International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-8, Issue-3 ,2021 Regular Edition E-ISSN: 2349-7084

A Novel Approach for Payment Systems in Accordance with Fingerprint Authentication

Piyush Suthar[1*], Neha Pandya[2]

[1*]*Information Technology Department, SPCE, Sankalchand Patel University, Visnagar, India*
[2] *Computer Engineering Department, GPERI, Gujarat Technological University, Mehsana, India*

e-mail: Piyush.s.suthar@gmail.com, neh.pandya@gmail.com,

**Corresponding Author: Piyush.s.suthar@gmail.com,*

Available online at: http://www.ijcert.org

Abstract: - Background/Objectives: Currently in the developing countries like India, the scenario of monetary transactions is rapidly moving towards cashless payments. Cashless payment modes include the vanishing debit card system, mobile wallets, UPI, and contactless cards.
Methods/Statistical analysis: To use above stated payment modes, either there is a need of mobile phone or a contactless card or both. So, to eliminate these limiting approaches it requires primarily two aspects one is fund security and the other is customer comfort.
Findings: So, to deal with both the aspects listed above a system can be implemented by incorporating proposed fingerprint payment system. The Finger print payment system is considered to have the safest and most secure operation in comparison with all other biometric authentication systems.
Improvements/Applications: The proposed system will greatly enhance customer comfort by providing easiness in any kind of payment by just a tap of a finger, further security aspects can be dealt with inclusion of several proposed protection measures.

Keywords: Authentication, Biometric, Fingerprint recognition, Payment, Transaction.

---

1. Introduction

Digital India movement gave boost to the electronic transactions. The number of users using cashless transactions in India is expected to amount to 697.8 million by 2023 [2]. Now a days we use electronic transactions while paying at grocery stores, petrol-pumps, medical stores, restaurants- the list will be very long. It is mandatory for people to carry cell phones and/or cashless cards for this kind of transactions. In recent transaction scenarios, banks are about to reduce the use of cashless cards considering fund security of users, also what if there is no need to carry wallet with us? The proposed solution can be considered to handle the scenarios depicted above.

Integration of digital technologies is eminent, nowadays biometrics are used in many sectors, in mobile phones for user authentication, in banks, in time and attendance monitoring system of any organization or in-home security system. Further considerable uses are border control, forensics, criminal identification, access control, Computer logins and e-commerce.

If we carefully assess the pattern of fingerprint, it is having different ridges and pores from person to person; no two persons can have the same pattern of ridges. Even if we consider twins, they may also have same pattern but fine details will differ undeniably.

Fingerprint sensors come in various shapes and sizes, but generally fall into two categories; area scan (or touch) sensor and swipe sensor. With a touch sensor, the user places and holds the finger on the sensor surface and impression transferred from the pad of the last joint of finger or thumb. Touch sensors are used mostly in fixed systems because of their size and shape [3]. These square-shaped

touch sensors are physically larger (in height and width) than swipe sensors and are used for example, in immigration access control applications. With a swipe sensor (a narrow row of sensors), the user slides a finger vertically over the surface. These sensors are preferably used in portable consumer electronics because of their size and shape [3, 4].

There are three main technologies available today for the capture of fingerprint images [5]:

1) Optical technology- this is the oldest and most popular form used for image capture. Essentially, a camera (located in the fingerprint recognition device) takes raw images of the fingerprint.

2) Silicon technology- a silicon chip is used, and the capacitive characteristics of the fingerprint are captured into images.

3) Ultrasound technology- Basically, an ultrasound image of the fingerprint is captured. This technology has proved to work better than the other two, because it can penetrate through different types of fingerprint dirt and residue.

One of the important reasons to consider the proposed solution is easiness of transaction by comforting user for the said transaction by the tap of a finger eliminating dependencies on mobile phones or cashless cards [1].

This paper evaluates specifically the need of updated system in accordance with the fingerprint authentication mainly. The performance of the existing system and its effects are being measured considering their accuracy. The research discovers the new adoption of fingerprint authentication that drastically improves the overall system efficiency. As we can see the transactions in the current era are now focusing on biometrics the proposed approach can yield good results.

Apart from the Section I that contains the introduction of payment systems having biometric authentication, remaining part of the paper is organized as follows, Section II contains the current technological scenario and the problem base, Section III contains the solution being proposed, Section IV contains the protections measures over the crucial issues in fingerprint authentication methodology, Section V concludes research work with future scope being highlighted.

2.Current Scenario and Problem Impact

Traditional passwords, PINs and ID cards have been used for personal identification [6][7] to secure the systems by restricting the access, but these can be easily breached. The passwords cannot be remembered and or Pin data gets damaged at any point of time [11], also ID can be pirated. Whereas the biometrics cannot be stolen, forgotten, borrowed or forged. Also, biometric features can be used with additional security [8]. Fingerprint is considered a biometric identifier that is dependent on biometric data for individuals [12].

American multinational technology company Apple Inc. in 2013, designed and developed a fingerprint feature called Touch ID and made available in its iPhone and iPad line-up. Another American multinational technology company Microsoft Corp. in 2016, made available "Windows Hello". Windows Hello is more personal way to sign in to Windows 10 devices with just a look (face) or a touch (fingerprint) which is enterprise-grade security without having to type in a password.

Deducing all, any mobile users are being comfortable with fingerprint identification for access as its simple and unique to each person. If we consider the key advantages of finger print authentication than the inclusions will be as follows:

1) Finger print authentication requires no user cooperation for recognition.

2) In finger print authentication the subject must have to be present at the time of authentication.

3) Performance in finger print authentication systems is reliable even in fraud or error nous identifications.

4) There is no need to remember the credentials to authenticate oneself.

5) No risk of losing the credentials.

6) Even by mistakenly no one can share the credentials.

3. Proposed Solution

By far the most contemporary biometric authentication technology is fingerprint authentication. Considering prominence of fingerprint authentication, using it for transactions provides complete sense as all above stated payment methods lacks in one or another crucial area of overall monetary transactions. Our proposed solution and its flow are described in the figure below which comprises of three main phases.

1) Linking/tie-up of bank with Payment Support Provider(PSP).

-- The banks which are willing to provide the service to user, should link themselves with the PSP.

-- Via PSP multiple banks can be incorporated for the provisioning of service to the customers having bank accounts in different or multiple banks.

2) Customer Registration with PSP

-- Customer who is willing to use the service should first register his/her fingerprint data and bank account details with the PSP.

-- While registering the customer, PSP will collect and authenticate the fingerprint with Aadhar [13] database and account with the bank. (Otp can be used for both cases).

-- If the authentication is successful than PSP will save the fingerprint with bank account number in its database.

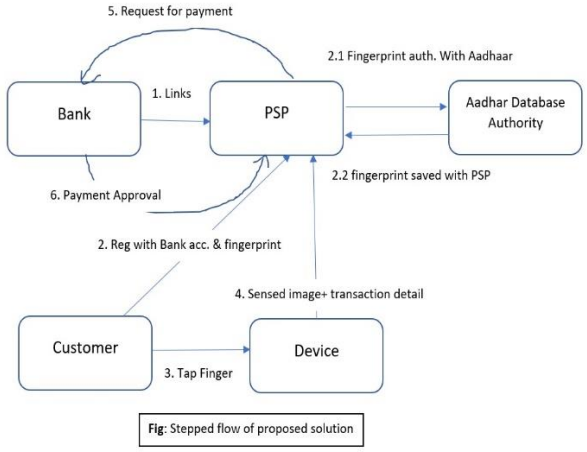

Fig: Stepped flow of proposed solution

3) Customer payment

-- Customer will tap the finger at merchant's device.

-- The device will transmit the sensed image+ payment details i.e. Transaction timestamp, amount, and geolocation to PSP.

-- According to the database, the PSP will request bank for the payment.

-- After the account is validated the bank will approve the payment.

4. Protection Measures

One of the major issues in using fingerprint lies in the authenticity in the sensed image of the finger. To deal with this issue we can consider fingerprint liveliness detection method. Fingerprint detection is prone to fake duplications made from cheap materials (i.e. artificial finger made of wax, sometimes Fingerprint can be recreated in lack using an object touched by that person) [9]. So that, it is crucial to identify the authenticity of the fingerprint by checking whether it is a real one or a fake before authorizing any transaction. Xia et al. [10] has provided weber-based solution that greatly enhances the chances to identify the liveliness of the fingerprint.

Also, another issue is finger print sometimes worn out or may be altered, to deal with this issue, user can be asked to reregister his/her finger print after intervals as and so required.

Sometimes fingerprint is also vulnerable to noise as well as distortions caused with dirt and twisting, further recognition of finger is problematic when user is having cuts, scars or missing finger. To address the stated both issues, user can register multiple fingers as and when required.

Further, to consider utmost safety to the users, payment transaction limit in the initial adoption of the proposed system can be restricted (i.e. up to several thousand rupees).

On top of above measures suggested, we have proposed transmitting geolocation along with transaction details, which is recorded by scanner device while sensing the fingerprint, to the PSP, and user can be reported accordingly, so that if user finds something suspicious about any transaction then same can be immediately reported to the bank or PSP.

5. Conclusion and Future Scope

This paper presents our new approach targeting the conventional biometric payment systems. In our proposal we have introduced concept of fingerprint sensing in monetary transactions along with the security measures for fraud detection by incorporating it with liveliness detection of the fingerprint and recording of geolocation for every transaction. With this approach there will be no need to remember any pin, any password or even no need to carry any plastic card or even wallet or mobile.

We hope our proposal will provide a new way to ease out the payment system in current cashless payment scenarios enhancing comfort and security.

References

[1] T.Sabhanayagam, Dr. V. Prasanna Venkatesan and Dr. K. Senthamaraikannan, "A Comprehensive Survey on Various Biometric Systems", International Journal of Applied Engineering Research Volume 13, Number 5 (2018) pp. 2276-2297.

[2] https://www.statista.com/outlook/296/119/digital-payments/india#market-users

[3] Domingo, D. Chan, A.Watson (2000) "Smart card research and advanced applications" Series: IFIP International Federation for Information Processing, Springer, 2000,Vol. 52

[4] N.Galy, B.Charlot, and B.Courtois (2007) "A Full Fingerprint Verification System for a Single-Line Sweep Sensor" IEEE Sensors Journal, 2007,Vol. 7, pp. 1054-1065

[5] www.htgadvancesystem.com.

[6] Jain K. Anil, Ross Arun and Prabhakar Salil, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, 2004, vol.14, no.1, pp. 4-20.

[7] A. K. Jain, A. Ross and S. Pankanti, "Biometrics, A Tool for Information Security", IEEE Transactions on Information Forensics And Security, 2006, vol.1, no.2, pp. 125 – 144.

[8] S.Prabhakar, S.Pankanti and A.K.Jain, "Biometric Recognition, Security and Privacy Concerns", IEEE Security & Privacy, 2003, pp. 33-42.

[9] A. Al-Ajlan, "Survey on fingerprint liveness detection," in Proc. Int. Workshop Biometrics Forensics (IWBF), 2013, pp. 1–5.

[10] Zhihua Xia, Chengsheng Yuan, Rui Lv, Xingming Sun, Neal N. Xiong, and Yun-Qing Shi (2018) "A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection" IEEE Transactions on systems, man, and cybernetics, IEEE 2018

[11] Nenad Badovinac, Dejan Simic, Beograd, Serbia (2019) "A Multimodal Biometric Authentication (MBA) in Card Payment Systems" International Conference on Artificial Intelligence: Applications and Innovations (IC-AIAI), 2019.

[12] Abdullah Saud, Nazar Elfadil(2020) "Biometric Authentication by Using Fingerprint Recognition System" 2020 International Journal of Scientific Engineering and Science, 2020.

[13] https://uidai.gov.in/

Authors Profile

Piyush Suthar received his Bachelor's degree in Information Technology from Gujarat University, Gujarat, India in 2011 and Master's degree in Information Technology from Gujarat Technological University, Ahmedabad, Gujarat, India in 2013. He is working as an Assistant Professor at Information Technology department of Sankalchand Patel University, Visnagar, Gujarat, India.

Neha Pandya received her Bachelor's degree in Computer Engineering from Sardar Patel University, Gujarat, India in 2009 and Master's degree in Computer Engineering from Dharmsinh Desai University, Nadiad, Gujarat, India in 2012. She is working as an Assistant Professor at Computer Engineering department of Gujarat Power Engineering and Research Institute, Mehsana, Gujarat Technological University, Gujarat, India.

