Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 22, No. 2, Maret 2023, pp. 299∼308
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v22i2.2700

Seamless Security on Mobile Devices Textual Password Quantification Model Based Usability Evaluation of Secure Rotary Entry Pad Authentication

Herman Kabetta , Hermawan Setiawan , Fetty Amelia , Muhammad Qolby Fawzan
Politeknik Siber dan Sandi Negara, Bogor, Indonesia

Article Info

Article history:

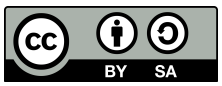
Received January 20, 2023
Revised March 14, 2023
Accepted March 25, 2023

Keywords:

JSON Web Token
Mobile Device
Rotary Entry Pad
Shoulder Surfing Attack
TQ-Model
Usability Evaluation

ABSTRACT

Mobile devices are vulnerable to Shoulder Surfing and Smudge Attacks, which should occur when a user enters a PIN for authentication purposes. This attack can be avoided by implementing a rotary entry pad mechanism. Despite this, several studies have found that using a rotary entry pad reduces user usability. This study uses a Design Research Methodology approach. It will implement a rotary entry pad authentication in the Android operating system as an authentication method to protect the device against Shoulder Surfing Attacks and Smudge Attacks. Furthermore, it combined JSON Web Token (JWT) to secure the authentication process from the client to the server. At the end of implementation, it compared with other studies in terms of usability and evaluated it using the TQ-Model, which showed that the usability aspect has improved. Regarding security, we conducted a shoulder surfing attack simulation to assess the efficacy of guessing PINs. The results showed that only a limited number of attempts were successful, with two out of five samples failing to guess any numbers and only one sample successfully guessing six 10-digit PIN combinations out of 10 to the power of 10. The security test results show that shoulder surfing attacks are more difficult to perform after implementing the rotary entry pad. The evaluation showed that the JSpinpad performed better, with seven parameters showing improvement, one parameter showing a decline, and ten parameters remaining unchanged.



Corresponding Author:

Herman Kabetta, +62-813-9461-6622,
Department of Cryptographic Engineering,
Politeknik Siber dan Sandi Negara, Bogor, Indonesia,
Email: herman.kabetta@poltekssn.ac.id

How to Cite:H. Kabetta, H. Setiawan, F. Amelia, and M. Fawzan, "Seamless Security on Mobile Devices Textual Password Quantification Model Based Usability Evaluation of Secure Rotary Entry Pad Authentication", *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 22, no. 2, pp. 299-308, Mar. 2023.

1. INTRODUCTION

The authentication system becomes an important part and the first line of defense when an unauthorized party tries accessing data or a device [1]. Today's most popular authentication method is using a numeric password [2] because users do not need to incur additional costs, and it is easy to remember.

The development of technology today focuses a lot on security for touch screen technology, which is often used on mobile devices [3]. However, after the widespread introduction of the mobile operating system a few years ago, many alternatives to device authentication emerged, such as the introduction of the Personal Identification Number (PIN), which is now widely used for information security, as well as other alternatives, such as biometrics, patterns, gestures, and graphical authentication [4, 5].

Several authentication methods and schemes have been tested in previous studies. For example, the method of entering a PIN must resist attacks such as recording with devices performed by attackers [6]. However, there are at least three security vulnerabilities in entering a pin code or pattern: Shoulder Surfing Attacks (SSA) and Smudge Attacks. As a result, some users are reluctant to use the security system and leave their devices without authentication [7].

Various methods of entering a PIN have been carried out previously [8], increasing the level of security by placing a button in a different position each time it is activated. Nevertheless, the PIN is still vulnerable to shoulder surfing attacks, where attackers observe when the user enters a PIN by looking directly at it or recording it [9]. Compared to biometric methods, which are still prone to errors, expensive costs, and cannot be changed, most of the following steps require the system to request a PIN code [9]. Another proposed method uses superimposition to produce hybrid image keypads in color [10]. Hybrid images are made by overlapping two images with different frequencies, resulting in an image that appears differently based on viewing distance. They can help prevent shoulder surfing. Rajarajan et al. discussed the PIN-based security authentication scheme by initiating a new scheme called Spinpad [11]. The Spinpad scheme is intended for devices that authenticate users without using the keyboard and use tokens issued by the application using voice. Spinpad does not directly enter its digits, so there is no chance of smudge attacks on this scheme.

Spinpad has the advantage of being strong in security schemes to prevent three types of attacks, such as Shoulder Surfing Attacks, Smudge Attacks, and Keylogging Attacks, which have the shape of a two-wheel circle, where the outer circle consists of the numbers 0 to 9. The inner circle consists of ten alphabetic letters. Unfortunately, the Spinpad scheme process requires additional tools, such as earphones/headphones, to get alphabet tokens during the authentication process. This becomes very difficult if the user does not bring the tool or does not have it [11], affecting the practicality and usability of the Spinpad scheme.

Based on the usability aspect, the Spinpad authentication scheme has a weakness in terms of time, and the user takes longer to enter the PIN. Based on these issues, we attempted to improve and create JSpinpad, a better scheme than Spinpad. We use a rotary dialer entry pad phone, also known as a rotary cable phone model that looks like one circular ring with a digit PIN in it, as an improvement model for the Spinpad scheme uses two circular rings. In Spinpad's initial scheme, the alphabetic ring that can rotate clockwise or counterclockwise aims to prevent SSA and Keylogging Attacks where the attacker cannot remember, record, or guess the user's PIN input. The position of the digit PIN on the entry pad of the rotary dialer phone will always change every time the user exits the application after entering the digits PIN, with the goal of preventing the attacker from guessing, remembering, or recording the digits PIN entered and from being seen from the fingerprint marks on the screen.

The verification process on Spinpad does not yet have security validation, whether the process is safe or not, so it is necessary to have a standard or method applied to this process [11]. We use the JSON Web Token (JWT), a security standard used to transmit data compactly and securely as JSON objects [12]. JWT is arguably secure because it can be verified and digitally signed using the HMAC (Hash-based Message Authentication Code) algorithm or a public/private key pair using RSA or ECDSA [13, 14]. In the last step of the study, we conduct the usability evaluation. Usability evaluation is commonly used to evaluate the ease of use of a system. Some usability evaluations, such as SUS (System Usability Scale), are used to evaluate a web-based Geographic Information System [15]. Another usability evaluation is TQ-Model (textual passwords-based quantification model), specifically used to analyze knowledge-based authentication schemes of a system [16]. Table 1 shows the differences between this study with several previous studies. This study aims to explore the implementation of a modified Spinpad integrated with a JWT mechanism on the backend, as well as to assess the usability of the resulting application using the TQ-Model evaluation approach.

Table 1. Related Work Comparison

Factor	Related Work					This Study
	[11]	[12]	[16]	[8]	[10]	
Spinpad	✓					✓
Random Position				✓	✓	✓
Usability Evaluation	✓					✓
JWT		✓				✓
TQ-Model			✓			✓
SSA Prevention	✓				✓	✓

2. RESEARCH METHOD

This study uses a Design Research Methodology approach that focuses on the problem analysis process and materials that support the research process. As shown in Figure 1, There are four stages: research clarification, descriptive study I, prescriptive study, and descriptive study II [17].

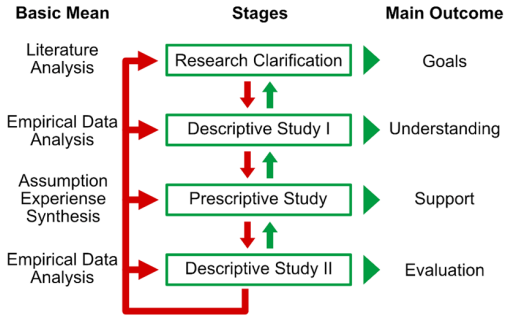


Figure 1. Research Methodology

The first stage is research clarification, which involves gathering evidence and theories that support achieving the research objectives [18]. The collection of evidence and theories will be based on a literature review that supports this research. The literature collected at this stage contains the problems in Spinpad authentication and the solutions implemented to solve these problems. The next stage is Descriptive Study I; in this stage, researchers have clear goals, and then a detailed description will be carried out to determine the factors that must be handled based on the research clarification stage. A prescriptive study will be conducted to solve problems by designing the JSpinpad application [19]. There are four stages, analysis, design, and implementation. The design process will apply the software development method with a prototype software development approach and implement Java as a programming language and MySQL as a storage database.

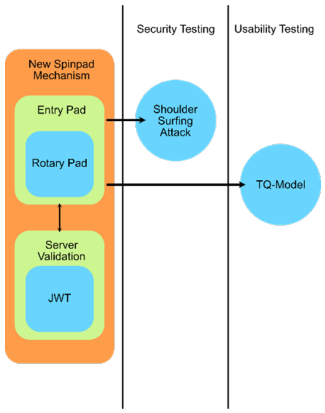


Figure 2. Descriptive Study II

Figure 2 shows that descriptive study II will conclude with a model evaluation [20] using the TQ-Model and security testing using shoulder surfing attack simulation. This study designs and builds improved authentication to be better than previous research, namely, PIN-based Spinpad schema authentication [11], by improving usability and authentication.

3. RESULT AND ANALYSIS

3.1. Design and Implementation

EA rotary entry pad is implemented into the log-in section of the application to enter the PIN into the PIN password field. On the registration page, the user enters the PIN that will be registered into the application as a credential along with an email. Users cannot reuse emails that are already registered. The user is asked to enter the same PIN twice when registering. The user automatically moves to the log-in page if it has been registered at the registration stage. As shown in Figure 3, the entry rotary dialer model is used to improve the usability aspects of Spinpad's previous research [11].

Figure 3. Rotary Entry Pad Design

As shown in Figure 4, the registration page is a page for users to register an account for authentication into an application where users are required to fill in the data in the form of email, password, and password confirmation. Furthermore, the credential data registered is saved in the database.

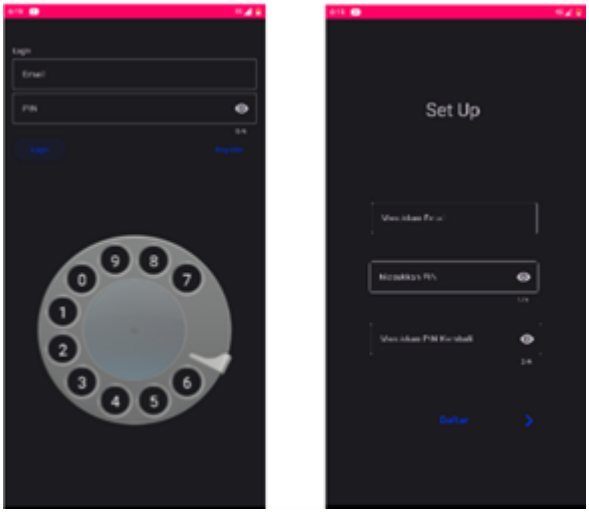


Figure 4. Implementation of JSpinpad on Android OS

JWT helps encrypt claims submitted in JSON form as a JSON Web Signature (JWS) payload or a plain text structure of JSON Web Encryption (JWE) for later claims to be digitally signed using a Message Authentication Code (MAC). A JWT is a string consisting of three structures, i.e.,

a. The JWT Header contains information about how the JWT signature will be computed. In the header, "alg" is the hash algorithm used.
   header = {typ:JWT:alg:HS256}
b. JWT Payload contains data stored in the JWT, which can be a user id, email, or related to the user.
   payload = {userId:example@email.com}

c. JWT Signature contains a predefined signature on the header and payload calculated using an algorithm.
data = header + .+ payload
hashedData = hash(data)
signature=base64urlEncode(hashedData)

3.2. Testing and Evaluation

Security testing was conducted to determine whether the JSpinpad as an Entry Pad Rotary Dialer could prevent a human-based Shoulder Surfing Attack. The application was tested against shoulder surfing attacks using research-based testing [21]. Figure 5 shows that participants were given a video showing the user entering a PIN combination during the authentication process. In addition, testing was performed on the type of SSA recording attacks. There were five samples in the test. First, the sample was given ten video recordings of people entering a pin combination, where one combination was six digits. Then, the sample tries to guess each combination digit entered in the application based on the videotape recorder. The results of the test can be seen in Table 2.

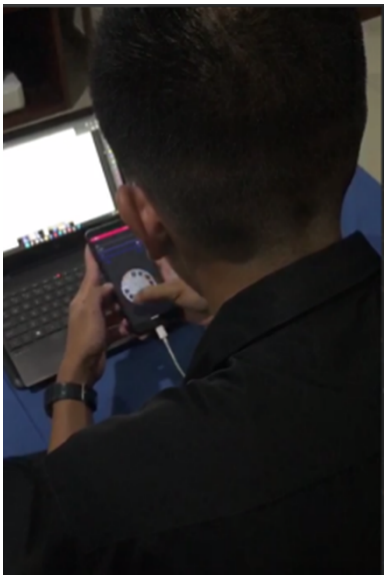


Figure 5. Shoulder Surfing Attacks Test

Sample A successfully guessed the one-digit PIN on the fifth PIN combination, Sample B of the six combinations successfully guessed the 10-digit PIN, Sample C of the three combinations successfully guessed the five-digit PIN, Sample D, and Sample E did not successfully guess the PIN on each variety.

Table 2. Results of Shoulder Surfing Attacks Test

No.	PIN Combination	Sample				
		A	B	C	D	E
1	First Combination	-	-	-	-	-
2	Second Combination	-	-	-	-	-
3	Third Combination	-	-	-	-	-
4	Fourth Combination	-	2	1	-	-
5	Fifth Combination	1	-	-	-	-
6	Sixth Combination	-	1	-	-	-
7	Seventh Combination	-	1	-	-	-
8	Eighth Combination	-	2	-	-	-
9	Ninth Combination	-	2	2	-	-
10	Tenth Combination	-	2	2	-	-

The TQ-Model was used to conduct the evaluation of usability. There are thirteen parameters in the usability aspect of the

TQ-Model, as shown in Table 3. It has been tested on three samples by taking the best results from the testing of each sample. The following is the result of data analysis from the Spinpad and JSpinpad TQ-Model measurements in Table 4. The comparison in Table 4 shows the results of measurements for Spinpad and JSpinpad. The results showed that JSpinpad improved the usability aspect of the application. The improvement is shown in the average parameter of the log-in time with a value of minus one (the required log-in time is 21 to 40 seconds) from the previous minus two (log-in time 41 to 60 seconds) because the time required for log-in is reduced by using the rotary entry dialer, physical effort with a value of zero (does not require excessive physical effort) because the method of entering a pin digit does not require carrying any tools and tokens for each authentication, unlike the previous minus one, which requires excessive physical effort every time the user performs the authentication.

Table 3. Usability Parameters [16]

Parameter	Criteria	Rating
Mean registration time	Less than 11 seconds	1
	From 11 to 20 seconds	0
	From 21 to 40 seconds	-1
	From 41 to 60 seconds	-2
	Greater than 60 seconds	-3
Mean log-in time	Less than 6 seconds	1
	From 6 to 10 seconds	0
	From 11 to 20 seconds	-1
	From 21 to 40 seconds	-2
	From 41 to 60 seconds	-3
	Greater than 60 seconds	-4
Password input methodology	Passwords are directly inserted	0
	Passwords are indirectly inserted	-1
Password input flexibility	Passwords are inserted through a keyboard or mouse	0
	Either keyboard or mouse is used for password insertion	-1
Physical effort	No significant effort required	0
	Require some effort	-1
Mental effort	No effort required	0
	Require some effort for password element searching	-1
	The high-level effort required for password element searching or insertion	-2
Requirements for execution	Hardware and software are not required	0
	Software required	-1
	Hardware required	-2
	Both hardware and software required	-3
Effect of human disabilities	No effect of common disabilities	0
	Have the effect of common disabilities	-1
Size of assets	Less than 100 kb	0
	From 101 kb to 500 kb	-1
	Greater than 500 kb	-2
Internal processing	No significant processing required	0
	High processing required	-1
Applicability	Execute smoothly on every kind of device	0
	It cannot execute smoothly on every kind of device	-1
	Designed for a specific category of devices	-2
Learnability	Easy	0
	Moderate	-1
	Difficult	-2
Graphical design	Pleasant	1
	Average	0
	Dull	-1

As shown in Table 4, the mental effort parameter of JSpinpad gets zero value because the user more conveniently remembers six-digit PINs. Compared to Spinpads mental effort parameter gets a minus one because the user must match the registered digit PIN with the received token every time he authenticates. JSpinpad also gets an enhancement score in the requirement for execution parameter, from minus two to zero, because the user does not need to bring any additional devices, such as earphones or headsets, to authenticate, as compared to Spinpad. The results show that JSpinpad performs better because the ten parameters are zero.

Table 4. TQ-Model Usability Evaluation

No	Parameter	JSpinpad	Spinpad [11]
1	Mean Registration Time	1	1
2	Mean Log-in Time	-1	-2
3	Password Input Methodology	0	0
4	Password Input Flexibility	0	0
5	Physical Effort	0	-1
6	Mental Effort	0	-1
7	Requirement for Execution	0	-2
8	Effect of Human Disabilities	0	0
9	Size of Assets	0	0
10	Internal Processing	0	-1
11	Applicability	0	0
12	Learnability	0	-1
13	Graphical Design	1	0

4. CONCLUSION

This study has successfully implemented JSpinpad as a secure mobile-based rotary entry pad authentication by implementing JWT on the backend. JSpinpad improvement follows the initial goal in formulating the problem, i.e., speed and ease of use, by evaluating the TQ-Model on the application. Additionally, it still fulfills the security element because of the use of JWT. The Shoulder Surfing Attack test samples managed to guess the PIN was in small amounts. Two of the five respondents failed to guess the numbers at all. Only 1 of 5 samples successfully guessed six 10-digit PIN combinations (2x1x1x2x2x2) from 10 combinations to the power of 10. For the first time, this study succeeded in conducting a usability evaluation on a mobile-based rotary entry pad authentication mechanism using TQ-Model. The usability evaluation with the JSpinpad shows better results where seven parameters increase, only one parameter is negative, and 10 of 13 are zero. There is a process of randomizing the numbers that each user dials up, and these results indicate that the TQ-Model can be applied appropriately to the JSpinpad. This study shows how to measure the usability of the authentication mechanism using the TQ-Model. The results of this study are expected to be a reference for other studies, especially on the authentication mechanism using a rotary entry pad. Nevertheless, it did not examine the security of randomness pin rotation. Therefore, further research can be carried out by applying a secure randomization algorithm for the pin rotation and re-evaluating its security and usability.

5. ACKNOWLEDGEMENTS

The authors would like to thank Politeknik Siber dan Sandi Negara, which has provided infrastructure support during the research and helped fund the publication of this research.

6. DECLARATIONS

AUTHOR CONTIBUTION

The first and fourth authors carried out the ideas, designs, and experimental designs; the implementation and treatment of tests were carried out by the fourth author; data collection and analysis were carried out by the second and fourth authors; the script writing was carried out by the first, third, and fourth authors; and the revision and finalization of the manuscript were carried out by the first and second authors.

FUNDING STATEMENT

This research is supported by the Center for Research and Community Service of the State Cyber and Crypto Polytechnic in the form of the cost of publishing an accredited national journal through the PPM Budget from the National Cyber and Crypto Agency.

COMPETING INTEREST

We have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] W. Liu, J. Song, H. Wu, W. Lei, F. Huang, W. Hou, H. Liang, and H. Wen, "Non-Crypto Authentication for Smart Grid Based on Edge Computing," *Journal of Physics: Conference Series*, vol. 1646, no. 1, 2020.

[2] R. Alomari and J. Thorpe, "On Password Behaviours and Attitudes in Different Populations," *Journal of Information Security and Applications*, vol. 45, pp. 79–89, 2019.

[3] A. Huang, S. Gao, J. Chen, L. Xu, and A. Nathan, "High Security User Authentication Enabled by Piezoelectric Keystroke Dynamics and Machine Learning," *IEEE Sensors Journal*, vol. 20, no. 21, pp. 13 037–13 046, 2020.

[4] T. M. Ibrahim, S. M. Abdulhamid, A. A. Alarood, H. Chiroma, M. A. Al-garadi, N. Rana, A. N. Muhammad, A. Abubakar, K. Haruna, and L. A. Gabralla, "Recent Advances in Mobile Touch Screen Security Authentication Methods: A Systematic Literature Review," *Computers and Security*, vol. 85, pp. 1–24, 2019.

[5] P. Markert, D. V. Bailey, M. Golla, M. Dürmuth, and A. J. Aviv, "On the Security of Smartphone Unlock Pins," *ACM Transactions on Privacy and Security*, vol. 24, no. 4, 2021.

[6] D. H. Nyang, H. Kim, W. Lee, S. bae Kang, G. Cho, M. K. Lee, and A. Mohaisen, "Two-Thumbs-Up: Physical Protection for PIN Entry Secure against Recording Attacks," *Computers and Security*, vol. 78, pp. 1–15, 2018.

[7] M. Monjirul Kabir, N. Hasan, M. D. Khalid Hassan Tahmid, T. A. Ovi, and V. S. Rozario, "Enhancing Smartphone Lock Security using Vibration Enabled Randomly Positioned Numbers," *ACM International Conference Proceeding Series*, 2020.

[8] A. Souza, Í. Cunha, and L. B Oliveira, "NomadiKey: User Authentication for Smart Devices Based on Nomadic Keys," *International Journal of Network Management*, vol. 28, no. 1, pp. 1–19, 2018.

[9] F. Binbeshr, M. L. Mat Kiah, L. Y. Por, and A. A. Zaidan, "A Systematic Review of PIN-Entry Methods Resistant to Shoulder-Surfing Attacks," *Computers and Security*, vol. 101, p. 102116, 2021.

[10] H. Anthonio and Y. H. S. Kam, "A Shoulder-Surfing Resistant Colour Image-based Authentication Method Using Human Vision Perception with Spatial Frequency," *2020 15th International Conference for Internet Technology and Secured Transactions, ICITST 2020*, 2020.

[11] S. Rajarajan, R. Kalita, T. Gayatri, and P. Priyadarsini, "SpinPad: A Secured PIN Number Based User Authentication Scheme," *2018 International Conference on Recent Trends in Advance Computing (ICRTAC)*, pp. 53–59, 2018.

[12] S. Ahmed and Q. Mahmood, "An Authentication Based Scheme for Applications Using Json Web Token," in *2019 22nd International Multitopic Conference (INMIC)*. IEEE, 2019.

[13] S. Dalimunthe, J. Reza, and A. Marzuki, "View of the Model for Storing Tokens in Local Storage (Cookies) Using Json Web Token (JWT) With HMAC (Hash-Based Message Authentication Code) In E-learning Systems," *Journal of Applied Engineering and Technological Science*, vol. 3, no. 2, pp. 149–155, 2022.

[14] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia, and G. Bianchi, "On the Design of a Decentralized and Multiauthority Access Control Scheme in Federated and Cloud-Assisted Cyber-Physical Systems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5190–5204, 2018.

[15] A. Y. Pangestu, R. Safe'i, A. Darmawan, and H. Kaskoyo, "Evaluasi Usability pada Web GIS Pemantauan Kesehatan Hutan Menggunakan Metode System Usability Scale (SUS)," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 1, pp. 19–26, 2020.

[16] S. Z. Nizamani, S. R. Hassan, and R. A. Shaikh, "TQ-Model: A New Evaluation Model for Knowledge-Based Authentication Schemes," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2763–2778, 2020.

[17] J. Trauer, S. Schweigert-Recksiek, C. Engel, K. Spreitzer, and M. Zimmermann, "What Is a Digital Twin? - Definitions and Insights from an Industrial Case Study in Technical Product Development," *Proceedings of the Design Society: DESIGN Conference*, vol. 1, pp. 757–766, 2020.

[18] I. Khairunisa and H. Kabetta, "PHP Source Code Protection Using Layout Obfuscation and AES-256 Encryption Algorithm," *Proceedings - IWBIS 2021: 6th International Workshop on Big Data and Information Security*, pp. 133–138, 2021.

[19] M. L. Kambanou and T. Sakao, "Using Lifecycle Costing (LCC) to Select Circular Measures: A discussion and Practical Approach," *Resources, Conservation and Recycling*, vol. 155, 2020.

[20] Y. Rosmansyah, M. Achiruzaman, and A. B. Hardi, "A 3D Multiuser Virtual Learning Environment for Online Training of Agriculture Surveyors," *Journal of Information Technology Education: Research*, vol. 18, pp. 481–507, 2019.

[21] M. Guerar, L. Verderame, A. Merlo, F. Palmieri, M. Migliardi, and L. Vallerini, "CirclePIN: A Novel Authentication Mechanism for Smartwatches to Prevent Unauthorized Access to IoT Devices," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 3, 2020.

[This page intentionally left blank.]