

Proposed E-payment System using Biometrics

Vishal Vishwas Jadhav^{#1}, Rahul Ratnakar Patil^{*2}, Rohit Chandrashekar Jadhav^{#3}, Adwait Niranjana Magikar^{#4}

*Department of Computer Engineering,
PES's Modern College of Engineering
Shivajinagar, Pune – 411005, India*

Abstract— In this paper we have proposed e-payment system which based on biometric characteristics.

We mainly, focuses on the problem facing due current e-payment system which uses conventional characteristics like user-name and password or security PIN and What solution is better for such problem.

Traditional techniques always suffer from a common problem of inability to differentiate between an authorized person and a person who fraudulently acquires the access privilege of the authorized person. Biometric easily identified authorized person and fraudulent impostor due to human's physiological or behavioural characteristics.

The purpose of this work is to generate an e-payment system based on biometric authentication in this case finger-print that are useful for the various services of government or organization or business.

Keywords— e-payment, finger-print, biometrics, verification, identification

I. INTRODUCTION

In our daily life, we use payment system i.e., Cash, Cheque, Debit Card, Credit Card, etc., each system suffer from common problem of to identify authorized person. The system may give chance to fraudulent person if he/she knows your password or Security PIN.

Thus we concluded that the Password is the weakest component of our payment system. Owing to this, we have to look towards the next generation payment system i.e., biometric system. Biometric uses human's physiological characteristics and sometime uses behavioural characteristics also.

The Physiological characteristics have good degree of uniqueness, availability, collectability. If we use this characteristics in our daily payment system, the system gives good performance also.

In this paper, we proposed architecture for e-payment system based on finger-print recognition.[1]

II. FINGER-PRINT FOR AUTHENTICATION

In this work, we emphasizes on e-payment system based on finger-print authentication.[2]

The finger-print have extend of collectability, universality and uniqueness. It is Permanence property of every human being.

We see Table I to compare various biometric methods:

TABLE I
COMPARISON BETWEEN VARIOUS BIOMETRIC TECHNIQUES [2]

Biometric Identifier	Performance	Acceptability	Circumvention
Face	Low	High	Low
Finger-print	High	Medium	High
Hand Geometry	Medium	Medium	Medium
Hand Vein	Medium	Medium	High
Iris	High	Low	High
Retinal scan	High	Low	High
Signature	Low	High	Low
Voice	Low	High	Low

In this table, we compare nine biometric techniques on the basis of the Performance, Acceptability and Circumvention.

- 1) Performance is defined as the achievable identification accuracy, the resource requirements to achieve an acceptable identification accuracy, and the environmental factors that affect the identification accuracy;
- 2) Acceptability is defined as the indicates to what extent people are willing to accept the biometric system;
- 3) Circumvention is defined as how easy it is to fool the system by fraudulent techniques.

If we compare Finger-print with Face, Signature, Voice, Hand, then in this race finger-print is always winner. But if we see comparison the fingerprint authentication method with iris and retina scanning, then retina and iris have high circumvention whereas finger-print has low.

If we use retina scanner, it creates extra burden on the customer while doing payment.

If we discuss about the plastic card, then security is a more important issue. The important feature of these card is mobility. This is the reason behind this popularity. Our

Finger-print also have mobility property.[6] We can use finger anytime and anywhere for authentication. The finger-print authentication system has maximum potential to replace plastic cards and wallet.

In this topic, a verification system based on fingerprints, and the terms authentication, verification, and identification are used in a loose sense and synonymously.

III. FINGER-PRINT UNIQUENESS

Fingerprints basically consist of:

1. Ridges
2. Valleys

Ridges means raised skin and valleys means lowered skin.[5][7]

The ridges and valleys are twist to form a distinct pattern. When a blue-inked imprint of a finger is made, the blue colour impression created is of the ridges while the valleys are the un-inked areas or white colour between the ridges. Although the manner in which the ridges pattern is distinct.

These features are particular patterns consisting of terminations or bifurcations or meeting or ending of the ridge/s. Moreover, all finger-prints can be classified into three categories based on their major central pattern viz., arch, loop, and whorl. See Figure 1 and 2



Fig. 1 Finger-print Uniqueness

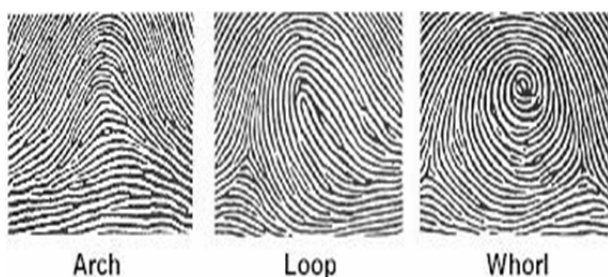


Fig. 2 Finger-print: Arch, Loop and Whorl

IV. APPLICATIONS

1. Biometrics, used in banking Transaction security, such as electronic fund transfers, ATM security, check cashing, and credit card transactions.
2. Biometrics, also used in physical access control, such as airport access control;
3. Biometrics, used in information system security, such as access to data bases via log-in privileges;
4. It is used in government benefits distribution, such as welfare disbursement programs
5. INPASS System is Customs and immigration, such as the USPASS (U.S. Passenger Accelerated Service System) which permits faster immigration procedures based on hand-print or finger-print geometry authentication
6. National ID systems, which provide a unique identification to the citizens and integrate different government services such AADHAR (Unique Identification System in India) card.
7. Biometrics also used in Voter and Driver registration, providing verification facilities for registration of voters and drivers.[2]

V. PROPOSED ARCHITECTURE

A. System Input

The input of our system is simply Finger print of the user (or Customer or Passenger). The Finger Print is taken by the System shown in the Figure 3.

The Embedded System have Thumb Scanner which takes finger-print of Thumb. It scans valleys and ridges on the thumb. It locates the points on the thumb where two ridges are separated or meeting together.

B. Transaction

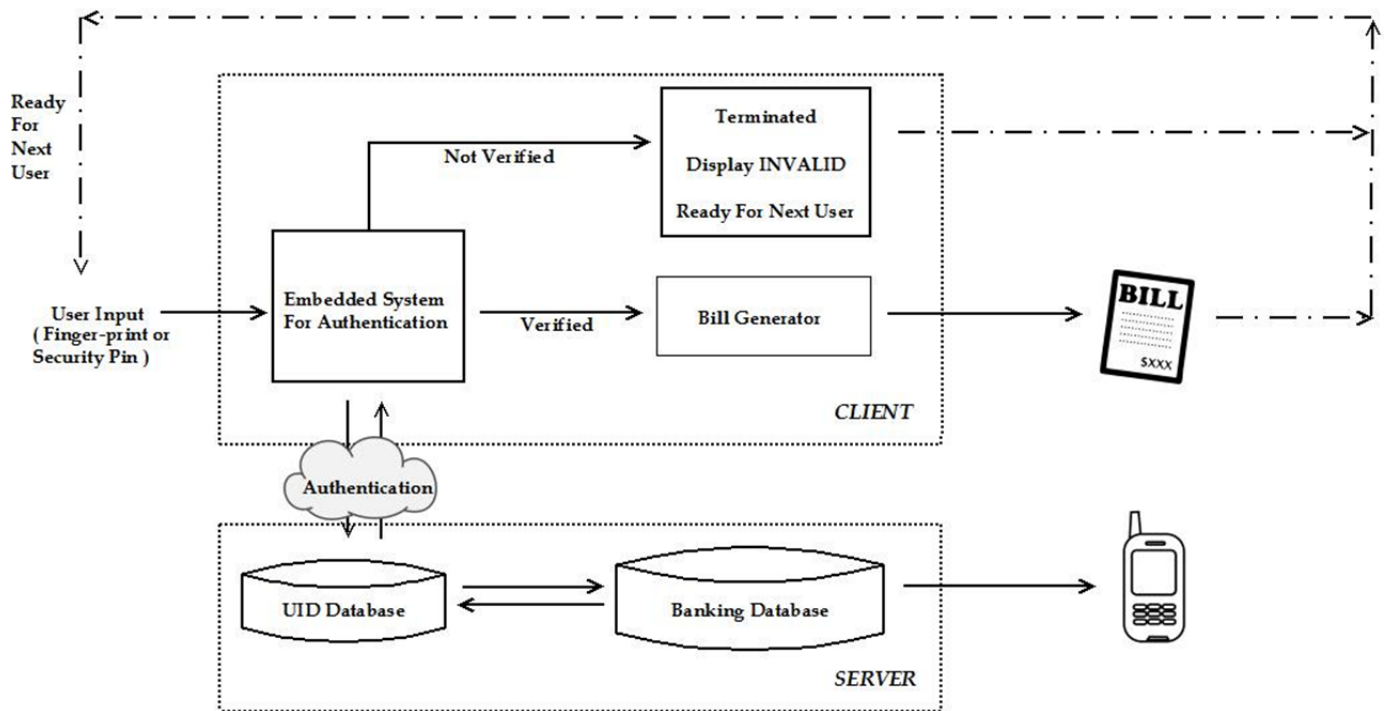
Based on the Authentication, the system will allow access to the user. In the biometric authentication system, identification and verification is done at the same time. After getting verification, the system will ask for the product and it shows the price of it.

After getting Confirmation, system automatically deducts the amount from the bank which is attached to that UID (Unique Identification) Number.

C. Output and Analysis

After Transaction, the system will generates the bill with information like Product details, Price, etc., at the same time, the bank sends the acknowledgment to the user via SMS service.

After that, the system will be closed and it will be ready for next user. Organization of the system will generates the reports which can help to improve it by analysing them.



VI. FINGER-PRINT VERIFICATION AND IDENTIFICATION

A. Verification

The Verification is formally stated as follows:

The given an input vector F_Q (finger-print extracted from biometric

Database or we can say that UID Database) and a claim that identity I , determine if $(I; F_Q)$ belongs to class c_1 and c_2 , where c_1 indicates that claim value is true and c_2 denotes the claim value is false.[3]

F_Q is matched against F_I , the template corresponding to user or customer I , to determine its class label. Thus

$$(I, F_Q) \in \begin{cases} c_1 & \text{if } S(F_Q, F_I) \geq t \\ c_2 & \text{otherwise} \end{cases}$$

Where, S is the function that measures the similarity between vectors F_Q and F_I and t is a predefined threshold. The value $S(F_Q, F_I)$ is termed as a similarity or matching score between the biometric measures of the user or customer and claimed identity.

Therefore, every claimed identity is classified into either c_1 or c_2 based on the variables F_Q , I , F_I and t and the function S .

The biometric measurements like finger-prints of the same individual taken at different times are never identical to each other. Therefore, the threshold t is introduced.

B. Identification

The identification, may be stated as follows:

Given an input vector F_Q , determine the identity I_c , c belongs to $\{1, 2 \dots N, N+1\}$. [3]

Here, $I_1, I_2 \dots I_N$ are the identities accepted in the system and I_{N+1} denotes the reject case where no suitable identity can be determined for the user or customer.

Thus,

$$F_Q \in \begin{cases} I_c & \text{if } \max_c \{S(F_Q, F_{I_c})\} \geq t, c = 1, 2, \dots, N \\ I_{N+1} & \text{otherwise} \end{cases}$$

Where, F_{I_c} is the biometric template corresponding to identity I_k and t is predefined threshold.

VII. REVIEW ON CURRENT SYSTEM

In current conventional payment system, there is a chance of encountering forged signature for transaction and in the E-payment system, the password of customer may be hacked and misused by the another person. Thus security is still a challenge in these payment applications. There are many techniques to secure the user or customer information and to protect from the possible forgery of signatures and password or security PIN hacking. Still, there are some problems with such payment systems. Today, single factor authentication, e.g. Passwords, is no longer considered secure in the internet and banking systems. Easy-to-guess passwords, such as names and age, are easily discovered by automated password-collecting programs which is harmful to our private data or bank account.

A biometric authentication technology makes sense for E-payment. In today's world, no one need pockets i.e., pocket less. That stuff jingling around in there keys, plastic cards (i.e., credit cards etc.), check books are replaced by something closer to the body. When you need to open a door or make a purchase, technology allows anyone to do so with a fingerprint or other biometric techniques also, like a voice command, or a computer scan of eyeball. A new approach to the fingerprint payment technology i.e. using E-payment with biometric technology is better because it won't just identify, but it will authenticate as well at same time (Dynamically).

VIII. FEASIBILITY OF THE SYSTEM

Biometric authentication systems that use:

1. Physiological (e.g., fingerprint, face, etc.)
2. Behavioural (e.g., speech, handwriting, etc.)

Traits are becoming increasingly popular, compared to traditional systems that are based on tokens (e.g., key) or knowledge (e.g., password).

Traditional authentication systems cannot distinguish between a person who fraudulently acquires the access privileges (e.g., key, password/Security PIN) of a genuine user and the genuine user himself/herself. Furthermore, biometric authentication system can be more convenient for the users since there is no password to be forgotten or security key to be lost and a single biometric trait (e.g., fingerprint) can be used to authorized personality without the burden of remembering passwords or any Security PIN.

The system is also economically feasible. It gives the positive economic benefits to the organization. Operational Feasibility of the system gives the better performance. The system uses only fingerprint instead of user-name and password in conventional system.[7]

IX. SCOPE

The E-payment is a part of daily routine for an individual life. The existing system has several drawbacks in its authentication. Firstly hacking, from the network any one can hack the user-name and password and the result is the person gets access to owner account or our private data. So for this issue secured payment applications on e-payment system using finger-print geometry based biometric authentication is proposed.

Electronic payments using biometrics are still largely in their youngest stage. Trials are underway in the U.S.A., Australia and a limited number of other countries like India. Most biometric e-payments involve using fingerprints as the identification and access tool, though companies like Visa International are piloting voice recognition technology and retina and iris scans are also under consideration. A finger-print authentication could replace the plastic card like credit card or smart card and more securely identifies the personality undertaking the transaction.

X. MARKET POTENTIAL AND COMPETITIVE ADVANTAGES

The world market for Fingerprint Authentication is projected to reach US dollar \$ 11.9 billion by 2020, driven by growing biometric authentication system investments in government and enterprise sectors to provide support e-Governance, national/civil ID, e-passports, law enforcing, and access control and user authentication applications as well as Indian AADHAR project.[4]

Fingerprint Biometrics, also known as Fingerprint Identification Technology, is one of the oldest and widely

used biometric technologies in the world. Using fingerprint pattern of ridges, lines, valleys, arch, loop and whorl which are unique to each individual personality represents one of the most reliable among biometric technologies.

Fingerprint authentication technology, besides being widely adopted for forensic investigations, is also used for other applications such as e-Governance, e-passports, national ID, citizen ID, law enforcing, ATM money transaction and immigration and border management applications. The increasing number of deployment of access control systems by organization is further creating a strong pillars of business case for fingerprint authentication technology.

XI. CONCLUSION

The Proposed system of E-payment using Biometrics, the security and potential of existing E-payment system will be enhanced. This system will be generic and it can be used by multiple government services like payment of Electricity bill, Telephone bill, Income Tax returns, etc. Due to this, Government will be able to make fair and accurate decisions for Public Welfare. Optimized strategies extracted from this decisions can be developed to increase potential and profit of Organization.

Hence, this paper presented a type of this kind of e-payment system i.e., biometric e-payment system that can be easily implemented. Meanwhile, the full implementation of such a model will help to achieve our objectives like security, efficiency, reliability and easy-to-use e-payment system by many people in the world.

ACKNOWLEDGEMENT

Our thanks to the experts who have contributed towards survey of this paper.

REFERENCES

- [1] Mangala Belkhede, Veena Gulhane, and Dr. Preeti Bajaj. Biometric mechanism for enhanced security of online transaction on android system: A design approach. International Conference on Advanced Communications Technology, February 2012.
- [2] ANIL K. JAIN, LIN HONG, SHARATH PANKANTI, and RUUD BOLLE. An identity-authentication system using fingerprints. IEEE, 1997.
- [3] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. IEEE, 2004.
- [4] Karamjeet Kaur and Dr. Ashutosh Pathak. E-payment system on e-commerce in india. International Journal of Engineering Research and Applications, 2015.
- [5] Dileep Kumar and Yeonseung Ryu. A brief introduction of biometrics and fingerprint payment technology. International Journal of Advanced Science and Technology, 2009.
- [6] Ajeet Singh, Karan Singh, Shahazad, M. H. Khan, and Manik Chandra. A review: Secure payment system for electronic transaction. International Journal of Advanced Research in Computer Science and Software Engineering, 2012.
- [7] Umut Uludag and Anil K. Jain. Attacks on biometric systems: A case study in fingerprints. The International Society for Optical Engineering, 2004.