TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 20, No. 6, December 2022, pp. 1297~1306
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v20i6.22157

Design and develop authentication in electronic payment systems based on IoT and biometric

Ahmed Abdulkarim Talib, Ayman Dawood Salman
Computer Engineering Department, Computer Engineering, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Nov 03, 2021
Revised Sep 17, 2022
Accepted Sep 27, 2022

Keywords:

Biometrics
E-payment system
Fingerprint
Internet of things
M2M connections

ABSTRACT

Biometrics is a highly reliable technology where it has become possible to use the characteristics of a person or user (biometrics) along with traditional passwords, and we can even say that it has become an indispensable complement in modern authentication systems today, especially with regard to bank accounts, banks, financial technology (FinTech) internet of things (IoT) devices and all a process related to money and privacy, and biometric methods are multiple and increasing day by day, the most famous of which is (iris, face chart, palm, fingerprint, and others). Biometric systems are immune and immune from modern electronic attacks, such as plagiarism or electronic theft, because the authentication here takes place when all conditions are met. Then the authentication is done and the process is completed, and the aim is to reach the highest levels of accuracy and security and to make the user more comfortable to deal with these modern systems that provide him with many advantages and high privacy.

Corresponding Author:

Ahmed Abdulkarim Talib
Computer Engineering Department, Computer Engineering, University of Technology
Baghdad, Iraq
Email: ce.19.02@grad.uotechnology.edu.iq

1. INTRODUCTION

Nowadays, with the development of modern science, there has become an urgent need to consider electronic verification systems for user accounts. It is now possible to accomplish most buying and selling operations, accounting, balance transfer, and electronic payment through electronic payment techniques via the internet [1], [2]. From this need came the development of electronic verification systems and the emergence of a new system known as the biometric verification system. Which came as a revolutionary solution and a great development in this field.

In the beginning, electronic verification systems were traditional. They relied on traditional passwords in the first place. However, these methods were vulnerable to electronic attacks and theft, especially with the development of piracy sciences and the spread of account theft phenomena via the internet, from here the idea came to create a verification system based on these traditional methods in addition to methods others, more reliable and more qualitative, were the biometric verification systems, due to their uniqueness and high reliability. Each person has distinctive characteristics that are not repeated in a second person, and this modern biometric system was the main idea of the presence of the same person during the verification process to reduce data theft [3]. Biometric payment and verification systems provide many advantages, such as speed in performance and convenience in paying bills. These systems depend on storing users' data in the main database linked to several branches. When each electronic payment process is changed or authenticated, user data is verified and compared to the original in the database, and upon verification, the operation is completed successfully [4], [5].

Several studies have focused on security issues without decreasing performance and purchase time. Aigbe and Akpojaro [6] discuss electronic payment system security issues. Each payment option offers advantages and disadvantages for both customers and merchants. The analysis of security levels concerning fraud vulnerability is highlighted, and they evaluate how this relationship reduces or improves user confidence. Farawn *et al.* [7] The researcher propose an electronic payment system using radio frequency identification (RFID) card, which can be applied in universities or institutions and discusses one of the most important challenges, which is securing the system using iterated salted hash algorithm through encryption password by (SHA-256) algorithm to prevent any unauthorized entry into the system. Khanboubi *et al.* [8] the research study discusses the evolution of internet of things (IoT) in the financial system and its impact on bank operations, which will revolutionize traditional banking methods. It explains whether the new system replaces the traditional system or works to improve its infrastructure.

On the other hand, Ya'acob *et al.* [9] designed a website for an electronic payment system using a smart card and my structured query language (MySQL) database with hypertext preprocessor (PHP) language to manage purchases for children in schools through parents. The system sends alerts via short message service (SMS) and e-mail when the purchase reaches the limit set by the parents. Croock and Taaban [10] developed an e-payment system that relies on software engineering technology and neural networks to secure payment processing by generating keys to increase the system's security and authorise users' devices via a mobile application. The current paper aims to provide an electronic payment system based on IoT devices and biometrics technology like a fingerprint that specifies the user's real identity and discussion of different levels of security and privacy remains an important and necessary factor in the use of electronic payment systems.

2. PROPOSED METHOD

This paper presents the electronic payment system with one of the most reliable biometrics authentication methods by using fingerprint and IoT devices like RFID cards and keypads for personal information number (PIN) passwords. In addition to comparing the confidence of authentication between each of them as individually or together. This section illustrates the system under five sub-sections.

2.1. Fingerprint authentication

The process of authentication through fingerprints is the process through which the identity of the user is recognized, and there has been an old benefit from this process in the field of medical services and criminal investigations in cases and crime scenes, so the fingerprint is the digital identity of the person [11]. Biometrics is a behavioural and physiologically identifiable characteristic that captures an image and compares it to a time stamp. E-banking authorization and customer identity verification are critical components of electronic bank financial services. The verification system compares the customer's identity to pre-stored finger, palm, and iris biometrics in the biometric system using a biometric template [12].

Fingerprint identification is one of the branches of biometric measurements through which subscribers can complete many operations and benefit from services via the internet the fingerprint. Today's technology is widespread in most of the devices we use in modern automated teller machine (ATMs), smart tablets, personal computers, and payment devices invoices [13]. At first, the user registers and enters his data into a central database (passwords and fingerprints) so that the user is later identified when any process he performs; for example, when the user pays an invoice, he is asked to enter the password and confirm with the fingerprint to be authenticated and verified locally (verification process is a local process that takes place at the sales centre) after which a special code is sent to the main provider (the main database) to give the user the right and permission to complete the process, whereas the mentioned previously the biometric and verification devices are devices located locally in points of sale and various service, and information centres keep secret [14], [15].

2.2. Fingerprints types

Fingerprints are categorized into several major categories known as micro-details. The old verification system is still used today to classify fingerprint cards, but the scanners used to capture fingerprint images are better able to identify more details than the minutiae. This is shown in Figure 1, where we can easily observe the minutiae typography and characterization model [16]. In order to determine that the two fingerprints belong to one person, they must agree in the form (arcs, slopes), in the shape of the angle and the centre, in the amplitude, and in the presence of any traces of wounds or scars, and in the sub-characteristics of the lines forming the imprint in terms of the beginning and end of these lines and their deviation, branching or merging in another line, or islands are in the way of the line. It is often sufficient to have twelve points of agreement to say that the two fingerprints are the same, although obtaining a greater number of points of agreement is often possible [17], [18].

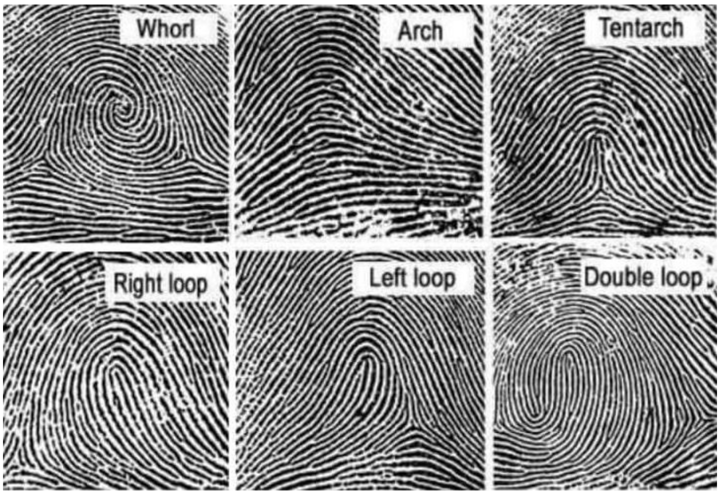


Figure 1. Types of fingerprint [17]

2.3. Fingerprint algorithm

Many algorithms can be used to analyze the fingerprint, like the Bozorth and Boyer-Moore algorithm, which can recognize fingerprints on a standard pattern fingerprint, a half-erased or rotated pattern [19]. There is new feature extraction technique based on fingerprint image blocks is presented [20], also many attempts to enhance most of the phases by working in two parts: pre-processing and postprocessing to remove the noise and make the clear fingerprint image for feature extraction [21] but the most famous is minutiae-based algorithm [22]. It is proposed to use simple pattern recognition to detect minutiae in fingerprints. When an ideal thinned ridge map with no loss of generality is available, this will be a simple process. If a pixel is on an eight-connected thinning ridge, we presume it has a value of one and zeroes otherwise. Let N_0, N_1, N_7 signify a pixel on a thinned ridge and (x, y) denotes a pixel on a thinned ridge. Make a list of its neighbours. A pixel (x, y) is a ridge ending by using (1) and a ridge bifurcation using (2) [23].

$$\sum_{i=0}^{7} Ni = 1 \tag{1}$$

$$\sum_{\mathrm{i}=0}^{7} \mathrm{Ni} > 2 \tag{2}$$

2.4. Fingerprint recognition process

The Fingerprint is the prominent formal lines and the low lines adjacent to them on the tips of the fingers, which characterize it upon contact with surfaces and bodies, especially smooth ones. Ethnicity leaves fingerprints on the surfaces of absorbent objects or on land. As for the low lines located between the prominent lines, the sense nerves end there, and they are the means by which we feel things when we touch them. The lines in the fingerprint are not subject to change. If the outer layer of the skin of a wound is damaged, the lines of the fingerprint are damaged. Those lines appear again in their original form when the wound heals without change and in the same place without leaving a trace, and the fingerprints do not match between two different people at all. Also, they are not identical in the case of identical twins [24], [25].

The tomogram Figure 2 shows the structure of the fingerprint sensor, which consists of the following components: 1-blue light emiting diode (LED) lights 2- printed circuit board (PCB) 3- touch sensor board 4- image sensor 5- processor and connectors. Inside the fingerprint scanner is a charged coupled device (CCD) which is the same optical sensing system used in digital cameras and camcorders. This device is an array of light-sensing diodes-photo sites that can generate electrical signals in response to the units of light. The job of each of these photo sites is to record a single pixel, which is a minor point representing the light that hits that spot [16], [17]. Can be illustrated in Figure 3.

When you put your finger on the glass surface, the scanning process begins. Where the CCD camera takes an image of the fingerprint. In fact, the CCD system generates an inverted image of the finger, which represents the darker or darker areas where the light is reflected from the bumps of the finger, while the lighter areas represent the less reflected light, which are the grooves between these bumps. Before comparing the fingerprint with the data stored in the device, the processing unit in the scanner makes sure that the CCD device has captured a clear image of the finger, and this occurs by checking the rate of darkness or the total values within a small sample of the image and rejecting the scanning process if it is illuminated the image is too strong or too weak. If the image is rejected, the scanner resets the brightness level by allowing in more or less light and then starts scanning again. In the event that amount of illumination is sufficient [27], [28].

The scanner then checks the image mapping, i.e. ensuring the accuracy of the image, and then the processing unit follows the straight lines extending horizontally and vertically over the image. If the finger image mapping is good, a continuous line is drawn perpendicular to the bumps of the finger, consisting of alternating segments of dark dots and light dots. If the processing unit finds that the image is clear and adequately exposed to light, then it will compare that fingerprint image with the fingerprint images stored inside the device [15], [28], as Figure 4.

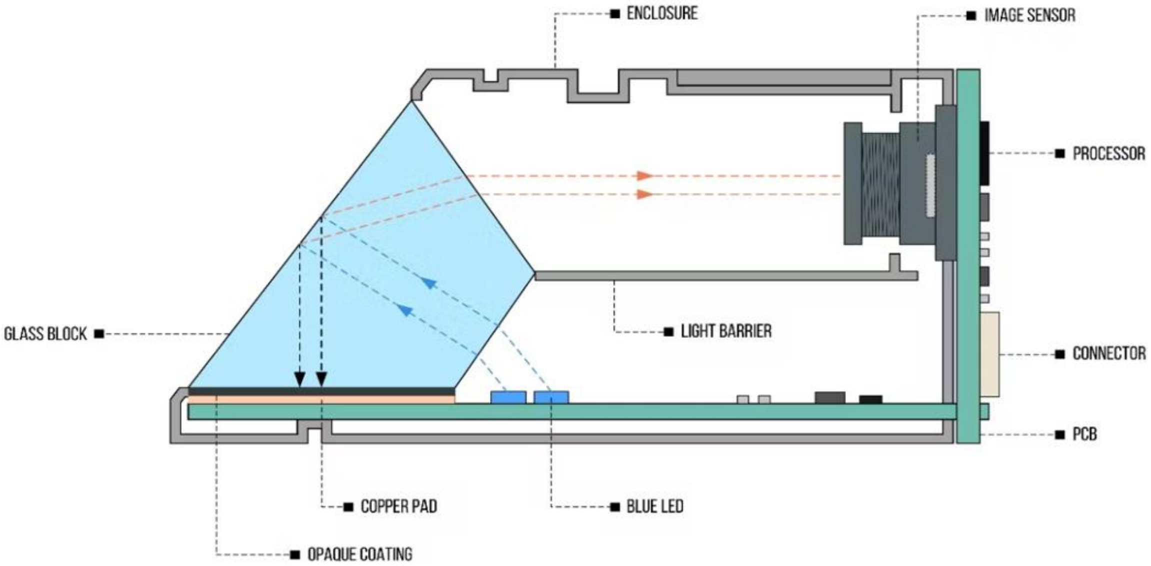


Figure 2. Fingerprint sensor [26]

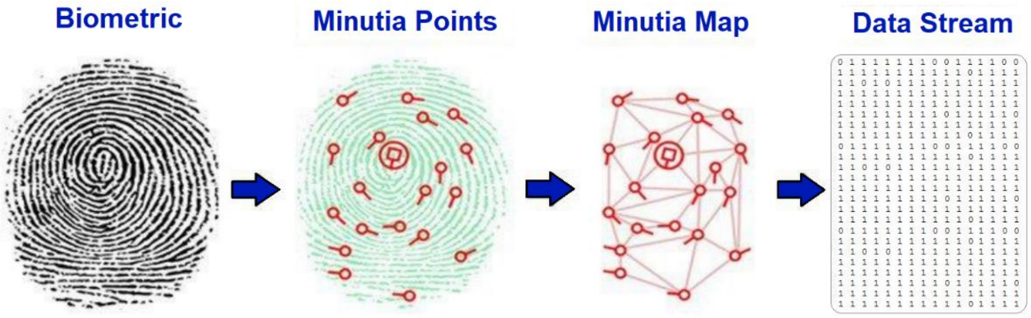


Figure 3. Convert biometric fingerprint to the data stream

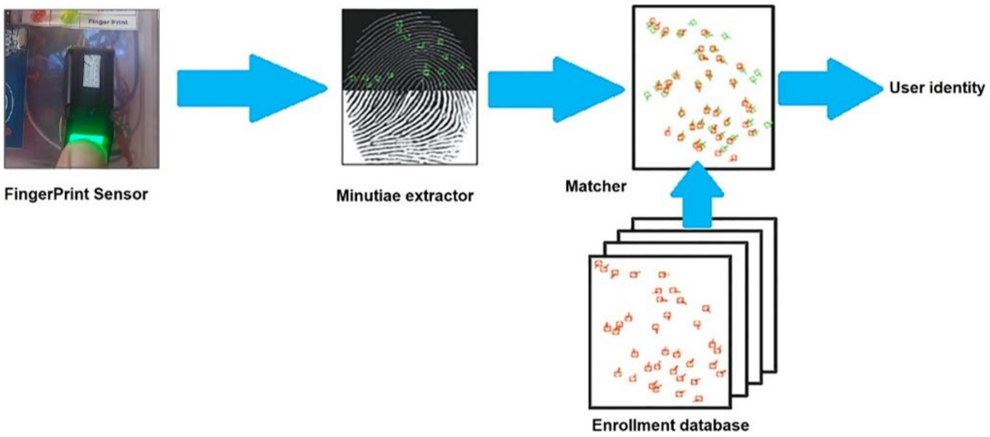
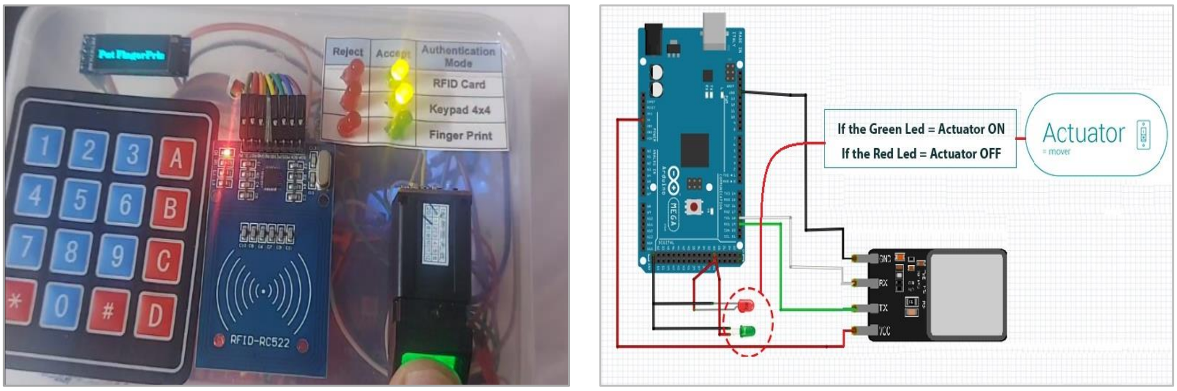


Figure 4. Compare fingerprint image with images stored

2.5. Implementation of proposal system

The payment system is a prototype designed using IoT devices, as shown in the following Figure 5(a). This model consists of three stages to verify the identity of the buyer, the first stage using the card, the second stage by using the keyboard, and the third stage using the fingerprint, which is the most critical stage in this model. In Figure 5(b) detail about the linking mechanism below, the process of linking the fingerprint device with the arduino mega device in Table 1. Where it contains PINs for the transmitter and receiver. After passing through the three steps, payment can be complete, but these steps can be reduced according to the place and circumstance without any complications.



(a) (b)

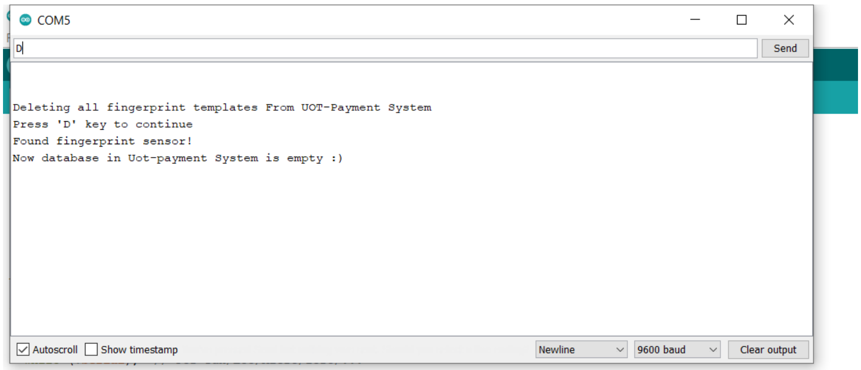
Figure 5. The proposal system: (a) structure of the proposal system and (b) diagram of fingerprint connection

Table 1. The conection of arduino mega PINs with fingerprint sensor PINs

Arduino mega PINs	Fingerprint sensor PINs
D18	Serial data (SDA)
D19	Serial clock (SCK)
GND	Ground (GND)
3V/3V3	Voltage common collector (VCC)
D30	Success authentication
D31	Fail authentication

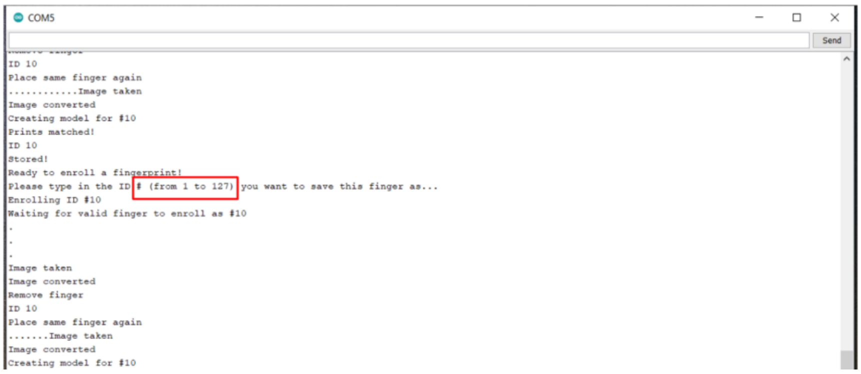
2.5.1. Program the software of the fingerprint device

The most important part is programming the electronic fingerprint using the arduino integrated development environment (IDE) through three steps. The first step is to clean the old fingerprint stored using the C software commands, as Figure 6. The second step is to add a new fingerprint to the device. The device has the ability to add 127 fingerprints. Each fingerprint is associated with a unique number that can be programmed, as Figure 7. The last step is to verify the extent of fingerprint matching and credibility by comparing the database stored in the device. Thus, the leading payment stage is completed, as Figure 8.



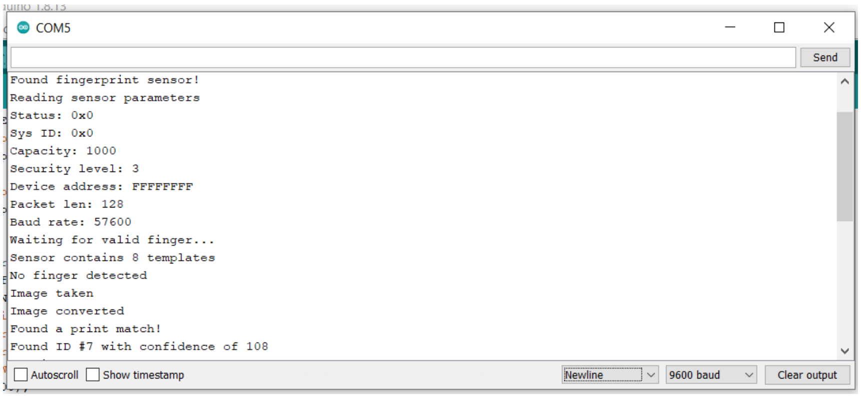
```
Deleting all fingerprint templates From UOT-Payment System
Press 'D' key to continue
Found fingerprint sensor!
Now database in Uot-payment System is empty :)
```

Figure 6. Delete fingerprint stored in the device



```
ID 10
Place same finger again
............Image taken
Image converted
Creating model for #10
Prints matched!
ID 10
Stored!
Ready to enroll a fingerprint!
Please type in the ID # (from 1 to 127) you want to save this finger as...
Enrolling ID #10
Waiting for valid finger to enroll as #10
.
.
.
Image taken
Image converted
Remove finger
ID 10
Place same finger again
.......Image taken
Image converted
Creating model for #10
```

Figure 7. Enrol fingerprint in the device



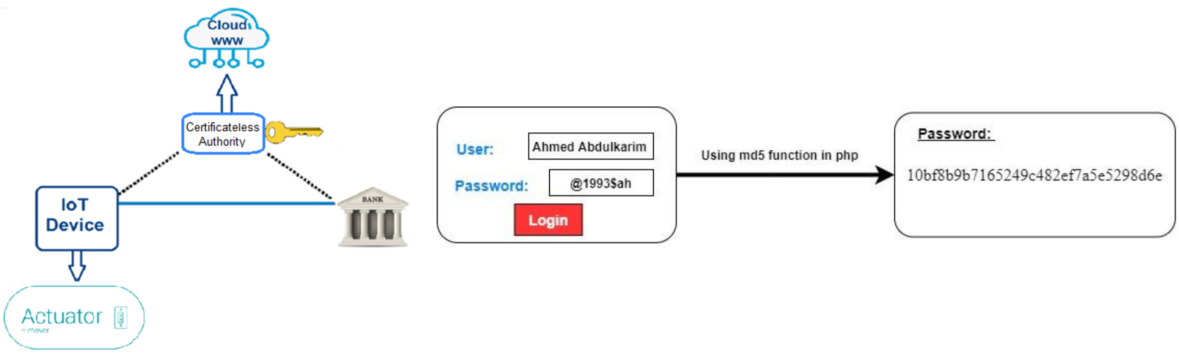
```
Found fingerprint sensor!
Reading sensor parameters
Status: 0x0
Sys ID: 0x0
Capacity: 1000
Security level: 3
Device address: FFFFFFFF
Packet len: 128
Baud rate: 57600
Waiting for valid finger...
Sensor contains 8 templates
No finger detected
Image taken
Image converted
Found a print match!
Found ID #7 with confidence of 108
```

☐ Autoscroll ☐ Show timestamp Newline 9600 baud

Figure 8. Fingerprint authentication

2.5.2. Authentication in the UOT-payment system

The sensitive information is must be kept secret from any intruders in any online payment transaction; therefore, necessary to develop a method and system to solve these issues. UOT-payment system provides the best method for user verification through three levels of authentication by using IoT devices and sending the data through a secure socket layer (SSL) [29]. Figure 9(a) represents an UOT-payment model based on the IoT framework [30]. The system's foundation layer connects it to other service providers. The IoT allows data to be accessed via secure and adaptable hardware resources. The platform layer is responsible for managing storage, parallel processing, and data mining, whereas the application layer is in charge of commercial e-commerce software [31]. In addition to encrypting clients' passwords in the database by using a hash function in PHP language for data security in the system [28], it can be explained in Figure 9(b).



User: Ahmed Abdulkarim

Password: @1993$ah

Password:

10bf8b9b7165249c482ef7a5e5298d6e

(a)

(b)

Figure 9. Authentication in the proposed system: (a) UOT-payment secure payment mode and (b) UOT-payment use the hash function

3. RESULTS AND DISCUSSION

When the client uses the UOT-payment system and needs to purchase some items on an e-commerce website, pay for bills of electricity or water, get services like IoT device operation, can use a unique smart card to confirm his identity, but this is not enough to complete the purchase, after checking the identity of the client in the database necessary to authentication by using PIN password to complete the process but the user may forget this password, therefore the biometric like a fingerprint is essential for any payment system in IoT techniques the condition check is matched 65% – 75% in the database, these procedures can be illustrated in the flowchart in Figure 10. A merchant or service provider can modify the system because it is flexible and has been designed to go through three steps of protection to obtain protection and be sure of reliability, or it passes through one step to obtain ease of use, that depending on the place in which it is used in Table 2. It can be illustrates that by using the table of LEDs. If the stage is passed, the green led will open and the red led means to fail to pass some step. The verification is formally stated as: can represent the appropriateness by sign (Ap) and represent the authentication by sign (Au) in Figure 11 can explain classify the system into four types represent by sign (S_1, S_2, S_3, S_4, S_5):

- S_1: if Ap > 75% and Au > 75% by using biometrics (fingerprint).
- S_2: if Ap > 50% and Au < 50% by using RFID card only.
- S_3: if Ap < 50% and Au > 50% by using RFID card + PIN password.
- S_4: if Ap < 50% and Au > 75% by using RFID card + PIN password + fingerprint.
- S_5: if Ap < 25% and Au < 25% mean failed system.

A comparison between four levels of an aspect can be done according to security type and system level. Assume the sign (S_L) denotes system level, sign (S_T) denotes security type. In Figure 12(a), the first system-level can represent by using an RFID card only; this level can provide less level of security, high risk of fraud, and lack of user confidence. In Figure 12(b), the second system level using RFID card and PIN passwords can increase the level of security, decrease the risk of fraud, and increase user confidence, in Figure 12(c), the third system level by using an RFID card, PIN password, and biometric provides more level of security and very high user confidence, but it is not suitable to use therefore can, using biometrics only is sufficient to achieve security system requirements, can represent in Figure 12(d).

Table 2. Authentication mode of UOT-payment system

Reject	Accept	Authentication mode
0	1	RFID card
0	1	Keypad 4×4
0	1	Fingerprint

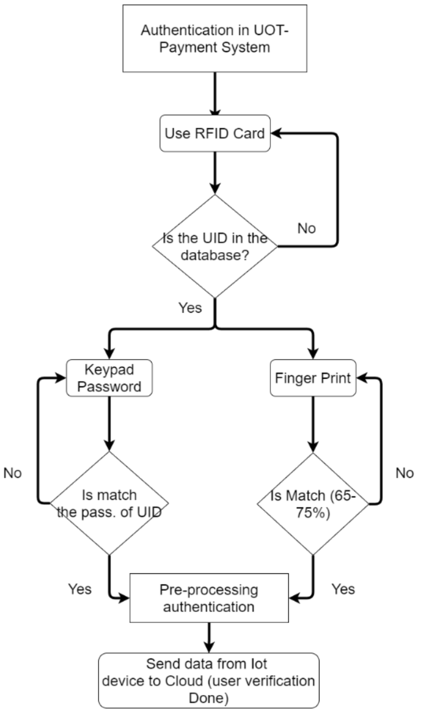

Authentication in UOT-Payment System
Use RFID Card
Is the UID in the database?
No
Yes
Keypad Password
Finger Print
No
Is match the pass. of UID
Is Match (65-75%)
No
Yes
Pre-processing authentication
Yes
Send data from Iot device to Cloud (user verification Done)

Figure 10. Flowchart of authentication in UOT-payment system

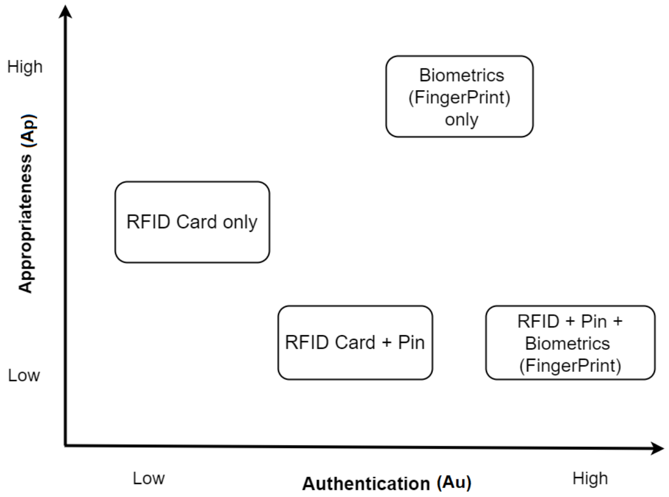
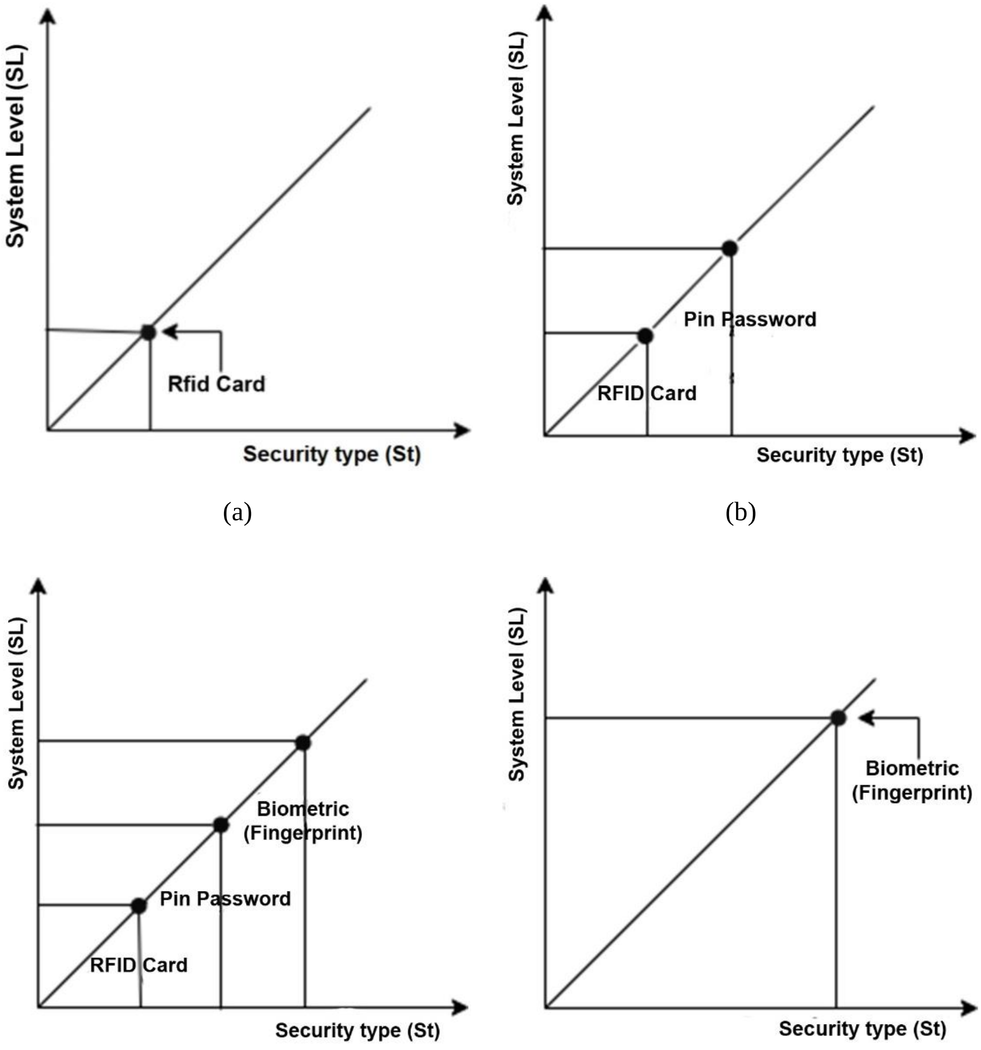


Figure 11. Research model of UOT-payment



(a)

(b)

(c)

(d)

Figure 12. Security types and levels of UOT-payment: (a) first system-level of RFID card; (b) second system-level of RFID and PIN password; (c) third system-level of RFID, PIN, and biometric; and (d) forth first system-level of fingerprint biometric

4. CONCLUSION

Many factors and features favor the use of fingerprints in online electronic payments today, integrating protection and efficiency biometrics, which offer defense against fraudulent activities occurring in the context of online payments. Biometrics make it difficult, even if a fraudster manages to get their hands on the cardholder’s PIN or password. Provide excellent user experience, biometrics are better than traditional authentication techniques utilizing PINs and passwords with capital letters and special characters. Biometrics are non-transferable, which means that in order for authentication to be successful, the rightful cardholder must be present. Difficult to impersonate, biometric identification relies on physical characteristics that are impossible to fabricate and are unique by definition, meaning that no other individual has that identical attribute. Moreover, the future of electronic payment systems depends on flexibility while reducing complexity by customizing security levels according to the service provider and the organization’s work environment.

REFERENCES

[1] L. Kovács and S. David, “Fraud risk in electronic payment transactions,” *Journal of Money Laundering Control*, vol. 19, no. 2, pp. 148–157, 2016, doi: 10.1108/JMLC-09-2015-0039.

[2] M. A. Ali, N. Hussin, and I. A. Abed, “Electronic payment systems: architecture, elements, challenges and security concepts: An overview,” *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 11, pp. 4826–4838, 2019, doi: 10.1166/jctn.2019.8395.

[3] T. A. Al-Maaitah, A. Osman, M. Suberi, D. Al-Maitah, and F. Al-Dhmour, “review study on the security of electronic payment systems,” *International Journal of Economics, Commerce and Management*, vol. 3, no. 9, pp. 821–829, 2015, doi: 10.13140/RG.2.2.11231.48808.

[4] C. Asiminidis, G. Kokkonis, and S. Kontogiannis, “Database systems performance evaluation for IoT applications,” *International Journal of Database Management Systems (IJDMS)*, vol. 10, no. 6, 2018, doi: 10.2139/ssrn.3360886.

[5] R. Lionnie, E. Agustina, W. Sediono, and M. Alaydrus, “Biometric identification using augmented database,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 1, pp. 103-109, 2019, doi: 10.12928/telkomnika.v17i1.11713.

[6] P. Aigbe and J. Akpojaro, “Analysis of security issues in electronic payment systems,” *International Journal of Computer Applications*, vol. 108, no. 10, pp. 10–14, 2014, doi: 10.5120/18946-9993.

[7] A. Al Farawn, H. D. Rjeib, N. S. Ali, and B. Al-Sadawi, “Secured e-payment system based on automated authentication data and iterated salted hash algorithm,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 1, pp. 538-544, 2020, doi: 10.12928/telkomnika.v18i1.15623.

[8] F. Khanboubi, A. Boulmakoul, and M. Tabaa, “Impact of digital trends using IoT on banking processes,” *Procedia Computer Science*, vol. 151, pp. 77–84, 2019, doi: 10.1016/j.procs.2019.04.014.

[9] N. Ya’acob *et al.*, “A cashless payment transaction (CPaT) using RFID technology,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 1, pp. 191-199, 2019, doi: 10.11591/ijeecs.v16.i1.pp191-199.

[10] M. S. Croock and R. A. Taaban, “Software engineering based secured E-payment system,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4413-4422, 2021, doi: 10.11591/ijece.v11i5.pp4413-4422.

[11] P. Basak, S. De, M. Agarwal, A. Malhotra, M. Vatsa, and R. Singh, “Multimodal biometric recognition for toddlers and pre-school children,” in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 627–633, doi: 10.1109/BTAS.2017.8272750.

[12] Malathi R. and J. R. Raj R., “An integrated approach of physical biometric authentication system,” *Procedia Computer Science*, vol. 85, pp. 820–826, 2016, doi: 10.1016/j.procs.2016.05.271.

[13] G. W. Quinn, P. Grother, and J. Matey, “NISTIR 8207 IREX IX Part One Performance of Iris Recognition Algorithms,” US Department of Commerce, National Institute of Standards and Technology, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8207.pdf

[14] K. Alsing, “The outlook for biometrics security,” 2017. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/the-outlook-for-biometrics-security (accessed Sep. 23, 2021).

[15] D. M. L. Storisteanu, T. L. Norman, A. Grigore, and T. L. Norman, “Biometric fingerprint system to enable rapid and accurate identification of beneficiaries,” *Global Health: Science and Practice*, vol. 3, no. 1, pp. 135–137, 2015, doi: 10.9745/GHSP-D-15-00010.

[16] J. Ashbourn, *Practical Biometrics From Aspiration to Implementation*. London: Springer London, 2015. doi: 10.1007/978-1-4471-6717-4.

[17] N. Topaloglu, “Revised: finger print classification based on gray-level fuzzy clustering co-occurrence matrix,” *Energy Education Science and Technology Part A: Energy Science and Research*, vol. 31, no. 3, pp. 1307–1316, 2013. [Online]. Available: https://www.researchgate.net/profile/Nurettin-Topaloglu/publication/289246081_Revised_Fingerprint_classification_based_on_gray-level_fuzzy_clustering_co-occurrence_matrix/links/5a747437458515512079fd1e/Revised-Fingerprint-classification-based-on-gray-level-fuzzy-clustering-co-occurrence-matrix.pdf

[18] A. Gelb, A. Mukherjee, and K. Navis, “Digital governance in developing countries: beneficiary experience and perceptions of system reform in Rajasthan, India,” *Center for Global Development Working Paper No. 489*, 2018, doi: 10.2139/ssrn.3310458.

[19] C. Busch, “Standards for biometric presentation attack detection,” Springer, Cham, 2019, pp. 503–514, doi: 10.1007/978-3-319-92627-8_22.

[20] S. Supatmi and I. D. Sumitra, “Fingerprint identification using bozorth and boyer-moore algorithm,” *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 662, no. 2, doi: 10.1088/1757-899X/662/2/022040.

[21] S. A. Daramola and C. Wankwo, “Algorithm for fingerprint verification system,” J*ournal of Emerging Trends in Engineering and Applied Sciences*, vol. 2, no. 2, pp. 355–359, 2011. [Online]. Available: https://journals.co.za/doi/epdf/10.10520/EJC138526

[22] M. B. Patel, S. M. Parikh, and A. R. Patel, “An Improved approach in fingerprint recognition algorithm,” in *Smart Computational Strategies: Theoretical and Practical Aspects*, Singapore: Springer Singapore, 2019, pp. 135–151, doi: 10.1007/978-981-13-6295-8_12.

[23] D. Peralta, S. García, J. M. Benitez, and F. Herrera, “Minutiae-based fingerprint matching decomposition: Methodology for big data frameworks,” *Information Sciences*, vol. 408, pp. 198–212, 2017, doi: 10.1016/j.ins.2017.05.001.

[24] V. Espinosa-Duró, “Minutiae detection algorithm for fingerprint recognition,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 17, no. 3, pp. 7–10, 2002, doi: 10.1109/62.990347.

[25] R. B. -Gonzalo, C. Lunerti, R. S. -Reillo, and R. M. Guest, "Biometrics: Accessibility challenge or opportunity?," *PLOS ONE*, vol. 13, no. 4, 2018, doi: 10.1371/journal.pone.0194111.

[26] Y. Koda, T. Higuchi, and A. K. Jain, "Advances in capturing child fingerprints: A high resolution CMOS image sensor with SLDR method," in *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2016, pp. 1–4, doi: 10.1109/BIOSIG.2016.7736909.

[27] N. Agnihotri, "How to enroll and match fingerprint templates with Adafruit and R30X fingerprint scanner," 2021. https://www.engineersgarage.com/arduino-adafruit-r30x-r307-fingerprint-scanner/ (accessed Sep. 20, 2021).

[28] Y. Mittal, A. Varshney, P. Aggarwal, K. Matani and V. K. Mittal, "Fingerprint biometric based Access Control and Classroom Attendance Management System," *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1-6, doi: 10.1109/INDICON.2015.7443699.

[29] D. D. Khudhur and M. S. Croock, "Developed security and privacy algorithms for cyber physical system," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5379-5389, 2021, doi: 10.11591/ijece.v11i6.pp5379-5389.

[30] E. J. Hogan and C. M. Campbell, "Method and system for secure payments over a computer network," *U.S. Patent No. 9,672,515*, 2017. [Online]. Available: https://patentimages.storage.googleapis.com/3a/27/16/86781587b42a5c/US9672515.pdf

[31] M. F. Ali, N. Z. Abu, and N. Harum, "A novel session payment system via internet of things (IOT)," *International Journal of Applied Engineering Research*, vol. 12, no. 23, pp. 13444–13450, 2017. [Online]. Available: http://www.ripublication.com/ijaer17/ijaerv12n23_59.pdf

BIOGRAPHIES OF AUTHORS

Ahmed Abdulkarim Talib is an M.Sc. student in Computer Engineering at University of Technology, Baghdad, Iraq. he received the B. Sc, from University of Technology in 2016. His research field includes Computer Engineering, IoT, microcontroller boards, data science, Database of program language, Windows applications and Web applications. He can be contacted at email: ce.19.02@grad.uotechnology.edu.iq.

Ayman Dawood Salman received the B.Sc. degree in Electrical and Electronic Eng. From the University of Technology-Baghdad in 1998 and got his M.Sc. in Computer and Information Technology/Software Engineering from the University Technology-Baghdad also in 2004. Then he graduated with a doctor Eng. degree in the Communication Networks Group, Institute of Information Technology, Technical University of Ilmenau, Germany. Primary research focuses on MANETs, emphasising QoS routing and multimedia communication, IoT, WSN, and SDN. Currently, he works as an Assist Professor at the university of technology – department of computer engineering. He can be contacted at email: aymen.d.salman@uotechnology.edu.iq.