American Journal of Engineering and Applied Sciences

Original Research Paper

AI Based Mobile Bill Payment System using Biometric Fingerprint

[1]Ayyaswamy Kathirvel, [2]D. Sudha, [3]S. Naveneethan, [4]M. Subramaniam, [5]Debashreet Das and [6]Stewart Kirubakaran

[1,6,5]Department of CSE, Karunya Institute of Technology and Sciences, Coimbatore, India
[4]Department of IT, Sree Vidyanikethan Engineering College, Tirupati, India
[3]Department of CSE, SRM Institute of Science and Technology, Chennai, India
[2]Department of CS, Mother Teresa Women's University, Kodaikanal, India

Article history
Received: 20-09-2021
Revised: 26-10-2021
Accepted: 06-11-2021

Corresponding Author:
Ayyaswamy Kathirvel
Department of CSE, Karunya Institute of Technology and Sciences, Coimbatore, India
Email: kathirvel@karunya.edu

Abstract: Billions of payment transactions occur in our day-to-day life, but every payment method depends on a material to carry. It is common for users to possess various materials like cash, credit cards and even mobiles to make payment. Meanwhile, it is easy for these materials to be robbed or lost. These instances result in a terrible trauma for the people. This study gives a detailed portrayal of a biometric payment application developed to introduce a concept of material-less payment. It enables the user to make a payment at any location by enrolling their fingertip without possessing any material. It involves a one-time registration of the User details upon all further transactions are validated and processed based on the user's fingerprint where the App takes care of the whole process. This implementation results in a novel payment method and avoids the risk of carrying valuable materials outdoors. This App creates an efficient and safe payment for society.

Keywords: Biometric Payment, Fingerprint, Cash-Less Transaction and Android

Introduction

Payment transactions have been a part of our life from the early 16th century. It evolved right from the Barter system, where products interchanged in return to goods or services to the current form of transactions using cash, credit/debit cards, e-wallets and so on. Barter system was practised for a certain period until realised that it was not accurate due to the differences in the value estimation of the exchanged goods or services.

Later, a more standard transaction came into existence using coins made of valuable materials such as gold and silver. This method was convenient as it had a standardised value for every goods or service and was adopted by almost every King or ruler globally. With the formation of Governments and growth in civilisation, currency bills and coins introduced. Till date, currency bills are in practice. Many financial organisations such as bank have introduced various paper and card-based payment transactions to the society. With the advancement in technology and digitisation the use of the internet, e-commerce, e-payment, mobile banking and payment become popular. The similarity in all these transactions is that they depend on a material to complete the payment.

Users need to carry cash or credit/debit cards or e-wallets in the form of mobiles to identify their payment account. Then the transaction needs to be validated using OTP, PIN or passwords to prove its authenticity. After verification completes from the server-side, the transaction is complete and the amount gets deducted from the payer. This process needs to repeat involving the bank and the payment gateway to credit amount back to the payee. Also, people carrying valuables such as wallet worry about safeguarding them and be conscious not to misplace them. With the advancement in technology, this process could be simplified and yet be more secured.

The chapter introduces a novel method of material-less payment which makes the process of payment hassle-free. The customers are entitled not to carry any form of cash, debit/credit cards or mobile to make the payment. It allows the users to refrain from worrying about possessing and protecting their valuables while going out for shopping.

A secure system involving fingerprint developed in this project identifies every individual user uniquely. Fingerprint cannot be the same for more than one being it helps to identify the person (Yankov *et al*., 2019) and acts as a security gateway for the system. It involves minutiae extraction and minutiae comparison algorithms in the backend for analysing the fingerprints as discussed in the algorithm section of this study.

The user needs to complete a one-time registration after which the application lets the user enrol their fingerprint to initiate the transaction and pay to any vendor. A brief description of a few other payment methods in comparison to the proposed system will be in the literature review segment of this study.

Detailed Literature Review

The need for goods has been a part of our lives for several centuries. In a civilization, people demanded something in exchange for goods. It was called the Barter's system where goods exchanged in return for other goods. Eventually, it was not in favour of the value and quantity of goods differed from each other. It led to the emergence of currency. A decade ago, currency bills, cheque, demand draft and a few other paper-based transactions were widely used payment methods by society. Currency bills were one of the most convenient payment methods due to its simplicity. But in case of a higher amount, a large amount of cash had to be transported and was not comfortable.

Cash transactions lead to a lesser contribution to the GDP due to its difficulty to account (Hanzal and Homan, 2019). Cheques and demand drafts solve the higher volume of currency problem but turned out to be a much slower process which could take up to three working days.

Current Scenario

In today's scenario, the improvement in technology has led to various efficient methods of payment proposed. The introduction of payment cards as debit/credit cards was a breakthrough. Almost every bank in all countries adopted this mechanism. It allows the user to swipe it in a card reader machine, debits the amount from the user's account (Sajić *et al*., 2018). It comprises a magnetic strip which stores all the account information when swiped it prompts the user for a secure PIN which in turn authenticates the transaction. An improvement in payment introduced with the help of geo-location. It involves tracking the user's location using their smartphones and monitoring the user's regular geo-locations. So, when the user attempts to make a payment at a familiar place, the system avoids the PIN verification and prompts to enter one only at unusual or new places (Zolotukhin *et al*., 2018). This method may save time and make payment simpler for the user, but it is prone to be misused by an unauthorized person. If the smartphone is lost or stolen, any person could act as an imposter and make the payment.

Disadvantages of Current Payment Methods

The disadvantage of payment cards is the payee should have a card reader machine to debit the amount. It is difficult for small scale vendors to afford these machines as these require the vendors to pay an annual fee to the bank. Also, payment through cards has a minimum and a maximum limit. Moreover, carrying these cards might be very handy due to its sleek design contrarily it is prone to be lost.

Mobile Banking

Mobile banking has become handy for users with the use of smartphones. Payment through smartphones is convenient for people, contrarily the technique used weighs in here (Sun and Havidz, 2019). There are many applications provided by banks to transfer funds, but the payer needs the account details of the payee to be added as a beneficiary to complete the transaction. Although the transaction completed online, adding the payee details take more time in many circumstances (Tounekti *et al*., 2019). It is not a preferred option to fill in payee account details while making a payment at the location. Also, constant internet connection is required to make these transactions.

E-Wallets

Many private companies have successfully established e-wallets in which users can load money and pay using QR codes. It is a time-efficient method to complete a transaction as the user has to scan the QR code (Liu *et al*., 2020) with their smartphone. The users always need to have money preloaded in these applications these require a constant internet connection as all the transactions are online. It also includes that the user must agree to the conditions and trust these third-party applications with their money (Islamiati *et al*., 2019).

NFC Chips

An advanced method broadly used for payments in developed countries is Near Field Communication (NFC). Most smartphones sold in developed countries are built-in with NFC chips. It makes payment transaction simple as the users need to tap their device against another device to complete the transactions. It is highly time-efficient and has no intermediate steps for the user to perform (Al-Haj and Tameemi, 2018). A management authentication server communicates with the device and the application server using an adaptive protocol to complete the transaction. It may not be successful in developing countries as the smartphones available here are not equipped with NFC chips. Also, this technique does not include any level of authentication. So, it may not be the safest method to use.

Face Recognition

Even the use of face recognition put forward. This technique implemented as a payment method allows users to pay by scanning their face at the camera installed in the billing counter (Zhang and Kang, 2019). The problem is the registration as it requires a minimum of thousand images of input for a single person to be identified accurately. The database and server for processing and storing these data would be expensive not be practically

possible. Also, the system fails to differentiate identical twins. Iris recognition, the results are accurate, but the hardware required recognizing iris is expensive (Caron, 2018) and installing it in every shop would not be financially a good idea for most shops.

Biometrics Methods

Biometrics is efficient and generates accurate results, but the cost of implementation is a drawback. Thus, a cost-effective biometric system such as fingerprint proposed in the payment technology.

QR Code Methods

An innovative method of payment involving both QR code and face recognition discussed. It uses QR to identify the user and the account details and uses face recognition as an authentication mechanism (Ximenes *et al*., 2019). It is highly secure as it adds up the advantages of both the methods contrarily the drawbacks also sum up. No methods proposed in the paper to neither overcome the extensive use of a server to process the facial data nor to avoid constant internet connection for QR code to function. It also increases the overall process time.

IOT Methods

A separate device built using IoT components. A combination of the fingerprint sensor, a WIFI module, a keypad and an LCD connected to a raspberry pi which acts as a processor (Hualin *et al*., 2018). It is a stand-alone device which is portable and can be in any billing counter at a shop. The main drawback is that the IoT devices have not delivered notable result in the fingerprint matching. Proper training to be provided to employees to use the device. Failure of even a single component would lead to hindrance of the whole system. This device requires to be paired up via WIFI with a computer or mobile to send the collected data in dependence on the host and transfer of data through WIFI is prone to network and safety issues.

Finger Print Method

The use of fingerprint inspired many inventors to improvise the idea. A paper discussed the implementation of the fingerprint sensor on an existing contactless debit credit card. It aids the user to register a fingerprint in their card itself. Use it to make payments without entering the PIN. It ensures only the account owner can make the payment and the process self-authenticates as the user holds the card with the right finger on the sensor (Suwald and Rottschäfer, 2019). Challenge faced in this method is that the sensor needs to have a power supply to function properly. The card requires power to function as expected. It ultimately leads to opting for an adaptor for it at extra expenses. It also has the usual disadvantages of using a card which was discussed earlier in this study.

E-Cash Transaction

An intriguing and unusual proposal for payments using offline E-cash transfer put forth. Emphasis on using virtual cash instead of real hard cash with the help of blockchain technology. The idea involves payment tasks such as withdrawal, transfer and so on but with E-cash (Luo and Ming-Hour, 2018). It requires the user to register with their preferred bank and get a card and a mobile application for e-cash processes. It mentions that the transaction authenticated using the payer's signature on the smartphone itself. However, it only was conceptually discussed and working model not included.

Merits and Demerits of Biometric

Considering both advantages and disadvantages of all the above-discussed techniques, a biometric payment application using fingerprint is developed which composes of potential upsides and minimal drawbacks.

Bill Payment System Using Biometric Fingerprint

In this section, a novel approach to the payment transaction introduced. The concept of material-less payment with the use of fingerprint developed as an application for smartphones. The practice of carrying wallets and securing them is no longer needed as the users are encouraged to complete the transaction by just using their fingertip. This process requires a one-time registration where the users fill in their details with their fingerprint and a secured PIN for security. For data privacy reasons, sensitive data such as the fingerprint gets converted into numerical values inserted in a byte array. All the information gets securely stored in the real-time cloud database, function seamlessly without a server. After this process, the user can enter any shop using this application and pay the bill amount using their fingerprint and PIN.

Architecture Description

The architecture involves two roles, the payer and the payee. The payer is the person who purchases in a shop and makes a payment. The payee is the shopkeeper or the shop owner who must receive the amount. This system, the payer is not required to carry any materials or wallet to make the payment. The shopkeeper has the application connected to a USB fingerprint scanner as depicted in Fig. 1. The payee logs in the application after which the amount payable gets entered. The customer gives his details to complete the payment.

The application directly opens into the make payment activity for convenience where an option to register is present. The application also has a registration activity where the application prompts the user for their details and linking of their preferred payment account. Figure 2 depicts the actions performed by the user on the

application. This registration is a one-time process where the details are securely stored in the real-time database after which the user can directly make the payment using their fingerprint and PIN. The application authenticates the data by contacting the database. After proper validation, the amount is debited from the customer and credited to the shopkeeper's account. The application directly communicates with the database without any middlemen such as payment gateway makes it an efficient architecture.

Minutiae Extraction and Comparison Algorithm

The working of the algorithm comprises of five steps namely fingerprint acquisition, fingerprint pre-processing, fingerprint enhancement, feature extraction and minutiae matching (Liban and Hilles, 2018).

Fingerprint Acquisition

It is the process where the application retrieves the fingerprint input from the user through the fingerprint scanner. The scanner captures an image of the fingerprint placed on its surface. The application communicates with the scanner using device drivers and retrieves the fingerprint image into the application for further processing.

Fingerprint Pre-Processing

In pre-processing, the acquired image gets converted to pure grayscale. i.e., black and white. It makes sure that the ridges, ridge endings, bifurcations, valleys and whorls made distinct as shown in Fig. 3 and 4.

Fingerprint Enhancement

At this stage, the image quality is enhanced to the maximum to better differentiate between minutiae and white space. The image undergoes a quality check to ensure that it is adequate for the extraction process. Binarization makes every black ridge in an image considered as 0 and the white space considered as 1. It helps to identify the features of the fingerprint in the extraction process.

Feature Extraction

The image gets fully rooted for the binary bits with the value 0 as features. Every feature gets determined by the value it holds in each pixel. These binary values and the pixel values are computed using (1) and stored in a byte array (Gudkov and Lepikhova, 2018).

This byte array represents the entire fingerprint:

$$CN = 1/2\sum_{i=1}^{8}\left[P - P_{i+1}\right] \quad (1)$$

where, CN is Cross Number, P_i is the binary pixel value in the neighbourhood of P with P_i = (0 or 1)

Minutiae Matching

Since the byte array represents the entire fingerprint, the byte arrays of the desired two fingerprints get compared. As fingerprint input is not constant and tends to change orientation every time even for the same finger, a matching score gets generated as shown in Fig. 5 and 6. This matching score gives information regarding the similarity of the fingerprints taken into consideration. It finds whether the fingerprints match or not. If the generated result is above 100, then the fingerprints are similar upon an agreed standard. It gets considered as a match. Any outcome below that value gets considered as not a match.

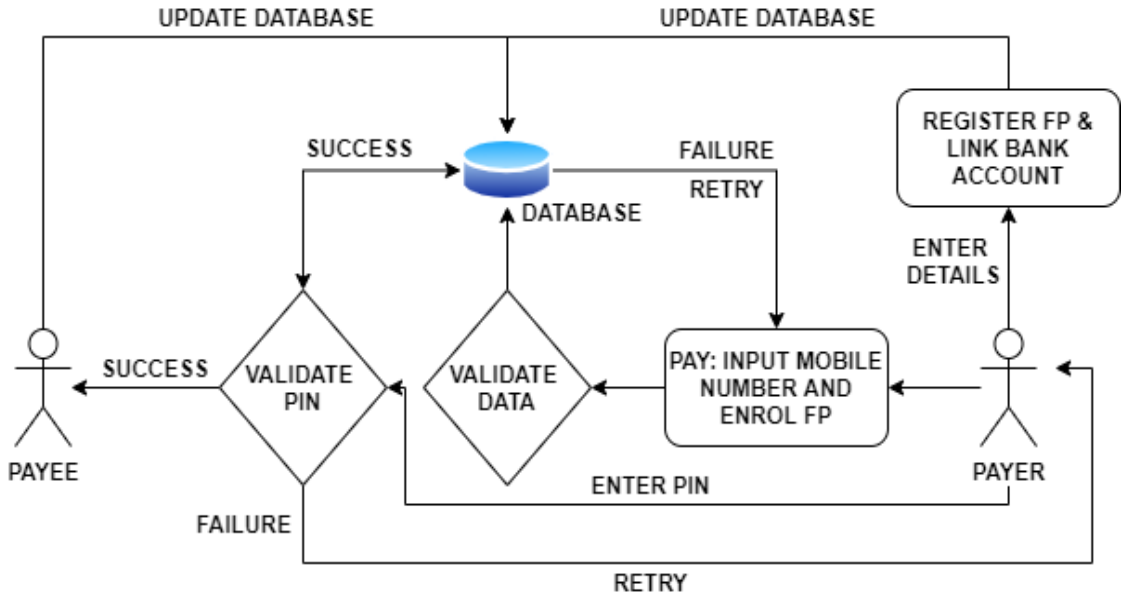

Fig. 1: The architecture of biometric payment application

Implementation

The application consists of two main activities, namely, biometric payment and user registration. When the user clicks the Register button, the registration activity opens. This module prompts the user to give input details for the registration process. The details such as name, mobile number or mail ID are collected.

The users require entering their bank account number and linking their preferred payment account with the application. Finally, for identification and security purposes, the user's fingerprint is collected. The user must press the capture fingerprint button and place their preferred fingertip on the external fingerprint scanner. It captures an image of the fingerprint for further process. The user also must enter a secure PIN for authentication of upcoming payments.

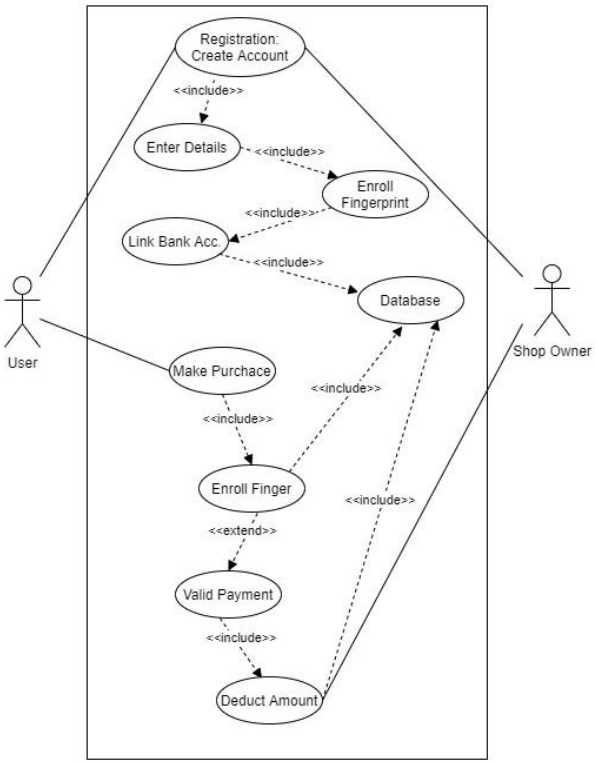

Fig. 2: Use case diagram of the biometric payment application

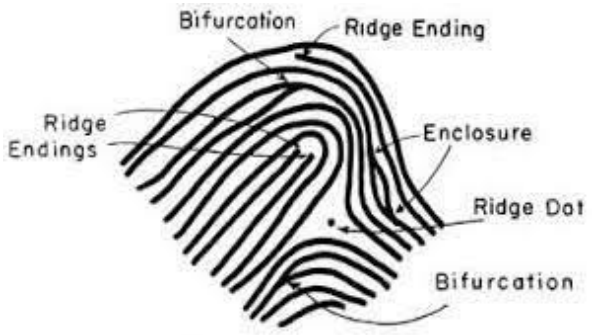

Fig. 3: Diagrammatic representation of fingerprint minutiae

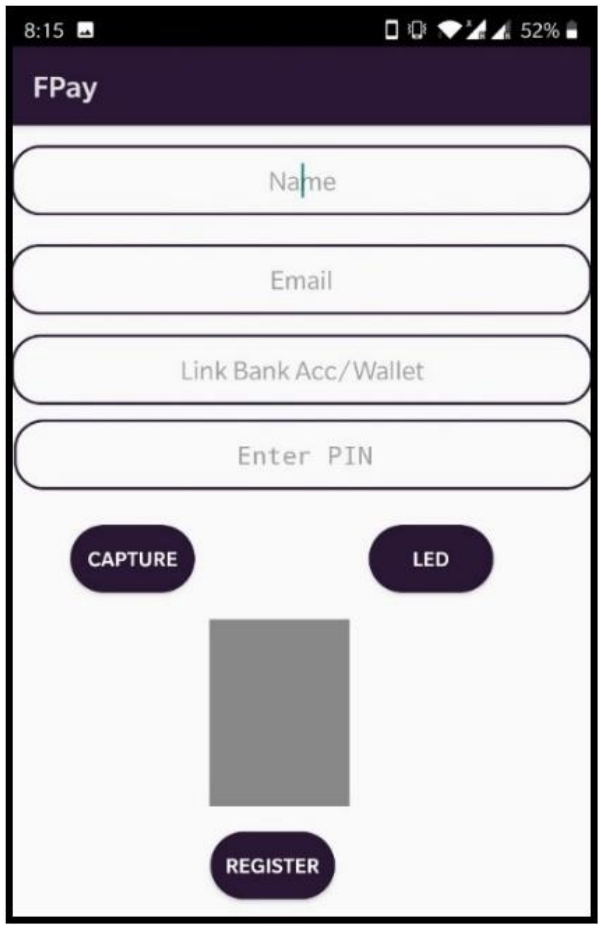

Fig. 4: Biometric payment registration activity

The fingerprint gets encoded to a byte array using the minutiae extraction algorithm. The PIN is also securely hashed. So, there is no storage of sensitive information. All these data are stored securely in a real-time cloud database. It is a one-time registration after this process the user can use this application at any location without further process. The user is notified with a success message instantly after sign-up. After registration, the users of this application are free to use this payment method wherever available.

The user need not carry any payment material to the shop as they can complete the shopping and scan their fingerprint, authenticate the payment and complete the transaction. The bill amount gets entered by the shopkeeper in the application. The user has to enter their mobile number, scan their fingerprint and enter the PIN to complete the transaction.

The process comprises three sub-processes, identification, validation and authentication. In the identification process, the user's mobile number is used as a primary key to select the details in the database. In the

validation process, the byte array containing the fingerprint is matched with the existing byte array in the database using the minutiae matching algorithm. When a successful match gets found, the application checks for sufficiency in the account balance. Once enough credit is available, the user receives a prompt with the PIN for authentication else informs the user that they do not have sufficient balance to continue with the payment.

Once the PIN matches, the application contacts the database (Fig. 7) and debits the specified amount. At the same time, the debited amount gets credited to the payee's account. Finally, a transaction success message gets displayed to the user. Fingerprints are unique for every person. It cannot get manipulated by anyone, adds security to this method.

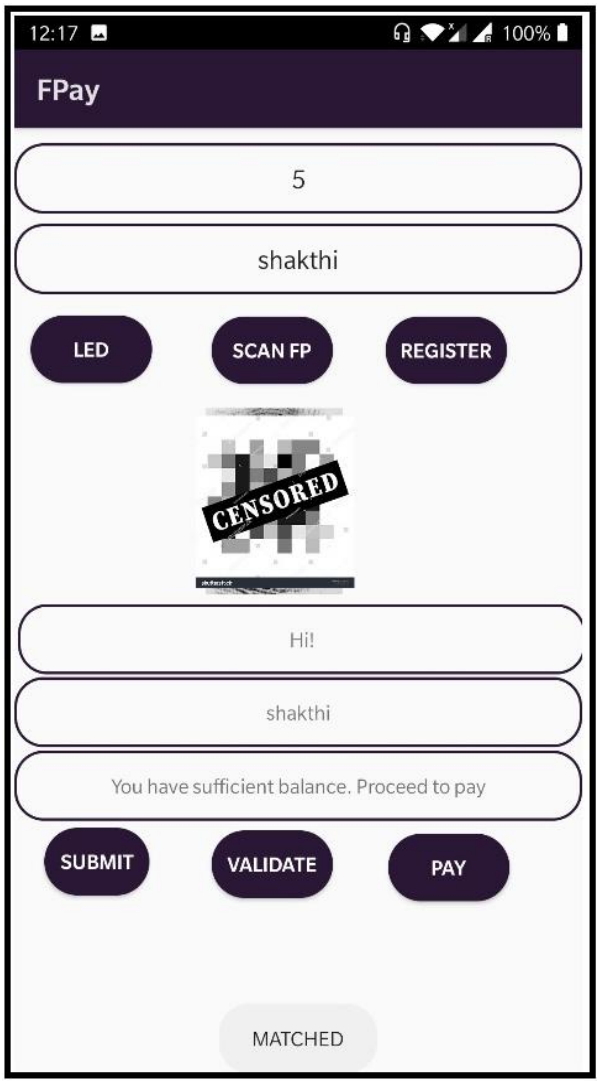

Fig. 5: Biometric payment activity

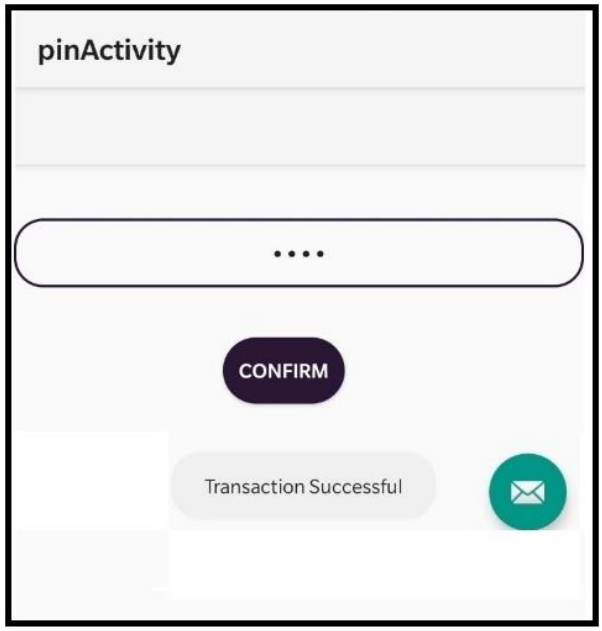

Fig. 6: Transaction success message

Experimental Results and Discussion

Thus, biometric payment application got designed, developed and implemented successfully. Also, a new technique of material-less payment got introduced to society. It reduces the pressure of people safeguarding their wallets everywhere. The application uses fingerprint and PIN for security which is simple and causes less confusion for the customers, unlike OTP and two-step authentications. The transaction gets completed with less number of inputs. It saves users from entering long account digits and speeds up the process.

The use of fingerprints makes it convenient to prevent unauthorised use as it is unique for every user. In terms of the minutiae matching algorithm accuracy, regression testing got 100% accurate results. In terms of the database, real-time database implementation makes data retrieval instant and does not require a server. It ensures zero server downtime.

The sensitive data such as fingerprints are converted into bytes and stored as a byte array. In terms of data security, the application is safe to use. No sensitive data gets lost. Finally, the payment transaction is done seamlessly and quickly without involving any middlemen such as payment gateways. Also, it is a good alternative instead of a card swiping machine which requires an annual subscription.

Conclusion and Future Scope

In conclusion, the biometric payment application paves a way to overcome material-based payment. The application combines all crucial upsides and eliminates most drawbacks discussed in the literature review.

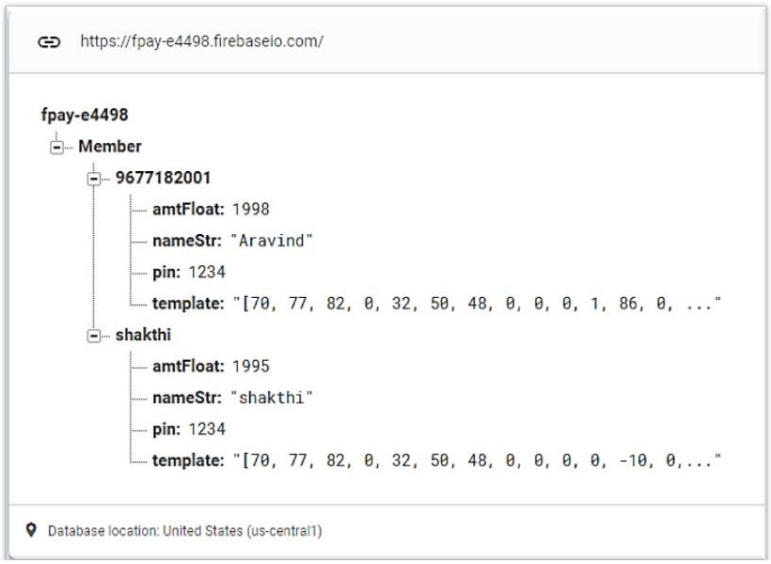

Fig. 7: Screenshot of cloud database schema

The application uses automation to solve the problem of the material dependency. Also provides various other advantages which got discussed in the result section of the paper. The application makes the users less worried about safeguarding their wallet or carrying the exact change to places. The overall user experience is made comfortable for both the payee and the payer. People adapt to this method without hassle as there are not many materials to be carried or processes to be done form the user's side.

In future sprints, a few new features will get released as updates. The application will get modified to register more than one fingerprint for every user. It ensures the user can use this system even if they have any problem with the previously registered fingerprint. A backup payment method will get added to cope up with any unexpected failure in the fingerprint sensor. Aadhar Enabled Payment System (AEPS) lets users make payment using their Aadhar card as it already got linked with their bank account. The proposed biometric payment application could collaborate with India Stack, the developers of Aadhar to make payment simple. It also makes the user skip the registration process as Aadhar card already has registered the user's fingerprint. It also enables an option to link a bank account or change an existing bank account associated with the biometric payment application entirely online. A few more basic features such as forgot PIN, a report bug feature and a feedback mechanism could get added as an update based on the requirements of the investor and convenience of the users.

Acknowledgement

The authors like to thank our HoD, NIOT Research Group and Management of Karunya Institute of Technology and Sciences provided wonderful environment of doing this research.

Author's Contributions

A. Kathirvel: Acquired, B.E.(CSE), M.E. (CSE) from University of Madras and Ph. D (CSE.) from Anna University. He has served in various positions at Deemed Universities, Autonomous Institution and Anna University affiliated colleges from 1998 to till date. He is currently working as Professor, Dept. of Computer Science and Engineering, Karunya Institute of Technology and Sciences at Coimbatore. He has worked as Lecturer, Senior Lecturer, Assistant Professor, Professor, and Professor & Head in various institutions. He is a studious researcher by himself, completed 18 sponsored research projects worth of Rs 103 lakhs and published more than 110 articles in journals and conferences. 4 research scholars have completed Ph. D and 3 under progress under his guidance. He is working as scientific and editorial board member of many journals. He has reviewed dozens of papers in many journals. He has author of 13 books. His research interests are protocol development for wireless ad hoc networks, security in ad hoc network, data communication and networks, mobile computing, wireless networks and Delay tolerant networks.

M. Subramaniam: (1974) is a Professor, in Department of Computer Science and Engineering, School of Computing, SRM Institute of Science and Technology *(Deemed to be University u/s 3 of UGC Act, 1956)* - Vadapalani Campus, Chennai- 600026, (INDIA).

He obtained his Bachelor's degree (B.E) in Computer Science and Engineering from University of Madras (1998), Master degree (M.E) in Software Engineering and Ph.D from College of Engineering Guindy (CEG), Anna University Main Campus, Chennai -25 in the year 2003 and 2013 respectively. His research focuses are Computer Networks, Software Engineering, AI & ML. He is an active life member of the Computer Society of India (CSI), the Indian Society for Technical Education (ISTE) and International Association of Engineers (IAENG). He has produced one doctorate and currently seven research scholars perusing Ph.D under his guidance. He has published many research papers in reputed journals. He is also reviewer in Springer- WPC, IEEE- International Journal of Communication Systems.

S. Navaneethan: Research Scholar, Department of CSE, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Chennai, Tamilnadu, India.

S. Stewart Kirubakaran: Have completed my Master's Degree from Kalasalingam University and I am currently pursuing my Ph.D. (Part-Time) at Anna University, Chennai. My Research Areas include Cloud Security, Network Security, Artificial Intelligence and Healthcare. I have 8.3 years of experience in teaching as Assistant Professor and 1.2 years of experience in the Industry as an SEO and PMO analyst. I have given my best during the NAAC, NBA and IET Accreditations. I have published 3 Indian Patents and 1 Australian Patent has been granted, 1 SCI publication, 6 Scopus Indexed publications, 5 non-Indexed publications, presented papers in various National and International Conferences. Also, I have attended more than 30 workshops, seminars and Hands-on Training in various disciplines. I am a lifetime member of IAENG and member of IET.

Debashreet Das: Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences at Coimbatore, Tamilnadu

D. Sudha: Department of CS, Mother Teresa Women's University, Kodaikanal, Tamilnadu, India.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Al-Haj, A., & Al-Tameemi, M. A. (2018, May). Providing security for NFC-based payment systems using a management authentication server. In 2018 4th International Conference on Information Management (ICIM) (pp. 184-187). IEEE. doi.org/ 10.1109/INFOMAN.2018.8392832

Caron, F. (2018). The evolving payments landscape: Technological innovation in payment systems. It Professional, 20(2), 53-61. doi.org/ 10.1109/MITP.2018.021921651

Gudkov, V., & Lepikhova, D. (2018, November). Fingerprint Model Based on Fingerprint Image Topology and Ridge Count Values. In 2018 Global Smart Industry Conference (GloSIC) (pp. 1-5). IEEE. doi.org/10.1109/GloSIC.2018.8570064

Hanzal, P., & Homan, J. (2019, June). Electronic Exchange SAF-T Standard of Data from Organizations to Tax Authorities or Auditors-Situation in the Czech Republic. In 2019 9th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 405-408). IEEE. doi.org/10.1109/ACITT.2019.8780001.

Hualin, Z., Qiqi, W., & Yujing, H. (2018, December). Design Fingerprint Attendance Machine Based on C51 Single-chip Microcomputer. In 2018 IEEE International Conference of Safety Produce Informatization (IICSPI) (pp. 536-539). IEEE. doi.org/10.1109/IICSPI.2018.8690368

Islamiati, D. S., Agata, D., & Besari, A. R. A. (2019, September). Design and Implementation of Various Payment System for Product Transaction in Mobile Application. In 2019 International Electronics Symposium (IES) (pp. 287-292). IEEE. doi.org/10.1109/ELECSYM.2019.8901643

Liban, A., & Hilles, S. M. (2018, July). Latent fingerprint enhancement based on directional total variation model with lost minutiae reconstruction. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-5). IEEE. doi.org/10.1109/ICSCEE.2018.8538417

Liu, W., Wang, X., & Peng, W. (2020). State of the art: Secure mobile payment. IEEE Access, 8, 13898-13914. doi.org/ 10.1109/ACCESS.2019.2963480

Luo, Jia-Ning and Ming-Hour, Y. (2018) "Offline transferable E-cash mechanism." In 2018 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1-2. IEEE, 2018. doi.org/ 10.1109/DESEC.2018.8625136

Sajić, M., Bundalo, D., Bundalo, Z., Stojanović, R., & Sajić, L. (2018, June). Design of digital modular bank safety deposit box using modern information and communication technologies. In 2018 7th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-6). IEEE. doi.org/10.1109/MECO.2018.8406014

Sun, Y., & Havidz, S. A. H. (2019, August). Factors Impacting the Intention to Use M-Payment. In 2019 International Conference on Information Management and Technology (ICIMTech) (Vol. 1, pp. 290-294). IEEE. doi.org/ 10.1109/ICIMTech.2019.8843758

Suwald, T., & Rottschäfer, T. (2019, November). Capacitive Fingerprint Sensor for Contactless Payment Cards. In 2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS) (pp. 241-245). IEEE. doi.org/10.1109/ICECS46596.2019.8964850

Tounekti, O., Ruiz-Martinez, A., & Gómez, A. F. S. (2019). Users supporting multiple (mobile) electronic payment systems in online purchases: An empirical study of their payment transaction preferences. IEEE Access, 8, 735-766. doi.org/ 10.1109/ACCESS.2019.2961785

Ximenes, A. M., Sukaridhoto, S., Sudarsono, A., Albaab, M. R. U., Basri, H., Yani, M. A. H., ... & Islam, E. (2019, September). Implementation QR Code Biometric Authentication for Online Payment. In 2019 International Electronics Symposium (IES) (pp. 676-682). IEEE. doi.org/10.1109/ELECSYM.2019.8901575

Yankov, M. P., Olsen, M. A., Stegmann, M. B., Christensen, S. S., & Forchhammer, S. (2019). Fingerprint entropy and identification capacity estimation based on pixel-level generative modelling. IEEE Transactions on Information Forensics and Security, 15, 56-65. doi.org/10.1109/TIFS.2019.2916406.

Zhang, W. K., & Kang, M. J. (2019). Factors affecting the use of facial-recognition payment: An example of Chinese consumers. Ieee Access, 7, 154360-154374. doi.org/10.1109/ACCESS.2019.2927705

Zolotukhin, O., & Kudryavtseva, M. (2018, October). Authentication Method in Contactless Payment Systems. In 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) (pp. 397-400). IEEE. doi.org/10.1109/INFOCOMMST.2018.8632065