

Comparative Study of Different Biometric Authorization for Mobile Payment System

Nikita Gupta

Department of Computer Engineering
Army Institute of Technology
Pune, India

Devendra Mani Tripathi

Department of Computer Engineering
Army Institute of Technology
Pune, India

ABSTRACT

The PIN based single level authorization of Mobile Payment System suffers several security leakage problems. Integrating biometric identifier as one more level of authorization increases the robustness of the payment system. But as mobile device and wireless network has certain constraint, so it is not possible to use any biometric identifier for authentication. This paper presents a comparative study of using different biometric identifier in authorization process of mobile payment system, in context of developing country like India. In this paper we discussed the possible integration of face, fingerprint, iris, keystroke dynamics and voice as possible biometric identifier.

General Terms

Biometric security, M-Commerce.

Keywords

Biometric Identifier, M-commerce, Mobile Payment, Multi-level Authentication.

1. INTRODUCTION

Mobile payment refers to all the purchase using mobile wireless device such as smart phone and PDAs, where mobile device is used for initiation or conformation of service or good [1]. Mobile payment is a new and rapidly-adopting alternative payment method in developing continent – especially in Asia and Europe. Survey revealed that the combined market for all types of mobile payments is expected to be more than \$600B globally by 2013 [2].

The mobile payment systems interact with the open networks thus it is always required to create a security centric design. Security introduces unique design requirements and a new set of challenges. Mobile payment can be done using application that send Text-SMS towards a payment or NFC near field communication in which phone is swiped against a purchasing station.

A multi level authorization for mobile payment system increases the robustness of the authorization system, when one of the biometric identifier is used for authorization then its robustness increase many times. But due to processing capability of mobile devices and constraint of wireless network these system is not as viable in current infrastructure of developing country like India.

Since in developing country like India the ratio of lower end mobile device to higher end mobile device is quite high, and the processing power of lower end mobile devices are limited to few MHz, so practical implementation of every biometric authorization is not possible in general context. So this paper presents a detailed study of using different biometric identifier and one more level of authorization in mobile payment.

The paper is organized as follows: Section II gives the details of literature present on the topic, section III presents the brief overview of mobile payment and biometric identifier. Section IV cover the viability of using different biometric in mobile payment. Finally section V concludes the discussion with scope of future work.

2. RELATED WORK AND MOTIVATION

2.1 Related Work

Mobile payment system drew a lot of interest among researchers. Various authorizations techniques using biometric identifier has been proposed by researchers but still this topic is not fully explored and there is lots of opportunity for researchers in this field. Dileep kumar and Yeonseung Ryu proposed a fingerprint based mobile payment system, in this paper the possible integration of fingerprint in payment system is discussed [3]. Michael Gordon discussed the implementation detail of using finger print in mobile payment system; in this paper the authors used J2ME as a platform to physically implement this system [4]. Jiehua Wang proposed a novel security mobile payment system based on watermarked voice [5]. In this paper the authors proposed watermarked voice as one more security level for authorization process. Huiqi lu proposed a iris based mobile authorization in payment system [6]. In this paper the authors used mobile camera as the image acquiring device.

2.2 Motivation

Most of the approaches mentioned above show that much of the work is not carried out in practical viability of their approaches. Most of the work just discussed just the possibility of such kind of payment authorization system. Few of the biometric identifier is not even searched for this system e.g. keystrokes dynamics. So there was a great need of summing up all the work done at one place, discussing the drawback and advantage and practical feasibility of such kind of system. This work provides a logical reasoning for the viability of adding biometric identifier in authorization process.

3. BACKGROUND

3.1 Mobile Payment

Mobile payment is the payment made for goods, services and bill/invoice with a mobile device (such as a mobile phone, smart-phone, or Personal Digital Assistant) by taking advantages of wireless and other communication technologies. Mobile devices can be used for payment for digital goods and services. Payments for physical goods are also possible, both at vending and ticketing machines, and at manned Point-of-Sale terminals. Typical usage needs the user to be connected with the authentication server with the help of mobile device.

Mobile based payment systems can be categorized into two types: 1) Remote Mobile Payment Systems and 2) Proximity Mobile Payment Systems. These systems are shown in Fig. 1. In case of remote payment system, payer and payee are not in the same vicinity, the customer uses his mobile device to send a payment request to a payment service provider. The payment service provider requests the payee for confirmation, payee then sends the confirmation message to the payment service provider. In case of proximity mobile payment system, the customer directly sends the payment request to the payee, payee then forwards the payment request to the payment service provider [7].



Figure 1: Mobile payment systems: remote and proximity based.

3.2 Biometric Identifier

Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance [8].

Biometric characteristics can be divided in two main classes as shown in Table 1.

Physiological are related to the shape of the body and behavioral are related to the behavior of a person.

Table 1. Biometric Identifier

Physiological	Behavior
Fingerprint	Keystroke Dynamics
Face	Voice Print
DNA	Signature
Palm print	
Hand Geometry	
Iris Recognition	
Retina Recognition	
Odor Recognition	

4. VIABILITY ISSUES

We are considering the fact that mobile device is used for acquiring the sample of biometric identifier and the same device is used for preprocessing of that sample. The payer will send the symmetric key encrypted feature vector not the sample, directly for further processing.

4.1 Fingerprint

Finger print is a viable for point of sale based mobile payment system like NFC payment, but using finger print in remote based have some problem like most of the cell phone and mobile device that are available in today's market does not have finger print scanner. Using camera phone for finger print scanning won't give good result.

Challenges:

- I. No scanning device present in most of the mobile device in today's market.
- II. Processing of finger print on low processing power mobile device is again a challenge.

4.2 Face Recognition

Face as another level security that can be for extra level of security and as per our study no research has been done on this combination.

Challenges:

- I. Low processing power of mobile device.

4.3 DNA Recognition

DNA is not a feasible because of time requirement for DNA matching even matching can take many hours.

Challenges:

- I. There is no sample acquisition capability in mobile device.
- II. The time required for DNA verification is in Hours.

For the time being this option seems to be impossible.

4.4 Palm Print

The problem with palm print is nearly the same that is with other physiological biometric identifier. The first problem is mobile device do not have palm print scanner with them.

Challenges:

- I. No scanning device present in mobile phone.
- II. Need high processing power.

4.5 Hand Geometry

No a feasible solution until some scanning device is attached with mobile device. Using mobile camera for scanning is not a good solution because of image quality.

Challenges:

- I. No scanning device present in mobile phone.
- II. Need high processing power.

4.6 Iris Recognition

Iris recognition is a feasible solution for POS (point of sale) based mobile payment system but for remote mobile payment this option could be implemented for the time being. We can implement this only if we have an acquisition device integrated in our mobile device.

Challenges:

- I. There is no sample acquisition capability in mobile device.

4.7 Retina Recognition

Retina recognition is a feasible solution for POS (point of sale) based mobile payment system but for remote mobile payment this option could be implemented for the time being. We can implement this only if we have an acquisition device integrated in our mobile device.

Challenges:

- I. There is no sample acquisition capability in mobile device.

4.8 Odor Recognition

The odor recognition is good alternative authorization purpose in mobile payment system. As mobile device do not have any such sample acquisition device.

Challenges:

- I. No sample acquisition device present.
- II. Processing power is high.
- III. Nearby smell can affect the payment process.

4.9 Keystroke Dynamics

Keystroke dynamics, or typing dynamics, is the detailed timing information that describes exactly when each key was pressed and when it was released as a person is typing at cell phone keypad. Key stroke based biometric is the best suitable for mobile payment authorization considering its processing time. A number of studies have been performed of key stroke analysis since its introduction in 1975. Table 2 shows the main research done on key stroke dynamics.

As literature says that even we can get a FAR and FRR as 0 using neural network but because of using neural network the time complexity of this system will be high. So we advocate the use of statistical method which gives low FAR and FRR.

Table 2. Literature Review

Study	Key Stroke Matrix		Classification technique	# of Participant	FA R (%)	FRR (%)
	Inter Key	Hold Time				
Joyce & Gupta 1990	yes	no	Statistical	33	0.3	16.4
Leggett et al. 1991	yes	no	Statistical	36	12.8	11.1
Brown & Rogers 1993	Yes	Yes	Neural Network	25	0	12
Clarke & Furnell 2007	Yes	No	Neural Network	32	5	5
Napier et al 1995	Yes	Yes	Statistical	24	3.8	3.8
Obaidat & Sadoun 1997	Yes	yes	Statistical	15	0.7	1.9
Obaidat & Sadoun 1997	Yes	yes	Neural Network	15	0	0
Monrose & Rubin 1999	yes	no	Statistical	63	7.9	7.9
Cho et al. 2000	Yes	yes	Neural Network	25	0	1
Ord & Furnell 2000	Yes	no	Neural Network	14	9.9	30

4.10 Voice Print

Voice print based mobile payment authorization system is also possible. But the main drawback is the problem while making payment in noisy surrounding. In that case because of background noise the verification process will become less accurate.

Challenges:

- I. Background noise will give imperfect matching result.
- II. Person near the payer can hear the voiceprint password.

4.11 Signature

Definitely signature is a good alternative but this can only be done with cell phones which have touch screen facility available on them but for other device we need to have a signature capturing device.

Challenges:

- I. The number of device that can support signature verification is very few, so we cannot make this as a standard for mobile payment.

TABLE 3. Mobile Device Sample Acquisition Capability

Biometric Technique	Sample Acquisition Capability As Per Standard	Accuracy
Finger Print	×	Very High
Face print	✓	High
DNA	×	Very High
Palm print	×	High
Hand Geometry	×	High
Iris	×	Very High
Retina	×	Very High
Odor	×	High
Key Stroke Dynamic	✓	Medium
Voice Print	✓	High
Signature	×	High

5. CONCLUSION AND FUTURE WORK

The survey reveals that the current single level PIN based authorization for mobile payment is not sufficient. On the basis of this finding it is evident that a stronger authentication process is required for authorization purpose. A two level authorization seems to be a better option, first level is PIN based and second level is biometric authorization. Considering the constraint of mobile device and wireless network, key stroke dynamic based authorization suits best for mobile payment service. We strongly suggest the use of key stroke based authentication for mobile payment. It must be noted that for our study we considered the developing country like India where most of the mobile device is of lower end.

There is scope of future work towards the implementation of keystroke dynamic based on mobile devices (cell phone).

6. REFERENCES

- [1] Norman Sadeh, M-Commerce, Wiley Computer Publishing 2002.
- [2] Juniper Research Forecasts Total Mobile Payments Grow Nearly Ten Fold by 2013. Available from: <http://www.juniperresearch.com/shop/viewpressrelease.php?pr=106>
- [3] Dileep Kumar and Yeonseung Ryu , “A Brief Introduction of Biometrics and Fingerprint Payment Technology”, *International Journal of Advanced Science and Technology*, Vol. 4, pp. 25-37, March, 2009.
- [4] Michael Gordon and Suresh Sankaranarayanan, “Biometric security mechanism in Mobile payments, Wireless And Optical Communications Networks (WOCN)”, in *Seventh International Conference*, 6-8 Sept. 2010, Colombo.
- [5] Jiehua Wang and Song Yuan, “A Novel Security Mobile Payment System Based On Watermarked Voice Cheque, Mobile Technology, Applications and Systems”, in *2nd International Conference*, 15-17 Nov. 2005
- [6] Huiqi Lu, Frederic Claret-Tournier, Chris Chatwin and Rupert C. D. Young, “M-Commerce Secured Using Web-enabled Mobile Biometric Agents”, *Web Intelligence and Intelligent Agent Technology Workshops, IEEE/WIC/ACM International Conferences*, 2007.
- [7] S. Agarwal, M. Khapra, B. Menezes and N. Uchat, “Security issues in mobile payment systems”, in *5th International Conference on E-Governance*, Hyderabad, India. 2007, pp. 142-152.
- [8] Wikipedia <http://en.wikipedia.org/wiki/Biometrics>