# Multilevel Secured Finger Print Payment System Simulation using Android

**N.ganesh, r.c. Narayanan**

***ABSTRACT---Owing to a lot of hacks and other security concerns with respect to the card payment system, biometrics is next in line as the authentication module for payment systems. The hassle the user has to put up with in a card payment system by having to carry different cards and having to remember passwords is appalling and losing the card is another issue altogether. Usually fingerprints are used to authenticate the card and pin number that have been entered.Our system has been designed to let customers pay the bills using only their registered mobile number and fingerprint. In this paper, we have developed a simulation of an android application that is used on the sales side to emulate the process of authenticating a user using his fingerprint to let him access his prepaid balance and make his payment to the retail store. The proposed system uses multilevel security using SHA 256 and AES algorithm.***

***Keywords – Finger Print Payment; Simulation; AES; SHA 256; Android App***

## I. INTRODUCTION

Biometrics is the measure and activity to analyze the people's physical and behavioural characteristics. It helps in identifying a particular person and to provide access or control to a particular activity of an individual.Every human being is unique and can be recognized by his traits. Biometric payments will become the buzz word in the near future. Biometric payments is highly secured, user friendly and it eradicates the fraudulent payment transactions.It as well frees the individual by carrying payment cards during biometric payments. In the recent days, almost all the individuals use many credit and debit cards for transactions. The major setback in using this card is the individual should remember the secret codes or passwords of all the cards that they use. Alternatively, in the case of our proposed design since the biometric system is used the verification is done on one to one basis. The trained data which is in encrypted form will be stored in the database. After verification of the database with the captured biometric data then the person will be going for an easy payments.

In this paper, section II depicts literature review and section III demonstrates the working methodology of the proposed design and in section IV algorithm design is discussed. In section V experimental results had been discussed. Finally, Section VI concludes the paper.

## II. LITERATURE REVIEW

Augmented Biometrics System[1] is usedwith secure online transaction checks for different levels of security but it takes longer time for authentication. Shweta Gaur [5] has given an elaborative study on the review of biometric recognition techniques. The methodologies adopted cannot be utilised for any application oriented transactions. SulochanaSonkamble [3] has implemented biometric system for authentication purpose and predominantly it has been deployed in various utility computing. But the main drawback in this method is the system has been incorporated with password based design. A paper [2] about the review of transition to cashless economy deals with electronic payment system with minor level of security.

UPI [7] is designed as a mobile app which is widely used for online banking transactions and merchant payment system. As OTP alone used for authentication, the level of security provided for transaction is vulnerable to Denial of Service attacks. A survey paper by Sravya [6] has given the overall merits and demerits of finger print biometric system. They analysed all the biometric systems and concluded that finger print based system is user friendly and very less time consuming authentication.

## III. FINGER PRINT PAYMENT SYSTEM DESIGN

The overall design of the system can be broken down into three components as shown in Fig.1. First, Android application, Encryption and Decryption modules and the user database.


**Fig.1. Proposed System Design**

Fig.2. describes the detailed architecture of the proposed system. The application opens up to the login page and demands the user to enter his/her details as username and phone number and it also leads to the register page for first time users to register with their information.

**Revised Manuscript Received on June 10, 2019.**

**Dr. N.GANESH,**Department of Computer Science and Engineering Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College ,Chennai, Tamil Nadu, India.(E-mail: gannram@gmail.com)

**Dr. R.C. NARAYANAN,**Department of Computer Science and Engineering Sona College of Technology, Salem, Tamil Nadu, India.. (E-mail:rc.narayanan@gmail.com)

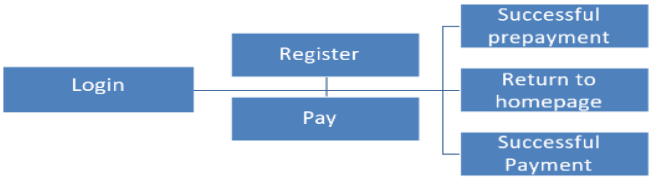


**Fig.2. Working Model Design**

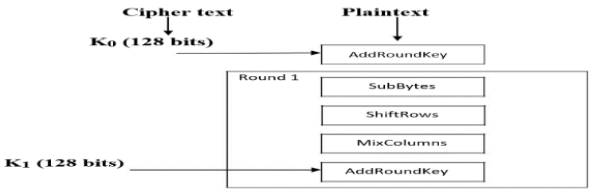


**Fig.3. Encryption Process in AES**

If the username already exists, the user is authenticated to the payment page. The system flow can be clearly understood from the diagram above. Asks for the name and the mobile number from the user to login.The registration page helps register a new user on to the application and lets the user make his prepayment which will be stored as the user's balance on the database.

The details this page demands from the user are Age, Email, balance and all the details are added to the database. The billing staff enters the amount payable, and the user is prompted to place his/her registered fingerprint to complete the payment.Upon successfully logging in, the payment page displays the balance in the user's account along with the amount to be paid for the products/services now. The sales person enters the amount to be paid just like as in a card payment system, except here, the swiping of the card is substituted by reading of the user's fingerprint using an individual fingerprint scanner. Here, the fingerprint data that was stored when the user was registered is retrieved to check for the authenticatingthe user for the payment. The fingerprint data is retrieved from the database in an encrypted format, and then decrypted at the time of verification. To add balance to the existing account, fingerprint is used. This ensures that no tampering can occur. All access to the database, or rather, a particular person's record in the database, is made only through that person's fingerprint. This ensures that no tampering can take place at the seller side. Encryption of the record is carried out using the fingerprint data and a 256 bit key. The record once updated, is encrypted again, before being written onto the database. The entire payment process is secured through the use of encryption and fingerprint authentication.The final page on the application to indicate the successful prepayment upon registering on the registration page and successful payment upon payment after authentication on the payment page, from which a touch anywhere is validated to reach the home page for other payments. This page also indicates successful payment upon addition of balance to the database.

## IV. MULTILEVEL SECURITY USING SHA AND AES

Unlike DES, the number of rounds in AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys and hence AES is variable and depends on the length of the key. Fig. 3 represents the same. Each round uses a different 128-bit round keywhich is derived from the original AES key. This is mainly implemented for finger print payment system for authentication purpose.

The SHA-256 uses a 512-bit message block and a 256- bit intermediate hash value. It is a 256-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key. Fig. 4 shows the same. The hash message is padded. Suppose the length of the message M, in bits. Append the bit \1" to the end of the message, and then k zero bits, where k is the smallest non-negative solution to the equation `+1+k 448 mod 512. Append at the last, the 64-bit block which is equal to the number ` written in binary. Then the message is parsed into N 512-bit blocks M(1); M(2) ;:::;M(N) . The first 32 bits of message block i are denoted M(i) 0 , the next 32 bits are M(i) 1 , and so on up to M(i) 15 . Big-endian convention is used exclusively. As a result, in the each 32-bit word, the left-most bit is stored in the most significant bit position.Then the hash value is computed.

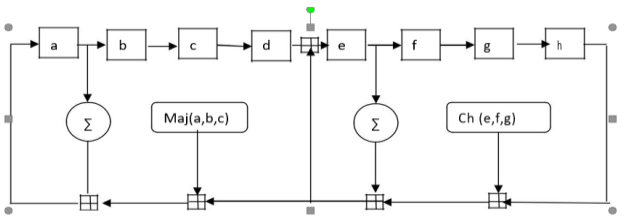


**Fig.4. SHA-256 Encryption**

With larger words with a size equal or greater than 32 bits, the execution can be made faster by combining the SubBytes and ShiftRows steps with the MixColumns step. Sequence of table lookups is considered. One kilobyte for each table is required. A round can then be done with 16 table lookups followed by four 32-bit exclusive-or operations in the AddRoundKey step. The table lookup operation can be performed with a single 256-entry 32-bit table by the use of circular rotates. Using a byte-oriented approach, SubBytes, ShiftRows, and MixColumns steps can be combined and consolidated into a single round operation.

## V. RESULTS AND DISCUSSION

The application opens up to the login page and it requests internet access to be enabled.The user is taken to the Dual SIM & Networks for him to enable internet settings. This is the interface for the users to enter his/her name and phone number details which is used to either login or register.The user needs to enter a valid name within 32 characters and the phone number should be a registered one with 10 numbers. Otherwise, the validation checker notifies the user of it.

Similar check used to validate phone number. Upon pressing of the login button.A case is where the login fails because the user is not registered already. In this case , the user has to register with the register button using android.
This is the registration page used to register a new user on to the system and it demands details like Age, E-mail, and Balance which is put into the database.The registration page provides validation for age, and similarly validation is done for email and balance as well.The application asks for permission to access the external USB device.

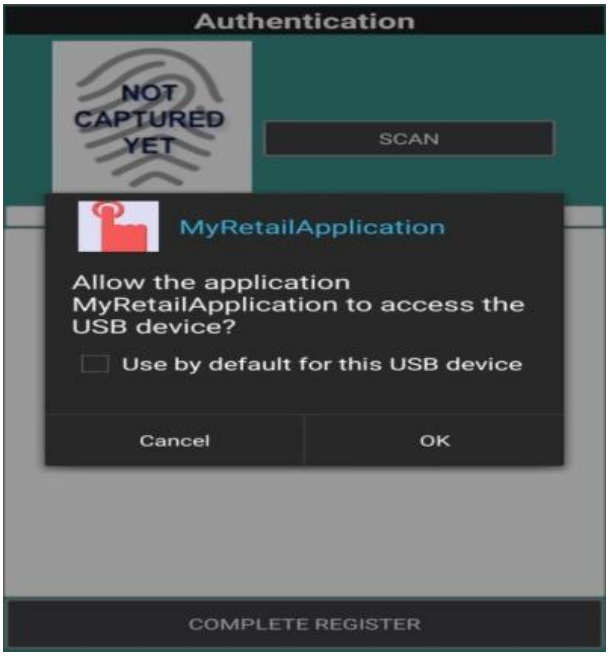


**Fig.5. Application request for USB**

This completes the process of registration In Fig.5, it is shown that the application requests the user to access the USB device which is via the fingerprint scanner is connected.


**Fig.6. Finger Print Scanning Process**

This is an instance of a fingerprint being read via the fingerprint scanner. A fingerprint can be seen on the image shown in Fig.6. and Fig,7. The person is authorised and the payment has been made.

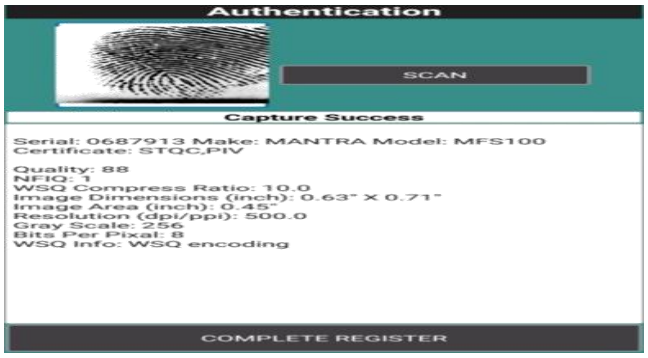


**Fig.7. Finger Print Authentication**

The development of a smart mobile application that will be used to read a fingerprint and to extract a person's corresponding account details and to perform CRUD operations on that data. The purpose of this project is to provide a hassle free, yet personal solution to the payment system in retail outlets and franchisees, wherein the customers can pay the bills using only their registered mobile number and fingerprint instead of the hassle of carrying cards or cash.

## VI. CONCLUSION

The proposed work showcases the artefacts of a card-less payment gateway for the user whose details are verified by having the finger print of an individual and this by itself act as a biometric data. In the modern world every single user requires easy payment when they go for shopping malls and at the same time they require the system to be reliable, secure and hassle free. The important aspect of the design is the cost of implementation is very less as it requires only finger print scanner on the merchant side. The algorithm incorporated is multilevel encryption of the captured biometric data so high level security is enforced. User need not carry cash or cards for executing any transaction. The authentication and authorization has been done only on the finger print data, the system is ease of use from the merchant side as well as on the customer side. Such Biometricpayments will provide consumers to have a seamless trouble free payment experience.

## REFERENCES

1. Adegboyeg,, Secure on-Line Transaction through Augmented Biometrics System, Global Journal of Computer Science and Technology: G Interdisciplinary Volume 15 Issue 2 Version 1.0 Year 2015, ISSN: 0975-4350
2. Oginni Simon Oyewole, El-Maude, JibreelGambo, Mohammed Abba, Michael Ezekiel Onuh, Electronic Payment System and Economic Growth: Review of Transition to Cashless Economy in Nigeria, International Journal of Scientific Engineering and Technology Volume No.2, Issue No.9, pp : 913-918 1 Sept. 2013, (ISSN : 2277-1581).
3. SulochanaSonkamble, Dr.RavindraThool, BalwantSonkamble, Survey Of Biometric Recognition Systems And Their Applications, Journal Of Theoretical And Applied Information Technology © 2005 - 2010 Jait.

4. Shweta Gaur, V.A.Shah, ManishThakkar, Biometric Recognition Techniques: A Review, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 1, Issue 4, October 2012.
5. Sravya V, RadhaKrishna Murthy, RavindraBabuKallam,Srujana B., A Survey on Fingerprint Biometric System, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 4, April 2012 ISSN: 2277 128X.
6. VishalVishwasJadhav,RahulRatnakarPatil,RohitChandrashekarJadhav,AdwaitNiranjanMagikar,Proposed E-payment System Using Biometrics, International Journal of Computer Science and Information technologies,Vol.6(6),2015,4957-4960,ISSN:0975-9646.