How Can Fingerprint Improves The Payment Experience of a Drink Vending Machine?

1st Satria Hutomo
School of Computing
Telkom University
Bandung, Indonesia
satriahutomo@students.telkomuniversity.ac.id

2nd Parman Sukarno
School of Computing
Telkom University
Bandung, Indonesia
psukarno@telkomuniversity.ac.id

3rdRahmat Yasirandi
School of Computing
Telkom University
Bandung, Indonesia
batanganhitam@telkomuniversity.ac.id

***Abstract*—Many examples of technology on the payment scheme already help and facilitate transactions in Indonesia such as internet banking, ATM or debit cards, e-money, and also mobile banking. Included on drink vending machine, it is a sale that utilizes machines. Today's commonly, drink vending machines still use coins or smart cards, which based on the Legal and Ethical Experience this factor is still have many weaknesses and threats, that can occur in this payment system. So the payment authentication factor is needed to pay more attention to user experience components, some of which are ownership, privacy, and security.So that in this study, the implementation of the fingerprint authentication scheme was made as an e-payment factor based on user experience. This study uses a mixed-method in analyzing every pain problem of the research. Where to conduct exploratory studies through literature review and direct observation in the case of the application of the vending machines, especially in developing countries such as Indonesia. This research shows that the payment authentication system can solve the problem of the risk of system attack, the risk of topping up fails, it can harm the user (R1), if the user loses a smart card, the smart card is at risk of being used by not the owner (R2), if the data on the smart card is cloned, it can poses a risk to the system (R3). The conclusion of the proposed payment system can overcomes the existing problems obtained from the system security testing scenario. In addition, user agreement testing (R4 and R5) are also done by providing a questionnaire comparing the level of satisfaction of the existing and proposed payment systems, the results of this test shows that the user feels comfortable with the proposed payment system.**

***Index Terms*—Payment, Biometric, Fingerprint.**

I. Introduction

In Indonesia, a vending machine that provides products that are only drinks (as know as called the drink vending machine) is very easy to find and widely spreads around. The payment method of this machine popularly used is 2 authentication factors, there are money and smart card [1]. Payment with money, general inconvenience related to the availability and condition of the money itself. Money is a factor payment that's not easy to bring anymore. If using money as an authentication factor, then it must always be carried and must be in a physical condition (banknotes) that is not defective [2]. On the other hand, Smart cards as a factor of payment, the same as money, which has some vulnerability aspects. Smart card can be to being lost, stolen or cloned and then used in addition to their owners and misused. This paper discusses the importance of the elements of user experience. Based on holistic view in user experience, one of the weaknesses that exist in the payment method in the drink vending machine today is around of the Legal and Ethical components including ownership, privacy, security [3]. Based on the background that has been described, it is concluded that the formulation of the problem raised in the factor authentication of payment process. Commonly, like if a user loses/ forgets bring money/ smart card then it can not be used. So this research applies the authentication factor at a higher level than existing. Namely factor authentication at the level of "what you are" , and biometric is one of the factors of this level. Fingerprint has been widely used in various fields because authentication using biometric fingerprint is generally proven to be faster, more convenient, and more secure [4]. Fingerprints are said to be faster because users do not need to enter or remember the authentication factor (at level of "what you know" such as passwords / PINs) that can slow down the authentication process, other than that the use of fingerprint authentication increases security. After all, every human being has a different fingerprint from one another. Hypothetically, the problem studied is based on the user experience, especially in the Legal and Ethical Components, making the proposed payment scheme with fingerprint as the authentication factor can be better than the existing system. Especially in 3 aspects of ownership, privacy, and security.

II. Related Works

In a study conducted by Aneeqa Ramzan, Saad Rehman and Aqib Perwaiz entitled "RFID Technology: Beyond Cash-Based Methods in Vending Machines" [2]. Said that the traditional payment system on vending machines has many weaknesses such as hacking, auditing, depositing money, detecting currencies that have not been coded/stored in a database, the system only accepts banknotes in good condition. This research introduces a secure and new cash payment system using a smartcard (RFID). Another study was design the presence system using fingerprint has good effectiveness, such as saving administrative paper and the most important thing is to overcome the problem of fraud committed by teachers and employees in time corruption [5], [6]. Then, some studies of the fingerprint authentication system was designed to open the door [7]–[9]. Biometric authentication systems have many ad-

978-1-7281-6142-6/2020/$31.00 ©2020
Authorized licensed use limited to: University of Manchester. Downloaded on January 12,2021 at 12:14:54 UTC from IEEE Xplore. Restrictions apply.

vantages when compared to traditional authentication systems based on passwords or smartcards. Traditional authentication is lacking in terms of security because it is vulnerable to attacks, users can forget passwords and if using a smartcard is vulnerable to lose or theft. Whereas in the research on employee activities include employee attendance, employee tracking, employee leave, and payment of promotional salary modules [10]–[12]. The use of fingerprints to make this system has many advantages including fingerprint recognition only takes a few seconds it is faster than entering a password, besides that, on the security side, the use of fingerprints is very well proven because in this system employees cannot manipulate the presence they. Another else of objectivity research is to build a payment system based on fingerprint authentication for the Point of Sale system [13], [14]. In contrast to this research, there are case studies and are not based on user experience. Furthermore, the final research conducted by Insan Isa Mulia, Parman Sukarno and Rahmat Yasirandi entitled "Multi-Factor Authentication Using Smartcards and Fingerprint (Case Study: Parking Gate)" which carried out several attack scenarios that can occur on smartcards [15], [16]. The results of this study prove that the threat of attack that can occur can be overcome by fingerprint authentication.

A. User Experience of Payment Process

User Experience is the attitude, behavior, and emotions of users when using a product, system or service [17], [18]. This experience is an individual's perception related to the perceived benefits and the ease of getting [19]. Meanwhile, according to Jesse James Garret explained that user experience is an experience created by a product for people who use it. A product is made or developed, the person is concerned about it (user experience) or not. From this, we can distinguish successful products from products that fail. Electronic payments (E-payments) are payments made using information and communication technology. Electronic payments can include credit cards, debit cards, payments through smartphones, and also web payments. The purpose of usability is to make it easier for users to do something, but strong security measures make it difficult for users. This is where security is needed but it is not difficult for the user but can facilitate the user especially when authenticating when paying. From the previous discussion which explained that the current authentication factor has many weaknesses and threats that can occur in the payment system, then biometric authentication is expected to make authentication in payment more secure and the user also feels more ease to use the process. E-Payment is divided into two methods, the Cash E-Payment System and the Credit Payment System]. In E-Payment there are also several parties involved including:

- Issuer is a bank or non-banking institution.
- Consumers are parties who make E-Payment.
- Seller is the party that receives E-Payment.
- Regulators who are usually the government whose job is to make regulations to control E-Payment scheme.

III. Design and Implementation

A. Defining Risks

Table 1 shows the elaboration of 3 elements in the experience type of Legal and Ethical. Where for this type of experience reflects user protection. In the stage of defining risks, the individual experience is used as a methodological for analysis.

TABLE I
REFLECT INDIVIDUAL EXPERIENCE OF USER DATA [3]

Elements	Properties	Descriptions
Ownership	User ideas and content	Protection of ideas or any content created by users.
Privacy	Personal data protection Selective use permission	The degree to which personal data are protected. Selective authorisation to use personal data.
Security	Protection of access	Reliable system environments

Furthermore, any risk that may arise will be described based on the experience elements that have been defined previously. There is possible that a risk appears from one or more elements of legal and ethical experience.

1) R1: the risk if the top-up of smart card balance fails, it can harm the personal data (to solve the threat problem when top-up)
2) R2: the risk of threats that can occur if a user loses a smart card, then the smart card can be used by non-owners (to solve the threat problem when payment).
3) R3: the risk of threats that can occur if the data that is on the smart card is cloned, then it can endanger the system (to solve the problem of threats when payment).
4) R4: the risk if the money is not in good condition, then the user cannot make a purchase (to solve the problem of a threat when payment).
5) R5: the risk if currency detection is not possible for currencies that have not been coded/stored in a database, this causes users to not be able to make purchases (to solve the problem of threats when payment).

B. The Proposed Payment Protocol Design

This proposed biometrics payment scheme is designed with 3 stages. The first stage is the user enrollment stage where the Customer CU is registered by using the website application of Administration System AS. Every new customer must fill in the data form and it is pushed with API Service to the database of Server.

1) *CU → AS: input form (personal data)*
U registration of personal data such as full name, username, email and password that will be stored in the database

2) *AS → CU: error display (invalid data)*
Administration System AS confirms the invalid data to Customer CU to re-processed to the next chance.

Authorized licensed use limited to: University of Manchester. Downloaded on January 12,2021 at 12:14:54 UTC from IEEE Xplore. Restrictions apply.

3) *AS → CU: request biometric (valid data)*
Administration System AS confirms the valid data to Customer CU and request to register their fingerprint.

4) *AS → CU: display (register info)*
The Administration System AS will authenticates and allocates the fingerprint and provides information if the Customer CU was successfully registered.

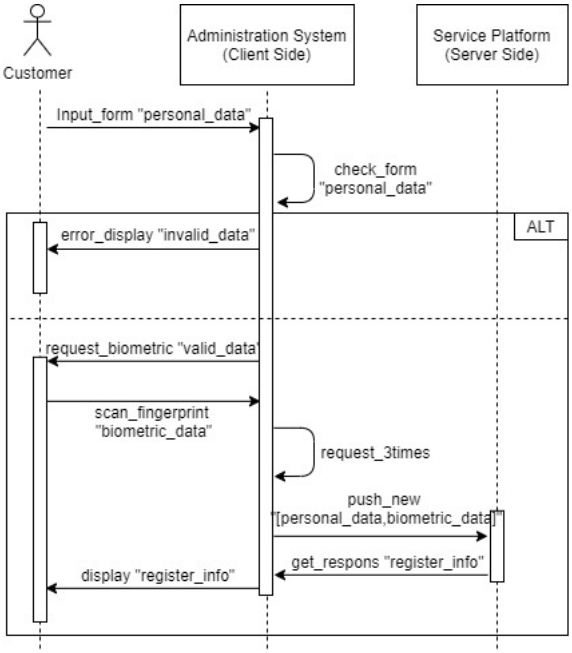

Fig. 1. Protocol of Enrollment Stage

Next is the Balance Top-Up Stage. Administrator A need to help every customer to top up their balance. the customer must select and give their money to change for being their virtual money. chooses the amount of money to be filled in by the Admin.

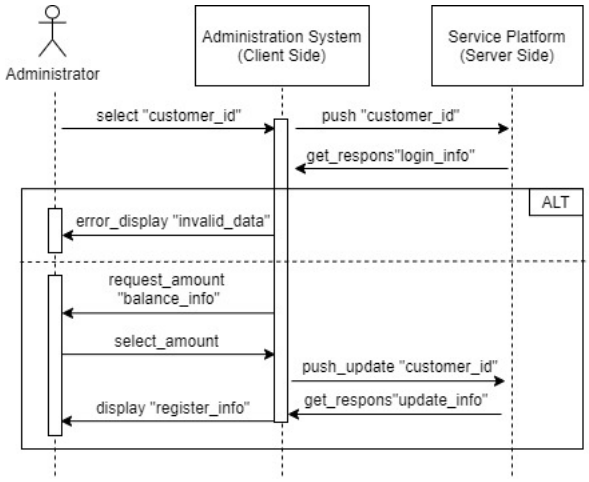

Fig. 2. Protocol of Balance Top-Up Stage

1) *A → AS: select (customer id)*
Administrator A chooses the user based on id, and get selected customer information form Administration System AS.

2) *AS → A: error display (invalid data)*
Administration System AS confirms the invalid data to Administrator A to re-processed to the next chance.

3) *AS → A: request biometric (valid data)*
Administration System AS confirms the valid data to Administrator A and requests to select amount.

4) *AS → A: display (register info)*
The AS will top-ups and updates the balance and provides information if the process was successfully done.

The third stage is the purchase stage, when Customer CU using Vending Drink Machine DVM and try to buy a product. Every Customer CU need to selects the items to be purchased with push selected button, then the system will check the volume of items purchased and amount of their balance also. After the check is successful the VDM will pull out the selected product.

1) *CU → VDM: push buttom (product id)*
Customer CU push the button of selected product, and Vending Drink Machine DVM will checks based on id.

2) *VDM → CU: error display (invalid data)*
Vending Drink Machine DVM confirms the invalid data to Customer CU to re-processed to the next chance.

3) *AS → CU: request biometric (valid data)*
Vending Drink Machine DVM confirms the valid data to Customer CU and requests to scan their fingerprint as a factor authentication.

4) *AS → CU: display (register info)*
Vending Drink Machine DVM will pulls up the selected product, updates the balance and provides information if the process was successfully done.

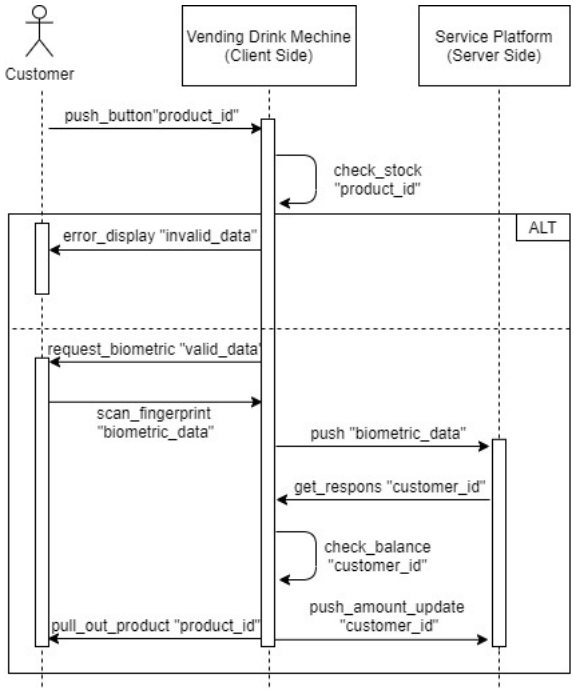

Fig. 3. Protocol of Purchases Stage

Authorized licensed use limited to: University of Manchester. Downloaded on January 12,2021 at 12:14:54 UTC from IEEE Xplore. Restrictions apply.

IV. Scenarios of Test

In the test scenario 2 stages of testing will be carried out on the current system with the system proposed by the author. First is a system security comparison test. Second is testing user agreement. After getting the results of the system security testing, the user agreement testing is then conducted to determine whether the proposed system has fulfilled the user agreement and resolved the existing problems. This test focuses on Legal and Ethical components including ownership, privacy, security [3]. "Ownership is the power that is supported to hold control of something that is owned exclusively and use it for personal purposes which includes user ideas content and personal image", "Privacy is the ability of one individual to control the flow of information about themselves which includes personal data protection, anomality, selective use permission"," Security is a condition which is free from danger or threat which includes protection of digital identity data, protection of access ".

A. System Security Testing

Payment system security testing is a test conducted to obtain a comparison of security between existing payment systems and the proposed payment system, where the existing system uses money and smartcards as a means of payment while the proposed system uses a biometric fingerprint as a payment authentication tool. For a comparison of the system can be seen in table II.

TABLE II
Comparing All Systems

System	Cash Money	Smart Card	Fingerprint
The Existing System	V	V	X
The Proposed System	X	X	V

To get the results of a comparison of the security of the existing payment system with the proposed payment system. Several threat scenarios can occur in the payment mechanism authentication in vending drinks. This scenario is based on research that has been done about threats that can occur on smartcard authentication systems [10]. The research proves that threats that occur in smartcard authentication can be mitigated by fingerprint authentication. Here are test scenarios for some risks(risk 1, risk 2, and risk 3), while test scenarios for other risks (risk 4 and risk 5) will be delivered in the next part at the user agreement testing scenarios.

1) System Security Testing for Risk 1: Threats of risk when users top-up. Users top up with the desired amount. Next Admin will fill the balance on the user. However, top-up failures of e-money can occur [20]. So the expected results of testing scenario 1 is when the user fails to top up, Admin can immediately top up again. The test scenario can be seen in the picture.

2) System Security Testing for Risk 2: The attacker is trying to purchase a vending drink using an authenticated smartcard but the smartcard does not belong to the attacker. Then the system will authenticate the smartcard. So the expected results of testing scenario 2 is that authentication fails and the attacker can't make a purchase on a vending drink. The test scenario can be seen in the picture.

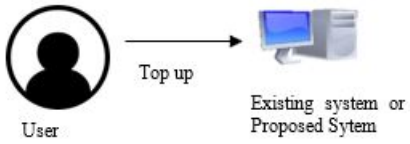

Fig. 4. Protocol of Purchases Stage

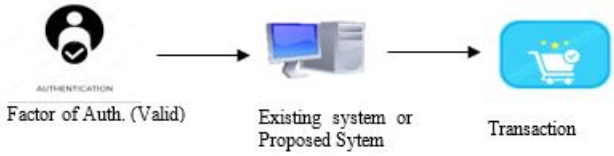

Fig. 5. Protocol of Purchases Stage

3) System Security Testing for Risk 2: The attacker tries to purchase a vending drink using a smart card that is cloned from an authenticated original smartcard. Then the system will authenticate the cloned smartcard. So the expected results of testing scenario 3 is that authentication failed and the attacker can't make a purchase. The test scenario can be seen in the picture

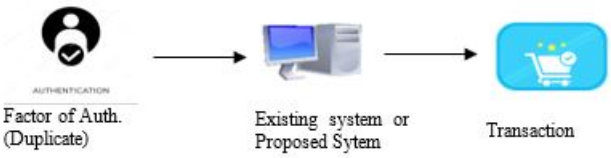

Fig. 6. Protocol of Purchases Stage

B. User Agreement Testing

User agreement testing is testing to find out that the proposed payment system is accepted by the user. To get the results of this test, 30 people were tested. This test using qualitative testing that is intended to prove if the risk 4 and risk 5 are still appears. Qualitative testing is testing by asking the response rate of both systems (existing systems and proposed systems) utilizing the Likert scale [21], which is often used in qualitative testing to obtain numerical values. This user agreement test scenario will be carried out by giving questions 4 and 5 to the respondent and asked to give grades 1-5 referring to the quality of the mitigation system [21]].

$$RelativeLikertIndex = \frac{\sum W}{N}$$

$$\frac{\sum W}{N} = \frac{5n_1 + 4n_2 + 3n_3 + 2n_4 + 1n_5}{N}$$

Authorized licensed use limited to: University of Manchester. Downloaded on January 12,2021 at 12:14:54 UTC from IEEE Xplore. Restrictions apply.

The following explanation is for the relative likert index. W is given weight for each factor by respondents, range from 1 to 5 :

n_1 : Extremely uncomfortable,
n_2 : Very uncomfortable,
n_3 : Fairly uncomfortable,
n_4 : Comfortable, and
n_5 : Very comfortable.
N : The total number of respondents, this result will be mapped into the Likert Scale.

V. Evaluation

In the evaluation section, the results of testing the two procedures are explained in the previous chapter. 4.1 Test Results The results of the first test procedure can be seen in Table IV:

A. Analysis of System Security Testing.

TABLE III
Security System Testing Results

Scenarios	Existing System	Proposed System
Scenarios of Risk 1	The process is not immediate, it must be proof of transfer screenshots, verification by admin 3 days.	The threat does not apply, the admin only needs to repeat the top-up process.
Scenarios of Risk 2	the threat successfully to penetrate the system	The threat failed to penetrate the system
Scenarios of Risk 3	the threat successfully to penetrate the system	The threat failed to penetrate the system

The results of testing the first scenario are when the user does a top-up on the existing system but fails. This failure is detrimental to the user because the process for reporting top-up failures must go through several stages and the process is not immediate. Next is the result of testing the first scenario on the proposed system. The result of this test is that when a user fails to top up, the admin only needs to do top up again. So that the proposed system can overcome the risk threats that exist in the first scenario problem. The second scenario test results are the threat of an attacker purchasing an existing system using a smart card that is not his and the attacker successfully passes the purchase authentication process, this occurs because the smart card cannot ensure the user of the smart card user so that in this second test scenario the existing system is successful penetrated by the attacker by using a smart card that is not his authenticated. Next is the result of testing the third scenario on the proposed system. The results of this test the threat of an attacker cannot pass the authentication process on the proposed system. This is because the user's fingerprints cannot be used by non-owners, which means that fingerprints can only be used by the user himself. So the proposed system successfully authenticated the second test scenario. It can be concluded that the proposed system can overcome the problems that exist in the second test scenario. The result of the third scenario test is the threat of an attacker purchasing an existing system using a cloned smart card. As a result the attacker can pass the purchase authentication process, this can occur if the attacker clones data from a user's smart card that has been authenticated. So that in this third test scenario the existing system is successfully penetrated by the attacker by using a smart card cloned from a authenticated smart card. Next is the result of testing the third scenario on the proposed system. The results of this test the threat of an attacker cannot pass the authentication process on the proposed system. This is because it is difficult to clone a user's fingerprint biometric data. So the proposed system successfully authenticated the third test scenario. It can also be concluded that the proposed system can overcome the problems that exist in the third test scenario.

B. Analysis of User Agreement Testing

Testing result of the second procedure (user agreement testing) can be seen in the following diagram based on user interviews regarding risk 4 and risk 5:

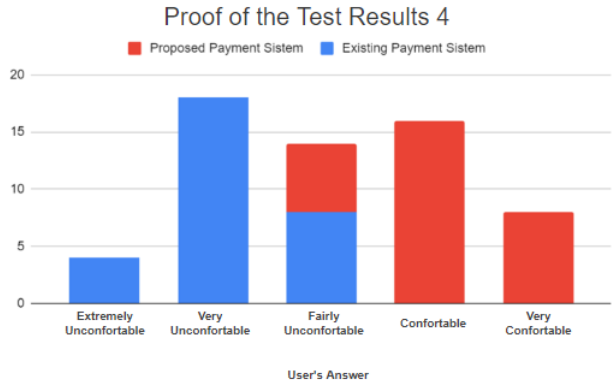

Fig. 7. Result of User Aggrement Testing on Risk 4

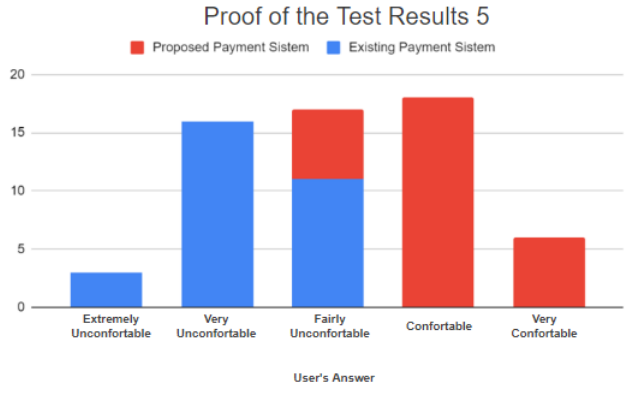

Fig. 8. Result of User Aggrement Testing on Risk 5

The results of testing the user agreement about problem 4 is that the user feels uncomfortable when faced with problem 4 in the current payment system. But after the authors provide a solution of problem 4 by applying the fingerprint as a means of

Authorized licensed use limited to: University of Manchester. Downloaded on January 12,2021 at 12:14:54 UTC from IEEE Xplore. Restrictions apply.

payment, the results of respondents feel comfortable with the proposed payment system. The results of the calculation of the Likert index relative based on questionnaire data of risk 4 in the existing payment system is 1.9 where the value tends to be inconvenient. While the results of the calculation of the Likert index relative based on questionnaire data of risk 4 in the proposed payment system are 4.3 whose values tend towards comfortable. While the results of testing the user agreement on risk 5 is that the user feels uncomfortable when faced with risk 5 in the existing payment system. But after the authors provide a solution of risk 5 by applying the fingerprint as a means of payment, the results of respondents feel comfortable with the proposed payment system. The results of the calculation of the Likert index relative based on questionnaire data of risk 5 on the existing payment system is 2 where the value tends towards uncomfortable. While The results of the calculation of the Likert index relative based on questionnaire data of risk 5 on the proposed payment system are 3.7, the value of which tends towards comfortable.

VI. Conclusion

After a series of tests, namely payment system security testing and user agreement testing, it can be concluded that the proposed payment system successfully resolves problems including Risk 1 R1, Risk 2 R2, and Risk 3 R3 on the existing payment system and based on the results of the system's security testing, the proposed system addresses the threat of an attack there is. Besides, the results of the user agreement test show that the user feels comfortable with the proposed payment system to replace the existing payment system. In the future, payment systems using fingerprints can be applied to another machine that are popular today, such as e-toll's machine and others.

References

[1] S. Mulyani and R. Hartono, "Vending machine and influence on life in indonesia," *IOP Conference Series: Materials Science and Engineering*, vol. 662, p. 052001, Nov. 2019. [Online]. Available: https://doi.org/10.1088/1757-899x/662/5/052001

[2] A. Ramzan, S. Rehman, and A. Perwaiz, "RFID technology: Beyond cash-based methods in vending machine," in *2017 2nd International Conference on Control and Robotics Engineering (ICCRE)*. IEEE, Apr. 2017. [Online]. Available: https://doi.org/10.1109/iccre.2017.7935068

[3] M. Pallot and K. Pawar, "A holistic model of user experience for living lab experiential design," in *2012 18th International ICE Conference on Engineering, Technology and Innovation*. IEEE, Jun. 2012. [Online]. Available: https://doi.org/10.1109/ice.2012.6297648

[4] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decision Support Systems*, vol. 106, pp. 1–14, Feb. 2018. [Online]. Available: https://doi.org/10.1016/j.dss.2017.11.003

[5] M. Alhothaily, , M. Alradaey, M. Oqbah, and A. El-Kustaban, "Fingerprint attendance system for educational institutes," *Journal of Science and Technology*, vol. 20, no. 1, pp. 34–44, Jun. 2015. [Online]. Available: https://doi.org/10.20428/jst.20.1.4

[6] B. K. P. Mohamed and C. V. Raghu, "Fingerprint attendance system for classroom needs," in *2012 Annual IEEE India Conference (INDICON)*. IEEE, Dec. 2012. [Online]. Available: https://doi.org/10.1109/indcon.2012.6420657

[7] J. Baidya, T. Saha, R. Moyashir, and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, Jan. 2017. [Online]. Available: https://doi.org/10.1109/ccwc.2017.7868448

[8] M. Kader, M. Y. Haider, M. Karim, M. S. Islam, and M. M. Uddin, "Design and implementation of a digital calling bell with door lock security system using fingerprint." in *2016 International Conference on Innovations in Science, Engineering and Technology (ICISET)*. IEEE, Oct. 2016. [Online]. Available: https://doi.org/10.1109/iciset.2016.7856484

[9] Swati and R. P. Gupta, "Implementation of biometric security in a smartphone based domotics," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*. IEEE, Oct. 2018. [Online]. Available: https://doi.org/10.1109/icacccn.2018.8748672

[10] M. D. a. Chiwa, "Secured employee attendance management system using fingerprint," *IOSR Journal of Computer Engineering*, vol. 16, no. 1, pp. 32–37, 2014. [Online]. Available: https://doi.org/10.9790/0661-16133237

[11] M. Olagunju, A. E., and T. O., "Staff attendance monitoring system using fingerprint biometrics," *International Journal of Computer Applications*, vol. 179, no. 21, pp. 8–15, Feb. 2018. [Online]. Available: https://doi.org/10.5120/ijca2018916370

[12] O. MuhtahirO., A. A. O., and A. K. S., "Fingerprint biometric authentication for enhancing staff attendance system," *International Journal of Applied Information Systems*, vol. 5, no. 3, pp. 19–24, Feb. 2013. [Online]. Available: https://doi.org/10.5120/ijais12-450867

[13] H. Vats, R. Ruhl, and S. Aghili, "Fingerprint security for protecting EMV payment cards," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, Dec. 2015. [Online]. Available: https://doi.org/10.1109/icitst.2015.7412065

[14] R. K. Garg and N. K. Garg, "Developing secured biometric payments model using tokenization," in *2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)*. IEEE, Oct. 2015. [Online]. Available: https://doi.org/10.1109/icscti.2015.7489549

[15] R. Yasirandi, Y. A. Setyoko, and P. Sukarno, *Security Document for Smart Parking Gate based on Common Criteria Framework*, *2019 7th International Conference on Information and Communication Technology (ICoICT)*, Malaka, Malaysia, jul 2019.

[16] I. M. Insan, P. Sukarno, and R. Yasirandi, "Multi-factor authentication using a smart card and fingerprint (case study: Parking gate)," *Indonesia Journal on Computing (Indo-JC)*, vol. 11, no. 4, pp. 55–66, Nov. 2019. [Online]. Available: https://doi.org/10.21108/INDOJC.2019.4.2.309

[17] Z. J. Liu, B. Ferry, S. Lacasse, S. Fonte, R. Matthieu, and G. Larsen, "A scalable automated system to measure user experience on smart devices," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, Jan. 2019. [Online]. Available: https://doi.org/10.1109/icce.2019.8662093

[18] S. Nam, G. Ko, K.-W. Suh, and J. Kwon, "User experience- and design-oriented virtual product prototyping system," in *2019 11th International Conference on Knowledge and Smart Technology (KST)*. IEEE, Jan. 2019. [Online]. Available: https://doi.org/10.1109/kst.2019.8687418

[19] T. Arsan, "Smart systems: From design to implementation of embedded smart systems," in *2016 HONET-ICT*. IEEE, Oct. 2016. [Online]. Available: https://doi.org/10.1109/honet.2016.7753420

[20] H. Godschalk and M. Krueger, "Why e-money still fails - chances of e-money within a competitive payment instrument market," 05 2000.

[21] J. Robinson, "Likert scale," in *Encyclopedia of Quality of Life and Well-Being Research*. Springer Netherlands, 2014, pp. 3620–3621. [Online]. Available: https://doi.org/10.1007/978-94-007-0753-5$_1$654

Authorized licensed use limited to: University of Manchester. Downloaded on January 12,2021 at 12:14:54 UTC from IEEE Xplore. Restrictions apply.