Implementation of NFC into the authentication system of the IOT devices

Lim Pei Hui[1], Intan Farahana Binti Kamsin[2], Zety Marlia Zainal Abidin[3] and Hemalata Vasudavan[4]
[1'2'3'4] Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
[1]limmelina2011@gmail.com, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my, [4]hemalata@staffemail.apu.edu.my

***Abstract*— The Internet of Things (IoT) is a popular technology that creates a network by connecting and with other devices and systems over the internet. Due to its popularity and weak security, it has become one of the prime targets for the attackers. This research aims to propose a new authentication system for IoT devices to solve the security issue found in default passwords. A questionnaire is proposed to be conducted to IoT users in different age range to understand more on their experience in using IoT devices. The information collected will be beneficial for the research. The proposed solution is discussed in this research. By combining NFC technology and MAC address, it can replace the current password authentication used in IoT devices. The solution is more user friendly, and it helps to strengthen the security in IoT devices. Although the proposed solution will aid on the default and weak password part of the IoT devices, there is also vulnerabilities in the system. The research will help to bring more insight and attention to researchers to research more about the security of IoT devices in the future.**

***Index Terms*— Internet of Things, Near Field Communication, Authentication, Security, MAC Address**

1. Introduction

The Internet of Things (IoT) is a network of physical items that are integrated with technology. Technologies such as sensors and software are used to link and share data with other devices and systems over the internet. IoT has emerged as one of the most essential technologies in today's world, with applications ranging from simple domestic gadgets to industrial machinery. [1]

Due to its popularity, IoT is also one of the popular targets of cybercriminal. Research shows that 10% to 40% of the IoT devices are vulnerable to attacks due to the implementation of default settings and default passwords. [2]

This research proposed a more secure environment in IoT devices by utilizing NFC technology and MAC addresses. The solution helps to protect user privacy by limiting the access to the IoT configuration settings to prevent unauthorized use by attackers. This research also discusses the issues that exist in IoT, NFC and other similar technologies. The study also proposed a data collection method as well as an overview that demonstrates how the proposed system works.

2. Literature Review

2.1 Research Domain

2.1.1 Internet-of-Things

Internet of Things (IoT) refers to the items in the world to be networked and interact with one another over the Internet [3]. IoT devices have implemented many technologies such as radio frequency identifications (RFIDs), and cloud computing to establish the communication between the components in the IoT devices. [3] [4]

Today, billions of IoT users communicate with one another over the Internet using TCP/IP and share various data throughout the day [4]. IoT devices are estimated to be responsible for 50% (14.7 billion) of all global connected devices by 2023, with roughly one-third of those being wireless IoT devices [5].

IoT systems are vulnerable to multiple attacks, as well as data leaks [4] [6]. Many IoT devices have default/generic accounts and simple passwords as it is cheaper to implement [7].

Users like the simplicity of default passwords and are frequently unaware of information security issues. Thus, the creation of the Mirai botnet, to exploit weak passwords in IoT devices [8]. Mirai operates by scanning IP addresses for IoT devices, identifying IoT devices with a table of over 60 default usernames and passwords, and then logging into the system and infect them with the Mirai virus. Infected devices will be slower, and more bandwidth is used. [9]

Therefore, in this research, it is proven that the security of IoT devices is weak due to huge cost and insufficient knowledge of user in this matter.

2.1.2 Near Field Communication

Near-field communication (NFC) is a limited range wireless communication technology. It is bidirectional, which means that data may be sent in both directions at a transmission range of less than 10 cm and running on the unregulated 13.56 MHz frequency band. To communicate between any mobile devices and the NFC tag, either the tag is contacted with the reading device, or they are held together tightly [10] [11] [12].

Because of its shorter range, NFC is more secure than RFID, but RFID has a higher risk for unwanted tag readings, also known as eavesdropping [11]. Reference [10] states that NFC

operates in three modes which are peer-to-peer, read/write, and NFC card emulation.

NFC is implemented in various sectors especially in the mobile payments sector and many mobile phones have built-in NFC sensors [2] [13]. Referring to [14], it stated that the NFC reader uses high power consumption which will not be suitable for personal use.

Therefore, in this research, it is proven that NFC is a suitable technology to be implemented in IoT devices to replace passwords.

2.1.3 Media Access Control Address

Media Access Control (MAC) Address is a 48-bit address that is allocated to a device permanently. The manufacturer of the devices is responsible for assigning this address. Every host on a network has a unique MAC address to allows them to connect with other hosts [15] [16].

The MAC address is used in an Ethernet network to uniquely identify each device on the network. To guarantee that packets travel to their destination, every packet broadcast across the network must include the MAC address of the intended recipient [17].

Therefore, in this research, it is stating that MAC address can be used as an identifier to authentication as each devices contains different MAC addresses.

2.2 Similar System

2.2.1 Text-based Password

Text-based passwords are an extensively used authentication technique. Password authentication is straightforward to set up since, unlike biometric authentication, it requires no equipment and relies simply on the users' memory. As a result, people generally use easy-to-remember passwords such as "admin." IoT default passwords are similarly text-based and easy to crack [18].

A user's IoT account may be used to manage many IoT devices. As a result, if an attacker gains access to the account, they can manage the device via the app. A brute-force attack is an attack that is used to test the potential passwords of the device [19].

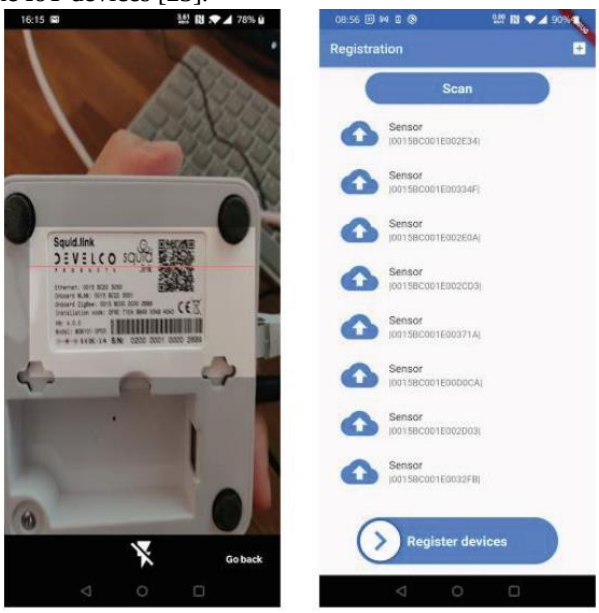
One of the examples of password attack in IoT devices is the Mirai Botnet. It is targeted to IoT devices with a flaw in its security system, particularly one whose login and password have not been updated or uses a weak password [20].

2.2.2 Quick Response Code

A QR code is a square-shaped barcode and can be read rapidly by a digital device. Senso Wave invented it in 1994 [21].

QR code can also be used in authentication into a system. The QR code stores the login key to the system. When the user scans the QR code using a QR code scanner, the user will be granted access to the system [22].

Referring to a journal, it shows that static QR codes are printed in the IoT devices [23].



(a) QR code scan. (b) Mobile app.

Figure 1: IoT device registration using QR code [23].

Static QR codes are readily duplicated and altered, and there are significant security flaws as users are unable to change or replace the QR codes [24].

2.2.3 Near Field Communication

NFC is a radio technology that allows two NFC-enabled devices to communicate to each other in a short range. Communication happens when two NFC compatible devices are brought together within 10 cm of each other. It runs at 13.56 MHz and has a data transfer rate of 424 Kbits per second [25].

The flexibility of NFC over other wireless protocols is its key benefit. Contacting a reader, another NFC device, or an NFC compliant tag initiates transactions automatically. The downside of NFC is that it cannot interact with another NFC reader or device if the distance between them exceeds 10 cm. As a result, it cannot be used to transfer data across great distances [25].

NFC technology was created to assist rapid financial transactions such as purchasing tickets, goods, or services, allowing it to become one of the digital wallets in addition to credit cards. NFC technology has also been implemented in mobile phones for digital wallets [26].

3. Problem Statement

The Internet of Things (IoT) helps to improve the user's lifestyle by connecting most of the objects to create a new digitized service. Currently, various IoT applications, such as wearables, and connected cars, have a direct influence on our everyday lives. Regardless of the numerous benefits given by the IoT technology, it brings a few security concerns [3].

Because botnets are frequently employed in IoT devices, IoT devices have been an enticing target for attackers. One of the limitations of IoT devices is the lack of effective firmware. Furthermore, security ideas for IoT devices are typically associated with poor usability, discouraging users from relying on these notions [2].

One of the security concepts implemented in IoT devices are passwords. Most IoT device has a default password to allow the user to enter the configuration settings for the first time. Referring to [8], 61 percent of the applications examined had a default or blank password. When updating the password, 58% accepted a blank password and 35% allowed a weak password of one character. An incident that uses default password as a vulnerability happened in October 2016. About 100,000 hacked IoT appliances and formed the Mirai botnet.

4. Research Aims and Objectives

The aim of this research is to propose a new authentication system to solve the security issue found in default passwords by following the stated objectives:

i. To implement 2 interfaces into the IoT devices.

ii. To implement a Near Field Communication (NFC) sensor into the IoT devices to easily store the device information.

iii. To develop a system that can reactivate and deactivate the NFC sensor to preserve power.

5. Research Significance

The finding from this research will provide new insights into both IOT and cybersecurity sector. Through this research, there are few vulnerabilities found in the current technology used in accessing IOT configurations which are prone to users. After conducting research on the current issue, the researcher has proposed a system which can eliminate the problem and enable an easier approach for the user to access the configuration settings with the use of NFC. The findings in this research assure the safety of IOT devices. IOT devices attack will be reduced, and the privacy of the user will not be invaded. Other researchers can use the findings of this study to further investigate the vulnerabilities of the IOT technology to solve the security issue behind it.

6. Methodology

To effectively conduct this research, quantitative research will be conducted to determine the efficiency and safety of the configuration process of IoT devices. The data collection method for the research will be using questionnaire. This data collection method is used because it is easier to distribute to the respondents as it can be distributed online. Researcher can also use social media as their primary source of distributing the questionnaire to get more respondents. As we are in the midst of the pandemic, it is extremely hard to schedule an interview physically. Thus, it is better to use questionnaire as a data collection method because the respondents can answer the questionnaire when they have free time, and it takes only 5 to 10 minutes to finish the questionnaire. The questionnaire will be prepared and hosted using Google Form.

In the questionnaire there will be 2 types of questions which are open-ended questions and closed-ended questions. For openended questions, it is mainly focused on the respondent's personal experience in configuring the IoT devices. This type of question will require the respondents to write the answer in either point form or sentence form. By adding open-ended questions to the questionnaire, it gives the user the freedom to answer the question as much detailed as they like which gives the researchers more insight in the respondent personal experience. The respondents will also have the freedom to not answer the open-ended questions and proceed with answering the closed-ended questions.

For closed-ended questions, it will be focused on the technical side of the problem such as their mobile devices, types of IoT devices used and the password format used. It will also focus on the proposed solution of the research. A total of 5 multiple choice question and 5 questions with a Likert scale ranging from 1 to 5 will be implemented in the questionnaire. By adding closed-ended questions in the questionnaire, it allows the respondents to answer the questionnaire quickly. It also helps the researcher to analyze the data quickly as it can be easily analyzed especially when the questionnaire is conducted in Google Form. Google form can automatically analyze the data and provide a statistical analysis.

For conducting the questionnaire, the researcher used the stratified sampling method to distribute the survey. Using stratified sampling method can divide the respondent into multiple subgroups. In this research, the subgroups will be created based on the age because different age groups witnessed and participated in the different era of the evolution of technology which allows them to have a different opinion on the subject. 3 age ranges subgroups will be implemented which are 18-24, 25-50 and 50 and above. The questionnaire will also be made with a minimum of 50 respondent which have used IoT devices in their lives.

The study and solutions developed can be more precise by gathering information based on the respondents' real-life

experience and opinions through the questionnaire. This helps in the solving of actual problems encountered during the configuration on IoT devices.

7. Overview of the Proposed System

7.1 Register/Enroll the device to the authentication system

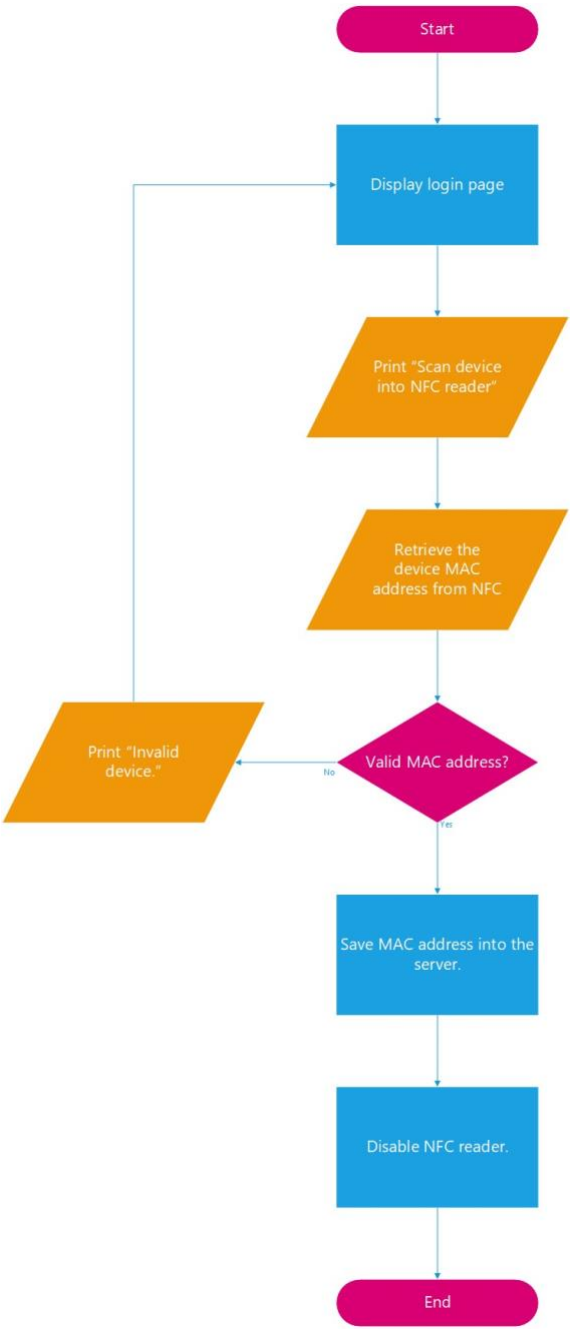


Figure 2: Flowchart for the registration function.

The flowchart above shows the device registration and enrollment process of the IoT authentication system. The IoT device will have an NFC reader that can be enabled and disabled to preserve power. First, by entering the IoT configuration login page, it will display a message that tell the user to scan their NFC enabled device into the NFC reader. The MAC address of the device will be retrieved during the scanning process as the NFC tag and reader will transmit the data. If the NFC device manage to get the valid MAC address from the user's device, it will save the MAC address into the IoT internal server and disable the NFC reader.

7.2 Login into the configuration settings using the authentication system.

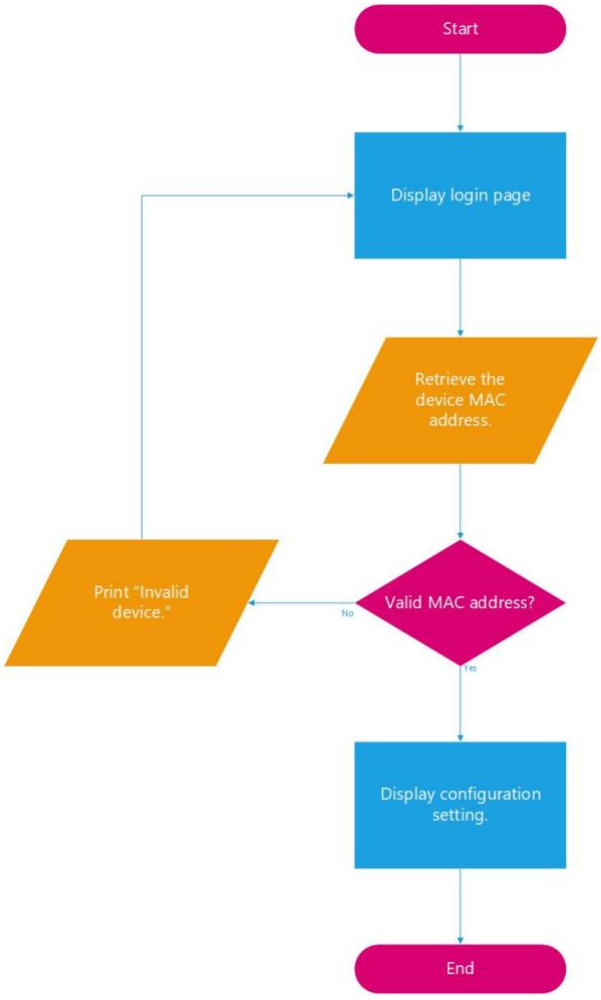


Figure 3: Flowchart for the login function.

The flowchart above shows that the login process of the IoT configuration settings after the user have enrolled their device into the authentication system. If there's a valid MAC address available in the server, it will show the IoT configuration page. Compared to the previous flowchart, this time the system will not tell the user to scan their NFC enabled device into the reader, instead it will get the MAC address of the user's current device and compare the MAC address to the saved MAC address in the server. If the MAC address is correct, it will login the user and display the configuration settings page.

7.3 Reset the authentication system

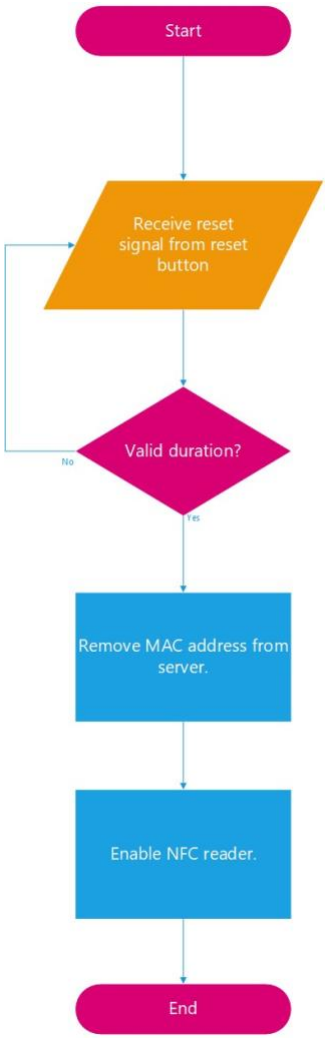


Figure 4: Flowchart for resetting the authentication system function.

The flowchart above shows the process on enabling the NFC reader. For security reasons, only 1 MAC address can be saved and used in the authentication system. If the user changed their device or MAC address, they would need to press the reset button on the IoT device for at least 5 seconds. After that, the system will enable the NFC reader and the user can enroll their device by scanning their NFC enabled device into the system.

8. Conclusion

This study proposed the use of MAC address in NFC technology for user authentication in IoT devices. When using MAC address and NFC instead of passwords, it ensures that only the authorized user can access to the IoT settings. It helps to simplify the authentication process too as user will no longer need to memorize passwords. This solution can effectively avoid security issues such as using default or weak password and vulnerability for attackers.

References

[1] Oracle. (2022). *What is the Internet of Things (IoT)?* https://www.oracle.com/internet-of-things/what-is-iot/

[2] Ulz, T., Pieber, T., Holler, A., Haas, S., & Steger, C. (2017, March 1). *Secured and Easy-to-Use NFCBased Device Configuration for the Internet of Things*. IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/8019776/;jsessionid=UH3SbYBTlBfurQl_cKNO3mShAY6ilHsPTZ2k-dZ8rVPcGc-BNsKu!624181834?arnumber=8019776&casa_token=RQUbKB6YauQAAAAA:lWneXcmDYIPYZy_CkhAZBbz_qApp0jUrb8W8u8v8LaDYEKBE334WtCrJL9YqezDinYj41g6SRw&tag=1

[3] Atlam, H., Alenezi, A., Alassafi, M., Alshdadi, A., & Wills, G. (2020). *Security, Cybercrime and Digital Forensics for IoT*. Research Gate. https://www.researchgate.net/profile/Hany-Atlam/publication/337259162_Security_Cybercrime_and_Digital_Forensics_for_IoT/links/5dcdd76f92851c382f3dfd60/Security-Cybercrime-and-Digital-Forensics-for-IoT.pdf

[4] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). *IoT Security Techniques Based on Machine Learning*. arXiv. https://arxiv.org/pdf/1801.06275.pdf

[5] Huang, Y., Hao, C., Mao, Y., & Zhou, F. (2021). *Dynamic Resource Configuration for Low-Power IoT Networks: A Multi-Objective Reinforcement Learning Metho d*. Arxiv. https://arxiv.org/pdf/2106.02826.pdf

[6] Choi, S., Yang, C., & Kwak, J. (2018). *System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats*. KSII. https://www.koreascience.or.kr/article/JAKO201810237886750.pdf

[7] AlBataineh, A. (2019). *IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries*. Research Gate. https://www.researchgate.net/profile/AreejAlbataineh/publication/335144913_IoT_and_the_Risk_of_Internet_Exposure_Risk_Assessment_Using_Shodan_Queries/links/5f6f177f299bf1b53ef453fa/IoTand-the-Risk-of-Internet-Exposure-Risk-AssessmentUsing-Shodan-Queries.pdf

[8] Knieriem, B., Zhang, X., Levine, P., & Breitinger, F. (2018). *An Overview of the Usage of Default Passwords*.

Research Gate. https://www.researchgate.net/publication/322271082_An_Overview_of_the_Usage_of_Default_Passwords#:~:text=Our%20study%20shows%20that%20default,weak%20password%20of%201%20character

[9] Zhang, X., Upton, O., Lang, N., & Choo, R. (2020). *IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers*. Science Direct. https://www.sciencedirect.com/science/article/pii/S2666281720300214

[10] Alrawais, A. (2020). *Security Issues in Near Field Communications (NFC)*. SAI. https://thesai.org/Downloads/Volume11No11/Paper_76-Security_Issues_in_Near_Field_Communications.pdf

[11] Daramola, C., Folorunsho, O., Ayogu, B., & Adewole, L. (2019). *Near Field Communication (NFC) Based Lecture Attendance Management System on Android Mobile Platform*. FUOYE. http://repository.fuoye.edu.ng/bitstream/123456789/1502/1/2019%20FUOYE%20Conference%20Proceedings.pdf#page=35

[12] Sunny, S. (n.d.). *NFC Smart Locker System*. University of Arkansas. http://csce.uark.edu/~ahnelson/CSCE5013/reports/SunnyNahian.pdf

[13] Prasad, A., Bangera, N., & Shekhar, U. (2022). *NFC Based Login for Mobile Apps and Websites*. IJRASET. https://www.ijraset.com/researchpaper/nfc-based-login-for-mobile-apps-and-websites

[14] Martins, T., Saldaña, J., & Noije, W. (2018, August 1). *A Programmable Gain Amplifier for Load Demodulation Channel in an NFC Reader Chip*. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8533230

[15] Asija, M. (2016, May 5). *MAC Address | Asija | IRAInternational Journal of Technology & Engineering (ISSN 2455–4480)*. IRA Academico Research. https://research-advances.org/index.php/IRAJTE/article/view/125/138

[16] Hashmi, A. (2020). *An Inexpensive but Smart MACAddress Based Attendance Monitoring System*. IEEE Conference Publication | IEEE Xplore. http://www.commnet-conf.org/pastEvents/CommNet20/papers_website_proceedings/1570650584.pdf

[17] Tiwari, T., Tiwari, T., & Tiwari, S. (2018). *View of A secured MAC address based Login System*. European Journal of Electrical Engineering and Computer Science. https://www.ejece.org/index.php/ejece/article/view/16/17

[18] Nam, S., Jeon, S., Kim, H., & Moon, J. (2020). Recurrent GANs Password Cracker For IoT Password Security Enhancement. *Sensors*, *20*(11), 3106. https://doi.org/10.3390/s20113106

[19] Wang, D., Zhang, X., Ming, J., Chen, T., Wang, C., & Niu, W. (2018). Resetting Your Password Is Vulnerable: A Security Study of Common SMSBased Authentication in IoT Device. *Wireless Communications and Mobile Computing*, *2018*, 1–15. https://doi.org/10.1155/2018/7849065

[20] Shouran, Z., Ashari, A., & Kuntoro, T. (2019). Internet of Things (IoT) of Smart Home: Privacy and Security. *International Journal of Computer Applications*, *182*(39), 3–8. https://doi.org/10.5120/ijca2019918450

[21] Kaspersky. (2022, April 5). *QR Code Security: What are QR codes and are they safe to use?* Www.Kaspersky.Com. https://www.kaspersky.com/resourcecenter/definitions/what-is-a-qr-code-how-to-scan

[22] Luna, J., Guzman, G., Rangel, F., Aceves, J., Acosta, M., & Vargas, V. (2022). *Authentication System Based on Fingerprint Scanners Network, QR Codes and IoT*. IJSTRE. http://www.ijstre.com/Publish/7202022/754235614.p df

[23] Madsen, S. S., Santos, A. Q., & Jørgensen, B. N. (2021). A QR code based framework for auto-configuration of IoT sensor networks in buildings. *Energy Informatics*, *4*(S2). https://doi.org/10.1186/s42162-021-00152-w

[24] Zhou, Y., Hu, B., Zhang, Y., & Cai, W. (2021). Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance. *IEEE Access*, *9*, 122362–122372. https://doi.org/10.1109/access.2021.3108189

[25] Masurkar, N., & Pandey, P. (2020). *Nfc Based Dual Authentication Access Control System With Biometric*. IJSRET.

https://ijsret.com/wpcontent/uploads/2020/01/IJSRET_V6_issue1_126.pd f

[26] Putra, E. P., Fifilia, F., & Juwitasary, H. (2018). Trend of NFC Technology for Payment Transaction. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *16*(2), 795. https://doi.org/10.12928/telkomnika.v16i1.8441