# ThinToken: An RFID Technology Based Alternative Physical Two-Factor Authentication Method for PC Web Applications


Theron Adrianne A. Bueno
*Computer Engineering,*
*Pamantasan ng Lungsod ng Maynila*
*City of Manila, Philippines*
taabueno2019@plm.edu.ph

James Laurence A. Cruz
*Computer Engineering,*
*Pamantasan ng Lungsod ng Maynila*
*City of Manila, Philippines*
jlacruz2019@plm.edu.ph

Jackilyn O. Lenizo
*Computer Engineering,*
*Pamantasan ng Lungsod ng Maynila*
*City of Manila, Philippines*
jolenizo2019@plm.edu.ph

Kristel Erica D. Paz
*Computer Engineering,*
*Pamantasan ng Lungsod ng Maynila*
*City of Manila, Philippines*
kedpaz2019@plm.edu.ph

Jeanne Rose P. Tuling
*Computer Engineering,*
*Pamantasan ng Lungsod ng Maynila*
*City of Manila, Philippines*
jrptuling2019@plm.edu.ph

Evangeline P. Lubao
*Computer Engineering Department,*
*Pamantasan ng Lungsod ng Maynila*
*City of Manila, Philippines*
eplubao@plm.edu.ph



***Abstract*— Two-factor authentication, also known as 2FA, is a security measure that helps prevent an account from being compromised. The use of physical 2FA is one of the most secure methods for protecting online accounts. At the moment, there are a few physical two-factor authenticators available on the market, given that the options are limited, the prices for these keys are expensive. This research study innovates the usual features of a security token using Radio Frequency Identification (RFID) and creates a physical two-factor authenticator that holds the encrypted user secret in an RFID card/tag making it portable and lightweight. This research employed the waterfall methodology in creating the ThinToken system which involves assessing the features of existing methods, designing, and implementing the system primarily using the time-based one-time password (TOTP) algorithm and AES-256 encryption, and evaluating the developed system. The System Usability Scale (SUS), which is a 10-item questionnaire, was utilized to evaluate the system in terms of ease-of-use. The data were analyzed using a two-tailed paired t-test to compare YubiKey to ThinToken's time-based efficiency and ease-of-use. The results found that ThinToken was a significantly better alternative to Yubikey in terms of time-based efficiency and ease-of-use.**



***Keywords—2FA, RFID, cybersecurity, one-time password, security key***


## I. INTRODUCTION

It is undeniable that the world will continue to evolve to a much more technology-reliant future. With the ongoing advancement in technology, criminals are now also attracted to making attacks on cyberspace. Phishing is a criminal act prevalently happening online. Currently, there are a few existing physical security keys to fend off these kinds of malicious attacks. According to [1] and [2], hardware-based 2FA methods have a slow adoption rate mainly because it is difficult to use, complex, and requires costly hardware.

The importance of 2FA is often neglected due to lack of recognition. Since the pandemic happened, employees adapting to new work environments outside the office may not prioritize security and secure authentication techniques. The quick and wide-ranging change in working methods, along with geographically dispersed personnel using a variety of nonstandard devices, creates a challenge to maintaining robust and safe cyber security. Decreased employee security and greater danger of phishing attacks raise the requirement for strong authentication and robust security practices. Too many firms still use passwords to access devices, applications, and networks. However, passwords are easy to guess, reused, and, of course, phished. Superior Multi-factor Authentication (MFA) methods, such as a mobile authentication app or a hardware security key, increase security without inconveniencing users. This is critical since employees will feel more isolated from IT help during remote working and rely on their own equipment and processes [3]. The HOTP and TOTP algorithms are quite comparable to one another. At TOTP, the movement factor will keep changing in response to time generation. The method of calculation is the same as that used for HOTP. The general expression for TOTP is usually expressed as TOTP = HOTP (K,T) where K is the pair's secret key and T is a time-related integer [4].

To address the problems stated, the general objective of the study is to develop a two-factor authentication device that can be an effective alternative for USB Based, physical two-factor authentication systems (2FA). The developed device will have three components, the reader, tag, and a web browser extension. The reader will read the data stored in the tags via radio-frequency identification (RFID). The device will utilize the concept of time-based one-time password (TOTP) algorithm to complete authentication challenges required in the login forms of web applications. Furthermore, the device to be developed aims to be an alternative to the existing two-factor authentication device in the market. The general research objective can be subdivided into more specific research objectives such as

a. Develop a physical two-factor authentication (2FA) device that can be used in authenticating into web applications that support the time-based one-time password (TOTP) standard.

b. To develop a physical 2FA device that is better than an existing USB-Based Physical 2FA system in terms of time-based efficiency.

c. To develop a physical 2FA device that is better than an existing USB-Based Physical 2FA system in terms of ease-of-use.

To arrive at a conclusion for the second and third research questions, the researchers have formulated the following hypotheses.

a. There is no significant difference between ThinToken and an existing physical second factor authentication system (YubiKey 5 NFC) in terms of time-based efficiency.

b. There is no significant difference between ThinToken and an existing physical second factor authentication system (YubiKey 5 NFC) in terms of system's ease of use.

## II. LITERATURE REVIEW

Physical security second-factor devices, or also referred to as hard tokens, are small devices that can be plugged into the USB port of a desktop computer in order to be used as the second factor in user accounts that use two-factor authentication. Hard tokens are expensive due to the specialized security hardware used in them. To add to this, since the device is physical, loss and damages are also another reason why they are costly [2]. In a study from [5], messages sent through the short message service (SMS) is problematic when it comes to transmitting confidential information since the information contained in the messages are transmitted as plaintext. Older adults use the internet to access important resources such as bank, retirement, and health insurance accounts. As a result, it is vital to secure their accounts so that they can confidently utilize these increasingly online services. A study by [1] discovered that technical skill, device incompatibility, and online accounts that do not support 2FA were all factors in older persons' decision to use or not to use 2FA.

The WebAuthn and FIDO authentication standards were created to replace or supplement the widely used username and password technique. WebAuthn is a new W3C authentication API that allows browsers to use hardware or software FIDO security keys instead of or in addition to login and password [6]. Another standard for two-factor authentication is the Time-Based One-Time Password (TOTP) algorithm. To calculate the one-time password (OTP), the HOTP method uses a shared counter. The service provider and the user's trusted device in HOTP has a local counter that starts at zero. The shared secret and current time will be inputted to the hash function in the implemented TOTP algorithm on the trusted device, while the server will use the same shared secret and current time to perform the same computation using Network Time Protocol (NTP). As a result, the service provider can verify the OTP entered by the user during registration and authentication because both the service provider and the user's trusted device utilize the same TOTP algorithm [7].

A qualitative study has shown that although majority of users found that a security key-based login is usable, many of them stopped using it because it tends to be slower that using the established password manager built in their browsers. Additionally, participants considered the security benefits to be primarily intangible or unnecessary [8].

A study by Balasta, resolves the problems of the lack security of simple messaging system (SMS) based one-time passwords, by encrypting the one-time passwords when generated from a server and then decrypted on the user side. The proponents of the enhanced TOTP algorithm used the AES-128 encryption method. The study presented that the enhanced algorithm with AES encryption was faster than the original algorithm. Further findings have shown that the enhanced algorithm is stronger than the original algorithm [9].

Radio Frequency Identification (RFID) has huge potential in security systems. From antitheft to physical access, the technology has been used to both enhance existing systems and create new ones. While not infallible, RFID in security systems is becoming increasingly popular. The adaptability of RFID is important when considering its extensive use in security systems. Both passive and active tags include features that improve the technology's overall efficiency. Making tags and readers mobile adds to the technology's popularity. Another key advantage of using RFID for security is cost. Tags may be made for cents on the dollar, allowing system designers to tag an unlimited number of items. Keeping expenses low allows for further expansion and reduced initial expenditures for new systems [10].

A study by Taoufik analyzes the reliability of RFID tags when put under thermal storage. The study subjected two sets of ultra-high frequency (UHF) passive tags, one set from a specific manufacturer under high temperatures. After subjecting the tags to high temperatures, the reflected power of each tag at varying distances from 20 cm to 105 cm were measured. Tags subjected to high temperatures have been observed to have a weaker reflected power in all distances overall compared to the tags that were not subjected to high temperatures. The common mode of failure for RFID tags subjected to high temperature is the formation of cracks on the antenna of the tags. Temperature presents a significant effect on the reliability of RFID tags and read failures [11].

The Time-based One Time Password (TOTP) algorithm creates a One-Time password using a shared key and the current time. The first step in the authentication process requires the user to input their username and password. After a successful submission, the server will ask for the TOTP to finish the login process. This time-based one-time password (TOTP) is produced on the user's smartphone or any other trusted device. The one-time password entered must match the one issued by the server for TOTP to be successful. The session between the server and the user is then established, and the user can securely access the system. TOTP is a variation of the HMAC-based One-Time Password (HOTP) technique that replaces the incrementing counter with the current time stamp in calculating the one-time password [12].

As this study aims to utilize a safe and secure encryption method, existing studies also found that Advance Encryption Standard (AES) is significantly faster and more secure. In uncompressed encryption, AES is 145768 microseconds faster than the Rivest-Shamir-Adleman (RSA) algorithm. AES is also 134193.45 microseconds faster than RSA when compressed. These tests use the same data length. RLE or Run-Length Encoding (RLE) works best when data input is repeated in alphabetical characters. Using this strategy, RLE could compress human input text with a character length of 16 between 12.5% and 50% efficiency. RLE also improved the RSA algorithm's encryption time by 6.39%. Because AES shifts each character numerous times, it is faster and safer than RSA [13].

The Bluetooth core specification (ver. 5.3) allows for secure communications between two devices. The security model of Bluetooth involved pairing, bonding, device authentication, encryption, and message integrity. Pairing is the process for creating shared secret keys to be used in authentication. Bonding is the process of storing shared keys during pairing for use in future reconnections. Device authentication is the verification process that checks whether communicating devices have identical keys. Encryption is the process of ensuring the confidentiality of messages sent and received via Bluetooth. Lastly, message integrity describes the protection against modification of the message by a malicious party [14].

## III. METHODOLOGY

The study utilized an experimental type of research. The ThinToken system has three distinct components, the ThinToken browser extension, the ThinToken Reader, and the ThinToken RFID Tag. Figure 1 shows the block diagram of the system.

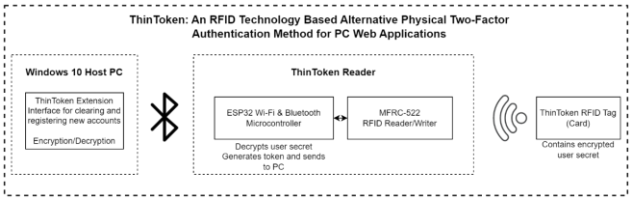


*Figure 1. Block Diagram of the System*

The ThinToken Browser Extension handles the automatic inputting of OTPs to the fields of web applications and performs adding or removing accounts to RFID tags. The ThinToken extension is also capable of encrypting or decrypting account data and TOTP secrets. The ThinToken reader applies the TOTP algorithm to generate OTP codes by decrypting the stored encrypted secret inside the ThinToken RFID Tags. The Advanced Encryption Standard (AES) with a 256-bit key using the Galois Counter Mode (AES256-GCM) was used in the encrypt/decrypt processes.

Figure 2 and Figure 3 shows the circuit diagram and PCB layout of the ThinToken Reader. The circuit can be powered by 4 AA batteries, with the researchers opting for AA rechargeable NiMH batteries. Figure 4 illustrates the enclosure where the reader circuit will be contained, which will be constructed with acrylic.

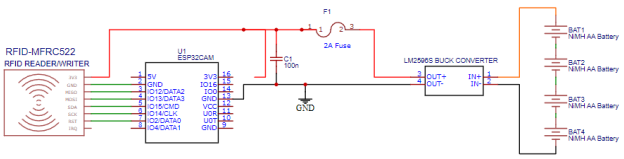


Figure 2. Circuit Schematic Diagram

The primary elements involved in realizing this design include an ESP32-CAM microcontroller, an MFRC522 RFID reader/writer module, and an LM2596S Buck Converter. This microcontroller communicates with host computers via Bluetooth, enabling wireless data transmission. There are some discrepancies between the circuit schematic diagram and the PCB design due to the addition of last-minute changes. For all intents and purposes, the accurate representation of the built system is in the circuit schematic diagram.

Figure 5 describes a high-level overview of the logic performed by the ThinToken Reader and the ThinToken Browser Extension. The left half describes the process when a user uses the system to complete an authentication challenge, while the right half describes the process when the user intends to use ThinToken to complete future authentication challenges.

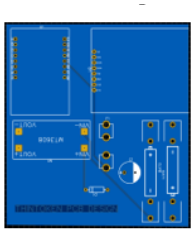

*Figure 3. Printed Circuit Board*

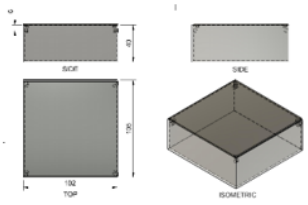

*Figure 4. Enclosure Schematic (in mm)*

Figure 6 shows the finished ThinToken Reader together with some ThinToken RFID Tags. All the components in the schematic diagram are reflected in the built design. However, some discrepancies can be found with the silk screen markings on the PCB schematic since there were last minute changes to the circuit after the PCBs were printed. For this purpose, the researchers are advising readers to use the schematic diagram as the final guide instead of the PCB design.

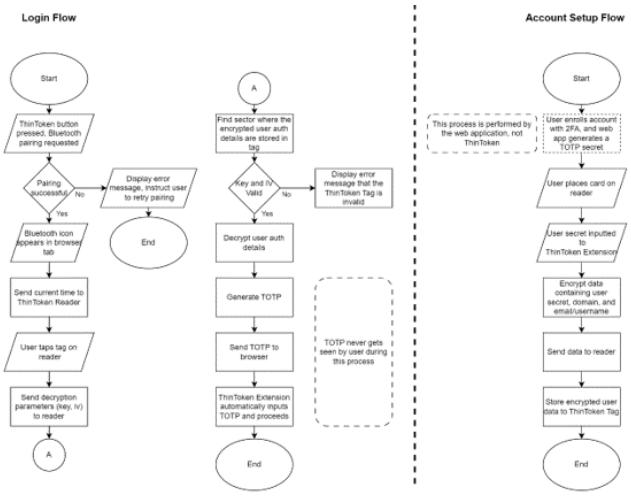


*Figure 5. System Flowchart*

*Figure 6. Built ThinToken Reader and ThinToken Tags*

Figure, Figure, and *Figure* shows the developed ThinToken Browser Extension. The ThinToken extension, besides communicating with web pages for 2FA prompts, also acts as an interface to register accounts to a ThinToken tag.


Figure 7. Extension Landing Page

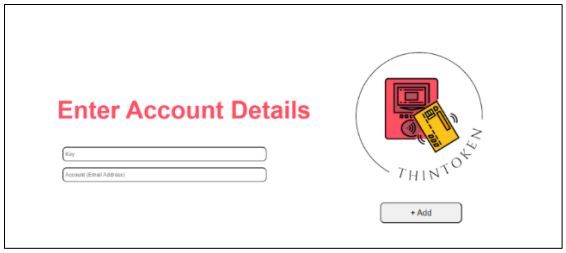


Figure 8. Extension Add Account Form

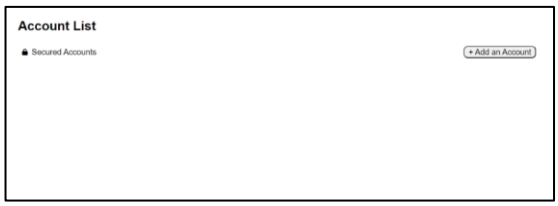


*Figure 9 Extension Account List Page*

The ThinToken Tags are MIFARE Classic 1K RFID tags which can store 1 KB of data, divided into 16 sectors. Each sector has 64 bytes of data, however only 48 bytes of each sector can be written to, therefore, only four accounts can be stored for each ThinToken Tag. The Bluetooth Low Energy implementation for the reader defines various *characteristics*. In Bluetooth Low Energy, characteristics can be described as holders for data where the ThinToken Extension can read or write to. To implement AES-256-GCM to the ThinToken Extension and ThinToken Reader, widely adopted 3rd party libraries were used to ensure a correct and safe implementation of AES. For the ThinToken Extension in the browser, the *SubtleCrypto* library was used which is available by default with many modern browser versions such as Chrome 11, Edge 12, and Firefox 21. For the ThinToken Reader implementation of AES-256, the *mbedtls* library was used, which is readily available for use in ESP32 platforms.

The research study was conducted at Pamantasan ng Lungsod ng Maynila (PLM). The participants of this study are 4th year BS Computer Engineering regular students of PLM. The study utilized the purposive sampling method in choosing 65 participants. The number of participants was obtained using Slovin's formula using a confidence level of 95% and a 5% margin of error. The time to login and SUS score data will be treated with a two-tailed paired t-test with a 0.05 level of significance and a critical value of 1.9977 to reject the null hypotheses.

The participants were asked to use both devices in logging in to a Google account provided by the researchers. During this, the time elapsed from the appearance of the 2FA prompt to the successful login of the account is measured by a stopwatch. Afterwards, the participants answered a 10 question 5-point Likert scale based on the System Usability Scale [15]. To compute for the SUS score of a single participant for one device, Equation 3 were used. Equation 1 was used to compute $s$ for odd numbered survey questions, while Equation 2 was used for even numbered questions.

$$s = scale\ position - 1 \qquad \text{Equation 1}$$

$$s = 5 - scale\ position \qquad \text{Equation 2}$$

$$SU = \sum_{n=1}^{N} s \cdot 5 \qquad \text{Equation 3}$$

## IV. Results

The developed system was compatible with Google, Facebook, Yahoo, and Microsoft 365 (via the accounts issued by PLM). ThinToken was measured to be faster, with a mean time of 22.09s, than the Yubikey 5 NFC, with a mean time of 24.57, during the login process as shown in Figure 10. Additionally, ThinToken was also deemed easier-to-use, with a mean SUS score of 92.19, than the Yubikey, with a mean SUS score of 84.19 as shown in Figure 11.

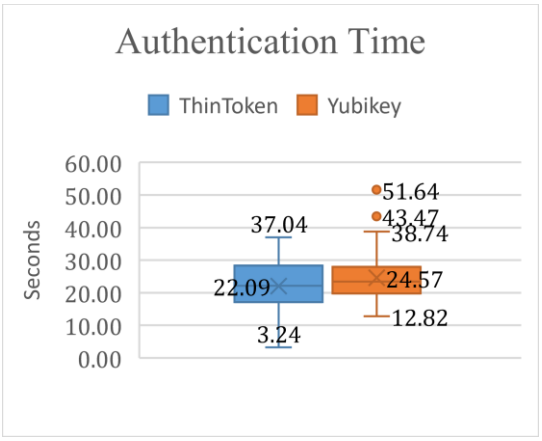


Figure 10. Authentication Time Comparison

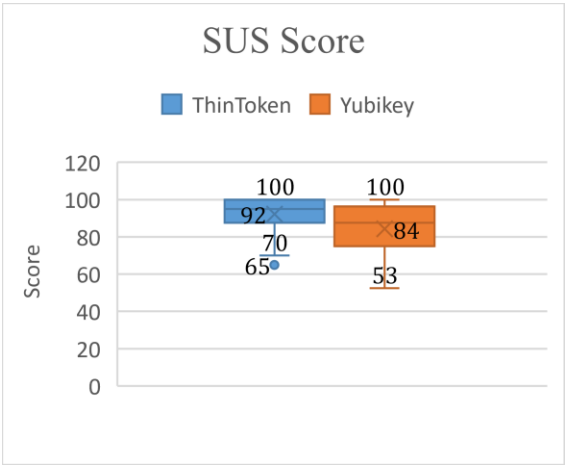


Figure 11. SUS Score Comparison

To validate the authentication time and SUS score data for ease-of-use, a two-tailed paired t-test was used. Table 1 and Table 2 below show a summary of the values obtained for both tests. The results of the t-tests for both the authentication time and ease-of-use show that the ThinToken is significantly faster than the Yubikey, and significantly easier to use than the Yubikey.

TABLE 1 .TWO-TAILED T-TEST FOR AUTHENTICATION TIME.

| | ***Auth Time (ThinToken)*** | ***Auth Time (Yubikey)*** |
|---|---|---|
| Mean | 22.0897 | 24.5692 |
| Variance | 56.9636 | 55.5464 |
| Observations | 65 | 65 |
| df | 64 | |
| **t Stat** | **-2.3610** | |
| P(T<=t) two-tail | 0.0213 | |
| **t Critical two-tail*** | **1.9977** | |

*$\alpha = 0.05$

TABLE 2. TWO-TAILED PAIRED T-TEST FOR EASE OF USE

| | ***SUS Score (ThinToken)*** | ***SUS Score (Yubikey)*** |
|---|---|---|
| Mean | 92.1923 | 84.1923 |
| Variance | 80.5679 | 179.1226 |
| Observations | 65 | 65 |
| df | 64 | |
| **t Stat** | **4.9674** | |
| P(T<=t) two-tail | 5.3384E-06 | |
| **t Critical two-tail*** | **1.9977** | |

***$\alpha = 0.05$

## V. DISCUSSION

The findings and the statistical treatment performed on the findings suggest that the ThinToken is a viable alternative two-factor authentication device. The researchers have met the desired goal of the study to develop a better physical two-factor authentication device than an existing market solution. The results of the measured authentication times show that the ThinToken is 2.48s faster than the Yubikey when logging in to web applications. In terms of ease-of-use, the ThinToken's adjective rating according to the System Usability Scale is "Best Imaginable" for a mean SUS score of 92.19, while the adjective rating for the Yubikey is "Excellent" for a mean SUS score of 84.19. The slower outliers in the auth time data for the Yubikey possibly came from participants not noticing the prompt of the Yubikey to touch the gold disk on it, or difficulty in finding the correct orientation of the USB port. On the other hand, the lower SUS score outlier for the ThinToken possibly came from the system's inconsistency, difficulty to carry, and lack of confidence in the system.

## VI. CONCLUSIONS AND RECOMMENDATIONS

In conclusion, the results have shown that the objectives of the study have been met, to develop an alternative physical 2FA device that is superior in terms of authentication time and ease-of-use. ThinToken is significantly faster than Yubikey in terms of authentication time recorded during user testing. Physical 2FA devices, such as ThinToken offer a second-factor authentication method that offer the security benefits of the time-based one-time password algorithm with a faster and easier-to-use experience for the end user compared to an existing USB based security key.

Based on the findings and conclusions of this study, the following actionable recommendations are offered:

1. Adaption of ThinToken as a substitute for Yubikey: For organizations and individuals seeking an efficient and easy-to-use two-factor authentication solution, ThinToken presents itself as a better option.

2. Expanding ThinToken website compatibility using AI: ThinToken's current website support is limited to Google, Yahoo, Facebook, and Microsoft. Use of Large Language Models or other AI-based solutions can automate compatibility to more websites.

3. Improve ThinToken's accuracy: While ThinToken displays a marginally lower accuracy rate than YubiKey (91% vs. 98%), it remains crucial to probe deeper into the causes of this disparity. By pinpointing and addressing potential concerns with the device – such as user error, connectivity complications, or hardware constraints in future research, it may be feasible to elevate ThinToken's accuracy, which can solidify its position as an even more compelling alternative to Yubikey.

4. Enhancing ThinToken's design and usability: User feedback during the study can be valuable for refining ThinToken's design and features. Implementing improvements based on user preferences and suggestions may lead to elevated levels of satisfaction and ease of use.

5. Broadening the research scope: To substantiate this study's findings further, it is recommended to conduct additional research with a more extensive and diverse sample of participants. This will allow for a broader understanding of user experiences with ThinToken and Yubikey and help to generalize the results.

6. Exploring alternative microcontroller options: Although the ESP32-CAM microcontroller was chosen for its ready availability, it is imperative that future research ventures into the use of alternative microcontrollers. These alternatives may well provide enhanced performance, superior energy efficiency, or supplementary features, ultimately culminating in a more robust and versatile ThinToken system.

These recommendations expound upon the potential of ThinToken as a feasible alternative to Yubikey and suggest avenues for future research and development. By considering the study's findings and recommendations, stakeholders can make more rational decisions regarding implementing and refining two-factor authentication systems.

## VII. IMPLICATIONS

The results of the study show that ThinToken offers better time efficiency and ease-of use when compared to Yubikey, a USB based security key. The better time-efficiency can translate to an increase of adoption with ThinToken, since slow authentication times are a factor in user dissatisfaction, therefore leading to a decline in adoption rates. The better ease-of-use of the ThinToken can also lead to better adoption rates since users are more inclined to adopt a product that is

simple to use and comprehend. Another thing in this regard is that more user-friendly devices can lessen the possibility of human error.

## ACKNOWLEDGEMENT

Obstacles and trials are part of our life. These trials may seem difficult or hard to overcome. But through Christ our Lord and savior, all things are possible.

The authors want to share this triumph and express their appreciation and sincerest gratitude to the following people, who in one way or another, generously and patiently helped in completing this study.

Above all, the researchers would like to give their sincerest and warmest appreciation, to their Lord, and Savior, almighty God, who is the source of their strength, knowledge, and skills, who always hears their prayers, guide their path, and never leave their side throughout their journey in life.

The authors express their deep appreciation for Engr. Evangeline P. Lubao, for guidance and imparting her knowledge and wisdom that were essential for the success of the study. Her dedication to guide the researchers despite the given circumstances were greatly appreciated.

The community of Pamantasan ng Lungsod ng Maynila is also thanked by the researchers for their willingness to participate in the study and their valuable insights that were used in the study.

Lastly, the friends and parents of the authors, for their patience, understanding, support for the authors, and external insights pertaining to the project and the research itself.

## REFERENCES

[1] S. Das, A. Kim, B. Jelen, L. Huber, and L. J. Camp, "Non-inclusive online security: Older Adults' experience with two-factor authentication," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2020-Janua, pp. 6472–6481, 2021, doi: 10.24251/hicss.2021.779.

[2] [2] B. Segal, "Key Differences Between Hard and Soft Tokens," Telnyx, 2021. https://telnyx.com/resources/hard-token-vs-soft-token (accessed Mar. 30, 2022).

[3] [3] N. Sarginson, "Securing your remote workforce against new phishing attacks," Comput. Fraud Secur., vol. 2020, no. 9, pp. 9–12, Jan. 2020, doi: 10.1016/S1361-3723(20)30096-8.

[4] [4] H. Seta, T. Wati, and I. C. Kusuma, "Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication," in 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Oct. 2019, pp. 115–120. doi: 10.1109/ICIMCIS48181.2019.8985196.

[5] [5] N. Saxena, H. Shen, N. Komninos, K. K. R. Choo, and N. S. Chaudhari, "BVPSMS: A Batch Verification Protocol for End-to-End Secure SMS for Mobile Users," IEEE Trans. Dependable Secur. Comput., vol. 17, no. 3, pp. 550–565, 2020, doi: 10.1109/TDSC.2018.2799223.

[6] [6] M. Rivera-Dourado, M. Gestal, A. Pazos, and J. M. Vázquez-Naya, "An Analysis of the Current Implementations Based on the WebAuthn and FIDO Authentication Standards," p. 56, 2021, doi: 10.3390/engproc2021007056.

[7] [7] G. Chamika, "Time-based one-time passwords (TOTP) - identity beyond borders," Medium, 2021. https://medium.com/identity-beyond-borders/time-based-one-time-passwords-totp-9e7506a9a928 (accessed Apr. 02, 2022).

[8] [8] F. M. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. Dürmuth, "'You still use the password after all' - Exploring FIDO2 Security Keys in a Small Company," Proc. 16th Symp. Usable Priv. Secur. SOUPS 2020, pp. 19–36, 2020.

[9] [9] D. U. Balasta, S. M. C. Pelito, M. C. R. Blanco, A. J. Alipio, K. E. Mata, and D. M. A. Cortez, "Enhancement of Time-Based One-Time Password for 2-Factor Authentication," Int. J. Innov. Sci. Res. Technol., vol. 7, no. 6, 2022, Accessed: Nov. 22, 2022. [Online]. Available: https://www.ijisrt.com/assets/upload/files/IJISRT22JUN522.pdf

[10] [10] J. Ketterer and M. M. Chowdhury, "An Evaluation of RFID Security Systems and their Effectiveness," 2021 IEEE Int. Conf. Electro Inf. Technol., 2021, doi: 10.1109/EIT51626.2021.9491901.

[11] [11] S. Taoufik, P. Dherbecourt, A. El Oualkadi, and F. Temcamani, "Reliability and Failure Analysis of UHF RFID Passive Tags under Thermal Storage," IEEE Trans. Device Mater. Reliab., vol. 17, no. 3, pp. 531–538, 2017, doi: 10.1109/TDMR.2017.2733519.

[12] [12] C. Sudar, S. K. Arjun, and L. R. Deepthi, "Time-based one-time password for Wi-Fi authentication and security," in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sep. 2017, pp. 1212–1216. doi: 10.1109/ICACCI.2017.8126007.

[13] [13] M. Valentino, "Secure RFID Using Data Encryption and Compression Algorithm," 2021, [Online]. Available: http://repository.unika.ac.id/27123/

[14] [14] Bluetooth SIG, "Bluetooth Core Specification." pp. 266–267, 2021.

[15] J. Brooke, "SUS: A 'Quick and Dirty' Usability Scale," Usability Eval. Ind., pp. 207–212, 1996, doi: 10.1201/9781498710411-35.

## APPENDIX

TABLE A- 1. THINTOKEN TESTING AND SURVEY DATA

| # | Timestamp | Auth Time (s) | System Usability Scale | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Q8 | Q9 | Q10 |
| 1 | 4/20/23 15:04:15 | 33.80 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 2 | 4/20/23 15:08:51 | 20.46 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 3 | 4/20/23 15:16:05 | 28.45 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 4 | 4/20/23 16:23:18 | 29.55 | 5 | 2 | 5 | 5 | 5 | 1 | 5 | 2 | 4 | 3 |
| 5 | 4/22/23 12:10:52 | 36.42 | 4 | 1 | 5 | 2 | 5 | 1 | 5 | 1 | 4 | 4 |
| 6 | 4/22/23 12:42:30 | 31.12 | 5 | 1 | 5 | 2 | 5 | 1 | 5 | 1 | 5 | 1 |
| 7 | 4/22/23 12:50:05 | 30.29 | 5 | 1 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 1 |
| 8 | 4/22/23 13:01:39 | 15.32 | 5 | 2 | 5 | 4 | 5 | 4 | 5 | 4 | 4 | 1 |
| 9 | 4/22/23 13:29:23 | 26.98 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 10 | 4/22/23 13:39:27 | 12.64 | 5 | 1 | 5 | 4 | 5 | 4 | 5 | 4 | 2 | 3 |
| 11 | 4/22/23 13:45:04 | 10.72 | 4 | 1 | 5 | 1 | 5 | 1 | 5 | 2 | 5 | 1 |
| 12 | 4/22/23 13:54:10 | 31.94 | 5 | 5 | 5 | 4 | 4 | 1 | 4 | 1 | 5 | 3 |
| 13 | 4/22/23 14:03:51 | 30.40 | 4 | 2 | 5 | 1 | 5 | 1 | 5 | 2 | 5 | 1 |
| 14 | 4/22/23 14:09:41 | 20.85 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 15 | 4/22/23 14:21:29 | 20.42 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 16 | 4/22/23 14:46:28 | 12.67 | 5 | 2 | 5 | 1 | 5 | 1 | 4 | 3 | 5 | 1 |
| 17 | 4/22/23 16:57:20 | 15.08 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 3 |
| 18 | 4/24/23 8:56:10 | 8.48 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 19 | 4/24/23 9:04:48 | 3.24 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 20 | 4/24/23 9:26:10 | 6.03 | 4 | 1 | 5 | 1 | 5 | 1 | 5 | 2 | 5 | 1 |
| 21 | 4/25/23 13:07:33 | 23.70 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 22 | 4/25/23 13:12:20 | 17.05 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 23 | 4/25/23 13:23:20 | 34.36 | 5 | 3 | 5 | 1 | 5 | 1 | 5 | 1 | 4 | 2 |
| 24 | 4/25/23 13:44:17 | 30.37 | 4 | 1 | 5 | 1 | 5 | 1 | 5 | 4 | 4 | 1 |
| 25 | 4/25/23 14:40:16 | 26.98 | 5 | 1 | 5 | 2 | 5 | 1 | 4 | 2 | 4 | 2 |
| 26 | 4/26/23 10:06:52 | 32.45 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 27 | 4/26/23 10:15:40 | 28.27 | 4 | 2 | 5 | 3 | 5 | 1 | 4 | 2 | 5 | 1 |
| 28 | 4/26/23 10:25:48 | 20.10 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 29 | 4/26/23 10:26:47 | 19.56 | 5 | 4 | 4 | 3 | 5 | 1 | 3 | 3 | 4 | 1 |
| 30 | 4/26/23 10:34:09 | 14.14 | 4 | 1 | 5 | 5 | 5 | 1 | 5 | 2 | 4 | 1 |
| 31 | 4/26/23 10:45:30 | 13.04 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 32 | 4/26/23 10:54:55 | 23.51 | 4 | 4 | 5 | 1 | 5 | 1 | 5 | 3 | 5 | 1 |
| 33 | 4/26/23 11:02:43 | 24.73 | 5 | 2 | 5 | 2 | 5 | 1 | 5 | 1 | 5 | 1 |
| 34 | 4/26/23 11:17:48 | 17.44 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 35 | 4/26/23 11:28:00 | 30.15 | 5 | 3 | 4 | 1 | 5 | 1 | 5 | 1 | 5 | 2 |
| 36 | 4/26/23 11:31:39 | 30.97 | 5 | 1 | 5 | 2 | 5 | 1 | 5 | 1 | 5 | 1 |
| 37 | 4/26/23 11:37:33 | 26.54 | 4 | 1 | 5 | 2 | 5 | 1 | 5 | 1 | 5 | 3 |
| 38 | 4/26/23 11:48:54 | 31.91 | 5 | 5 | 5 | 3 | 5 | 1 | 5 | 1 | 4 | 1 |
| 39 | 4/26/23 11:57:15 | 15.34 | 4 | 2 | 5 | 2 | 4 | 1 | 5 | 2 | 5 | 3 |
| 40 | 4/26/23 12:03:43 | 23.86 | 5 | 1 | 5 | 3 | 5 | 1 | 5 | 1 | 5 | 3 |
| 41 | 4/26/23 12:08:13 | 22.53 | 5 | 2 | 5 | 3 | 5 | 1 | 5 | 1 | 5 | 3 |
| 42 | 4/26/23 12:13:46 | 22.65 | 5 | 3 | 4 | 2 | 4 | 3 | 5 | 2 | 4 | 4 |
| 43 | 4/26/23 12:20:20 | 22.26 | 5 | 2 | 5 | 4 | 5 | 1 | 4 | 2 | 4 | 1 |
| 44 | 4/26/23 12:28:35 | 21.11 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 45 | 4/26/23 12:46:11 | 25.78 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 46 | 4/26/23 13:30:48 | 14.21 | 5 | 1 | 5 | 3 | 5 | 2 | 5 | 1 | 5 | 1 |
| 47 | 4/26/23 13:35:52 | 37.04 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |

TABLE A- 2. YUBIKEY TESTING AND SURVEY DATA

| # | Timestamp | Auth Time (s) | System Usability Scale | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Q8 | Q9 | Q10 |
| 1 | 4/20/23 15:04:15 | 32.51 | 5 | 1 | 5 | 1 | 5 | 2 | 5 | 1 | 5 | 1 |
| 2 | 4/20/23 15:08:51 | 20.88 | 3 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 3 | 1 |
| 3 | 4/20/23 15:16:05 | 17.09 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 4 | 4/20/23 16:23:18 | 17.74 | 3 | 2 | 4 | 2 | 4 | 1 | 5 | 1 | 4 | 2 |
| 5 | 4/22/23 12:10:52 | 16.80 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 4 | 3 |
| 6 | 4/22/23 12:42:30 | 28.15 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 7 | 4/22/23 12:50:05 | 32.65 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 1 | 5 | 5 |
| 8 | 4/22/23 13:01:39 | 20.04 | 5 | 2 | 5 | 2 | 4 | 4 | 5 | 4 | 5 | 1 |
| 9 | 4/22/23 13:29:23 | 31.68 | 5 | 2 | 5 | 3 | 3 | 2 | 4 | 4 | 5 | 4 |
| 10 | 4/22/23 13:39:27 | 23.50 | 2 | 4 | 4 | 4 | 4 | 2 | 3 | 2 | 3 | 2 |
| 11 | 4/22/23 13:45:04 | 19.34 | 5 | 1 | 5 | 1 | 5 | 1 | 4 | 1 | 5 | 1 |
| 12 | 4/22/23 13:54:10 | 27.24 | 4 | 3 | 4 | 3 | 4 | 1 | 4 | 1 | 4 | 3 |
| 13 | 4/22/23 14:03:51 | 21.53 | 3 | 3 | 3 | 2 | 4 | 2 | 4 | 3 | 2 | 1 |
| 14 | 4/22/23 14:09:41 | 20.31 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 2 | 5 | 2 |
| 15 | 4/22/23 14:21:29 | 25.04 | 4 | 2 | 4 | 1 | 3 | 2 | 3 | 5 | 3 | 2 |
| 16 | 4/22/23 14:46:28 | 23.66 | 5 | 2 | 5 | 3 | 4 | 1 | 5 | 1 | 5 | 4 |
| 17 | 4/22/23 16:57:20 | 16.96 | 2 | 4 | 5 | 2 | 4 | 2 | 4 | 1 | 4 | 4 |
| 18 | 4/24/23 8:56:10 | 25.75 | 4 | 1 | 5 | 1 | 4 | 2 | 5 | 1 | 5 | 1 |
| 19 | 4/24/23 9:04:48 | 26.80 | 4 | 2 | 4 | 1 | 4 | 1 | 4 | 2 | 4 | 2 |
| 20 | 4/24/23 9:26:10 | 12.82 | 5 | 1 | 5 | 4 | 5 | 1 | 5 | 3 | 5 | 1 |
| 21 | 4/25/23 13:07:33 | 26.62 | 4 | 1 | 5 | 1 | 5 | 1 | 4 | 1 | 4 | 1 |
| 22 | 4/25/23 13:12:20 | 14.04 | 4 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 23 | 4/25/23 13:23:20 | 34.27 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 2 |
| 24 | 4/25/23 13:44:17 | 27.82 | 4 | 1 | 4 | 1 | 4 | 1 | 4 | 1 | 5 | 1 |
| 25 | 4/25/23 14:40:16 | 31.73 | 4 | 2 | 4 | 2 | 5 | 2 | 4 | 1 | 4 | 2 |
| 26 | 4/26/23 10:06:52 | 24.99 | 3 | 1 | 4 | 1 | 5 | 1 | 5 | 4 | 5 | 1 |
| 27 | 4/26/23 10:15:40 | 51.64 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 3 | 1 |
| 28 | 4/26/23 10:25:48 | 23.81 | 4 | 2 | 4 | 2 | 4 | 2 | 2 | 2 | 2 | 2 |
| 29 | 4/26/23 10:26:47 | 21.71 | 4 | 3 | 5 | 3 | 4 | 1 | 3 | 1 | 3 | 3 |
| 30 | 4/26/23 10:34:09 | 20.75 | 4 | 2 | 4 | 3 | 4 | 3 | 3 | 2 | 4 | 4 |
| 31 | 4/26/23 10:45:30 | 32.67 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 32 | 4/26/23 10:54:55 | 43.47 | 3 | 3 | 3 | 4 | 5 | 1 | 3 | 1 | 5 | 3 |
| 33 | 4/26/23 11:02:43 | 26.24 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 34 | 4/26/23 11:17:48 | 20.23 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 35 | 4/26/23 11:28:00 | 23.39 | 4 | 3 | 5 | 2 | 4 | 3 | 4 | 2 | 5 | 2 |
| 36 | 4/26/23 11:31:39 | 33.66 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 2 |
| 37 | 4/26/23 11:37:33 | 38.39 | 4 | 1 | 5 | 4 | 5 | 1 | 5 | 1 | 5 | 3 |
| 38 | 4/26/23 11:48:54 | 36.66 | 4 | 4 | 5 | 1 | 5 | 1 | 1 | 1 | 4 | 1 |
| 39 | 4/26/23 11:57:15 | 27.74 | 3 | 3 | 3 | 2 | 4 | 2 | 3 | 1 | 3 | 2 |
| 40 | 4/26/23 12:03:43 | 38.74 | 4 | 3 | 4 | 2 | 4 | 2 | 4 | 1 | 4 | 3 |
| 41 | 4/26/23 12:08:13 | 19.90 | 5 | 2 | 4 | 3 | 5 | 1 | 5 | 1 | 5 | 5 |
| 42 | 4/26/23 12:13:46 | 27.57 | 5 | 2 | 4 | 2 | 4 | 2 | 3 | 2 | 4 | 2 |
| 43 | 4/26/23 12:20:20 | 25.72 | 4 | 1 | 4 | 4 | 5 | 1 | 4 | 1 | 4 | 4 |
| 44 | 4/26/23 12:28:35 | 21.87 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 45 | 4/26/23 12:46:11 | 12.90 | 5 | 4 | 3 | 4 | 5 | 3 | 4 | 3 | 4 | 3 |
| 46 | 4/26/23 13:30:48 | 20.63 | 5 | 2 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 |
| 47 | 4/26/23 13:35:52 | 19.70 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 5 | 5 | 1 |

TABLE A- 3. SUS QUESTIONNAIRE LEGEND

| Q# | Question |
|---|---|
| 1 | I think that I would like to use this system frequently |
| 2 | I found the authentication process unnecessarily complex |
| 3 | I thought the system was easy to use |
| 4 | I think that I would need the support of a technical person during the authentication process. |
| 5 | I found the various functions in this system were well integrated |
| 6 | I thought there was too much inconsistency in this system |
| 7 | I would imagine that most people would learn to use this system very quickly |
| 8 | I found the system very difficult to carry or use |
| 9 | I felt very confident during the authentication process |
| 10 | I needed to learn a lot of things before I could use the system |