International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
***Article Received:** 25 January 2023 **Revised:** 12 March 2023 **Accepted:** 30 May 2023*

A Comprehensive Analysis of Password Authentication for Enhancing Security in Internet of Things (Iot)

P. Padmasini,
Research Scholar, Department of Computer Science, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India – 620023
padmasaravanmohit2020@gmail.com

Dr. K. Muthuramalingam,
Assistant Professor, Department of Computer Science, Bharathidasan University,
Tiruchirappalli, Tamil Nadu, India – 620023
muthuramalingam@bdu.ac.in

Abstract
Recently, there has been a significant increase in customer demands and the variety of services provided due to the increasing use of mobile devices and the development of new networking technologies such as the Internet of Things (IoTs) and Big data networking. The proliferation of future smart cities, smart transport systems, and other Internet of Things (IoT) application areas presents a significant vulnerability to a multitude of security risks that can have detrimental impacts on the economy, the environment, and society. This vast range of functions raises several security concerns, such as data protection, virtualization vulnerabilities, segregation risks, network connectivity issues, and monitoring challenges. The objective of identity and access management is to ensure that the right individuals have access to the right resources. Implementing user identification and identity verification establishes a robust security measure that effectively separates potential attackers from accessing sensitive data. This study use a Systematic Literature Review (SLR) methodology to conduct a comprehensive review of security concerns and various computing approaches to mitigate them. Despite the existence of various approaches to address the specific challenges related to application design, security, and privacy, there is still a need for a comprehensive research study. This study should focus on the challenges and requirements of targeted applications, which currently have limited security enhancement solutions.
Key Words: Internet of Things, Systematic Literature Review, Security Threats and Password Authentication.

1. Introduction

The Internet of Things (IoT) and its components can be interpreted and understood in several ways. People frequently engage in conversations about the objects, equipment, and sensors that connect the physical world to the digital realm. Like other disruptive technologies such as artificial intelligence, smartphones, and cloud computing, the Internet of Things (IoT) has shown its capacity to profoundly influence society by changing various institutional organizations, industries, and aspects of our everyday lives. The Internet of Things (IoT) envisions a future when billions of interconnected objects will be linked to the Internet and engage in communication with each other. This suggests that a substantial amount of data will traverse the network, undergo processing, and be exchanged among the devices. Moreover, with the increasing proliferation of intelligent devices and the introduction of mobility characteristics, the Internet of Things (IoT) is susceptible to many security vulnerabilities inherent in its adaptable communication architecture. The extensive utilization of IoT infrastructure raises numerous complex concerns, including cloud computing, big data analytics, accessibility, reliability, interoperability, mobility, and modular sensor design. Upon first examination of the components of the Internet of Things (IoT), a recent paper provides valuable insights that could facilitate the establishment of standards and encourage the adoption of formalization, logical reasoning, simulations, reliability measures, and security risk analysis for the IoT [1]. IT risk analysis is a service that identifies and evaluates potential risks, and determines the most effective strategies to mitigate harm to users or organizations connected to a network. The risk analysis function utilizes an algorithm to study and assess risk event data, taking into account the most up-to-date pattern, as long as a risk condition is present. Subsequently, it presents the findings of the study and recommends the necessary supplementary actions that, when executed, will mitigate the risk [2].

The growing urbanization necessitates the implementation of efficient and sustainable intelligent

solutions in transportation, the environment, energy, and government issues for the development of smart cities. An excellent choice is the smart city infrastructure, which integrates the Internet of Things (IoT), Big Data, and Energy Internet. It presents several challenges, such as inadequate IoT security, challenges in equipment maintenance and upgrades, high operational expenses related to constructing extensive data centers, limited resilience to damage, difficulties in establishing trust among Internet users, vulnerability to user privacy breaches, an inappropriate business model, and additional concerns. The offered solutions address many difficulties such as insufficient security in IoT, enhancing equipment maintenance, and updating. These solutions are identified by evaluating their unique qualities and comparing their shared features [3].

The proliferation of IoT devices on the Internet is rapidly increasing in tandem with the advancement of IoT technology. IoT devices have undergone a transformation, enabling them to efficiently communicate with the physical world, detect it, and autonomously make judgements. Consequently, they have become increasingly popular in several fields of application. The proliferation of IoT devices has undoubtedly enhanced consumer convenience, although the escalating apprehensions over security have resulted in a surge of threats targeting IoT security. Given that IoT devices incorporate a Web application system for device managers [4], ensuring the security of this system is of utmost importance. It enables the monitoring, control, and configuration of device information and status. Continuous research poses challenges due to the need for ongoing updates to verification procedures when the IoT device and Web system undergo upgrades. Web devices were logged using password information and authentication mechanism. The prevalence of weak web passwords is a significant concern due to the lack of security awareness among many employees. The current widespread use of billions of interconnected IoT services, applications, and devices requires a thorough reassessment of security concerns.

2. Addressing Potential Risks through Internet of Things

IoT devices have advanced to possess the capability to perceive the physical environment and autonomously make decisions. Consequently, due to their successful interaction with the real world, they have garnered widespread popularity in several application domains. The concept of the Internet of Things (IoT) is introduced by the rapid proliferation of Internet-connected devices, which encompass a wide range of objects such as vending machines, electronic appliances, cameras, smart bulbs, smart locks, thermostats, and more. These devices include small sensors as well as cloud servers. The widespread adoption of IoT infrastructure presents several challenging issues, such as accessibility, reliability, compatibility, and mobility. The Internet of Things (IoT) encompasses a wide range of network applications, such as those for smart cities, smart agriculture, smart education, smart health care, smart waste management, smart surveillance, logistics, supply chains, and more [5]. With the widespread utilization of billions of interconnected IoT devices, services, and apps, it is imperative to reassess the security issues associated with the Internet of Things. IoT devices employ the store-carry-forward approach to transmit packets while having limited storage capacity. This results in the generation of a substantial volume of data, which in turn presents a vulnerable target for potential attacks. This endeavor aims to optimize user autonomy and adaptability by exploring strategies for effectively overseeing privacy concerns in IoT devices. Users have a particular anxiety regarding the documentation of their private activities and the gathering and dissemination of their personal information. This is why security is commonly regarded as a major obstacle to the implementation of Internet of Things (IoT) technology. Users of IoT medical devices are particularly concerned about the potential obstacles associated with the collection and sharing of personal data, including dietary choices, exercise statistics, running routes, and sleep habits, with third parties [6]. Transparency enables individuals to comprehend the use and handling of their personal data. Data transparency is crucial for ensuring security, especially given the advancements in big data and the utilization of machine learning methodologies. Due to the utilization of distinct identifiers in most communication protocols to conceal user identities, there is an increased vulnerability to misuse as a result of centralized data analysis and unauthorized entry. Attaining absolute anonymity is improbable due to the potential misuse of IoT devices. End users may grant consent to IoT device manufacturers for accessing and analyzing their data, provided that they receive some form of value in return.

The essential factors for achieving success in reducing dangers in IoT devices were identified and consolidated through a comprehensive analysis of the available literature [7]. A design that is basic or straightforward facilitates the user's comprehension of aspects such as layout, interface organization, functionality, structure, workflow, and framework. Before collecting personal data, explicit permission refers to the act of seeking approval or authorization. In order to safeguard the security of IoT device users, explicit authorization is necessary. Additionally, the consent form

must explicitly state that the data will not be utilized for any reasons other than those originally intended. The objective of this study is to identify the most effective approaches for mitigating privacy risks in IoT devices, with a focus on adopting a user-centric strategy that empowers users with greater freedom and control.

3. Future for IoT connected Devices.

The Internet of Things (IoT) is an extensive network including interconnected intelligent devices that gather environmental data and transfer it to other devices or their controllers. The Internet of Things (IoT) leverages the concept of ubiquitous computing, communication protocols, and applications to convert ordinary objects into intelligent ones. Policies and procedures are designed to guide IoT devices in data exchange, determining data boundaries, and complying with the specific functions required for different applications. The applications themselves determine the granularity and scope of the IoT device, as well as the volume of data that is inputted for analytics purposes.

The vast capacities offered by 5G networks have enabled the movement of large amounts of private and sensitive data between 5G-IoT devices. However, if these networks were to be targeted by adversaries, the potential implications might be catastrophic. These Internet of Things (IoT) gadgets are equipped with integrated sensors that allow them to gather environmental data. The presence of diverse devices with varying communication and security designs in 5G-IoT networks introduces an additional challenge [8]. Attaining ideal levels of Quality of Service (QoS) while ensuring high levels of security and privacy protection is both necessary and challenging. 5G networks are utilized to transmit Internet of Things (IoT) communications, resulting in networks with significantly reduced latencies, superior energy efficiency, enhanced capacity, reliability, high speeds, and adaptability. This is done to enhance Quality of Service (QoS) and meet diverse user demands. 5G-IoT networks, however crucial in people's lives, are susceptible to many storage and security issues due to their numerous vulnerabilities.

Communication protocols commonly employ unique identifiers to conceal the identity of users, hence increasing the potential for abuse due to centralized data analysis and unauthorized access. Upon thorough examination of the existing literature, designers have compiled and organized the essential success characteristics that are highly regarded for mitigating hazards in IoT devices. The implementation of 5G networks to facilitate communication between devices is a response to the need for improved quality of service (QoS) and security in Internet of Things (IoT) networks [9].

4. Software Enhancements for Internet of Things

Contemporary software systems are intricate, featuring a multitude of interrelated and interacting elements. Contemporary software systems often need to upgrade its interconnected and complex components to solve problems, fix security flaws, add or remove functionality, and perform other vital actions. Software upgrades are frequent, and a significant number of them exhibit incorrect behavior under specific circumstances. By utilizing the feature of the upgrade, users of the latest software version can effectively mitigate a significant number of these concerns. Due to the vast number of potential environment configurations and user inputs, developers cannot predict or test every single scenario that could be utilized to operate the software. As a result, many updates either fail or lead to unfavorable outcomes for certain users [10].

As a firm expands, it can choose for a freemium approach, offering both complimentary items and exclusive services, or it can persist with its existing strategies and sell its products. In the presence of piracy and premium services, it is advisable for a corporation to apply copyright protection since it can effectively reduce competition in terms of pricing between the original product and the enhanced version. Unless both of the following criteria are satisfied: the disparity between the initial product and the enhanced version must be negligible in terms of consumer preference and moderate in terms of product value. When it comes to these situations, the freemium technique consistently surpasses the standard strategy [11]. Most contemporary IoT devices are equipped with sensors as their fundamental component, facilitating a diverse array of user-friendly applications and ensuring constant connectivity between the devices and the external environment. Security is a significant concern in IoT networks due to the proliferation of diverse goods and the escalating hazards to our daily lives.

5. Software Standardization for Internet of Things

The Internet of Things (IoT) has experienced significant growth since its inception, but the standardization process for safe IoT systems is still in its early stages. Researchers have produced numerous meticulous review publications on the frameworks, designs, and vulnerabilities of IoT at different levels. However, a significant portion of the existing research has overlooked the security implications of firmware in the IoT platform. Consequently, there is a dearth of comprehensive research on IoT software security that specifically defines the primary factors contributing to system software vulnerability in IoT and enumerates vulnerabilities [12]. The functionality of IoT devices has

evolved to include the ability to see the physical environment and make independent judgements. As a result of their efficient communication with the physical world, IoT devices have gained significant popularity across several application domains. After gathering and analyzing the synthesized knowledge, strategists made the decision to divide the development of the standardized technique into multiple phases.

The initial phase will entail refining the issues to be addressed in the protocol statement and performing an electronic brainstorming session with a team comprising users, specialists, and individuals experienced in this technology. Before doing an integrative evaluation using scientific resources, a few topics will be selected and refined, and the previously determined descriptors will be utilized. The protocol update and recommendations for additional investigation consist of the following stages, as well as peer review conducted by specialists. The evaluation step, which is preceded by implementation, is the final and crucial stage, followed by the diffusion of the protocol [13]. Computationally demanding tasks need to be sent to the cloud, which has exceptional processing and storage capabilities, as IoT networks are incapable of handling them. Furthermore, the use of cryptographic procedures such as Signcryption techniques for authentication and confidentiality, along with the broad connectivity and group key management policy, leads to an increase in the complexity of network resources [14].

6. Conclusion

Contemporary Internet of Things (IoT) devices rely heavily on sensors to facilitate a diverse array of user-friendly applications and ensure seamless interaction between the devices and the physical environment. Security is a paramount concern in Internet of Things (IoT) networks, which consist of a large multitude of interconnected devices. To efficiently address privacy risks in IoT devices, such as anonymity, transparency, simplicity, explicit agreement, and compliance with the General Data Protection Regulation, a user-centric approach is employed to enhance user control and adaptability. Robust cryptographic methods are developed and essential for ensuring data authentication, privacy, confidentiality, integrity, and other security aspects in order to safeguard the entire IoT architecture. These findings led to the creation of a self-assessment scorecard that allows analysts and decision-makers to evaluate their present performance in relation to best practices and successfully reduce privacy threats in IoT devices. A variety of privacy and security mechanisms have been developed, utilizing resources such as public key infrastructure, smart cards, passwords, and blockchain. Nevertheless, most of these protocols exhibit substantial deficiencies in terms of privacy and security, and a number of these schemes possess intricate structures that render them unsuitable for IoT devices. An authorization procedure is implemented by employing security tokens to validate access and membership, while also allowing entry for relevant groups, with the aim of thwarting user collusion and insider attacks by privileged individuals. A method is developed that uses biometrics and elliptic curve encryption to authenticate communication entities without relying on a central authority, which could potentially resolve single point of failure problems. The network resources have additional complexity due to cryptographic processes such as Signcryption techniques, which are employed for authentication and confidentiality. This is mostly due to the extensive connectivity and the need for managing group keys. Computationally demanding tasks need to be offloaded to the cloud due to the superior computational and storage capabilities it offers, as IoT networks are incapable of handling them.

Reference

[1] J. Voas, B. Agresti and P. A. Laplante, "A Closer Look at IoT 's Things," in IT Professional, Vol. 20, No. 3, Pages 11-14, May./Jun. 2018, doi: 10.1109/MITP.2018.032501741.

[2] H. Chung, S. P. Cho and Y. Jang, "Standardizations on IT risk analysis service in NGN," 16th International Conference on Advanced Communication Technology, 2014, Pages 410-413, doi: 10.1109/ICACT.2014.6778992.

[3] S. Li, "Application of Blockchain Technology in Smart City Infrastructure," 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), 2018, Pages 276-2766, doi: 10.1109/SmartIoT.2018.00056. [4] Inderpal Singh and Balraj Singh, “Access management of IoT devices using access control mechanism and decentralized authentication: A review”, Measurement: Sensors, Volume 25, February 2023, Article 100591

[5] Nipun Srivastava and Pallavi Pandey, “Internet of things (IoT): Applications, trends, issues and challenges”, Materialstoday Proceedings, Volume 69, Part 2, Pages 587-591, 2022,

[6] Sitesh Mohanty, Kathryn Cormican*, Chandrasekhar Dhanapathi, “Analysis of critical success factors to mitigate privacy risks in IoT Devices”, Procedia Computer Science 196, Pages 191–198, 2022.

[7] Kishori Kasat, D. Leela Rani, Bhola Khan, Ashok.J, M.K.Kirubakaran, P.Malathi, "A novel security framework for healthcare data through IOT sensors", Measurement: Sensors, Volume 24, December 2022, Article 100535

[8] Vincent Omollo Nyangaresi, "Terminal independent security token derivation scheme for ultra-dense IoT networks", Array Volume 15, September 2022, Article Number 100210

[9] Wanying Guo, Nawab Muhammad Faseeh Qureshi, Isma Farah Siddiqui, Dong Ryeol Shin, Cooperative Communication Resource Allocation Strategies for 5G and Beyond Networks: A Review of Architecture, Challenges and Opportunities", Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 10, Part A, Pages 8054-8078, 2022.

[10] Rekha Bachwani, Olivier Crameri, Ricardo Bianchini, Willy Zwaenepoel, "Recommending software upgrades with Mojave", Journal of Systems and Software, Volume 96, Pages 10-23, October 2014,

[11] Dan Wu Guofang Nan, Minqiang Li, "Optimal software upgrade strategy: Should we sell products or premium services in the presence of piracy?", Electronic Commerce Research and Applications, Volume 28, Pages 219-229, March – April 2018

[12] Ibrahim Nadir, Haroon Mahmood, Ghalib Asadullah, "A taxonomy of IoT firmware security and principal firmware analysis techniques", International Journal of Critical Infrastructure Protection, Volume 38, September 2022, Article Number 100552

[13] Lídia Maria Lourençön Rodriguesa, Inacia Bezerra de Limab, Luiz Ricardo Albano dos Santosa, Valdes Roberto Bollelaa, Maria Manuela Cruz-Cunhac, Rui Pedro Charters Lopes Rijod, Domingos Alvesa, "Towards a standardized protocol for conducting randomized clinical trial for software", Procedia Computer Science, Vol 138, Pages 125 – 130, 2018.

[14] Padmalaya Nayak, G Swapna, "Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview", Internet of Things, Volume 21, April 2023, Article Number 100641