IoT users and operators to maximally remain conscious of the vulnerability of IoT entities to cyber-attacks when ethics are being violated even nor matter the security architecture earlier established being implemented.

IV. Implementation of Secured Remote Access Methods during Configuration

The capability for the IoT user or operator to remotely communicate with the IoT devices through the internet has obviously introduced a significant deal of better functionality, meanwhile, secured access methods like Virtual Private Network (VPN), if remote access is necessary, it must be employed. for the operation of IoT systems. A VPN (Virtual Private Network) is a network that is connected to the internet but uses encryption to scramble all data transmission through the internet so that the entire network is 'virtually private'. It is a channel that encodes data transmitted through it for using public IT infrastructure (such as the Internet) to send and receive data in a secure manner. With the use of a VPN, IoT operators/users can remotely access internal resources like IoT devices and components, systems, processes, files, printers, databases, even organizations' websites in a way that seems it is directly linked to the Internet of Things. This remote access method can be made even more secure by restricting the IP addresses that are allowed to connect to the network using network devices and/or firewalls to only certain IP addresses and/or ranges. Remember that a VPN's security depends on the devices that are connected through it. Malware-infected laptops have the potential to introduce those weaknesses into the network, resulting in new infections and undermining the VPN's security. The next stage in security optimization is to address this.

V. Implementation of Network Segmentation and Firewalls

Network segmentation is the classification and categorization of information technology (IT) assets, data, and personnel into predefined groups called segments, after which access to these groups or segments are being restricted considerably. A breach of one device or component cannot result in the exploitation of the entire system when internet resources are divided into various areas or groups of a network. Otherwise, hackers might exploit any flaw in an organization's Internet of Things (IoT) system, known as the "weakest chain in the link," to access important hardware and data and travel throughout the network. Being made aware of the emergence of the "Industrial Internet of Things," a phenomenon in which several previously non-Internet connected objects, systems, and processes, such as the supply chain, industrial processes, video cameras, and others, are now connected to systems and the internet. Therefore, it can be hazardous to ignore segmenting organizational networks.

Accurate Maintenance of Inventory for Control System Devices and Elimination of IIoT Equipment’s Exposure to External Networks.

Allowing any industrial control network device to directly communicate with any device on the Internet is extremely dangerous and devastating. Even though the industrial control systems of some organizations may not directly communicate with the Internet, a connection still exists between them if those systems are connected to a portion of the network, such as the corporate side, that does. This portion of the network is frequently known as non-trusted or external resources. Even though enterprises might not be aware of the connection, persistent cyber attackers can nevertheless identify such channels and utilize them to get access to and exploit industrial control systems to cause a physical catastrophe. In order to ascertain where pathways do in fact exist, firms utilizing the Industrial Internet of Things (IIoT) must conduct detailed examinations of their IIoT systems, including the corporate enterprise parts. To lessen network vulnerabilities, every link between IIoT devices on the control system and equipment on other untrusted networks must be broken.

Develop and implement Role-Based Access Controls and System activity Logging

Using this approach enables all network resources to be accessed and communicated to base on job function. This limits access to IoT devices, data, and areas of the system that attackers and even specific users shouldn't have access to at a certain time. Define permissions based on the degree of access required for each job function to carry out its responsibilities and collaborate with human resources to put SOPs in place to block network access for former workers and contractors. Additionally, restricting operator and employee access with role-based access controls might make it easier to track network incursions or other suspicious activity while a company is conducting an audit. When logging capabilities are enabled, it helps to properly monitor all system activities at every time instance. This makes it possible for businesses to carry out exhaustive root-cause studies to identify the causes of systemic problems, which may have been caused by internal or external activity. Organisations can identify whether a user is acting improperly or whether an outsider has access to the system by monitoring network traffic, giving them the chance to act before issues arise.

Default Passwords Must be changed to Strong Passwords

No IT device or system must be operated upon with its default password, as it is generally known and expected to be changed at first use during setup or configuration. For administrator accounts and control system devices in particular, default passwords must be updated upon the installation of new software and on a frequent basis thereafter. To keep your systems and data secure, you must use strong passwords and use distinct ones for each account. A "brute-force attack" is when a hacker uses easily accessible software tools to try millions of character combinations to log in without authorisation. Longer passwords are more secure and should have at least eight characters to give attackers a larger pool of characters to choose from. Every strong password must also contain both uppercase and lowercase letters, numbers, and special characters. Add additional password security elements, such as a lock-out mechanism for accounts that kicks in after a certain number of erroneous password entries. Organisations might also think about mandating multi-factor authentication, which requires users to confirm their identities each time they sign in by entering numbers given to previously registered devices.

Implement Policies for Operating IoT Systems with Mobile Devices.

Significant security concerns are presented by the widespread usage of personal laptops, tablets, cell-phones, and other mobile devices at work. Due to their portability, these devices may be vulnerable to external, hacked networks, programs, and criminal actors on the internet that users are unaware of. The growing practice of companies enabling employees to use their personal electronic devices for work reasons, or the "Bring Your Own Device (BYOD)" idea, is a serious problem that contributes to these vulnerabilities. Additionally, all devices must be password-protected to ensure that only authorized users may log in. If not, an unauthorized user can simply utilize a device belonging to an authorized user to access systems and resources that are restricted on the network. Similarly, IIoT employees and operators should refrain from using other people's devices for industrial or office tasks because they cannot be certain that those devices are appropriately secured. Such devices can be infected and using them could jeopardize the security of the networks, information, and industrial systems being accessed.

Involve Executives in Cybersecurity

Researchers have found that organizational leaders frequently lack sufficient awareness of cybersecurity dangers and requirements, despite the ongoing spread of cyber threats and the potentially significant effects that cyber -attacks could have. The State of Malware Detection and Prevention, research by Cyphort and the Ponemon Institute, was released in March 2016. It detailed the significant difficulties that businesses encounter when trying to avoid and identify cyberattacks as well as prioritize and investigate malware alerts. Only 36% of respondents said IT security and other security-related personnel have the knowledge required to advise the C-suite about cutting-edge dangers. Additionally, according to 34% of respondents, C-level executives are never informed of security problems, according to the research. Many businesses are still unprepared for cyber threats, even though firms are progressively elevating cybersecurity to the executive level by creating the position of Chief Information Security Officer (CISO). The Securing the C-Suite report by IBM surveyed 700 executives from around the world to gauge their knowledge of cyberthreats. The findings show that there are four indicators that a company is not ready for cybersecurity attacks. These include misclassifying the actual dangers, failing to appoint a chief information security officer (CISO), failing to involve the entire C-suite in cybersecurity planning, and being hesitant to share information about cybersecurity threats with outside businesses.

VI. Implementation of Measures for Intrusion Detection and Prevention Plan

Despite the numerous precautions that companies take, many nevertheless encounter compromises. In fact, several cybersecurity experts have pointed out that experiencing a hack is more of a matter of "when" than "if." The organizations that identify the problem as soon as it arises and have a plan in place to address it will fare the best in the event of a compromise. Implementing measures like anti-virus software, logs, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) can aid in the early detection of compromises. The majority of IDSs and IPSs utilize signatures to find malware, port scans, and other strange network interactions. Anti-virus systems are frequently programmed to automatically update themselves to hunt for the most recent threat signatures because new viruses are discovered every day. However, for the purpose of finding infections, administrators shouldn't rely entirely on antivirus software. It is important to keep an eye out for infection indications in the logs from servers, firewalls, and intrusion detection and prevention devices. A vital yet neglected part of emergency preparedness and resilience is incident response planning. A successful cybersecurity response strategy will limit damage, boost partner and consumer confidence, and cut down on recovery time and costs. Plans should contain actions for responding to malicious software that is detrimental in an ICS environment. Organizations should be prepared to "island" their ICS environments in such circumstances by cutting off access to non-ICS networks.

VII. Conclusion

The security issues in the IoT space have changed, as this article has demonstrated. This study's methodical mapping process demonstrates how the evolution has occurred, what sorts of issues and solutions are present, and what gaps still need to be filled. According to the current research, a lot of security issues still exist and IoT security still needs a lot of improvement before it can be widely accepted by the general population. The most common ones are lack of management (i.e. enforcement) mechanisms, identification, authentication, and authorisation concerns, as well as privacy issues. Since the IoT devices frequently capture sensitive, private data, such medical records, privacy is of the utmost significance.

VIII. Recommendation

Larger IoT systems with hundreds of resolution variables, such as smart manufacturing and automated transportation systems, can be easily scaled up from smaller IoT applications. Organizations' inability to consistently monitor the use of technologies to quickly respond to cybersecurity breaches and assaults can still be effectively encouraged. However, further study may be done to improve the part of IoT security authentication, authorization, and access control that is deficient. The importance of authentication and security has increased due to the proliferation of IoT devices in smart industries and users' daily lives. Findings indicate that there is a need for a global, effective, and scalable solution for IoT authentication concerns. The access control problem can be solved so that not everyone has access to everything.

REFERENCES

Atzori, L.; Iera, A.; Morabito, G.(2010) The internet of things: A survey. Comput. Netw. 2010, 54, 2787–2805.

Dhamdhere, A.; Dovrolis, C. (2008) Ten Years in the Evolution of the Internet Ecosystem. In Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement, IMC '08, Vouliagmeni, Greece, 20–22 October 2008; pp. 183–196.

Hejazi, D.; Liu, S.; Farnoosh, A.; Ostadabbas, S.; (2020) Development of use-specific high-performance cyber-nanomaterial optical detectors by e_ective choice of machine learning algorithms. Mach. Learn. Sci. Technol. 2020, 1, 025007.

Luigi A, Antonio L, Giacomo M, (2010) "The internet of things: A survey", , vol. 54, no. 15, pp. 2787-2805, 2010.

Malik, V.; Singh, S. (2019) Security risk management in IoT environment. J. Discret. Math. Sci. Cryptogr. 2019, 22, 697–709.

Mollah, M.B.; Azad, M.A.; Vasilakos, A. (2017) Security and privacy challenges in mobile cloud computing: Survey and way ahead. J. Netw. Comput. Appl. 2017, 84, 38–54.

Nadikattu R.R.,(2020) New Ways of Implementing Cyber Security to Help in Protecting America (May 14, 2020). Journal of Xidian University, VOLUME 14, ISSUE 5, 2020, Page No: 6004 - 6015. Available at SSRN: https://ssrn.com/abstract=3622822

Neisse, R.; Hernández-Ramos, J.L.; Matheu, S.N.; Baldini, G.; Skarmeta, A.(2019) Toward a Blockchain-Based Platform to Manage Cybersecurity Certification of IoT devices. In Proceedings of the 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, 28–30 October 2019; pp. 1–6.

Rachna Buch, Dhatri Ganda, Pooja Kalola, NiraliBorad, (2019) World of Cyber Security and Cybercrime. Recent Trends in Programming Languages .ISSN: 2455-1821 (Online) Volume 4, Issue 2.

Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A(2018) cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. 2018, 74, 340–354.

Srinidhi N.N., Dilip Kumar S.M., Venugopal K.R.(2019) "Network optimizations in the Internet of Things: A review" in Engineering Science and Technology, an International Journal 22 (2019) 1–21