

Research Article

A Robust Biometric Authentication and PIN Distribution Technique for Secure Mobile Commerce Applications

¹R. Arun Prakash, ²K.M. Mehata and ³C. Chellappan

¹Department of Computer Science and Engineering, University College of Engineering Ariyalur, Tamil Nadu, India

²Department of Computer Science and Engineering, B.S. Abdur Rahman University, Chennai, Tamil Nadu, India

³Department of Computer Science and Engineering, GKM College of Engineering and Technology, Chennai, Tamil Nadu, India

Abstract: In a mobile emerging world, user authentication, service provider authentication and security is very important in mobile commerce. User authentication is performed by using fingerprint based biometric methodology. Existing system used for Mobile purchasing/payment services in handheld devices does not analyze fingerprint matching and feature extraction techniques in an efficient way. Also the existing system is not secure and accurate for m-payments applications. We propose secure, efficient and accurate m-commerce architecture for m-commerce applications. This involves fusion of Minutiae Maps (MM) and Orientation Maps (OM) for fingerprint feature extraction. The fingerprint is sent to the biometric server in a secure way using Discrete Wavelet Transform (DWT) data hiding method. User fingerprint will be checked and compared using MM and OM methods to figure out the fingerprint threshold matching score. If the threshold is 80-99% PIN distribution process is initiated, otherwise user authentication is failed. The user PIN is converted into a unique sequence and divided into two parts. Along with the user PIN, user IP address, time stamp, user ID are encrypted using RC4 (stream cipher) algorithm. Also a hash function is appended to the cipher text using Secure Hash Algorithm (SHA4). One half is verified by the authentication server and the other half is verified by the external server. After verification both the servers sends only OK message to the bank. This study looks to provide a high secure and efficient solution for m-commerce applications.

Keywords: Biometric server, discrete wavelet transform, m-commerce, minutiae maps, orientation maps, secure hash function, stream cipher

INTRODUCTION

Mobile commerce (M-commerce) is a type of e-commerce technology attracted billions of users over the past few years. M-commerce is an emerging technology, where users can interact with the service providers through a mobile device with wireless network for information/service request, retrieval and transaction process. M-commerce is defined as “The delivery of trusted transaction services over mobile devices for the exchange of goods and services between consumers, financial institutions and merchants” (Arun Prakash *et al.*, 2014).

Mobile devices also have the potential to provide unauthorized users with access to corporate networks and to introduce viruses and other harmful software into these networks (Han and Schyndel, 2012). M-commerce is subjected to several security vulnerabilities such as Theft/Loss of device and

information, Clone, Hijacking, Malicious software (Malware), Phishing, and Wireless connection vulnerabilities (Arun Prakash *et al.*, 2014). 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 (Han and Schyndel, 2012). 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.

Enabling high security is considered as the success of M-commerce applications. Thus implementing high security in M-commerce applications would invite

Corresponding Author: R. Arun Prakash, Department of Computer Science and Engineering, University College of Engineering Ariyalur, Tamil Nadu, India

This work is licensed under a Creative Commons Attribution 4.0 International License (URL: <http://creativecommons.org/licenses/by/4.0/>).

Table 1: 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

many users to perform m-payment/transactions immediately and irrespective of infrastructures.

In this study, we examine fingerprint based biometric authentication for performing M-payment like shopping, bill/bank payments, ticket booking etc. To recognize a unique person, the human trait should be unique and not subject to change. The comparison of various biometric security solutions are shown in Table 1. This comparison will conclude that the finger print authentication is more advantageous than other biometric security solutions. The fingerprint authentication is more accurate and low cost when compared with other voice, face and iris recognition technologies.

This study is focused on secure M-commerce architecture using biometric devices and enabling high security/accuracy during transaction in M-commerce applications. To provide high secure M-commerce environment we can integrate biometric sensor in all smart mobile devices and the fingerprint feature are extracted using orientation maps and Minutiae maps techniques. The fingerprint image is secured using Discrete Wavelet Transform technique while transmitting to the biometric server. Adding to it, this paper proposes a unique sequence formation of the user PIN and along with the sequence, user ID, time stamp and user IP address are encrypted using RC4 (stream Cipher) algorithm. Also we focus on implementing secure m-commerce architecture for m-payments. Thus implementing the whole architecture is one of the best solutions to ensure confidentiality of the transactions among the m-commerce users.

LITERATURE REVIEW

Recent study states by the year 2017, 3 billion smart phones and 1 billion tablets will be used by the users globally. Also the online retail sales through mobile devices will grow from 11 to 25% by the year 2017 (Earley, 2014).

Mobile commerce has emerged and acquired many users in the last five years. In fact, Bank of America estimates US \$67.1 billion transactions will be done using mobile devices by the year 2015. Now, even banks and trading firms developed mobile apps to support online banking and trading. The main driver for online commerce is to provide strong security practices (Chang *et al.*, 2014).

Examining m-identity based approach can be found in Han and Schyndel (2012). This paper examines biometric Based Digital Identity Authentication (BDIA) based m-identity has been proposed for m-commerce application. To enhance security during m-commerce transactions a unique watermarking is generated for each biometric image taken by the mobile camera. M-identity has the information about the user biometric feature and respective mobile device. Authentication is passed only if both the parameters match.

Rajanna *et al.* (2010) presented finger print feature extraction using Orientation map method has the least processing time and high accuracy. OM method is the fast and effective technique in which image is divided in small blocks of size $W*W$ and computed the angle (0-180) by analyzing the block.

Ponnarasi and Rajaram (2012) analyzed Minutiae detection using core point of the fingerprint is more accurate. For the research fingerprint Database FVC2002 (DB1-a) was used and minutiae points from 100 fingerprints were identified. Thus they came to a result stating average performance of this technique was 92% consuming lesser time. But the false minutiae point was not detected in this algorithm.

For secure transaction on the WAP gateway 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 (Asokan *et al.*, 1996).

The secure pin distribution is discussed in Improved Pin Distribution Techniques in m-commerce System (Arunprakash *et al.*, 2011). This paper states high security in m-commerce application is achieved by using a more secure WAP gateway by framing double encryption model. The pin will be split into two half's and encrypted send to two servers. In the server side the pin will be decrypted and checked for matching score. If the matching score is good an acknowledgement message stating OK will be passed to the other server and finally the transaction is initiated.

The recent review on biometric mechanism for security can be found in Belkhede *et al.* (2012). Here

the extracted finger print is matched using core point detection technique. Also RSA algorithm is proposed for securing the finger print template on the WAP decryption can be done by a private key known only by the respective user. RSA takes large encryption time and memory usage (Shashi and Rajan, 2011).

Singhal and Raina (2011) stated symmetric key algorithms are very fast in nature. Analyzing the CPU process time, memory utilization, time taken for encryption and decryption RC4 is fast and efficient when compared with AES.

METHODOLOGY

Proposed architecture: The proposed architecture focuses on secure transactions in m-commerce among users, financial institutions (bank) and service providers (merchant). The overall system design shown in Fig. 1:

- Customer (user) sends the Product and customer details to the Service provider through the WAP gateway.
- Service provider verifies the Product and customer details and sends to the Biometric server through the WAP gateway.
- Biometric Server requests the customer details (Fingerprint) to the customer.
- Customer sends the fingerprint image and details to the Biometric server through the WAP gateway.

gateway. RSA algorithm is asymmetric which means it encrypts with a public key known by all users and

- Biometric server sends the Comparison result details to the Service provider. Analyzing the matching score service provider decides access or denies the process of customer.
- Once the user is authenticated, the Pin distribution process is initiated based on the threshold level. OTP authentication is sent to the user by the service provider.
- After authentication process the user PIN (Personal Identification Number), User ID, Time stamp and IP address are send to the Authentication and External server in secure way. Also SHA (Secure Hash Algorithm) is used to be sure that no one has messed with the PIN.
- The result is sent to the bank for transaction process as an OK or Not OK message.
- Merchant receives the payment from the financial institution.
- Finally, merchant delivers the order to customer.

The customer/user requests the product/service details to the merchant. The merchant will transfer the user details to the biometric server for user authentication. The biometric server requests the fingerprint information of the m-commerce user. The m-commerce user responds with his/her respective

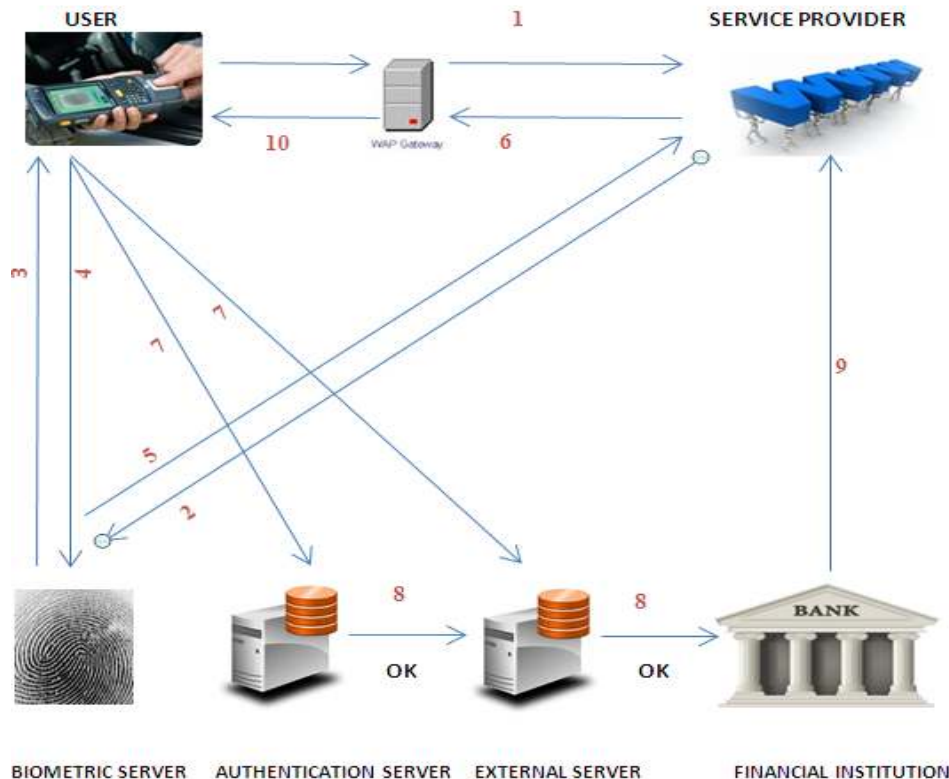


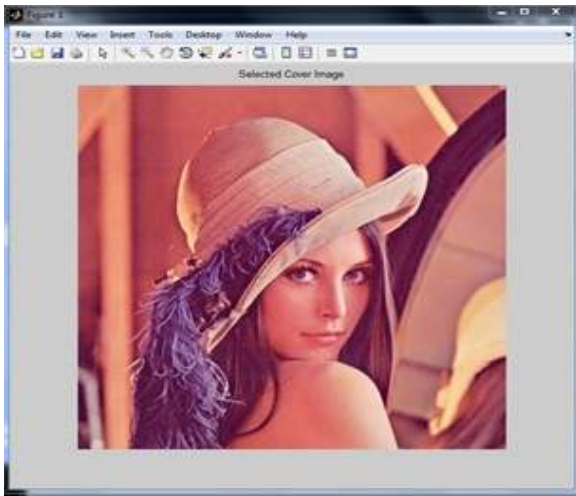
Fig. 1: Overall M-commerce proposed architecture diagram

fingerprint image. The user provides the fingerprint image using the biometric sensor integrated with all the smart mobile devices. Thus the fingerprint image will be hidden in a cover image based on DWT technique (Abdelwahab and Hassaan, 2008) and sent to the Biometric server through WAP gateway for authentication.

In the authentication stage, the embedded secret image can be extracted with high visual quality. The user finger print feature will be extracted by fusion of two efficient feature extraction algorithms i.e., Orientation Maps (OM) and Minutiae Maps (MM). Thus the fusion of two different algorithms will enhance security, accuracy and performance. The finger print image is compared with the database to find the matching score. The matching score is sent to the merchant. If the matching score is above the threshold value the user will be requested to provide the unique

PIN number. If the matching score is lesser than the threshold value the user authentication will be failed and the user will not be allowed to do the purchase.

In the OTP stage the secure transaction on the WAP gateway is provided by splitting the 16 byte public key signature i.e., 128 bit into two parts. Each part will be converted into a unique sequence and encrypted. See below section for sequence formation. One part will be encrypted and send to authentication server and the other part will be encrypted and sent to the external server. RC4 algorithm is used for encryption and decryption. RC4 algorithm provides high security by invoking and encrypting all essential parameters like IP address, Timestamp, User ID along with the PIN number which is collectively termed as a token. A hash function using SHA is appended to this token to make sure no one has tried to mess up with it.



(a)



(b)



(c)



(d)

Fig. 2: (a) Cover image, (b) input image, (c) stego image, (d) extracted image

Meantime the merchant will be verified by the financial institution. Once both the authentication and external servers positively acknowledges with OK message the bank initiates the transaction. Finally merchant receives the payment from the bank and delivers the required product/service to the customer. Also in our architecture we can verify the user by pulling the user IP address, timestamp in the external server. The overall system design is shown in Fig. 1.

BIOMETRIC SERVER

User requisition: The m-commerce user requests the product/service details to the service provider (Merchant). The service provider verifies the user information and product/service details from the user. Once the verification is over, the merchant transfers the user details to the biometric server for fingerprint authentication.

Reversible fingerprint hiding: Biometric server receives the user information i.e., Customer identification number from the merchant. Biometric user verifies the user information and requests the m-commerce user to provide his/her fingerprint. The user responds by providing the fingerprint image using the biometric sensor integrated with all the smart mobile devices. The fingerprint image is hidden in a cover page using Discrete Wavelet Transform. The Stego image quality is analyzed by MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio):

$$PSNR = 10\log_{10} (R^2/MSE)$$

$$MSE = \sum M, N [I_1(m, n) - I_2(m, n)]^2 / M * N$$

where, M and N are the numbers of row and columns in the input image. R is the maximum pixel value. I1 is the cover image and I2 is the stego image. The lower MSE value indicates a better image quality (lesser distortion in the cover image) and the higher the PSNR value the better the quality of the image (Fig. 2). The stego image is sent to the Biometric server through WAP gateway for authentication.

The MSE and PSNR values are calculated below:

MSE Value during embedded: 4.4361
 PSNR Value during embedded: 191.7393
 MSE Value during extraction: 28.3855
 PSNR Value during extraction: 8.3759

Biometric verification: To improve the image quality, enhancement steps are essential before performing feature extraction. The process of fingerprint feature extraction is shown in Fig. 3.

Histogram equalization: Histogram equalization increases the overall contrast of the images, especially when the usable data of the image is represented by close contrast values.

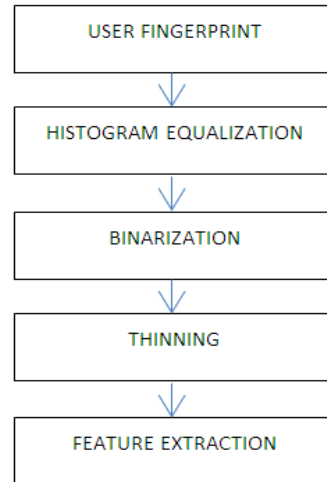


Fig. 3: Finger print quality enhancement steps



Fig. 4: (a) Input image from IIIT-Delhi fingerprint database, (b) binarized image

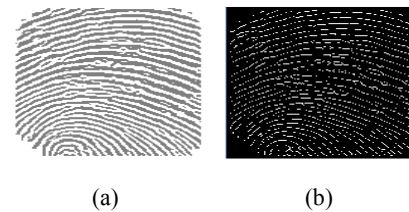


Fig. 5: (a) Input image from IIIT-Delhi fingerprint database, (b) thinning image

Binarization: Binarization converts a grey scale image to a binary image. In a binary image the pixel value will be described as either 0 or 1 (255). Binarization will enhance the ridges and valleys in the fingerprint image and this will be easy for extracting the feature of the respective fingerprint using minutiae algorithm (Fig. 4).

Thinning: Thinning is a technique applying morphological operations i.e., structural element to a binarized image. In this basic morphological operations like dilation and erosion are processed. Dilation is a process which adds pixels to the boundary in an image and sets the maximum value of all pixels. Erosion is a process which removes pixels on the boundary and sets the minimum value of all pixels (Fig. 5).

Feature extraction: In the proposed system, finger print feature extraction is processed by fusing two efficient algorithms OM and MM. The input image is

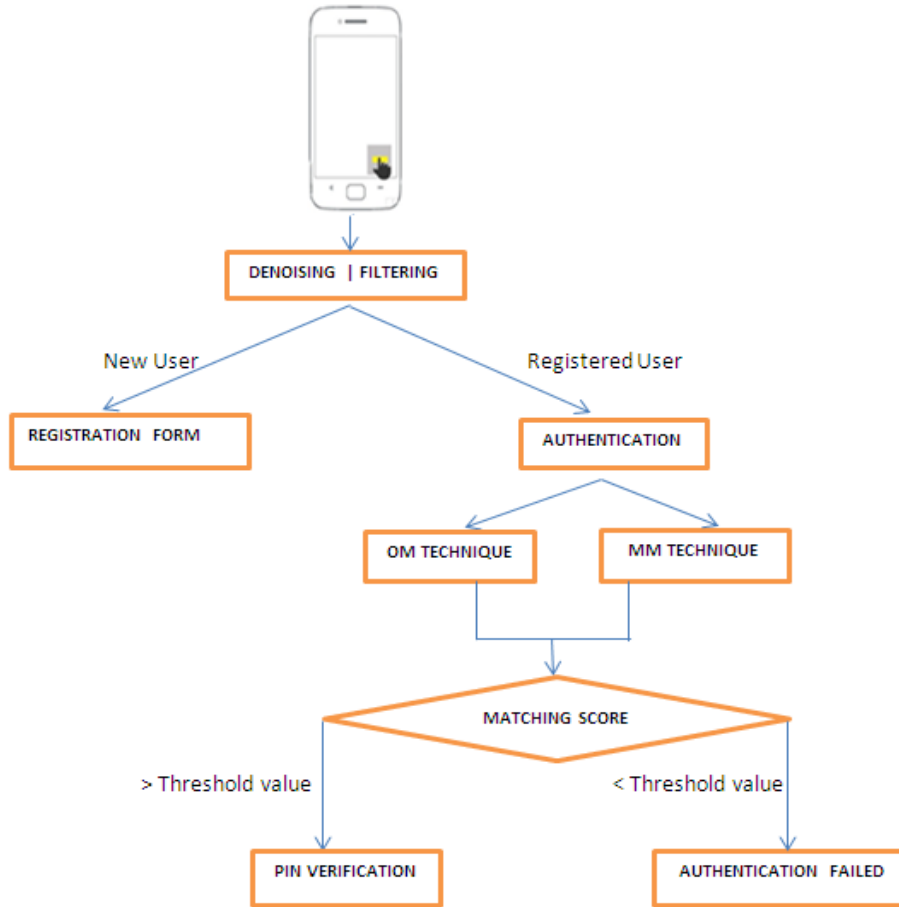


Fig. 6: Proposed m-commerce authentication system

processed using OM and MM methods simultaneously and the output images are saved separately for each user.

Orientation Maps (OM): Orientation maps technique represents the direction of the ridges. The fingerprint image is divided into number of non-overlapping blocks and an orientation representative of the ridges in the block is assigned to the block based on analysis of grayscale gradients in the block. The block size depends on the inter ridge distance (Kulkarni *et al.*, 2005). The orientation field is given by:

$$\Theta(i, j) = 0.5 \tan^{-1} \left(\frac{Vx(i, j)}{Vy(i, j)} \right) \quad (1)$$

$$Vx(i, j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=i-w/2}^{i+w/2} 2Gx(u, v) Gy(u, v) \quad (2)$$

$$Vy(i, j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=i-w/2}^{i+w/2} (G2x(u, v) G2y(u, v)) \quad (3)$$

where, w is the size of block or cell. Gx and Gy are the gradient magnitudes in x and y directions, respectively.

Based on the above equation a set of templates are stored for each fingerprint class according to Galton-Henry classification scheme (Henry, 1900). Overall 95% of the fingerprint can be classified in five classes. The five classes are as follows, Arch (A), Tented arch (T), Right loop (R), Left loop (L) and Whorl (W). The T and A classes may be combined into one single class resulting in four classes (Fig. 6). The orientation algorithm provides pattern which are easy to identify the classes (Table 2).

Minutiae Maps (MM): Minutiae features are very important for fingerprint analysis. Minutiae classification includes ridge termination, bifurcation and short ending. Ridge termination is the point at which ridge ends. Bifurcation is the point at which ridge splits into two halves. Short ending is the ridge smaller in length when compared to other ridges.

Minutiae features can be extracted from the resultant image obtained after binarization and thinning techniques. In this algorithm we consider the white pixels as 1 and black pixels as 0. The algorithm uses 3×3 windows to scan the image and the bifurcation and termination in the final output image shall be

Table 2: Orientation maps and minutiae calculation for few images from IIT-Delhi fingerprint database













Fingerprint image	Minutiae image	Orientation map image	Termination	Bifurcation	Total number of minutiae
			32	12	44
			22	7	29
			31	45	76
			35	33	68

Table 3: Sequence table

	9	8	7	6	5	4	3	2	1	0
1	Z	Y	X	W	V	U	T	S	R	Q
2	t	S	R	Q	p	o	n	M	l	K
3	P	O	N	M	L	K	J	I	H	G
4	a	B	C	D	c	f	g	H	i	J
5	@	#	\$	&	/	+	\	=	y	Z
6	A	B	C	D	E	F	u	V	w	X

represented by a dot. Also the concept of Crossing Number (CN) is applied for extracting the minutiae (Ponnarasi and Rajaram, 2012). The CN for a pixel P is calculated as follows:

$$\begin{aligned}
 &P_4 \ P_3 \ P_2 \\
 &P_5 \ P \ P_1 \\
 &P_6 \ P_7 \ P_8 \\
 &CN = 1 / 2 \sum_{i=1}^8 |P_i - P_{i+1}|
 \end{aligned}$$

where, P_i is the binary pixel value in the neighborhood of P with $P_i = (0 \text{ or } 1)$ and $P_9 = P_1$. Based on the CN value, we can consider the minutiae point will have ridge ending or bifurcation (Table 2).

Fingerprint matching: The user fingerprint image is checked with the database for matching score. The performance of the fingerprint is determined using two parameters False Match Rate (FMR) and False Non Match Rate (FNMR). False match occurs when an unregistered finger is falsely matched with a registered finger and false non match occurs when an already enrolled finger is not recognized by our system. The matching threshold is carefully chosen to allow the maximum percentage of false minutiae in the match. The matching score of both the algorithms are sent to the merchant. If the matching score is above the threshold value the user will be initiated to provide the unique PIN number. If the matching score is lesser than the threshold value the user authentication will be failed.

Pin distribution and authentication: For secure PIN distribution we propose a unique sequence which is encrypted using RC4 algorithm and sent to the authentication and external servers for verification. In

this system all important details of the user namely user id, timestamp, PIN number and user IP address (collectively termed as a token) are obtained. Our architecture proposes high secure PIN distribution technique by splitting the 4 digit PIN number into two parts i.e., 2 digits each and forming a sequence using our sequence (Table 3). Each part separately will be processed to produce the decimal sequence number. The PIN distribution is shown in Fig. 7.

Recently database query management plays an important role because whenever the new data is hit the administrator should know whether the actual user is only hitting the database and initiating the transaction. Hence our architecture obtains user id, time stamp and IP address and monitored whenever the query is processed by the user. Our sequence provides an efficient token system using sequence (Table 3).

For example sequence formation for a PIN number 1992 is as follows, randomly we generate 4 digit numbers for odd/even remainders. Randomly consider 1643 odd remainders and 2541 for even remainders. The PIN number will be converted to the base 10 i.e., $1992/10$. The remainder will be 2. So we will consider the 4 digit number 2541 for the sequence. Considering both PIN and digit numbers i.e., 1992 and 2541, the final sequence is framed mapping the values using the sequence table.

Sequence formation:

In the sequence table, check column 1 against row 2. The coincidence value is l.

In the sequence table, check column 9 against row 5. The coincidence value is @.

In the sequence table, check column 9 against row 4. The coincidence value is a.

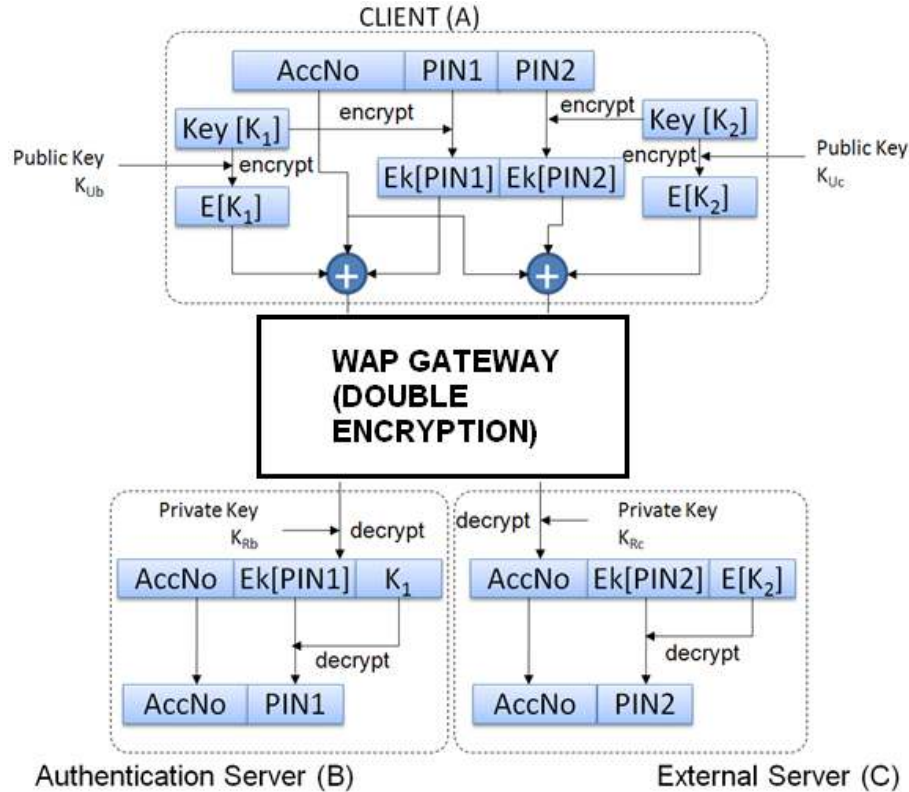


Fig. 7: Proposed PIN distribution architecture

In the sequence table, check column 2 against row 1. The coincidence value is S.

The final sequence is l@ for 19 and aS for 92 after splitting into two parts. This sequence is encrypted using RC4 and sent to the corresponding servers for verification. Also a hash function is appended to the cipher text using SHA to avoid intrusion.

The final sequence along with timestamp, user id, IP address is encrypted and sent to the external server. The authentication server verifies the 2 digit PIN number with the database and passes only the acknowledgement OK or NOT OKAY to the authentication server. The external server checks the acknowledgement from the authentication server and the 2 digit PIN number and passes the acknowledgement OK or NOT OKAY to bank for initiating the transaction. Once both the servers positively acknowledges with OK message the bank initiates the transaction. In the external server we can pull the m-commerce user IP address and timestamp and verify the user activities.

Dataset: In our experiments, the database used is obtained from publicly available in IIIT-Delhi fingerprint database (Sankaran *et al.*, 2012). The IIIT-D latent fingerprint database exclusively consists of only

latent fingerprint impressions. The dryness of the skin ridge is varied to get multiple impressions. These images are 500 and 1000 pixel/inch. The 500 ppi are the slap images captured using Crossmatch L1 scan. The 1000 ppi images are captured using SecuGen Hamster IV.

EXPERIMENTAL RESULTS

The fingerprint feature extraction and reversible data hiding is carried out using MATLAB v6.5.0. While the encryption, PIN distribution and SHA authentication is carried out in mobile environment using Android application. In the mobile environment we tried to identify and compare the performance time among four algorithms namely AES, RC4, 3DES and DES using the same user PIN (Fig. 8). The performance time is completely dependent on the processor speed and RAM.

The time is analyzed for processing the sequence and forming the cipher text using Sony C6602 (Quad core 1.5 GHZ, Qualcomm, Android OS v4.1.2 Jellybean, 2 GB RAM) which is shown in Table 4.

The time analyzed for processing the sequence and forming the cipher text using Moto G (Quad-core 1.2 GHz Cortex-A7 Android OS v4.4.4 (KitKat), 1 GB RAM) which is shown in Table 5 and Fig. 9.

Table 4: Comparative execution time between RC4, AES, DES and DES in sony C6602

File size	RC4 (msec)	AES (msec)	DES (msec)	3DES (msec)
File 1 (3 byte)	0.0787	0.0970	0.1464	0.1856

Table 5: Comparative execution time between RC4, AES, DES and DES in moto G

File size	RC4 (msec)	AES (msec)	DES (msec)	3DES (msec)
File 1 (3 byte)	0.0795	0.0985	0.1475	0.1872

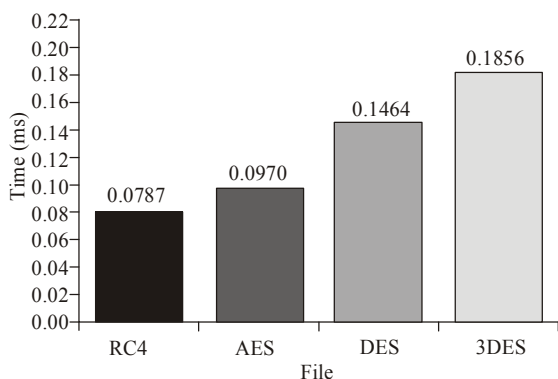


Fig. 8: Execution time between RC4, AES, DES and 3 DES in sony C6602

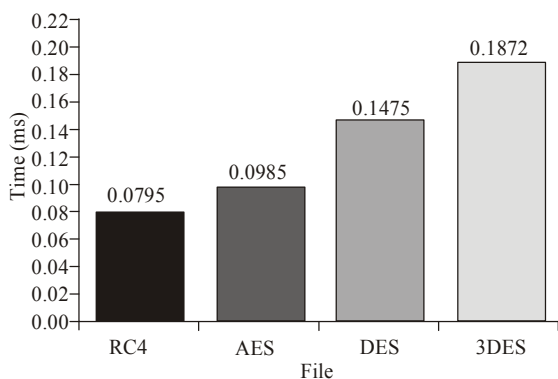


Fig. 9: Execution time between RC4, AES, DES and 3 DES in moto G

CONCLUSION

User authentication is important in M-commerce applications to ensure the communicating entity is the exact user and our proposed architecture ensures using fingerprint analysis. The fingerprint analysis is effectively performed by fusion of two algorithms namely Minutiae Maps (MM) and Orientation Maps (OM). By fusing and implementing both algorithms the finger print process is more accurate and effective. Also the fingerprint is sent to the biometric server through WAP gateway in a secure way using DWT data hiding technique. To add more security we introduce secure PIN distribution process using our proposed PIN distribution architecture, unique sequence formation, OK message concept, RC4 encryption algorithm and SHA algorithm for message authentication.

The execution time is analyzed and compared among encryption algorithms namely DES, 3DES,

AES, RC4 for processing the PIN split up, unique sequence and forming the cipher text in Sony C6602 and Moto G. The result shows that RC4 algorithm is faster and more effective in processing time when compared with other algorithms. Thus the proposed architecture ensures complete reliable and secure transaction for m-commerce users.

ACKNOWLEDGMENT

My sincere thanks to Stigmata Techno Solutions to complete this study.

REFERENCES

- Abdelwahab, A.A. and L.A. Hassaan, 2008. A discrete wavelet transform based technique for image data hiding. Proceeding of the National Radio Science Conference (NRSC'08), pp: 1-9.
- Arunprakash, R., K.M. Mehata and C. Chellappan, 2011. Improved pin distribution techniques in M-commerce system. Proceeding of the 3rd International Conference on Machine Learning and Computing.
- Arun Prakash, R., K.M. Mehata and C. Chellappan, 2014. A novel hybrid authentication method based on orientation maps and server aided signature for M commerce secured transactions. J. Theor. Appl. Inf. Technol., 64(1): 84-94.
- Asokan, N., G. Tsudik and M. Waidner, 1996. Server-supported signatures. J. Comput. Secur., 5: 131-43.
- Belkhede, M., V. Gulhane and P. Bajaj, 2012. Biometric mechanism for enhanced security of online transaction on android system: A design approach. Proceeding of the 14th International Conference on Advanced Communication Technology (ICACT, 2012). PyeongChang, pp: 1193-1197.
- Chang, J.M., W. Joseph and H. George, 2014. Mobile commerce. IEEE IT Prof., 16(3): 2-3.
- Earley, S., 2014. Mobile Commerce: A Broader Perspective. IT Prof., 16(3): 61-65.
- Han, F. and R.V. Schyndel, 2012. M-identity and its authentication protocol for secure mobile commerce applications. In: Xiang, Y. et al. (Eds.), CSS, 2012. LNCS 7672, Springer-Verlag, Berlin, Heidelberg, pp: 1-10.
- Henry, E., 1900. Classification and Uses of Fingerprints. Routledge, London.

- Kulkarni, J.V., R.S. Holambe and D.P. Bhushan, 2005. Fingerprint feature extraction: A review. Proceeding of the National Conference on Signal Processing, Communication and Control (SPCCN01-2005). Vishwakarma Institute of Technology, Pune, pp: 379-382.
- Ponnarasi, S.S. and M. Rajaram, 2012. Impact of algorithms for the extraction of minutiae points in fingerprint biometrics. *J. Comput. Sci.*, 8(9): 1467-1472.
- Rajanna, U., A. Erol and G. Bebis, 2010. A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion. *Pattern Anal. Appl.*, 13(3): 263-272.
- Sankaran, A., M. Vatsa and R. Singh, 2012. Hierarchical fusion for matching simultaneous latent fingerprint. Proceedings of the IEEE 5th International Conference on Biometrics Compendium, IEEE Biometrics: Theory, Applications and Systems, pp: 377-382.
- Shashi, M.S. and M. Rajan, 2011. Comparative analysis of encryption algorithms for data communication. *Int. J. Comput. Sci. Technol.*, 2(2): 292-294.
- Singhal, N. and J.P.S. Raina, 2011. Comparative analysis of AES and RC4 algorithms for better utilization. *Int. J. Comput. Trends Technol.*, 2(6): 177-181.