Asian Journal of Information Technology 15 (2): 243-254, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Enhancing Secure Transaction and User Authentication Method Based on Fingerprint Mechanism Using Fuzzy Logic Amalgam Encryption for PIN Distribution Process in M-Commerce

[1]B. Vanathi, [1]K. Shanmugam and [2]V. Rhymend Uthariaraj
[1]Department of CSE, Valliammai Engineering College, Kattankulathur, Chennai, India
[2]Anna University, Guindy, Chennai, India

Abstract: In a speedy technology, mobile commerce process is one of the best process compared to E-commerce. The major factors are security, authentication, confidentiality and integrity to which have to be focused successfully achieve M-commerce to be challenging one. In existing concepts, the lot of security and authentication schemes is provided. Even though, they need more authentication and security for the mobile purchasing, mobile payment and mobile banking schemes. The proposed system consists of biometric fingerprint authentication, using fuzzy logic to verify the fingerprint, find out the fingerprint threshold level. Based on the fingerprint threshold level the more authentications is provided by SMS authentication and One Time Password (OTP). Service provider (merchant) authentication, double encryption model, RC4 algorithm for encryption. Amalgam encryption (3-DES+RC4) is used for secure PIN distribution process. This amalgam encryption is increasing the secrecy values. The proposed RC4 algorithm has an improvement factor of 76.2% over AES algorithm. Amalgam encryption is better than other Block Cipher and Stream Cipher algorithm. This leads to the more security and authentication in mobile purchasing and payment process.

Key words: Mobile commerce, RC4 algorithm, fuzzy logic, amalgam encryption, India

INTRODUCTION

Mobile commerce is defined as the exchange or buying and selling of commodities, services or information on the Internet through the use of mobile handheld devices. M-commerce is purchasing from anywhere and superior to E-commerce in offering spatiotemporal access due to the ubiquitous nature of mobile devices. M-commerce has been receiving attention considerably and has high growth rate. The four major subjects of mobile commerce consists of mobile commerce systems, mobile handheld devices, handheld computing, mobile payment methods. Mobile commerce system structure is shown in Fig. 1. The mobile commerce system structure includes six components: mobile applications, mobile handheld devices, mobile middleware, wireless networks, wired networks and host computers. The features of M-commerce mainly focused on ubiquity, immediacy, localization, instant connectivity, pro-active functionality. Mobile commerce system structure as shown in Fig. 1. M-commerce is generally guided by five principles as:

- Legal enforceability of contracts
- Consumer protection
- Privacy of data (no unnecessary, unauthorized data collection)
- Confidentiality of data (protecting authorized data from misuse)
- Right of self-determination (to carry out or reject a communication)

Today, we are living in digital kingdom having computer as slaves, who make our life much easier but not necessarily more secure. With the advancement of science and technology our daily activities have become faster and easier at the cost of having complex tools and technologies. The online banking transactions are part of daily routine for an individual. The existing online banking system has several drawbacks (Belkhede *et al*., 2012). First drawback is hacking, from the internet any one can hack the username and password and the result is third person gets access to owner account. As, no one is using internet with twenty four hours on the internet, it takes some time to know that your account get hacked and third one can get transfer the money to his own account. The second drawback is every time one has to carry laptop or PC with them. To overcome this issue secured payment applications on mobile device in M-commerce is proposed (Belkhede *et al*., 2012).

Corresponding Author: B. Vanathi, Department of CSE, Valliammai Engineering College, Kattankulathur, Chennai, India

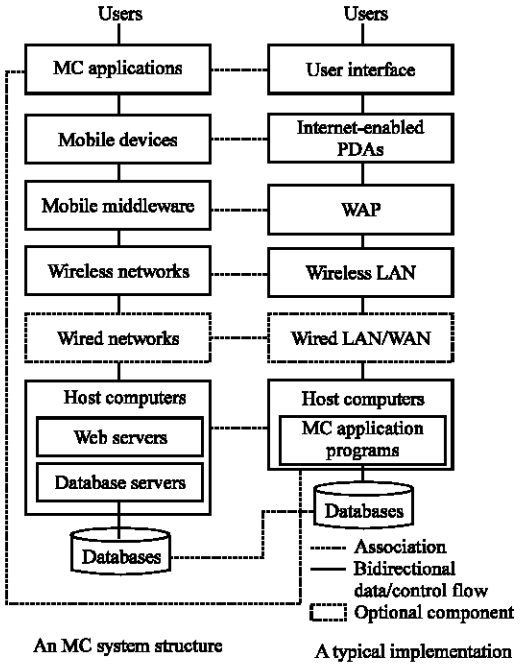

Fig. 1: Mobile commerce system structure

M-commerce in the context, provides a lot of services like mobile ticketing, mobile banking, mobile location based services, mobile auctions, mobile purchasing and so on. Mobile devices are rapidly becoming a key computing platform, transforming how people access business and personal information. Access to business data from mobile devices requires secure authentication, authentication is the act of verifying that an individual is who he claims to be. Today, we're using usernames and passwords but passwords are weak as many people write them down or forget them. Passwords may be captured by spyware or Trojan horses on an infected computer and they are 'easy' to guess. The ease of guessing depends on the password strength which is up to the user to define. Traditional authentication systems requires the user perform the cumbersome task of memorizing numerous passwords, Personal Identification Numbers (PIN), pass-phrase and/or answers to secret questions like "what is your nick name?", etc. in order to access various databases and systems. More often, it becomes almost impossible to the different formats due to case sensitivity, requirement of alphanumeric text and the necessity to change passwords or pass-phrases periodically to prevent from accidental compromise or theft. Many users choose passwords to be part of their names, phone numbers or something which can be guessed. Moreover, to handle the hard task of remembering so many passwords, people tend to write them in files and conspicuous places such as desk calendars which expose chances of security violation. Another authentication approach is biometrics which is a way of authentication through something your body is or can do rather than something you know (a password). Biometric authentication is the process of verifying if a user or identity is who they claim to be using digitized biological pieces of the user (Belkhede *et al*., 2012). It comes in all sorts of flavors' fingerprint, iris scan, hand geometry, face recognition, voice recognition, handwriting and typing dynamics most of these have different variants. Generally speaking, there are four factors of physical attributes that are used or can be used in user authentication:

- Finger print scans which have been in use for many years by law enforcement and other government agencies and is regarded as a reliable, unique identifier
- Retina or iris scans which have been used to confirm a person's identity by analyzing the arrangement of blood vessels in the retina or patterns of color in the iris
- Voice recognition which uses a voice print that analyses how a person says a particular word or sequence of words unique to that individual
- Facial recognition which use unique facial features to identify an individual

The rich set of input sensors on mobile devices, including cameras, microphones, touch screens and GPS, enable sophisticated multi-media interactions. Biometric authentication methods using these sensors could offer a natural alternative to password schemes, since the sensors are familiar and already used for a variety of mobile tasks. Biometrics has made it possible to identify individuals rapidly based on biological traits. Biometric system is essentially a pattern recognition system that operates by acquiring physiological and/or behavioral characteristics from individual (such as fingerprint, iris scan, retina scan, hand geometry, etc.) extracting a set of features from the acquired data and comparing this feature set against the set of templates pre-stored in the database. In a biometric system, each reference template stored in the database is usually associated with only a single individual (Rajanna *et al*., 2010).

Literature review:

Security in mobile commerce: Nambiar *et al*. (2004) was proposed the mobile payment techniques in secure way. Mobile payment is the process of two parties exchanging financial value using a mobile device in return for goods or services. This study is an analysis of the security issues in mobile payment for M-commerce. This study

introduces M-commerce and mobile payment. It discusses the public key infrastructure as a business for secure mobile technologies. It also study, the features for different security technologies employed in current M-commerce market including Wireless Application Protocol (WAP), Subscriber Identity Module (SIM) application toolkit and Java 2 Micro Edition (J2ME). This study also compares, the effectiveness of these security technologies in supporting a secure mobile payment and discusses research issues to enhance the security of mobile payment for large scale deployment of M-commerce. Disadvantages of this method which consists of by using WAP 1.0 because, WAP gap is occurred in WAP 1.0.

Mobile banking security using steganography: Pawar and Gawande (2012) was proposed a method for increasing security of the information requested by users with the use of steganography method. In this method, instead of direct sending of the information, it is hidden in a picture by the password and is put on a site. Then, the address of the picture is sent to the user. After receiving the address of the picture through Short Messaging Service (SMS), the user downloads the picture by a special program. After entering the password, the user can witness the information extracted from the picture if the password is entered correctly. This project is written in J2ME (Java 2 Micro Edition) language and has been implemented on Nokia mobile phones, models N71 and 6680. The steganography algorithm advantages are:

- The password is not stored in the stegano image, so it is difficult to detect the password.
- Because the password is used, it is difficult to detect the information hidden in the image
- The decoding program uses a few kilobytes of memory. Also, the program is fast enough

Disadvantages: Using Advanced Encryption Standard (AES) algorithm execution time, encryption and decryption time is high compared to stream cipher algorithm.

Online transactions on android system: Belkhede *et al.* (2012) was proposed only using the fingerprint biometric mechanism for mobile payment in online transaction. This research presents, the proposed biometrics mechanism for secure mobile payment and security at the wireless transmission level. The main research focuses is on the feature extraction from the runtime fingerprint image on the android mobile and send to the server for authentication. A newly proposed fuzzy logic based fingerprint matching algorithms will be implemented at the server side. A intruder in middle attacking at WAP Gateway is a great concern. So for securing, the biometric identification template on the WAP Gateway from client (mobile) to server (host server) Rivest-Shamir-Adlemen (RSA) algorithm will provide the enhanced security at transmission level. Disadvantages of this method consists of If the obtained finger print matches is partially true (60-99%) then, what will the solution considered is an issue. It does not focus on this issue. Next disadvantage is RSA algorithm used for encryption so RSA algorithm consists of lot of disadvantages that is it RSA algorithm, the key size is large and so requires significant amount of memory storage, decryption time increases, less time consuming key generation is complex.

2D-barcode techniques secure transaction model: Existing techniques of the 2D-barcode (Gao *et al*., 2009) increases the security in mobile payment transaction and ordering of the goods in secure way. Another advantage of the 2D-barcode is customers and mobile users can easily extract all related product information from 2D-barcode and reducing the user inputs. The limitations of this technique is merchant authentication is not provided. The customer details, PIN and account number and payment information are stored in customer mobile phone. So in the case of mobile theft, it can be easily identified by the intruder.

SET techniques: The Secure Electronic Transaction (SET) (Sanyal *et al.*, 2010; Mastercard, 1997) is an open protocol specification developed for credit card transactions over internet.

SET technique disadvantages:

- SET is designed for wired networks and does not meet all the challenges of wireless network
- SET protocol worked in the traditional model of payment data, so an end-to-end security mechanism was required
- Direction of transaction flow in SET. In SET, transactions are carried out between customer agent and merchant. It is vulnerable to attacks like transaction/balance modification by merchant
- The transaction flow is from customer to merchant so all the details of the users credit cards/debit cards must flow via the merchant's side. It increases the user's risk, since data can be copied and used later to access a customer account without authorization
- There is no notification to the customer from the customers bank after the successful transfer. The user has to logon to their bank online portal in order to get transaction and payment detail

Secure One Time Password (OTP) and biometric verification: Chang-Lung and Deng-Jie was proposed the One Time Password (OTP) and personal biometric have been combined with personal identification and password for verification while M-banking disadvantages of this study proposed idea is not focused the which mechanism is captured the biometric data and no secure encryption algorithm is provided to transmit the biometric fingerprint image to the server side and not focused the fuzzy logic threshold level rules.

Biometrics based user authentication technique: Existing biometric techniques used for user authentication is unique. User authentication is achieved by mobile device. The main advantage of this technique is as both users and service provider recognizes without an additional device. The merits of using Elliptic Curve Cryptography (ECC) for encryption methods are the process is small, efficient and requires low power. The limitations in biometric techniques are; it uses only encryption method for user and payment details for secure transfer of the data. By not using a security conversation mechanism like WAP Gateway, data's are not more secured. No merchant authentication is available in this technique. Fingerprint verification and identification method is does not focused. Fingerprint threshold level is does not focused. The limitation of using ECC is difficulty in counting the number of points on the curve and generating suitable curves. ECC is not yet fully understood and relatively has slow signature verification.

PIN distribution techniques: Arunprakash proposed the PIN distribution techniques. This study proposed the PIN distribution process by using AES encryption. Customer details and Payment details (PIN) are sending by using WAP 1.0. Only, the Mutual authentication is main advantages of this study. Disadvantages of this study using WAP 1.0 because WAP 1.0 consists of one security problem, known as the "WAP gap" is caused by the existence of a WAP Gateway in a security session. Encryption, decryption time and throughput is high by using AES algorithm.

Prliminaries: This study reviews the definitions (Shanmugam and Vanathi, 2014a, b) of WAP Gateway, Fuzzy logic based authentication, One Time Password (OTP) and SMS authentication and fingerprint recognition and comparison between Stream Cipher and Block Cipher algorithm.

WAP Gateway: The WAP Gateway is software which runs on the computer of the Mobile service provider. The WAP 1.x security uses the Wireless Transport Layer Security (WTLS) protocol. This protocol is the WAP equivalent of Secure Socket Layer (SSL) and it provides authentication, encryption and integrity services. WAP 1.0 consists of one security problem, known as the "WAP gap" is caused by the existence of a WAP Gateway in a security session. So, use a WAP 2.0 in proposed work.

Fuzzy logic: Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact. In contrast with traditional Logic theory where binary sets have a truth valued logic: true or false, fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth where the truth value may range between completely true and completely false (Shanmugam and Vanathi, 2014a) structure of fuzzy logic controller as shown in Fig. 2.

One Time Password (OTP): The purpose of the onetime password is to make, it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password as is done with a onetime password, this risk can be greatly reduced.

Short Message Services (SMS): The bank or financial institution stores user cell number to send SMS to their customers for their transaction confirmation. Cellular network uses separate channel to send and receive SMS over wireless medium (Shanmugam and Vanathi, 2014a). Here, we assume that users carry their cell phone with them regularly and therefore can receive the short message and reply SMS to confirm or deny their financial transaction. As a result, only valid users will receive SMS from the authentication server. After getting the SMS, a

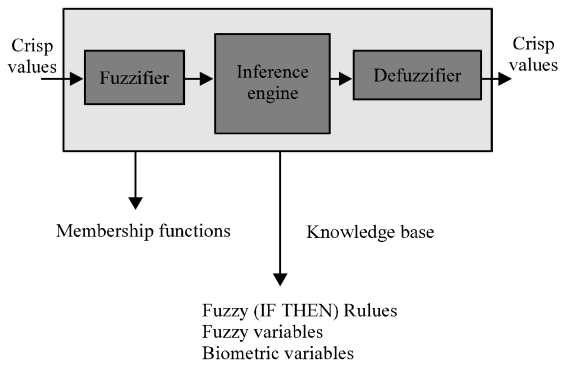

Fig. 2: Structure of fuzzy logic controller (Shanmugham and Vanathi, 2014a)

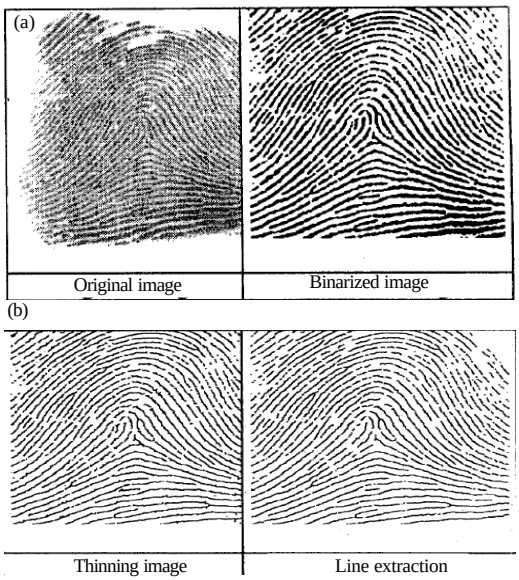

Fig. 3: Sample of the pre-processing described-over a fingerprint image (Shanmugham and Vanathi, 2014a)

user can acknowledge the choices. When the authentication server receives "YES" it knows that the user is valid and that the user has approved their initiated transaction.

Finger prints recognition: Fingerprint recognition techniques analyze global pattern schema on the fingerprint along with small unique marks known as minutiate which are the ridge endings and bifurcations or branches in the finger print ridges. The data extracted from fingerprints are extremely dense where density explains why fingerprints are a very reliable means of identification. Preprocessing steps as shown in Fig. 3.

The feature extraction will consist of finding the ridge endings and ridge bifurcations from the input fingerprint images, being each minutia described by its location (x, y coordinates) and its orientation (θ). The final ridge structure will be used to generate a fingerprint feature vector or minutiae map which will characterize the fingerprint. This one will be a template formed by a list of minutiae and a list of number of ridges between each pair of minutiae and it will be stored by the system (Shanmugam and Vanathi, 2014a).

Comparison between stream cipher and block cipher algorithm: Stream cipher is still being a favorite method for mobile devices for the following valid reasons:

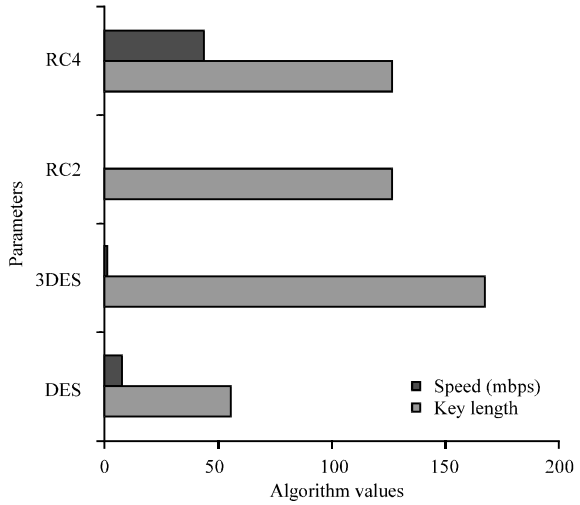

Fig. 4: Various algorithm performance results on encryption

Table 1: Algoritm encryption performance (Weerasinghe, 2012)

Cipher	Key lengths	Speed (Mbps)
DES	56	9.0
3DES	168	3.0
RC2	Variable	0.9
RC4	Variable	45.0

- Stream ciphers are typically faster than the block cipher which ensures the low consumption in energy and memory-both of which could drain the battery life
- Block cipher typically requires more memories, since they work on a larger chunks of data and often have "carry over" from previous blocks whereas since, stream ciphers work s on only few bits at a time they have relatively low memory requirements
- Stream ciphers doesn't need padding as requires by block ciphers which operates on complete blocks stream and block cipher comparison as shown in Table 1 and Fig. 4.

MATERIALS AND METHODS

Proposed work: Mostly for secure data transfer, only encryption is done for user and payment details and no secure conversation mechanism was used. This leads to the proposed model, in the proposed model re encrypt the data in the application-level so that data exposure to WAP Gateway by using WAP 2.0 is still being encrypted and protected. No service provider (merchant) authentication, fingerprint threshold level is does not focused and no secure PIN distribution process are used in existing concepts. These problems leads to the proposed work (Fig. 5).

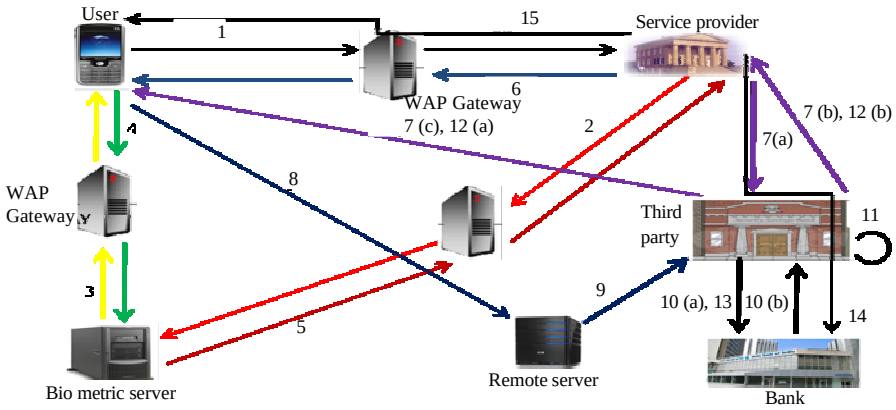

Fig. 5: Proposed architecture

Over all process of proposed architecture: In the proposed architecture as shown in Fig. 5, the following of events are as given below. In 1 point customer (user) sends the product and customer details to the service provider through the WAP Gateway. In 2 point service provider verifies the product and customer details and sends to the biometric server through the WAP Gateway. In 3 point biometric server requests the customer details to the customer. In 4 point customer sends the fingerprint image and details to the biometric server through the WAP Gateway and biometricserver verifies the fingerprint by using fuzzy logic and also compares the send details of service provider and customer. In 5 point comparison result details send to the service provider. In 6 point finally, service provider decides access or denies the process of customer. In 7a point customer and service provider Id and time stamp values are send to the third party by service provider (merchant). In 7b point service provider is authenticated by third party. In 7c point after generating the key K_{ab} by using RC4 algorithm and third party finds the A's profile and sends the other information to the consumer. Consumer completes the authentication process once the calculated hash code is correct and merchant is authenticated. In point 8 before sending the payment details and PIN distribution process, user authentication is verified by using fuzzy logic and based on the threshold level, SMS authentication, OTP authentication is provided. After authentication process PIN and payment details send to the remote server in secure way. In 9 point remote server sends the PIN and payment details to the trusted third party. In 10a point trusted third party connects to the bank for payment transaction in authorized way. In 10b point the acquiring financial institution treats the demand and response send to the third party. In point 11 all details and response about the transactions are stored by trusted third party. In 12a point third party sends the payment reference and other details to the customer. In 12b point third party sends the response to the merchant. In 13 point the third party makes all the payment transaction. In 14 point merchant receives the payment from the financial institution. In 15 point finally, merchant delivers the order to customer the customer.

User and service provider (merchant) authetication process: The module 1 description as explained in this study. User and merchant authentication process are as shown in Fig. 6. Step1-6 process explained in unit1 from Fig. 6.

User sends the user and product details. They are encrypted by using double encryption model. This encryption model encrypt the details by Key(K) and Key (K1) and send to the WAP Gateway through, the SSL/TLS. Key(K1) is decrypted by SSL/TLS. Next, WAP Gateway Encrypt the details by using another Key(K2) and send to the Service provider through the SSL/TLS. Key(K2) is decrypted by SSL/TLS. Finally, serviceprovider decrypt the Key(K) and show the details of user and product. The detailed double encryption process is showed follows in Fig. 7, the snapshots in Fig. 8 and 9:

- Serviceprovider verify the details and send the user details to biometric server for user authentication by using double encryption method through the WAP Gateway
- Biometric server requests the user details to the user. User captures the fingerprint image from the mobile and send the finger image and user details to the biometric server by using double encryption model through the WAP Gateway

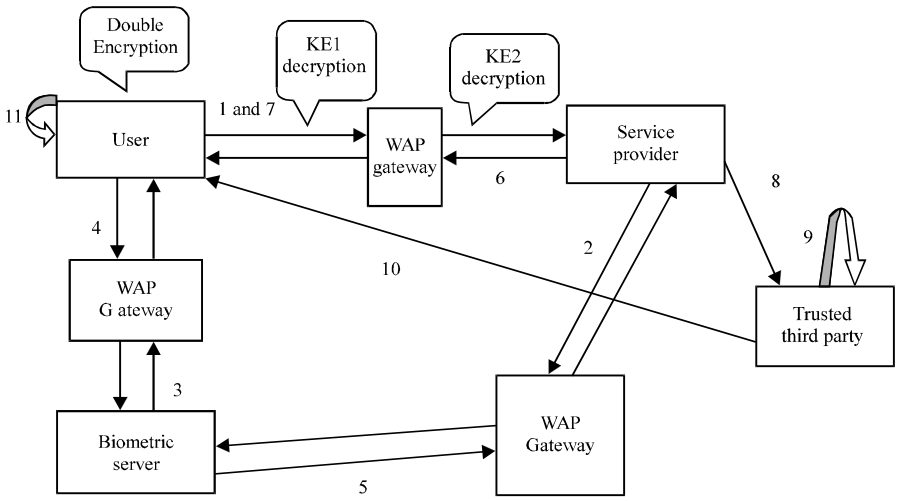

Fig. 6: User and merchant authentication process

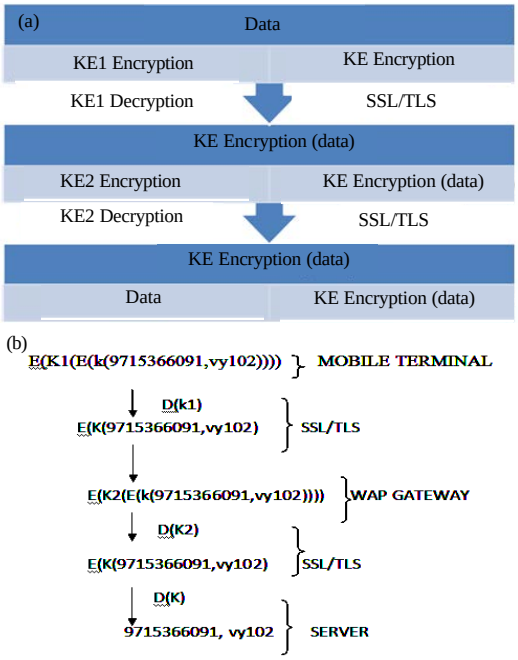

Fig. 7: a) Double encryption model; b) Double encryption process

- Biometric server verified the finger image by using fuzzy logic and find the threshold level and also compare the send details of user and service provider finally, found the user authenticated or not and send the authentication details to the service provider
- Based on the user authentication details, service provider inform to the user is authenticated or not and also decided the access or deny the process

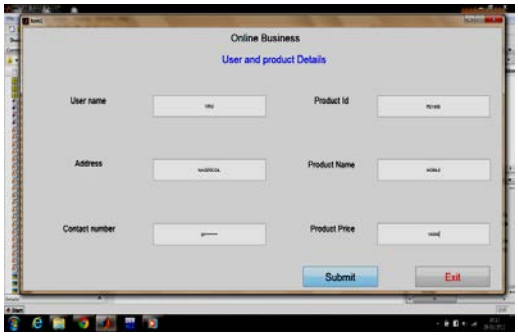

Fig. 8: User and product details

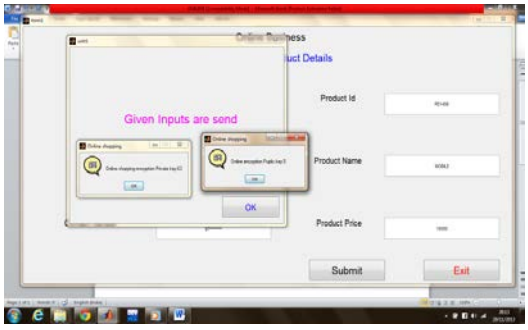

Fig. 9: User details encrypted by double encryption model

RC4 and AES algorithm comparison: The RC4 encryption time is less compare to the AES algorithm, encryption time based on different packet size in Fig. 1. The proposed double encryption method using RC4 algorithm has an implementation factor of 76% over AES algorithm. Encryption time of RC4 and AES as shown in Fig. 10 and Table 2.

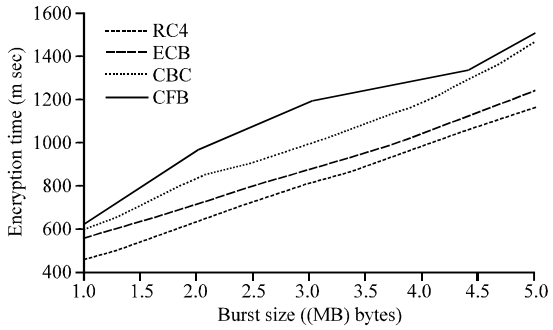

Fig. 10: Encryption time of RC4 and AES

Table 2: Encryption time of RC4 and AES

Burst size (bytes in MB)	RC4 (m sec)	AES (ECB) (m sec)
1.0	460.8	560.3
2.5	635.0	720.6
4.0	810.0	880.3
4.5	985.7	1035.5
5.0	1160.0	1235.6

$$\text{Average of RC4} - \text{Average of AES} = \text{Improvement factor}$$

$$\frac{4052.2}{5} = \frac{380.01}{5} = 76.02\%$$

Improvement factor is 76.02%

Merchant authentication process Unit 2: The module 2 (Merchant authentication process) description as explained in this study. Step 7-11 process explained in unit2 from Fig. 6.

- User send the user ID and time stamp value to the merchant
- Merchant is forward the User ID, Merchant ID and timestamp of user and merchant details to the trusted third party
- Third party generates the key by RC4 algorithm and find the user details key generation as shown in Fig. 11
- Send other information to the user
- User extracts the key and calculates the hash code by SHA algorithm after receiving the information. User completes the authentication process once the calculated hash code is correct and merchant is authenticated

QrsecPTA (Quick response secure payment details and PIN distribution transaction authentication process) Unit 3: User send the payment details to the remote server, in this case first, again the user authentication is done by remote server. User captures the finger image from the mobile and sends to the remote server. Remote server verified the finger image by fuzzy logic. Fuzzy logic verify the finger image and found the threshold level which consists of 100, 60-99% and below 60%. Based on the threshold level, remote server provides the SMS and One Time Password (OTP) authentication (Fig. 12).

Fingerprint threshold possibility: The P = 1/3 so Exhaustive number of cases consists of 100, 60-99% and below 60%:

$$P(\text{Fingerprint threshold}) = m / n = \frac{\text{FAvourable number of cases}}{\text{Exhastive number of cases}}$$

P = 1/3 so, exhaustive number of cases consists of 100, 60-99 and below 60%.

Positive correlation: Fingerprint image threshold level and User authentication level is 100% . Using the Positive correlation, if threshold level is high then user authentication level is also high and if threshold level is low then user authentication level is also low.

User authentication process for payment details transaction by Remote server: Fuzzy logic here are used to calculate the percentage of various features presents in the given fingerprint. If feature matching percentage is 100% then the biometric system successfully authenticate the user and to provides the another SMS authentication in this threshold level and then else the matching percentage is 60-99% then the system will ask some security questions that are already stored in the database system during registration process or OTP is generated and also SMS authentication is provided. In case of below 60% matching the user authentication should be failed and user may reenter the fingerprint and try it again. These proposed work architecture is given Fig. 12 and 13.

The matching percentage is 60-99% then the system will ask some security questions that are already stored in the database system during registration process or OTP is generated. After OTP authentication, SMS authentication is started. The OTP is send by amalgam encryption method.

RC4 encryption mode: The fingerprint template is encrypted by using the RC4 algorithms and sends it to the remote server. The RC4 algorithm is best for Image based encryption method. The RC4 is a stream cipher model. Stream ciphers are more efficient for real time processing.

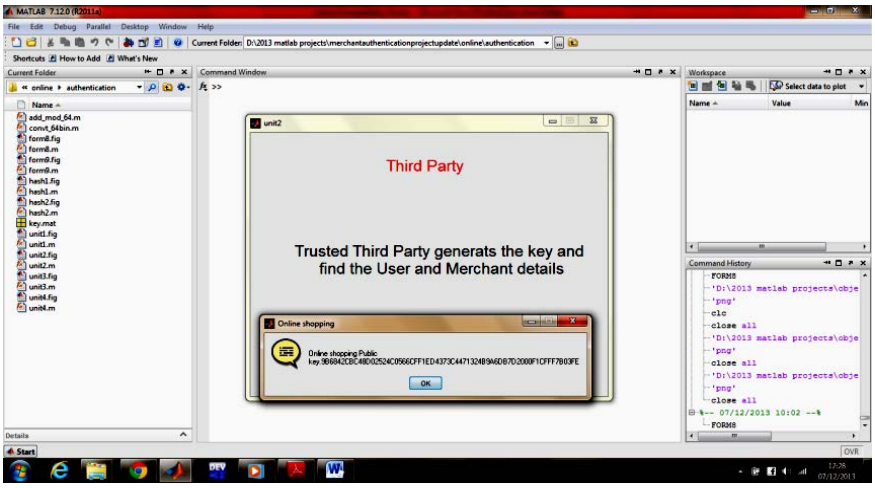

Fig. 11: Key generation

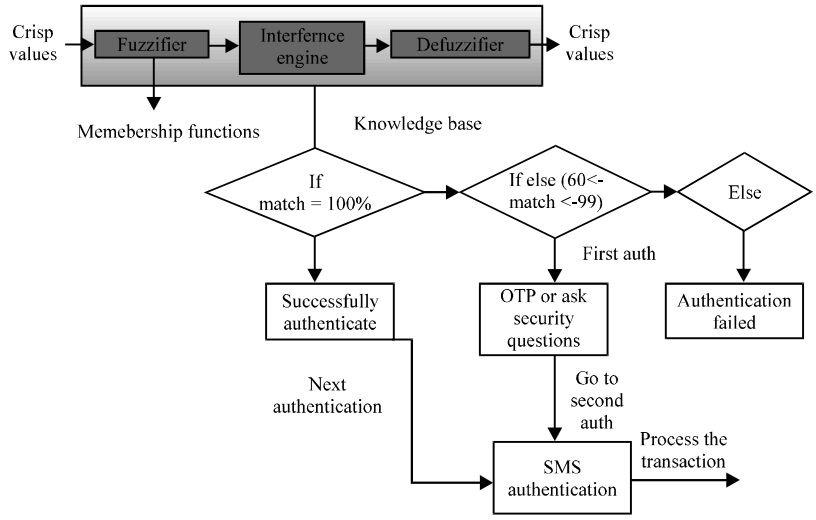

Fig. 12: Process of fuzzy logic

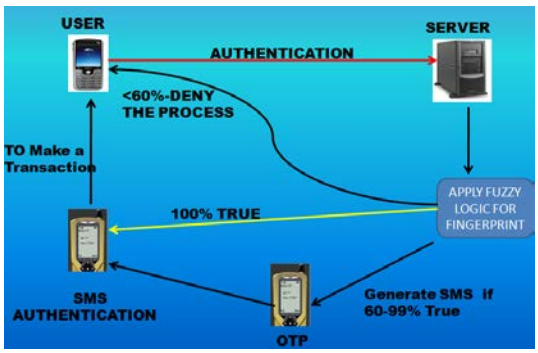

Fig. 13: User authentication for payment details transaction

Stream cipher is faster than block cipher (RC4, 2011; Weerasinghe, 2012). Stream ciphers fulfill the requirements of multimedia applications of high throughput, low H/W complexity and are technology specific. The RC4 algorithm is simple, fast and easy to explain. It can be efficiently implemented in both software and hardware. The RC4 takes less time to take encrypt and decrypt the files w.r.t AES.RC4 is better than AES. RC4 execution time is lesser than AES. The RC4 is a stream cipher model. Stream ciphers are more efficient for real time processing. Stream cipher is faster than block cipher (Weerasinghe, 2012).

Short Message Service (SMS): The security of the system also depends on the security of the messages sent

by SMS and SMS messages which are encrypted and protected by using Rc4 (Ron's Code) and Triple Data Encryption Standard (3-DES) algorithm. The user will get a SMS with the required details which are essential to identify and recognize the users initiated transaction. By this SMS, a user will confirm their transaction by "YES" or "NO".

RESULTS AND DISCUSSION

Implementation results by using MATLAB: User finger image is verified by fuzzylogic for payment transaction process in secure way as shown in Fig. 14 and 15.

PIN distribution process-unit-4: In this process, send the user Pin number and payment details in secure way. Pin number is encrypted by amalgam encryption. Amalgam encryption means, Encrypt the pin number by using combination of triple data Encryption Standard (3-DES) and RC4 algorithm. Amalgam encryption is does not used for secure transaction in Mobile commerce so current system will be used in this encryption process.

Pin verification process of proposed system: The PIN given by the customer is divided into two halves (P1 and 2). PIN 1 is encrypted by amalgam encryption method and verified by remote server. PIN 2 is encrypted by amalgam encryption method and verified by Authentication server. Two halves of the pin verified separately by using amalgam encryption. Finally, verification PIN sends to the Third party by remote server for further process. PIN verification process as shown in Fig. 16.

One half (PIN1) of the PIN is encrypted by using 3-DES algorithm and get the cipher text of 3-DES encryption. This cipher text is again encrypted by using RC4 algorithm and get the amalgam (Hybrid) encrypted data. This amalgam encrypted data is send to the remote server for verification. Another half (PIN-2) of the PIN is encrypted by using similar way as shown in Fig 17.

Implementation results in MATLAB: Amalgam PIN distribution process are shown in Fig. 18-21.

PIN decryption process: Amalgam encrypted data is decrypted by using RC4 algorithm and get partial plaintext. This Plain text is again decrypted by using 3-DES algorithm and got the one half of the PIN 1. This amalgam encrypted data is decrypted by the remote server and verify the correct one half of the PIN. Another half (PIN-2) of the PIN is Decrypted by using similar way as shown in Fig. 11. Another Half of the PIN is verified by authentication server and send to the remote server. Remote server is verified the whole original PIN number

Fig. 14: User authentication process

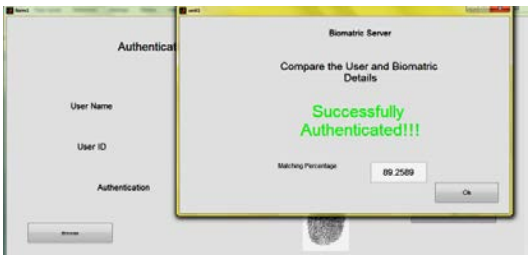

Fig. 15: User authentication process for payment details transaction process

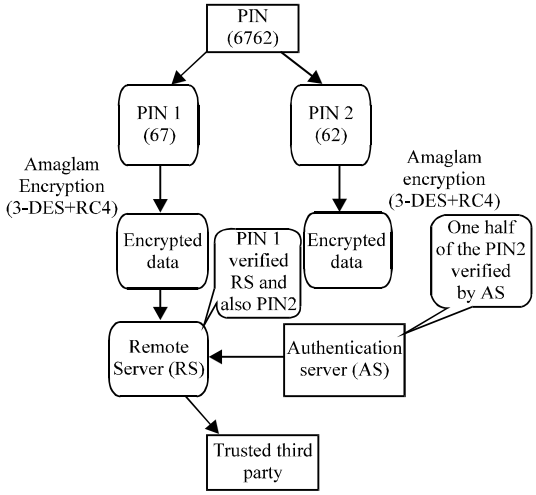

Fig. 16: PIN verification process

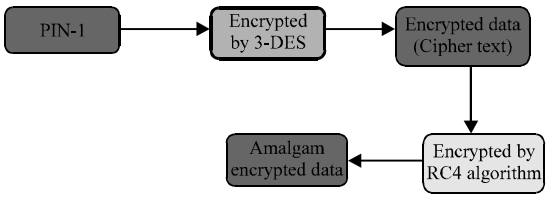

Fig. 17: Encryption process

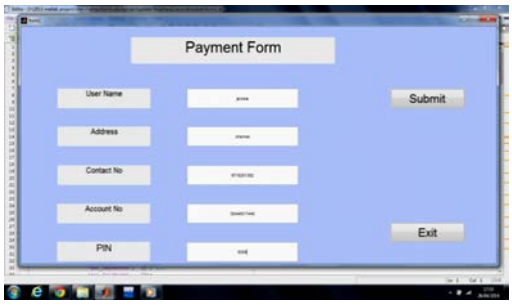

Fig. 18: Payment form

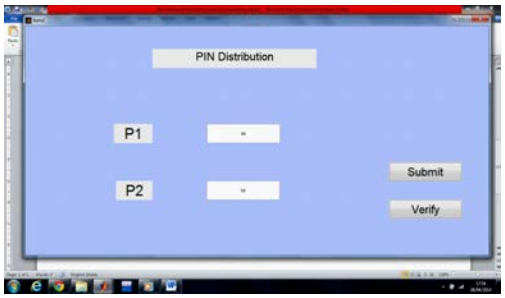

Fig. 19: PIN is divided into two halves

Fig. 20: P1 PIN is encrypted by 3-DES algorithm

Fig. 21: Encrypted PIN is again encrypted by RC4 algorithm

given by user. Finally, PIN number is send to the Third party in verification is successful case. Otherwise, process is rejected. In this amalgam encryption process

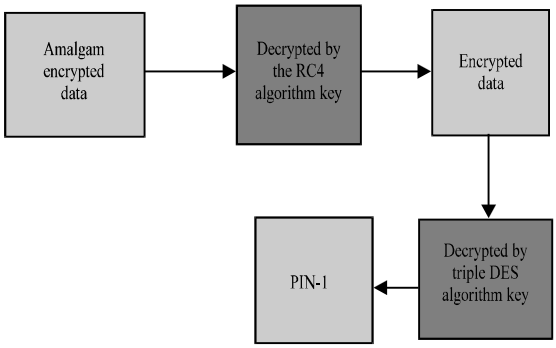

Fig. 22: Decryption process

Hybrid -1 (3-DES+RC4) combination process is better than Hybrid- 2(AES+RC4) combination process (Weerasinghe, 2012) as shown in Table 3 and Fig. 8. Increasing the more Secrecy only by triple DES and RC4 combination (Weerasinghe, 2012). Figure decryption process as shown in Fig. 22.

PIN verification process: One half (PIN1) of the PIN is verified by Remote server. Another Half (PIN2) of the PIN is verified by authentication server and send to the remote server. Remote server is verified the whole Original PIN number given by user.

Finally, PIN number is send to the Third party in verification is successful case. Otherwise, process is rejected.

Benefits of the proposed model:

- The use of double encryption helps to build a more secure channel between mobile terminal and content server
- Overcome the WAP gap by using WAP 2.0
- Here is no need of any special hardware to be added to the mobile, since there is priority communication cost of the encryption consultations between mobile terminals and servers increases connection speed and security degree in mobile commerce transactions
- Data integrity is ensured due to SSL/TLS protocols between mobile terminal and WAP Gateway, TLS/SSL protocol between WAP Gateway and content server. In this message authentication code mechanism is employed
- Merchant authentication: This process gives full satisfaction to the customer. It is simple since it uses Secure Hash Algorithm (SHA) to calculate message digest. Thus, it is highly efficient and effective

- Proposed work performed the two different authentication (One Time Password (OTP), SMS authentication) methods for More authentication and found the threshold level (100, 60-99 and <60%) reported the results on their security compromise in fingerprint authentication
- The possibility of experiments fingerprint dataset show that the three threshold level for particular fingerprint so, representing a new identity can potentially be used for authentication. This gives the better level of security mechanism for M-commerce system
- Amalgam encryption is provided more security and increasing the secrecy value compared to the single block cipher or stream cipher encryption process
- Data confidentiality is achieved by using the distributed the PIN. The PIN is divided into two parts and sent. Even if the impostor with the succeeds to trap one half of the PIN, it becomes plentiful to crack the other half of the PIN simultaneously. The cracking of the entire PIN becomes extremely difficult and a tedious process providing enhanced security to this system

CONCLUSION

User authentication provides the assurance that the communicating entity is claimant person. User authentication is done by WAP Gateway, Double Encryption model and biometric server. Merchant authentication provides vast security, thereby assuring the customer that the transaction is carried out with right person. Merchant authentication is done by trusted third party. To add on with this the introduction of a more secure WAP Gateway which involves the "Double encryption model" to another key point to ensure the safety and reliability of the mobile E-commerce transactions? By using fuzzy logic work, the possibility of experiments fingerprint dataset show that the three threshold level for particular fingerprint so representing a new identity can potentially be used for authentication. This gives the better level of security mechanism for M-commerce system. PIN distributed process is ensured the confidentiality security and frustration the intruder. The proposed architecture, it serves to provide a high level security because at each stage a more improved mechanism is introduced to ensure a complete reliable and secure transaction. The proposed RC4 algorithm has an improvement factor of 76.2% over AES algorithm. observed by this improvement factor RC4 algorithm is best based on the encryption and decryption time. To add on with this the introduction of a more secure amalgam (Hybrid) encryption to another key point to ensure the security and reliability of the mobile E-commerce transactions. Secure OTP and voice authentication for mobile banking process will future work.

REFERENCES

Belkhede, M., V. Gulhane and P. Bajaj, 2012. Biometric mechanism for enhanced security of online transaction on android system: A design approach. Proceedings of the 2012 14th International Conference on Advanced Communication Technology (ICACT), Feburary 19-22, 2012, IEEE, PyeongChang, pp: 1193-1197.

Gao, J., V. Kulkarni, H. Ranavat, L. Chang and H. Mei, 2009. A 2D barcode-based mobile payment system. Proceedings of the MUE'09. Third International Conference on Multimedia and Ubiquitous Engineering, 2009, June 4-6, 2009, IEEE, Qingdao, China, pp: 320-329.

Nambiar, S., C.T. Lu and L.R. Liang, 2004. Analysis of payment transaction security in mobile commerce. Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, IRI 2004, November 8-10, 2004, IEEE, New Jersy, USA., pp: 475-480.

Pawar, P.Y. and S.H. Gawande, 2012. M-Commerce security using random LSB steganography and cryptography. Int. J. Machine Learn. Comput., 212: 427-430.

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: 263-272.

Sanyal, S., A. Tiwari and S. Sanyal, 2010. A Multifactor Secure Authentication System for Wireless Payment. In: Emergent Web Intelligence: Advanced Information Retrieval. Chbeir, R., Y. Badr, A. Abraham and A.E. Hassanien (Eds.). Springer London, England, pp: 341 369.

Shanmugam, K. and B. Vanathi, 2014a. Enhancing secure transaction and identity authentication in m-commerce. Int. J. Adv. Sci. Eng. Technol., 1: 2321-9009.

Shanmugam, K. and B. Vanathi, 2014b. Fuzzy logic implementation of fingerprint mechanism for secure transaction and identity authentication in m-commerce. Int. J. Recent Adv. Eng. Technol., 2: 2347-2812.

Weerasinghe, T.D.B., 2012. Secrecy and performance analysis of symmetric key encryption algorithms. Int. J. Inf. Net. Secur., 1: 77-87.