Modern Education
and Computer Science
PRESS

Best Practices for Facing the Security Challenges of Internet of Things Devices Focusing on Software Development Life Cycle

Ratun Rahman*
Software Engineer, Islamic University of Technology, Gazipur, Bangladesh
E-mail: ratunrahman@iut-dhaka.edu
ORCID iD: https://orcid.org/0000-0001-6718-0112
*Corresponding Author

Md Rafid Islam
Software Engineer, Islamic University of Technology, Gazipur, Bangladesh
E-mail: rafidislam@iut-dhaka.edu
ORCID iD: https://orcid.org/0009-0004-1140-7962

Abstract: In the past few years, the number of IoT devices has grown substantially, and this trend is likely to continue. An increasing amount of effort is being put into developing software for the ever-increasing IoT devices. Every IoT system at its core has software that enables the devices to function efficiently. But security has always been a concern in this age of information and technology. Security for IoT devices is now a top priority due to the growing number of threats. This study introduces best practices for ensuring security in the IoT, with an emphasis on guidelines to be utilized in software development for IoT devices. The objective of the study is to raise awareness of the potential threats and emphasize the use of secure software development lifecycle. The study will also serve as a point of reference for future developments and provide a solid foundation for securing IoT software and dealing with vulnerabilities. This paper divides the most common concerns with Internet of Things (IoT) security into three primary categories, and then further subdivides each of those categories into other subcategories.

Index Terms: IoT, Security, SDLC, Security challenges, Best practices

1. Introduction

Online threats and breaches have proved to be a real challenge for securing digital devices. IoT devices include more than just smartphones and computers; they can be almost anything that connects to the internet and communicates [1]. The number and variety of IoT devices are increasing daily, along with the vast amount of data they generate. Now the challenge is to keep this significant amount of data secure because there is always a looming threat of this data being stolen by potential cyber criminals [2]. IoT is used in various sectors, including the medical sector, and a cyberattack on the Internet of Medical Things can expose sensitive data about a patient and jeopardize his safety. By hacking into a smart home or smart car system, the safety of an individual can be compromised as well [3]. That is why ensuring IoT security is of utmost importance.

It is crucial to secure internet-connected devices and networks from cyber threats and intrusions. It can be accomplished by detecting, analyzing, and resolving potential security flaws across all devices [4]. Utilizing Safe Software Development Life Cycle (SSDLC) techniques to develop software in a secure manner is an efficient strategy to defend against threats [5]. The software development lifecycle consists of several stages: planning, design, building, testing, release, maintenance, update, etc. [6]. In order to address the many problems and challenges associated with IoT security, we have presented secure software development life cycle (SSDLC) that incorporates security at each of the previously listed stages. The purpose of the research is to increase people's knowledge of the potential risks and to place an emphasis on the adoption of a secure software development lifecycle.

In section 2, the concept of IoT devices, followed by security and types of threats for IoT devices. Relative works are mentioned after that. Security aspects in IoT are divided into 3 categories- people, processes, and technologies, and then broken down into various subcategories in section 3. Sections 4 and 5 cover the result and conclusion.

2. Related Works

This section will focus on introducing the new terms of the research as well as the previous experiments and research that were conducted in a similar field.

2.1. Background Study

2.1.1 IoT devices:

IoT stands for the 'internet of things', which represents physical devices with modern technologies [7]. These devices use the internet or other communication networks to connect and communicate with other devices and exchange information [8]. For example, smart doors use cards to read the data within them as a key and verification method. As a result, people do not have to carry a door key anymore. Some household devices have a common remote control system through a mobile phone. Therefore, a user can simply use that mobile phone to control all other technologies within its range. This reduces the complexity of lifestyles, and a user can control every technology with ease [9]. As the usage of modern devices is increasing rapidly and more and more devices are being added every year, it is safe to say that IoT is the future [10].

2.1.2 Securities for IoT devices

As the IoT may control critical functionalities and use the internet or other communication networks to work, the devices can be extremely vulnerable and a potentially high target for a hacker's attack [11]. Even the data from these devices can be used to exploit the user's lifestyle and other important information. This is why security is a major concern for the IoT. Therefore, almost all IoT devices have some built-in security features [12]. However, if the user is not careful and knowledgeable enough, a hacker can bypass the security. The U.S. Department of Defense has promulgated the Five Pillars of IoT Security, which are: confidentiality, integrity, availability, authenticity, and non-repudiation [13].

2.1.3 Types of threats and attacks for IoT devices

According to byos, six common attacks can be conducted on IoT devices. These attacks include

a) Botnets

Botnets are typical malware attacks where an attacker sends them through an email or device and the user accidentally or unknowingly accesses them. There are many anti-malware tools available, especially for botnets. However, they require storage space, which is very difficult to manage in IoT devices [14].

b) Ransomware

Ransomware on IoT devices mainly impacts the core functionalities and blocks them from functioning properly [15]. For example, attacking a security camera and stopping it from recording footage.

c) Convergence

All IoT devices are connected to some type of network to be controlled remotely [16]. Having a separate network to control the devices could stop coverage, however, people's demand has increased and they want to control it from anywhere. Thus, the Internet becomes the only viable option. This then provides attackers an easy option to bypass the internet protocol and control their functionalities if the user makes a human error [17].

d) Invisibility

As the usage of the devices is continuously increasing, it is becoming very difficult to monitor all the processes and traffic for abnormal patterns and threats [18].

e) Unencrypted data

Most IoT devices do not have an encrypted way to record data to save cost and complexity. They are mostly dependent on some types of clouds, which are particularly vulnerable to eavesdropping, espionage, and hijacking [19].

f) Rogue Devices

Rogue devices are solely built on doing harm to a system and stealing data and information. As many people are still unaware of IoT devices and how they perform, it is easier to install an extra or auxiliary device within an IoT device that goes undetected [20].

2.1.4 Software Development Life Cycle

The software development lifecycle (SDLC) is a methodological, multistage process that aims to produce productive and reliable systems in accordance with their functional and design specifications. When figuring out risk,

the whole IoT ecosystem needs to be taken into account. This includes both the Internet and the physical systems outside of IoT that use it. So, it is clear that IoT software must be secured in a systematic way throughout the lifecycle of IoT systems and services if they are to provide solutions that are reliable and failsafe. In this regard, it is necessary to secure the SDLC as a whole and take the appropriate factors into account [21].

Fig. 1. SDLC Phases

2.2. Relative Work

There have been some works and research that introduce and provide information about the security of IoT devices, mostly in recent years. 'Internet of Things' name was first mentioned by Kevin Ashton in 1999 when he proposed to put radio frequency identification chips on products for their tracking in a supply chain [22] but is was very simplistic point-of-view.

In order to observe who was at his door while he was working in the garage, Jamie Siminoff created the Ring doorbell in 2011, as he kept missing deliveries because he couldn't hear the doorbell from the garage [23], it was the first practical approach of IoT.

IoT keeps getting smarter after the introduction of the smart city in 2012. Smart City Switzerland has introduced over 60 projects, including traffic and air quality monitoring, smart transportation and parking, smart buildings, security, heating, lighting, etc [24] and things started to get more complex along with the functionalities where many people were involved. As many people were involved, the security concern grew more and more.

In 2015, IoT was connected with smartphones, which enabled new features and modifications to the devices as well as adding more devices to IoT. As mobile phones are the most common devices, they helped to connect all other modern devices, and the IoT industry has grown rapidly ever since [25].

In October 2021, May Mobility launched a pilot program to test its self-driving software. Self-driving vehicles are recent additions to the IoT [26].

Internet of Things (IoT): A literature review by Madakam, S., Lake, V has given a brief idea about IoT, its importance, and the future of IoT devices [27] but it does not talk about the security aspect of it. IoT security: ongoing challenges and research opportunities by Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K. and Shieh, S talked bout the threats and security issues of IoT [28] but does not provide any solution to the problem. Several surveys have also been conducted on the security of IoT. A survey on IoT security: application areas, security threats, and solution architectures by Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. [29] and The internet of things security: A survey encompassing unexplored areas and new insights by Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H. [30] are some examples. But they also does not give a proper guideline or instructions to overcome the issue. Security of IoT application layer protocols: Challenges and findings by Nebbione, G. and Calzarossa, M.C. has also added more information about the attacks on IoT devices and how to prevent them [31]. But it is mainly focusing on the application level where the user has no connection or have barely any connection to control or impact it.

3. Research Methodology

This section of the paper is going to focus on the good practices and guidelines that should be followed to address the threats that have a detrimental impact on the software development lifecycle of the IoT. The most frequently mentioned topics in regard to IoT security are grouped into three main categories, and they are broken down into subcategories, which are discussed in detail below:

3.1. People

From the software developers to the end users of the product, 'people' are security issues that impact all stakeholders involved in the life cycle of IoT software solutions.

a) Training and Awareness

Setting an organizational plan for specialized security training and raising awareness among all the personnel that is involved is the first step [32]. At all organizational levels, awareness should be increased. After that, an assessment should be made to determine if there is a need for skills or if resources need to be updated to keep them aligned with the latest developments. If the need arises, adequate resource allocation should be ensured by the organization to face any new threats.

b) Roles and Privileges

Appropriate people should be assigned after the roles are defined and the minimum level of privilege required for the roles is identified. After that, responsibilities and activities should be separated for the teams. Security controls should be implemented to prevent privilege abuse in the process, and resources need to be allocated to monitor it. A security officer must also be assigned to safeguard the physical facilities.

c) Security Culture

Incentives should be given to certain skilled people so that the organization can retain them. Along with that, to improve the process, security experts should be consulted. Threats or risks may arise at any time, necessitating, in addition to monitoring, a prompt response to security incidents.

3.2. Processes

Process is when a software project is conceptualized, developed, and brought to market, secure development processes ensure that security concerns are addressed.

a) Third-party Management

Integrity needs to be ensured by setting up a plan for managing the supply chain that includes a security framework. Software dependability should be evaluated while keeping security in mind. Before integrating third-party processes, they must be tested, and the third-party software components should be verified. Data leakages can be prevented by specifying confidentiality clauses.

b) Operations Management

There should be a well-defined plan put in place to deal with incidents and vulnerabilities. Also, a plan needs to be defined for change, patch, and configuration management.

c) SDLC Methodology

It is important to have an authorization policy in place so that only authorized users can use restricted resources. The automation of SDLC processes will decrease human error and effort. Additionally, testing must be incorporated into each phase of the SDLC.

d) Secure Deployment

To dispose of the solution, along with its data and components, a disposal strategy is required. To deal with evolving threats, a process for monitoring and updating should be established. Along with that, an automated testing and secure deployment strategy should be utilized.

e) Security Design

Firstly, a security framework and the least privilege principle are required. The security controls should be verified, and a design review should be conducted. After that, it is necessary to specify security requirements and conduct a risk assessment. The implementation of threat modeling and data classification is also essential.

f) Internal Policies

A communication plan should be established so that the entire organization is aware of the security measures. To

prevent information disclosure, it is necessary to implement security controls. It is also important to make sure that the security documents are up-to-date and to have backup plans ready in case some resources aren't available.

3.3. Technologies

Technologies are technological tools and procedures used in the software development process to minimize vulnerabilities and defects.

a) Access Control

In addition to storing user credentials securely, it is essential to implement authorization to ensure that applications have the appropriate permissions. Physical protection should be deployed to prevent physical damage.

b) Third-Party Software

When utilizing third-party software components, it is essential that they are patched for the most recent threats discovered. It is better to rely on known secure frameworks.

c) Secure Communication

For secure communication using proven encryption techniques, implementing secure web interfaces and session management are necessary.

d) Secure Code

Secure coding practices and software development techniques should be implemented, and audit capability should be provided in the development phases. Countermeasures are required against rogue code and unauthorized code modification.

e) Security Reviews

It should be ensured that source code is evaluated in terms of security and that attack surface analysis is performed, followed by IoT SDLC tests. In the event that any SDLC phase is interrupted, a contingency plan should be in place.

f) Security of SDLC Infrastructure

Logs should be kept of the different tools used in SDLC phases and IoT systems. A physical detection system and a mitigation plan are required to protect SDLC infrastructure.

g) Secure Implementation

The first step is to modify the default settings and then put restrictions on component customization to prevent losing security functionalities. Additionally, end users should be provided with secure configuration.

This methodology represents if all three of the main categories are implemented properly and effectively in SDLC model, it can be considered as the best practice to secure an IoT device.

4. Result and Discussion

It is evident that people, procedures, and technologies all play vital roles in the security measures for IoT devices. Recent years have seen a significant increase in malware and other types of cyberattacks [32]. Both the consumer and the developer of IoT devices will surely benefit from using the security protocols discussed in this article to address some security concerns. To increase knowledge and adjust the development process appropriately, additional research must be done on the specifics of these protocols. It is challenging to switch to a new, modern system nonetheless [33]. But because the Internet of Things (IoT) is so new and has lately become popular, it is imperative to introduce these protocols. A more effective security defense against vulnerabilities can be achieved by using the software development life cycle (SDLC). This approach can also be used to address a number of additional IoT device issues. So, a significant outcome of this study is the introduction and utilization of secure SDLC in IoT devices.

5. Conclusions

It is crucial to assess the ever-increasing cybersecurity threats and put in place suitable countermeasures to deal with typical vulnerabilities that can result from unsecure practices in various SDLC phases. The purpose of the study was to give IoT software developers, maintainers, testers, and system engineers something they could use as a reference and benefit from in the long run. During different stages of software development, such as design, implementation, testing, integration, and maintenance, guidelines and principles to keep in mind for ensuring security are pointed out.

Acknowledgment

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Samie, F., Bauer, L. and Henkel, J., 2016, October. IoT technologies for embedded computing: A survey. In *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)* (pp. 1-10). IEEE.

[2] Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A. and Kamal, T., 2015. A review on internet of things (IoT). *International journal of computer applications*, *113*(1), pp.1-7.

[3] Zeng, E., Mare, S. and Roesner, F., 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (pp. 65-80).

[4] Frustaci, M., Pace, P., Aloi, G. and Fortino, G., 2017. Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal*, *5*(4), pp.2483-2495.

[5] ul Hassan, S.Z. and Ahmad, S.Z., 2021. The Importance of Ethical Hacking Tools and Techniques in Software Development Life Cycle. *International Journal*, *10*(3).

[6] Roman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), pp.2266-2279.

[7] Rayes, A. and Salam, S., 2019. Internet of things (IoT) overview. In *Internet of Things from hype to reality* (pp. 1-35). Springer, Cham.

[8] Alam, T., 2018. A reliable communication framework and its use in internet of things (IoT). *CSEIT1835111/ Received*, *10*, pp.450-456.

[9] Botta, A., De Donato, W., Persico, V. and Pescapé, A., 2016. Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, *56*, pp.684-700.

[10] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), pp.1645-1660.

[11] Abomhara, M. and Køien, G.M., 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, pp.65-88.

[12] Blythe, J.M. and Johnson, S.D., 2018, March. The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1-7). IET.

[13] Zhang, N., Demetriou, S., Mi, X., Diao, W., Yuan, K., Zong, P., Qian, F., Wang, X., Chen, K., Tian, Y. and Gunter, C.A., 2017. Understanding IoT security through the data crystal ball: Where we are now and where we are going to be. *arXiv preprint arXiv:1703.09809*.

[14] Bertino, E. and Islam, N., 2017. Botnets and internet of things security. *Computer*, *50*(2), pp.76-79.

[15] Yaqoob, I., Ahmed, E., ur Rehman, M.H., Ahmed, A.I.A., Al-garadi, M.A., Imran, M. and Guizani, M., 2017. The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, pp.444-458.

[16] Almusaylim, Z.A. and Zaman, N., 2019. A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Wireless networks*, *25*(6), pp.3193-3204.

[17] Biswas, A.R. and Giaffreda, R., 2014, March. IoT and cloud convergence: Opportunities and challenges. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 375-376). IEEE.

[18] Bhardwaj, A., Al-Turjman, F., Kumar, M., Stephan, T. and Mostarda, L., 2020. Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems. *IEEE access*, *8*, pp.104956-104966.

[19] Wood, D., Apthorpe, N. and Feamster, N., 2017, November. Cleartext data transmissions in consumer iot medical devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (pp. 7-12).

[20] Surya, L., 2016. Security challenges and strategies for the IoT in cloud computing. *International Journal of Innovations in Engineering Research and Technology ISSN*, pp.2394-3696.

[21] Dias, J.P. and Ferreira, H.S., 2018. State of the software development life-cycle for the internet-of-things. *arXiv preprint arXiv:1811.04159*.

[22] Ashton, K., 2009. That 'internet of things' thing. *RFID journal*, *22*(7), pp.97-114.

[23] Suresh, P., Daniel, J.V., Parthasarathy, V. and Aswathy, R.H., 2014, November. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In *2014 International conference on science engineering and management research (ICSEMR)* (pp. 1-8). IEEE.

[24] Anthopoulos, L.G., 2015. Understanding the smart city domain: A literature review. *Transforming city governments for successful smart cities*, pp.9-21.

[25] El Khaddar, M.A. and Boulmalf, M., 2017. Smartphone: the ultimate IoT and IoE device. *Smartphones from an applied research perspective*, *137*.

[26] Uhlemann, E., 2016. Connected-vehicles applications are emerging [connected vehicles]. *IEEE Vehicular Technology Magazine*, *11*(1), pp.25-96.

[27] Madakam, S., Lake, V., Lake, V. and Lake, V., 2015. Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), p.164.

[28] Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K. and Shieh, S., 2014, November. IoT security: ongoing challenges and research opportunities. In *2014 IEEE 7th international conference on service-oriented computing and applications* (pp. 230-234). IEEE.

[29] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B., 2019. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, pp.82721-82743.

[30] Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H., 2022. The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, p.102494.

[31] Nebbione, G. and Calzarossa, M.C., 2020. Security of IoT application layer protocols: Challenges and findings. *Future Internet*, *12*(3), p.55.

[32] Rahman, R., Islam, M.R., Ahmed, A., Hasan, M.K. and Mahmud, H., 2022, November. A Study of Permission-based Malware Detection Using Machine Learning. In *2022 15th International Conference on Security of Information and Networks (SIN)* (pp. 01-06). IEEE.

[33] Islam, M.R., Rahman, R., Ahmed, A. and Jany, R., 2022. A Survey of Software Metrics for Transitioning to An Updated Version of The Current Existing Framework Or A New Framework.

Authors' Profiles

Ratun Rahman graduated with his Bachelor of Science degree in Software Engineering from the Islamic University of Technology (IUT) in 2022. He also published his first research in the same year. His research interest includes Human-Computer Interaction. His BSc thesis was focused on permission-based malware detection using machine learning.

Md Rafid Islam graduated with a Bachelor of Science in Software Engineering from the Islamic University of Technology in 2022. His bachelor's thesis was in the field of software security, focusing on malware detection. Apart from software engineering, he is interested in cybersecurity, IoT, and cloud computing.