Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL HYBRID AUTHENTICATION METHOD BASED ON ORIENTATION MAPS AND SERVER AIDED SIGNATURE FOR M COMMERCE SECURED TRANSACTIONS

[1]R.ARUN PRAKASH, [2]K.M.MEHATA, [3]C.CHELLAPPAN

[1]Department of Computer Science, Anna University, Chennai, Tamil Nadu, India
[2]Department of Computer Science, B S Abdur Rahman University, Chennai, Tamil Nadu, India
[3]Department of Computer Science, Anna University, Chennai, Tamil Nadu, India
E-mail: [1]arunitvijay2014@gmail.com, [2]hodcse@bsauniv.ac.in, [3]drcc@annauniv.edu

ABSTRACT

Mobile commerce (m-commerce) refers to the ability to perform wireless commerce transactions using mobile applications in mobile devices. It is an innovative concept and is emerging in a context of an established norms, regulations and standards. This paper presents a study of adoption determinants for mobile commerce, focusing on end-users of a mobile commerce pre-paid service. The main objective of the study is twofold; to determine an algorithm that improves security and decreases the time delay for processing of an adoption model by applying it to the results of the study. In order to investigate the field of mobile commerce service adoption, information related to its' end-users was gathered. The framework was applied to the results of the study in order to validate its concepts. We proposed a model based biometric identification with SAS algorithm to obtain digital signature over the conventional method of merely algorithms to acquire signature. Biometric Identification Systems are widely used for unique identification of humans mainly for verification and identification. Biometrics is used as a form of identity access management and access control. Fingerprints are considered to be the best and fastest method for biometric identification. Hence we have adopted the finger print recognition for improving security. They are secure to use, unique for every person and do not change in one's lifetime. The findings of the case study indicate strong support for triangulating the three perspectives namely secured access, lesser processing delay and better signature generation method. The results of the same have been analysed and presented in this paper.

Keywords: *M Commerce, Biometric Authentication, RSA Signature, SAS Signature, Feature Extraction*

1. INTRODUCTION

M commerce involves the use of mobile devices to transact, communicate and entertain M-commerce is defined as "The delivery of trusted transaction services over mobile devices for the exchange of goods and services between consumers, merchants and financial institutions. Mobile Commerce is an evolving area of E Commerce, where users can interact with the service providers through a mobile and wireless network, using mobile device for information retrieval and transaction processing. M-Commerce services and applications can be adopted through different wireless and mobile networks, with the aid of several mobile devices. However, constraints of both mobile networks anddevice influence their operational performance. Therefore, there is a strong need for taking into consideration those constraints in the design and development phases of M Commerce services and applications. Another important factor in designing M Commerce services and applications is the identification of mobile user's requirements. Furthermore, M Commerce services and applications need to be classified based on the functionality they provide to the mobile users.

This kind of classification results in two major classes: the directory and the transaction-oriented services and applications. Today M-commerce has enabled Voice messaging systems, emails

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

that are "spoken" to you instead of having to read them (Tellme, Conversay) It means being able to complete banking transactions at any time of day or night, and with global roaming systems and at the technological high-end of satellite phones, anywhere in the world.Being able to mimic the functions of a PC and "surf" WAP enabled sites (Rogers, Telus, Verizon).Typically today, commerce is the ability to purchase goods and services through a mobile device. Mobile services benefit from three major factors that boost information value to end-users: personalization, time-sensitivity, and location awareness. Combining these elements adds even more value to the M commerce [1]. Although there are many systems supporting mobility and many solutions for wireless access, there are issues influencing the performance of the various mobile systems that need to be considered in the design of M Commerce services and applications. This applies also to mobile devices that exhibit some major drawbacks compared to desktop systems.

2. CLASSIFICATION OF M-COMMERCE

One way to classify m-Commerce services and applications is based on the functionality they provide to the mobile users. This kind of classification results in two major classes: the directory and the transaction oriented services. The major categorization between these two classes of services is that in the former a mobile user performs only read requests to the directory, whereas in the latter a user performs read and write requests to the transaction server. It is necessary to note that an M Commerce application can be a combination of both classes. The directory-oriented class of M Commerce services comprises applications that provide information to mobile users. This information can be location, content and user dependent, being localized and personalized in ways appropriate to the specific mobile user. For example a mobile user being away from the home, needs up-to-date information regarding his current location, and local facilities that time he may use directory-oriented M-Commerce. The transaction-oriented class comprises various services and applications with, which the mobile user conducts transactions with the service provider. The transactions contain read and write operations on behalf of the mobile user. For example, a banking service for mobile users falls into the transaction oriented class of M Commerce services. The current mobile and wireless technologies suffer from constraints due to the wireless and mobile environment.

As we know, mobile phone is originally developed for convenient wireless communication. The added value of Mcommerce service is developed as a by-product of wireless communication technology. To guarantee high level of security while keeping the convenience of ubiquity is a perplexed reality in M commerce applications. This challenge prevents the widely deployment of M-commerce services. Even when acceptably authenticated at the start of a transaction sequence, it is possible for messages to be intercepted, most likely within a compromised device prior to sending or within the network. The prerequisite requirement for security in M commerce services is that both the user and their mobiledevice involved in a transaction are genuine. However, most of the mobile networks use pre-stored password or PIN to control access. As the existing mobile networks residing the whole security infrastructure to a simple PIN mechanism [1]. The rest of the authentication process relies on pre stored secrets on identifier. This further makes the vulnerable mobile computing environment less secure. In addition, mobile devices are normally identified by unique IMEI, and activated by SIM. The diversity of devices on the market makes a generic device verification method very difficult [2].

3. SECURITY VULNERABILITIES IN M-COMMERCE

The main vulnerability in mobile computing is summarized as follows.

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1.Theft/Loss of device and information: Data stored in the device is easily accessed physically if the device is lost or stolen.

2. Clone: Placing a chip into a mobile phone such that the ESN can be modified.

3 Hijacking: Control the communication session between two entities, masquerade as one of them.

4. Malicious software (Malware): Malicious codes in the form of virus, worm or other malware to perform unauthorized process.

5. Phishing: Tracking a victim into disclosing sensitive personal information or downloading malware.

6. Wireless connection vulnerabilities: Confidential data sent over various unprotected wireless network can be captured "from the air" by intruders. The above mentioned risks threaten were not only in the mobile device itself but also the networks, which the mobile device connects to. It has been identified that the most serious security threats with mobile devices are unauthorized access to data and credentials stored in the memory of the device. This threat can be mitigated only with an appropriate user identity authentication [2]. Access control is especially important for mobile devices.To ensure that only authorized people are able to access the device and the system is the most important point for enhancing the security level in M commerce applications.

The rest of the paper is organized as follows. Section 4 gives the overview of existing biometric technologies and various feature extraction methods for finger print feature extraction. Section 5 will have our proposed SAS signature generation.

4. EXISTING BIOMETRIC TECHNOLOGY AND SOLUTIONS

There are four types of biometric-based security technologies for mobile user identification which is shown in figure 1. They are listed below:

1)Voice recognition,

2) Face recognition,

3) iris recognition and

4) Finger print recognition.

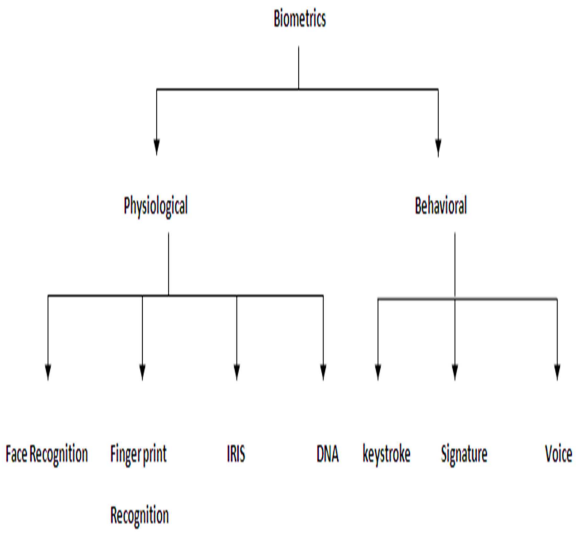


Figure 1: Classifications Biometrics

a) Voice identification:

Voice-based biometric security technology identifies authentic mobile users based on their voice inputs. We all know the limitations produced by the password system and the identity card system (i.e) other people who know our password or has our ID card can gain access to our private documents or cabins. In order to eliminate this type of limitation, the voice identification was introduced. The identifier store a reference voiceprint and this reference are compares the voice produced by the person requesting access. This voice identification technique's accuracy is medium and it is prone

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to errors when there is presence of noise signals [3].

b) Face-print recognition:

Face recognition biometric systems are considered as the most effective security solutions for mobile users which is shown in figure 2. Since every phone comes with a camera, this type of recognition is also widely used. This type of recognition involves taking a facial image of the user and pre-processing & feature extraction are the common steps in enrolment and verification process. During verification, the recognition device compares the image with the image inthe database. First it looks at the overall image and then it looks at the edges of the image. Through this process, it recognizes the userand allows access. The limitations seem to be a big problem here. The image should be captured with good amount exposure to sunlight or some other light source. Its accuracy is above average around 69%.

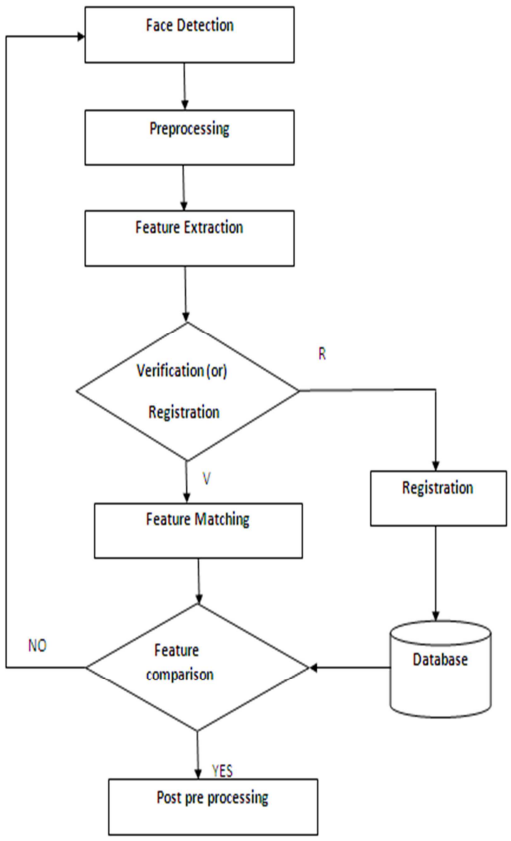


Figure2:Face-print Recognition

c)Iris Recognition:

Iris recognition is another effective biometric security approach. The Iris is the colored part in the eye, located behind the cornea, surrounding the pupil. Iris recognition technology is built around the uniqueness of each iris. The irises are different even in identical twins so there is less possibility for two people to have the same type of iris. Having this concept in mind, the iris recognition was introduced. Firstly each person's iris code is obtained with their permission. Whenever the iris recognition is to be used the iris of the respective person is evaluated. There should be a match between the iris code and the person's iris. Thus, recognition is obtained. This type of recognition has certain limitations [3]. It will produce problems when sunglasses and other glasses are worn during the recognition process. The most advantageous part is that, it alarms the security when there is no match obtained between the person's iris and the iris code.

d) Fingerprint recognition:

The fingerprint technology is the oldest one among all biometric identification. It is based on the series of three dimensional lines, called ridges, and the space between then, called valleys. The ridges and valleys differ from person to person. The recognizer sets points on the reference fingerprint from which the template is extracted. The template is encrypted and saved in the mobile phone. It occupies space. It has higher accuracy when compared to others. The live fingerprint is compared with the reference fingerprint. If they match, then they gain access. Its limitations are due to cleanliness [4]. It can be prevented easily by keeping yourself clean. Since it is less expensive and produces high accuracy results, we are discussing about this type of recognition in detail. The comparison of various biometric security solutions are shown in Table 1. From this comparison we can conclude that finger print authentication is more advantageous than other biometric security solutions.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TABLE I: Comparison between various Biometric Security Solutions

Attributes Vs Security solutions	Finger print Authentication	Voice Reorganization	Face Reorganization	Iris Reorganization
Type of Biometric	Image based	Voice based	Image based	Image based
Hardware Requirement	Finger print sensor	Any standard type speech transducer	Digital camera	Digital camera
Factors affecting the efficiency	Pressure of finger Cut in the finger Cleanliness Aging Blood flow level	External noise Atmospheric effects Aging Cold	Lighting Brightness and contrast Weather	Usage of reading glasses Eye related problems
Accuracy	Very High	Medium	Medium	Very high
Limitations	Quality of Finger print images	Speech patterns of the users and Input Quality	Image quality and sensitivity of camera	Capturing the iris image may need some practice
Cost	Low	Low	Low	High

4.1. Finger Print Feature Extraction Methods

A. Gabor Maps

Gabor texture features have proven to be effective for analyzing remote sensed imagery. They were standardized in 2002 by the MPEG-7 Multimedia Content Description Interface after they were shown to outperform other texture features in which one of the evaluation datasets consisted of remote sensed imagery. Gabor texture features are extracted by applying a bank of scale and orientation selective Gabor filters to an image. A filter bank with R orientations and S scales results in a total of RS filtered images considered differently, this data cube represents an RS dimension feature vector at each pixel location. We term these the set of local Gabor texture featuresfor an image. We form a single global Gabor texture feature by computing the mean and standard deviation of the filtered images. A 2RS dimension feature vector, GaborGLOBAL, is formed as

Gabor GLOBAL= [μ11, σ11, μ12, σ12, . . . ,μRS, σRS] ,

Where μrs and σrs are the mean and standard deviation of f{rs(x, y)}. Finally, to normalize for differences in range, each of the 2RS components is scaled to have a mean of zero and a standard deviation of one across a dataset.

Their system uses a circular tessellation. The circular tessellation is defined by the collection of sectors for a given finger print image. Therefore the use of four concentric bands around the core point is employed. The composition of each band can be approximated by 20 pixels in width and it can be segmented into 32 sectors. Therefore the total contribution will be of 32× 4=128 sectors, resulting in a circle of radius 100 pixels which is the centered core point [5].

The objective of Gabor filters are to obtain both the frequency related and local orientation information from the fingerprint of an image the specific information about the frequency and the orientation information can be obtained by tuning the Gabor filters to the required frequency. This method is very much suitable for extraction of texture based information from an image. These filters are used to extract thedistinguishing features from human iris. The Gabor map method for finger print and iris are shown in figure 3.

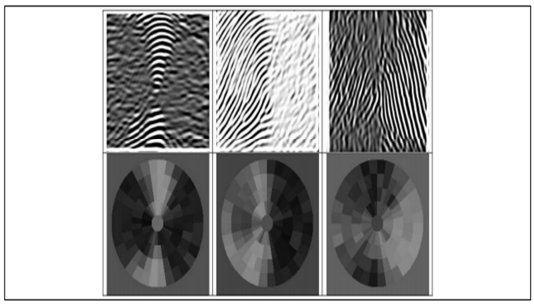


Figure 3:Gobar Map method for Finger Print and Iris

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

B. Minutuae Features

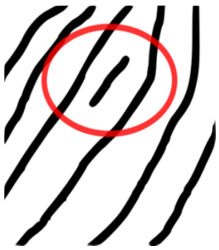
Minutiae features are very important for the analysis of finger prints. This serves as the basis of analysing the different human skin using some imaging technologies. The major classification of minutiae features includes the ridge ending, bifurcation and short ending are shown in figure 4.

Ridge Ending:The point at which a ridge terminates is called ridge ending.

Bifurcation:The point at which a ridge splits into two halves is called bifurcation.

Short ending: Classification of ridges such that ridges are smaller in length when compared with other ridges [6] [7].

Ridge ending Bifurcation



Short ending

Figure 4:Minutuae Features

C. Orientation Maps

The orientation is an angle forms by the rigid inclination and the horizontal lines. As the ridge has no direction, the term orientation are used instead and the angle varies from 0 to 180.Each region of the fingerprint, except the region of singularities, has a common ridge orientation, therefore instead of computing the orientation at each pixel point, generally they are computed for each block [8].

The most simple and a common method used for orientation map are based on gradient computation. Initially,the horizontal and vertical gradient are computed at each pixel using some operator eg.sobel operator, then the image is divided in small blocks of size W×W and computed the angle by analysing the block. This method is fast and performs well for good quality images. For low quality images are necessary to use complex and robust techniques. The original image and oriented images are shown in figure 5.

A B

Figure 5: A. Original image and B. Oriented image

D. Core Point Detection

The core point in a finger print image can be detected by two ways. This core point can be detected by using core point detection in point care method and core point detection using slope. The core point of a fingerprint image can be detected using multiple techniques also [8]. First, we divide the input fingerprint image into non overlapping blocks with size W×W and compute the gradient $G_{x\,(u,v)}$ and $G_{y\,(u,v)}$ at each pixel (i, j) which is the centre of the block [10]. The gradient operator can be chosen according to the computational complexity. By this way the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

optical core point can be detected and is shown in figure 6.

E. Processing Time

Besides considering classifications accuracy, it is also very much important to take account the processing time of various algorithms. We implement the above four feature extraction algorithms using Matlab vR2012a and we evaluate the average processing time of each algorithm. From this evaluation we can conclude the OM algorithm is taking minimum processing time than Gabor feature extraction method. This comparison is shown in Table 2.

Figure6: Core Point Location

Table 2: Time Processing Comparisons of various Feature extraction methods

Method	Average Processing Time (msec)
Orientation Maps	30
Minutiae maps	150
Core point Detection	1100
Gabor Features	2600

5. NEW KEY-BASED APPROACHES TO MOBILE ACCESS SECURITY

The conventional methods of encoding and decoding messages or data are carried out using the symmetric and asymmetric keys. Now incorporating these existing solutions onto the mobile networks to support mobile accesses encountered several problems in a wireless network working platform. They are a) weak and unreliable connectivity, b) limited processing power and memory, c) limited battery operation time, and d) very limited inputs. To deal with these, there are several approaches to using key-based security techniques.

• Offloading complex computations to a server

• Reducing network traffic with better protocols

•Allowing cryptography algorithms to run in offline (disconnected) modes

• Improving cryptography algorithms

• Adding specialized chips to perform cryptography

An approach that is currently being followed uses symmetric or/and asymmetric key cryptographic techniques neglecting the limitations of mobile devices and networks. In networks like GSM and GPRS, only the private keys are used to perform cryptographic solutions. The private key is stored in the SIM card and a random number is obtained from the service provider.One major disadvantage of this scheme is that it is a complex algorithm and involves a higher processing time [11].

Now, our proposed approach considers a technique of Biometric finger print Authentication with mobile key-based security solutions by modifying the existent Public-key algorithms. These methods involve innovative approach using combinations of cryptographic techniques and Biometric Authentication.

A) Cryptographically protected objects (CryPO)

This method focuses on security at an object-level using cryptographically protected objects. The CryPO requires a Tamper-proof environment whose sole purpose is to store a private key which is not known even to the mobile user. The technique uses a 2-Phase protocol that transfers objects to and from mobile devices. The two phases namely are the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Initialization phase and the Usage phase. In the initialization phase the manufacture publishes the public key to the device but the private key is never published. Also, the authentication certificate is sent to the object user. In the usage phase a request is sent from the object user to the object provider with the identification of the object that needs to be accessed and certified. The object provider encrypts the object using the public key before it is sent to the object user [12].

One main advantage of this method is that the object user cannot decrypt the object owing to the lack of private key. Once the object is downloaded into the mobile device, the mobile device decrypts the object using the private key associated with it. The main problem is to provide an ideal tamper-proof environment which is nearly impossible.

Table 3: Energy Consumption between RSA and ECC

Algorithm (Key length)	Signature Energy cost (million Joules)		Key Exchange Energy cost (million Joules)	
	Sign	Verify	Client	Merchant
RSA(1024)	304	11.90	15.40	304
ECDSA(160)	22.82	45.09	22.30	22.30
RSA(348)	2302.70	53.70	57.20	2302.70

B) Elliptical curve cryptography (ECC)

ECC is an alternative to the RSA algorithm which uses the asymmetric key cryptography used to secure mobile devices. It is an improvement over the Discrete Logarithm cryptography. From the table we can see that for the same level of security the RSA requires more number of bits for the key over ECC. The main criteria are a smaller key associated to enable a faster arithmetic operation and lesser consumption of battery energy. In the battery consumption studies the authors compare two public key mechanisms involving two different key lengths that provide the same security.

The ECC is proved to be 13 times more efficient for signing when comparing RSA with ECDSA. Also, ESDSA has much less energy costs than RSA on server side for key exchanges. The figure provides comparison between RSA and ECC algorithms based on their processing times in signature generation, decryption and encryption times. The raw RSA, RSA with OAEP and RSA with PKCS1 use 2048 bits. The ECC based ECIES uses 256 bits. Clearly, ECC based ECIES is very efficient for generation of key and the disadvantage of its long times required for encryption/decryption times is offset by its efficientfunctionality [12].

C) Server-Aided signatures (SAS)

The computation of the public key signature is usually a CPU intensive operation thus the server aided signature is an efficient approach to offload the intensive security computation to a trusted server side. Here, the public signature is split into two parts; one part holds computed data on server side and the other holds data computed on the mobile side. Also, each part by itself is useless. Only the recombination of the two parts makes a secured signature which allows certification and non-repudiation [13]. We believes that a partially trusted sever is more secure than a fully trusted server owing to the fact that a fully trusted server holds all the data of every user and is more likely for a hack. Another solution to offload intensive processing is called Offline/Online Cryptography or SignCryption [14]. The SAS signature preparations is as follows

First, a client contacts its SEM (security Mediators) and provides the data to be signed as well as a one time ticket.

SEM checks the client's revocation status and, if not revoked, computes a half-signature over the data as well as other parameters (including one time ticket). SEM then returns the results to the client.

Now the client verifies SEM's half signature and produces its own half signature (Finger print

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Feature). Put together, the two respective half signatures and forms a full SAS signature. This flow is shown in figure 7.

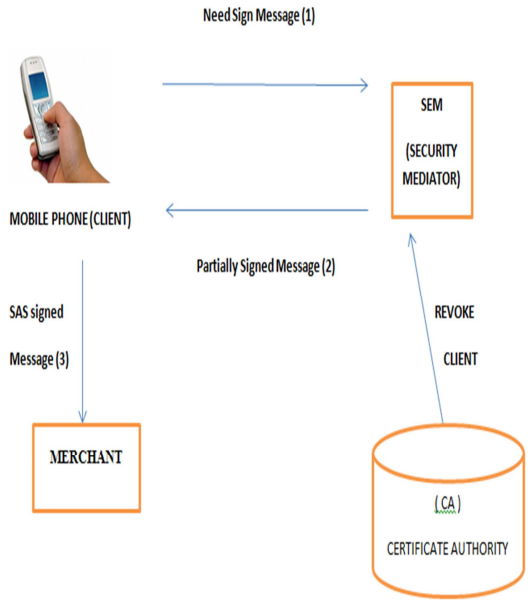


Figure 7: Generation of SAS signature

6. A COMPARISON OF PROCESSING TIMES BETWEEN RSA SIGNATURE AND SAS SIGNATURE

We compared the performance of the SAS algorithm with plain RSA algorithm signatures. According to these comparisons the process of the signature generation is faster in SAS algorithm than the plain RAS generation. The difference in signature generation times between the two algorithms is associated with the Processor speed. Slower the processor, the bigger is the difference between the two signature generation times. For example, for 1024 bits on a 233 MHz processor, RSA takes 40.3 ms, but SAS takes only 13.3 ms which are shown in figure 8 & 9. On the other hand, for faster processors, the difference is not so significant. This suggests that SAS is not efficient for very high-end devices. But utilizing the SAS algorithm in a network involving heterogeneous devices results in a lesser computational power on a mobile device.

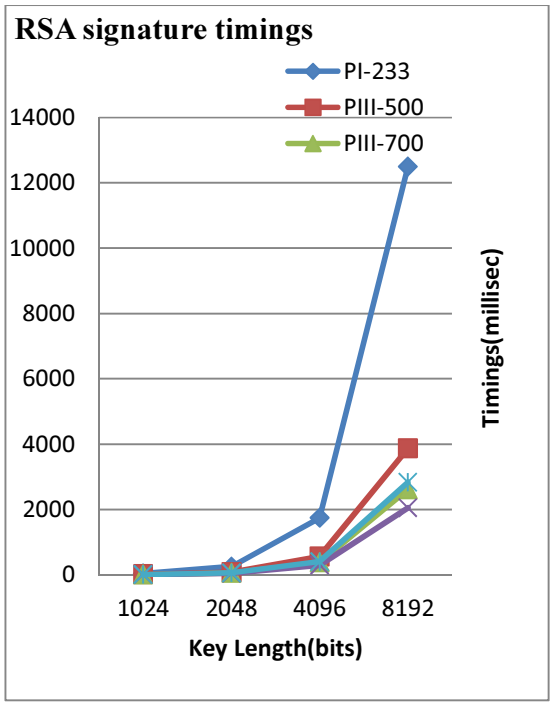


Figure 8: Generation of RSA signature timings

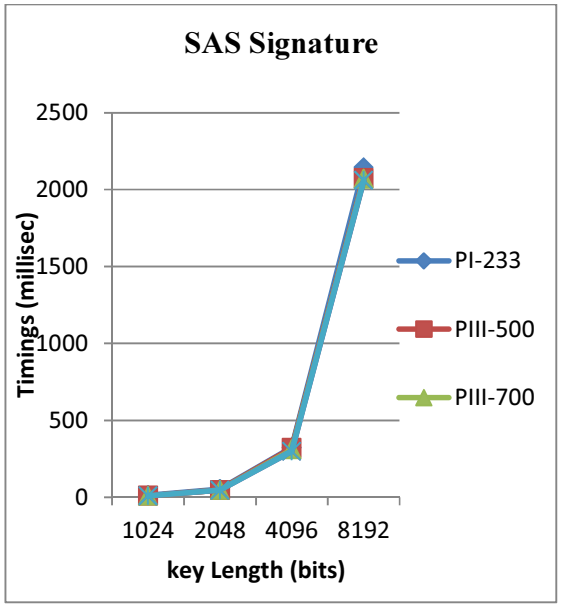


Figure 9: SAS signature timings

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

7. RESULTS AND DISCUSSIONS

Processor speed(MHZ)	Key Length(bits)			
	1024	2048	4096	8192
PI-233	43.3	82.4	352.5	2173.4
PIII-500	39.1	76.3	332	2100.2
PIII-700	38.5	75.1	329	2089.6
PIII-933	38.5	75.2	329	2090
PIV-1.2GHZ	38.5	75.4	329	2091

From our simulation we conclude that the SAS based biometric authentication will give more security for the M commerce applications. Also in the aspect of processing time, the SAS based OM Method is less than RSA based OM method which is shown in figure 10 & 11. For higher end processors the processing time is almost constant in SAS based OM method.

TABLE 4

Total time required for Full Signature generation using RSA and OM method

Processor speed(MHZ)	Key Length(bits)			
	1024	2048	4096	8192
PI-233	70.3	282.7	1771.7	12520
PIII-500	44.6	115.6	592.8	3903.3
PIII-700	39.2	85.7	407.8	2647.5
PIII-933	37.3	73.9	324.7	2082
PIV-1.2GHZ	39.3	88.7	431.2	2865

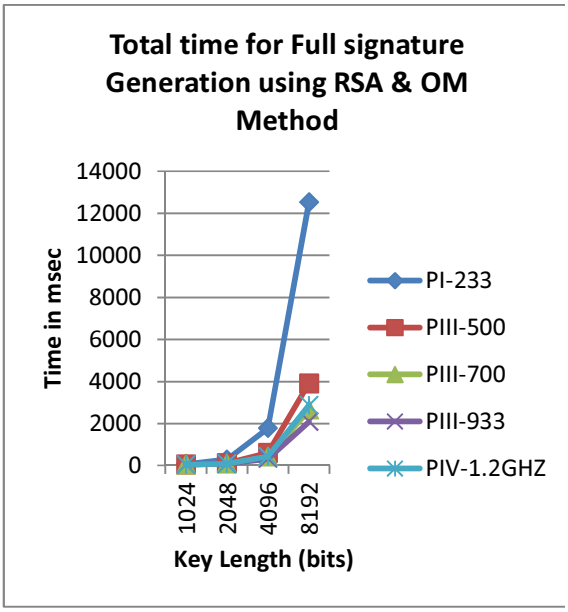


Figure 10: Total Time for full signature generation using RS4 based OM method

Table 5:

Total time required for Full Signature generation using SAS and OM method

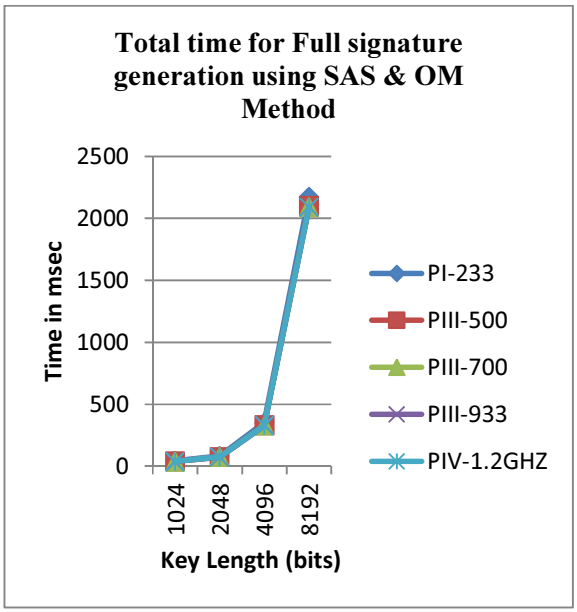


Figure 11: Total Time for full signature generation using SAS based OM method

7. CONCLUSION

The analysis points towards an improved method of mobile access for the purpose of m-commerce. The results of simulation indicates that the SAS based OM method requires less time as compared to RSA based OM method in terms of processing. For higher end processors the processing time is almost constant in SAS based OM method. Therefore the framework is better suited to m-commerce applications with respect to security and processing delay. Even though SAS is more advantageous to provide security solution for M Commerce application but we face the limitation that signature generation timings are almost constant for faster and higher end processors.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1]. RajaniDevi.T, Importance of Cryptography in Network Security: International Conference on Communication Systems and Network Technologies, 2013.

[2]. Javier Galbally, Sebastien Marcel and Julian Fierrez Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition: IEEE 2013.

[3]. Mahmood Al-khassaweneh, Bashar Smeirat and Talal Bin Ali, A Hybrid System of Iris and Fingerprint Recognition for Security Applications: IEEE conference 2012.

[4]. Vincenzo Conti, Carmelo Militello, FilippoSorbello and Salvatore Vitabile, A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal BiometricIdentification Systems : IEEE, July 2010, vol. 40.

[5]. Ching-Han Chen; Ching-Yi Chen Optimal fusion of multimodal biometric authentication using wavelet probabilistic neural network, Customer Electronics (ISCE), 2013 IEEE 17th International Symposium on June 2013, pp-55-56.

[6]. Raut, R.D.; Kulkarni, Sujata; Gharat, Neha N. Biometric Authentication Using Kekre's Wavelet Transform, Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on Jan 2014, pp 99-104.

[7] Yager N, Amin A (2004) Fingerprint verification based on minutiae features: a review. Pattern Anal Appl 7:94–113, 2004.

[8]. Qian Tao and Raymond Veldhuis, Biometric Authentication System on Mobile Personal Devices : IEEE, Vol. 59, No. 4, April 2010.

[9]. Li Huixian and Pang Liaojun, A Novel Biometric-based Authentication Scheme with Privacy Protection: International Conference on Information Assurance and Security, 2009.

[10]. Ratha N, Karu K, Chen S, Jain A (1996) A real-time system for large fingerprint databases. IEEE Trans Pattern Anal Mach Intell 18(8):799–813, 1996.

[11] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, \RFC2560: Internet public key infrastructure online certicate status protocol - OCSP," June 1999.

[12] R. C. Merkle, A digital signature based on a conventional encryption function," in Advances in Cryptology { CRYPTO '87 (C. Pomerance, ed.), no. 293 in Lecture Notes in Computer Science, (Santa Barbara, CA, USA), pp. 369 - 378, Springer-Verlag, Berlin Germany, Aug. 1988.

[13] N.Asokan, G. Tsudik, and M. Waidner, Server-supported signatures," Journal of Computer Security, vol. 5, no. 1, 1997.

[14] D. Boneh, X. Ding, G. Tsudik, and B. Wong, Instanteneous revocation of security capabilities," in Proceeding of USENIX Security Symposium 2001, Aug. 2001.