# A Novel Secure Transaction and Identity Endorsement in M-commerce

K.shanmugam[1] , Dr. B.vanathi[2]
[2]Professor & head
Department of Computer Science and Engineering, Valliammai Engineering College
Kattankulathur, Chennai, India
[1]rajshan2flower@gmail.com, [2]mbvanathi@yahoo.co.in

***Abstract* — This study focuses on an advanced mobile security system to provide rapid and highly secure human friendly M-commerce transaction. M-commerce transaction works in multistep process. The process involves User authentication, Merchant authentication, Message authentication, secure payment details transaction authentication. M-commerce provides availability, reliability and security in transaction phases. The M –commerce phases involves multiple steps like Offering goods (O) , searching for available goods (B) , ordering the goods(O) , paying (P),delivering (D) and distributing(D). The proposed work improves security in user authentication by Wireless Application Protocol (WAP) gateway, which in turn provides end to end security using Double encryption model. In double encryption model, transfer the authentication data and product ordered using Transportation layer security (TLS) Protocol instead of Wireless Transport Layer Security (WTLS) protocol due to requiring end-to-end security with all IP based technology in order to overcome the WAP gateway security breaches. SSL/TLS protocol is used to transfer data and product between Mobile terminal and WAP gateway and also in WAP gate way and server. WTLS and SSL/TLS protocols use a message authentication code (MAC) technique to provide the data integrity. In our proposed work is use a RC4 algorithm for encryption because Stream cipher algorithm is better than block cipher algorithm. Fuzzy logic is applied in biometric server to use fingerprint matches exactly or not and measure the threshold level consists of exactly 100% or 60-99% or below 60%. Merchant authentication is done by trusted Third party.**

***Index Terms*— M-commerce, MAC, WAP-Gateway, Double encryption model, RC4,Fuzzy logic.**

## I. INTRODUCTION

M-commerce is defined as "the delivery of electronic commerce capabilities directly into the hands, anywhere, via wireless technology" and "putting a retail outlet in the customer's hands anywhere."[1]. The M-commerce means purchase from everywhere and it is much easier then E-commerce. E-commerce means purchase from home/ working place. E-Commerce needs Internet connectivity. M-commerce does not need any connectivity. Video conferencing can be done in M-Commerce, which is not possible in E-commerce. Electricity is not a main factor in M-commerce. But it is a main factor in E-Commerce. M-commerce and its related technologies offer many different application fields, such as Location Based services (LBS), Mobile ticketing, Mobile shopping, Mobile Financial services, Mobile Marketing and Mobile Entertainment. M-Commerce users can do multitasks at the same time. M-Commerce users expect immediate response and provide the exact result based on context.

## II. REQUIREMENTS FOR M-COMMERCE

According to some market research institutes, by 2004 at least 40 % of customer-to-business e-commerce will come from smart phones using the WAP[2]. Many new applications are becoming possible, and many existing e-commerce applications can be modified for a mobile environment. To illustrate the great potential of the m-commerce, we just mention some potential applications such as selling and buying of different goods, mobile inventory management(tracking the location of goods and services), proactive service management (transmitting information about aging components, such as automobile parts, to the vendors), wireless reengineering(improving business services), mobile auction and reverse auction, mobile entertainment services, mobile office (services for business people, such as traffic jam reports, airport and flight information, procurement of products and services), mobile distance education (offering classes using streaming audio and video), wireless data center (providing downloadable information from data warehouses), and others[2]. To realize these applications, several functional components are needed. It starts with a network infrastructure integrating both wireless and wired communication transport and mobile devices with sufficient memory, an appropriate display and communication functionalities. The mobile middleware is the enabling layer of software to connect e-commerce applications with different mobile networks and operating systems without introducing mobility awareness. It unites different applications, tools, networks and technologies, giving users a common interface. Middleware gives applications better response times and far better reliability. The WAP is also middleware, because it facilitates interoperability among different wireless networks, devices, and applications. Beside on mobile devices and middleware, m-commerce applications depend on networking support. Factors like reliable and survivable wireless networks, wireless quality of service, roaming across multiple heterogeneous networks so that users can access m-commerce applications from anywhere, location management, and others are important for successful and well accepted m-commerce, but the security of the m-commerce transactions plays a decisive role.

In m-commerce, where the consumer (client) and the merchant(content or service provider) communicate indirectly via software entities and the Internet, trust must be somehow established between the two parties. In order to achieve trust the following security functions must be performed[3]:

- Authentication: Each party should authenticate its counterpart.
- Integrity: Each party should make sure that the received messages are not altered or fabricated by other than its counterpart.
- Confidentiality: Each party wants to keep the content of its communication secret.
- Message authentication: Each party wants to make sure that the received messages do really come from its counterpart.
- Non-repudiation: Each party wants to prevent that the counterpart later denies the agreements that it has approved earlier.

An ideal m-commerce system should also support user friendly payment scheme supporting micro payment.

## III. LITERATURE SURVEY

There are many techniques and algorithms used for secured transactions in mobile commerce. Algorithms like Rivest-Shamir -Adlemen (RSA) algorithm, Advanced Encryption Standard algorithm (AES), Data Encryption Standard (DES) algorithm.Steamcipher algorithm (RC4) is better than Block Cipher algorithm(DES,AES,RSA).
There are many techniques available in literature. A few techniques are listed below

*A) 2D-barcode techniques*:

Existing techniques of the 2D-barcode [4] increases the security in mobile payment transaction and ordering of the goods in secure way. Another advantages 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 in this technique are 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.

*B) Biometrics technique:*

Existing biometric techniques used for user authentication is unique[5]. User authentication is achieved by mobile device. The main advantages of this technique is as both users and service provider recognizes without an additional device. By merits of using (ECC) for encryption method are , the process is small ,efficient and requires low power.The Limitations in biometric techniques are, as it uses only encryption method for user and payment details for secure transfer of the data. By not using a security conversation mechanism such as WAP gateway data are not more secured. No Merchant authentication is available in this technique. The limitations of using ECC consists of, 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.

*C) Secure OTP and BIOMETRIC verification technique:*

Here User authentication is verified by one time password and Biometric method [6]. But it authenticate only user. The Major disadvantage is they have not discussed/used any secure algorithm for encryption method at transmission level. Restrictions of this technique are OTP operation is costlier than Quick Response Transaction Authentication Number (QR-TAN) techniques.

*D) SET technique:*

The Secure Electronic Transaction (SET)[7-8] is an open protocol specification developed for credit card transactions over internet. Some Limitations of this technique are attacks can be made over wireless network by means of sniffing. The entire PIN can be obtained if the external network is cracked. Problem in managing limited resources.

*E) Biometric authentication:*

The solution involves the use a biometric authentication mechanism [9]. A payment application would be installed onto a android device, for authentication finger print is taken at runtime. The finger print template would be captured by the phone and compared against a stored template on a database server. Disadvantages of this method, 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.

*F) 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[10].

*G) Finger prints Recognition:*

Fingerprint recognition techniques analyze global pattern schema on the fingerprint, along with small unique marks known as minutiae, 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.

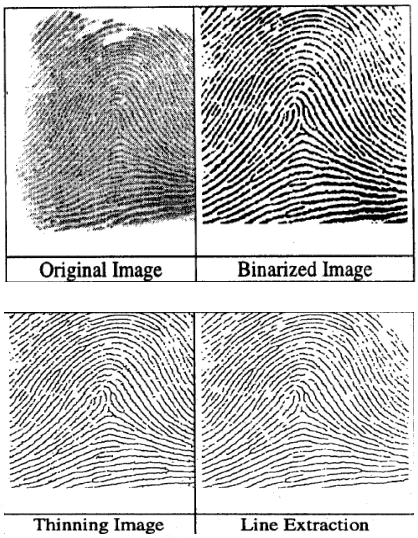



Fig.1: sample of the pre-processing described-over a fingerprint image [12]

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 [12].**

## IV. PROPOSED WORK

*A) Double encryption model:*

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 is still being encrypted and protected [11].
The proposed architecture is as shown in Fig. 2.

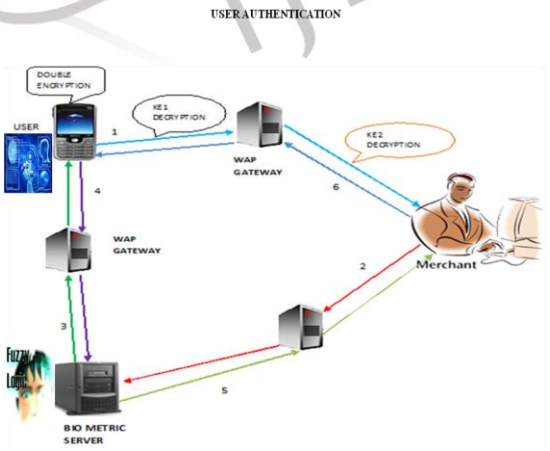



Fig. 2 Proposed Architecture

When the mobile terminal and content server are connected, a number of mutual authentication are processed to produce the session key and other parameters which only mobile terminal and content server know. Then use key to ensure end to end security between mobile terminal and content server, and the integrity of the other parameters.

*B) The process of mobile e-commerce Secure Transactions:*

The Double encryption model is as shown in Fig. 3.

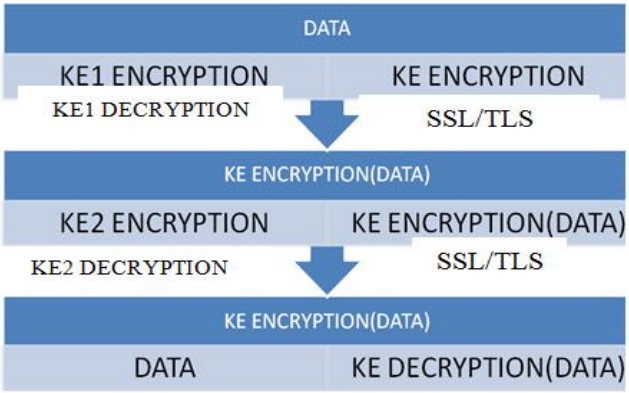



Fig. 3 Double encryption model

User sends the Product and user details are encrypted by using K, K1 keys and send to the WAP gateway through TLS protocol.TLS protocol is used to decrypt the Key K1 and send to WAP gateway.WAP gateway is used to Encrypted by another key K2 and send to the Service Provider through SSL/TLS and this protocol is used to decrypt the key K2 and Send to the Service Provider.finally, Servicprovider Decrypt the key K and get the user and product details.RC4 algorithm is used for Encryption and decryption.

*C) Reason to choose a RC4 algorithm:*

RC4 is a stream cipher model. stream ciphers are more efficient for real time processing. Stream cipher are faster than block cipher. Stream ciphers fulfill the Requirements of multimedia applications of high throughput, low H/W complexity and are technology Specific.RC4 algorithm is simple, fast and easy to explain. It can be efficiently implemented in both Software and hardware.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[12].

*D) Reason to choose the Double encryption model:*

To use the WAP gateway, it provides improved security based on Double encryption model, major advantages by this solution consists of To reduce the communication cost of the encryption between mobile terminals and servers, Short time, Increase the connection speed and security, Easy to implement.

*E) WAP security:*

WAP gateway is software which runs on the computer of the Mobile service provider.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.

*F) Process of the Proposed Method:*

These process based on user architecture shown in fig. 1 and 3.user authentication process consists of Step 1 to Step 6 and Merchant authentication process consists of Step 7 to step 11.

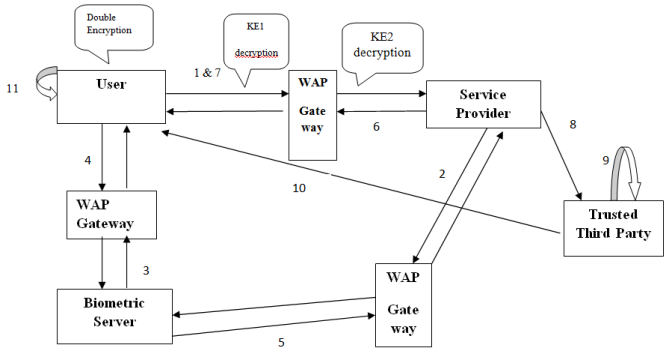
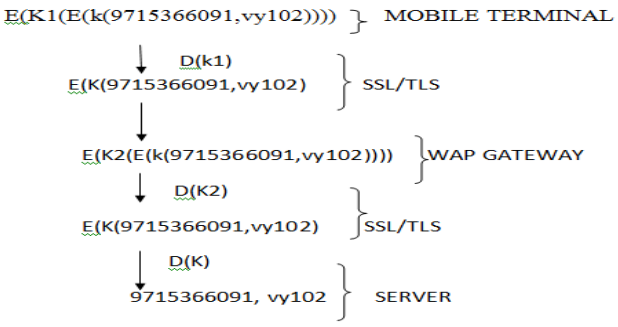



Fig. 3 process of proposed work

1) The **User** sends the mobile phone number and product information to the **Service provider (SP)** by using double encryption method.




2) The **Service provider (SP)** sends his identification and user's mobile phone number to the **Biometric Server by double encryption model**, and requests verification of the user's identity. The Biometric Server verifies the Service provider identification.

3) The **Biometric server (BS)** requests Fingerprint information image for authentication from the user by sending his identification.

4) The user captures and a hash fingerprint information image using the mobile device, and sends it with the mobile phone number to the Biometric server.

5) The BS compares the received and stored biometric information to verify the right user using fuzzy logic. Fuzzy logic find out the fingerprint threshold level(100%,60-99% or below 60%).The BS sends the result of the comparison with the user's phone number to the SP. The user's phone number is used to ascertain whose biometric information is to be checked.

6) The SP accepts or denies service to the user as a result of the comparison. User authentication is completed.

7) The customer sends his ID and timestamp value to the merchant.

8) The timestamp value and ID is forwarded by the merchant.

9) After generating the key $K_{ab}$ third party finds the A's profile and sends the other information to the consumer.

10) Consumer extracts the key and calculates the hash code after receiving the information.

11) Consumer completes the authentication process once the calculated hash code is correct and merchant is authenticated.

Implementation is done by using Mat lab and Experiment result is shown in Fig 4-7 below.

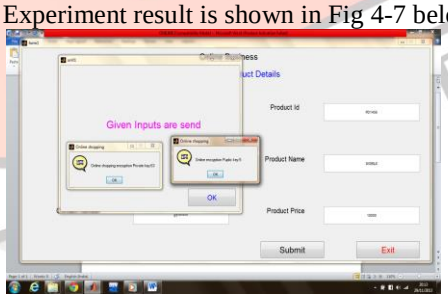



Fig .4 user and product details are encrypted by double encryption model.

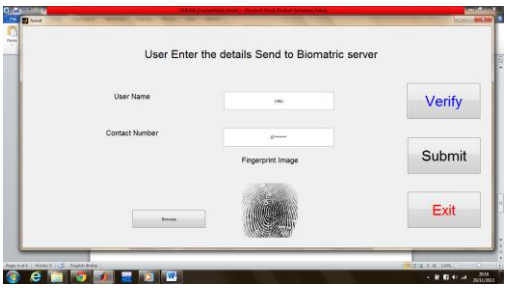



Fig.5 user Send the biometric information to biometric server.

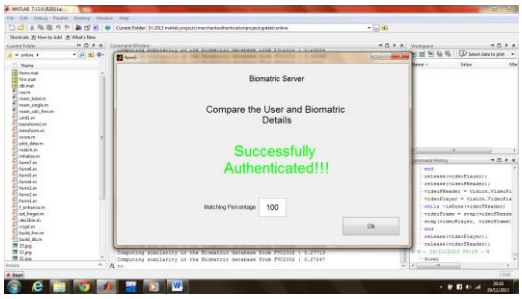



Fig.6 Biometric server compare the user biometric details by Fuzzy logic

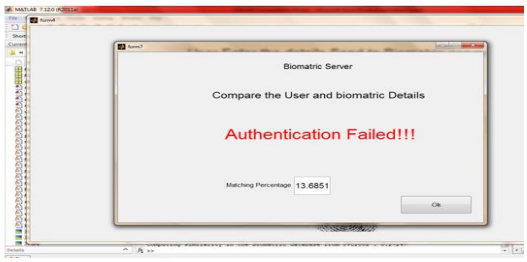



Fig.7 Fuzzy logic Compare the user finger print image and User is not authenticated by comparison result is below 60 %

## V. PROCESS 1

P is a USER
Q is a SERVICE PROVIDER
R is a BIOMETRIC SERVER

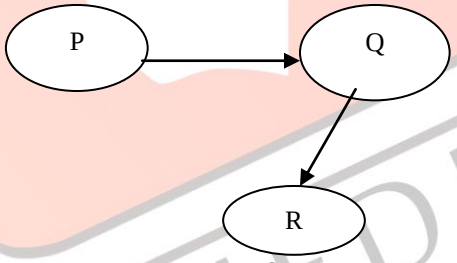



Fig. 8 Process diagram

P,P→Q,Q→R, from these premises ,to get the conclusion is R that means ,bio metric server verifies the user and service provider information is valid or not and R give the valid conclusion to the service provider. Process diagram as shown in Fig.8

**Statement:**

R is a legal conclusion (Valid inference) from these basis of argument, P, P→Q,Q→R

Proof:

**Step 1:**

P sends the phone number to the Q(P connects and conditional(→) with the Q)

1. P (introduce the premises)
2. P→Q (Introduce the next premises)

Note: → means the connective conditional

**Step 2:**

Q sends the user information to R.
To use the modus phones implication rule
(P,P→Q => Q) so,
Get from (1) & (2)

3. Q ( by modus phones )
4. Q→R ( Introduce the premises)

**Step 3:**
R verifies the information and gives the valid conclusion.

5. R (by modus phones rule-from (4) & (5) )

So, proves

| If U1,U2,U3…..Un and P imply Q ,then U1,U2,U3…….,Un imply P→Q |
|---|

That means, P implies Q , P send the phone number to Q ,then implies convert the tautological implication(P → Q)
Example:
P : user send the phone number to service provider (True)
Q : user is authorized (True)

TABLE 1: Truth Table

| P | Q | P→Q |
|---|---|---|
| T | T | T |

P-→ Q : If user send the phone number to the service provider then user is authorized.

## VI. PROCESS 2

Let consider, P-USER,Q-SERVICE PROVIDER,R-BIOMETRIC SERVER.Transition Diagram as shown in Fig.9
Condition:
Let assume that,
P:0→ user send the details and phone number
Q: 0→ service provider sends the user details
R:0→request the user information
P:1→ user accept the request and send the details to Biometric server
R:1→biometric server accept the user details and compare the details and send the comparison result to service provider
Q:1→service provider accept the result and accept the user process or not.

A) Transition table:

**TABLE 2: Transition Table**

| | 0 | 1 |
|---|---|---|
| →P | Q | R |
| Q | R | P |
| *R | P | Q |

B) TRANSITION DIAGRAM:

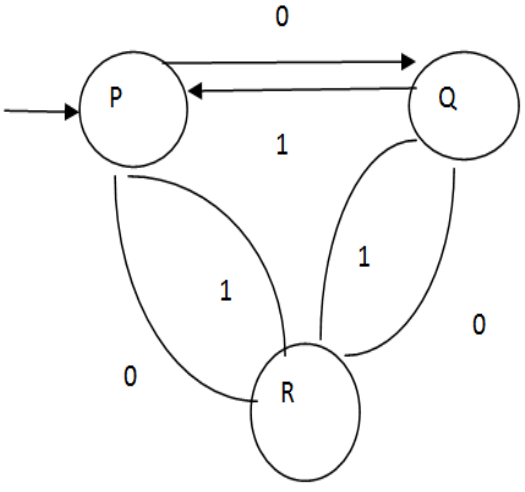



Fig.9 Transition Diagram

Since every DFA is an NFA ,it is clear that the class of languages accepted by NFA's includes the regular sets.

C) Markov process:

Random process is the Markov process, where the value of the process depends only upon the most recent previous value and is independent of all values in the more distant past.

D) Markovian:

User authentication process { X(t) } is said to be Markovian if

$P[ X(t\ n+1) \leq xn+1 / X(tn) = Xn, X(tn-1) = xn-1 \ldots X(t0)=x0)]$

$= P[X(tn+1)/xn+1 \leq X(tn) = Xn]$

Where $t0 \leq t1 \leq t2 \leq \ldots \leq tn \leq tn+1$

Here $X_0, X_1, X_2, X_3 \ldots X_n, X_{n+1}$ like the user state($X_0$), service provider state($X_1$), bio metric server state($X_2$) are called the states of the process. If the random process at time tn is in the state $X_n$, the future state of the random process $X_{n+1}$(bio metric server) at tn+1 depends only on the present state $x_n$ (service provider state) and not on the past states(user state) $X_{n-1}, X_{n-2}, \ldots X_0$.

## VII. MERCHANT AUTHENTICATION

A) Merchant Authentication and Customer to Third party:

When the Transaction Merchant authenticates himself to third party. The authentication takes place as below

**Step 1:**

Using the Predicate calculus, x is a Merchant

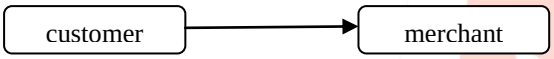
Here, predicate is " is a merchant" and it is denoted by M subject is "x" and it is denoted by x.

"X is a merchant" can be denoted by M(x).

In similar customer Id and timestamp denoted by $ID(c) \wedge Ts_b(c)$

**Process 1:**

$ID(c) \wedge Ts_b(c)$




$ID(c) \wedge Ts_b(c) \rightarrow M(x)$ : customer sends his Id and time stamp value to the merchant.

**Step 2:**

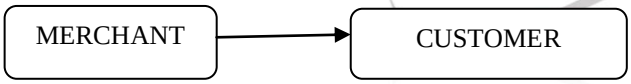
$C(y) : ID(c) \wedge Ts_b(c)$

Merchant id and time stamp denoted by $ID(m) \wedge Ts_a(m)$

Z is a customer so denoted by c(z)

**Process 2:**

$ID(m) \wedge Ts_a(m) \wedge c(y)$




$ID(m) \wedge Ts_a(m) \wedge c(y) \rightarrow c(z)$: The time stamp value and id is forwarded by the merchant.

**Step 3:**

W is a Third party, it is denoted by Tp(w)

Process 3:

$ID(m) \wedge Ts_a(m) \wedge c(y) \rightarrow Tp(w)$

**Step 4:**

Tp(w) : w is a Third party

K(w) : w Generates the key

**Process 4:**

$Tp(w) \rightarrow k(w) \wedge$ finds M(x) then $Tp(w) \rightarrow c(z)$ : After generating the key kab Tp(w) finds the M(x) and sends the other information to the customer.

**Step 5:**

E(c ) : c is extract the key.

H(c) ; c calculates the hash code

**Process 5:**

$C(z) \rightarrow E(c) \wedge H(c)$: customer extracts the key and calculates the hash code after receiving the information.

**Step 6:**

H (c) is true then c (z) is completes the authentication process.

Merchant(Service provider) authentication implementation is done by using matlab.

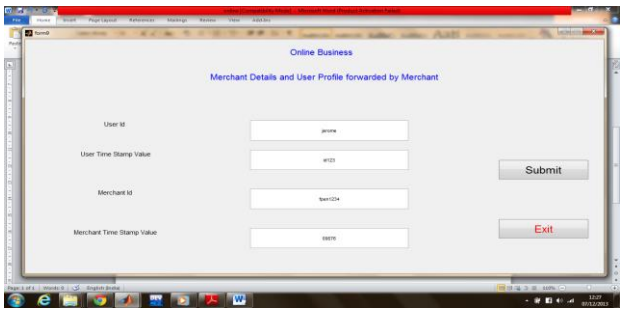



Fig. 10 : User details and merchant details are send to Trusted third party

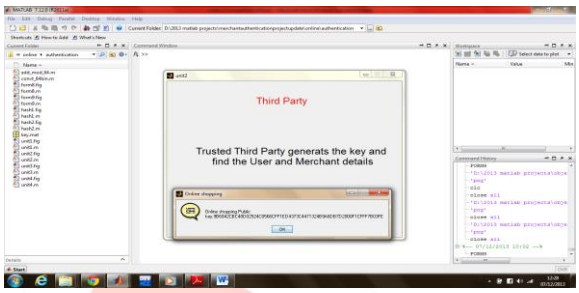



Fig 11 : Third party generates the key by RC4 algorithm and find the user and Merchant profile.

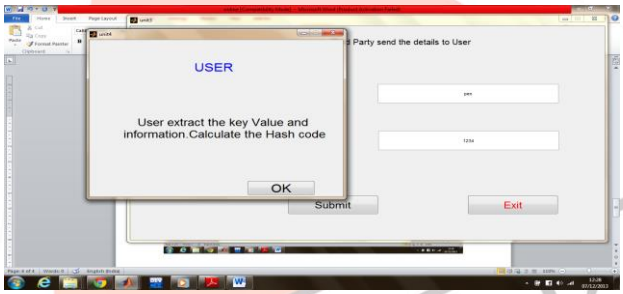



Fig.12 User extract the key and calculate the hash code to find the Merchant is authenticated are not.

## VIII. CONCLUSION

This paper only explained the User authentication, Merchant authentication. 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 safely and reliability of the Mobile E-commerce transactions. Customer details and pin distribution in secure manner, this secure transaction deals with in next paper.

## REFERENCES

[1] www\\htttp:\\mobile commerce
[2] Meeker, Mary ,Global Technology Internet Trends Morgan Stanley, November 15,2005 .
[3] Vesselin TzvetkovArcor AG & Co.K¨olner Strasse 5, WAP Protocol Security Solutions for Mobile Commerce2002.
[4] Jerry Gao, Vijay Kulkarni, Himanshu Ranavat, Lee Chang, A 2D Barcode-Based Mobile Payment system**,** 2009 IEEE .
[5] Wan S. Yi1, Woong Go2, Dongho Won1, Jin Kwak2∗, Secure Authentication Protocol with Biometrics in an M-Commerce Environment.
[6] Chang-Lung Tasi, chun-jung chen, Deng-jie Zhuang, secure OTP and Biometric verification scheme for Mobile Banking, IEEE, 2012.
**[7]** Sugata Sanyal, Ayu Tiwari and Sudip Sanyal, **A Multifactor Secure Authentication System For Wireless Payment.**
[8] MasterCard Inc.: (1997), **SET Secure Electronic Transaction Specification**, Book 1: BusinessDescription, MasterCard Inc., May 1997.

[9] Mangala Belkhede, Veena Gulhane, Dr. Preeti Bajaj, **Biometric Mechanism for enhanced Security of Online Transaction on Android system:** A Design Approach, Feb. 19~22, 2012 ICACT2012.
[10] www\\http:\\Fuzzylozic
[11] Suzhen Waang,Lijie Fan,"A solution of mobile e-commerce Security problems**"**,IEEE,2010.
[12] Virginia Espinosa-Dur6, Minutiae Detection Algorithm for Fingerprint Recognition, IEEEAESS S)istems Mugazine, March 2002.