Scheming an Hybrid Architecture for High Secure M-Commerce Applications

[1]W.S.Callina Jeba Kumari,[2]Mrs.P.Asha

[1]Student, [2]Associate Professor & Head
M.N.M Jain Engineering College, Chennai

Abstract - Mobile Commerce is having the biggest benefit of providing mobility to the customers anywhere at any time. Here namely three types of authentication like User, Merchant and Message authentication is been guaranteed providing availability, reliability and security in transaction phases. Wireless Application Protocol is been established to provide end to end security using encryption model. TLS/SSL protocol is used to transfer data and product between WAP gateway and server. WTLS and TLS/SSL protocols use a message authentication code (MAC) technique to provide the data integrity. The Proposed work improves user authentication by Biometric based Finger Print Reversible data hiding technique, Fingerprint feature extraction , PIN distribution, Encryption and Decryption techniques. (abstract)

IndexTerms - MAC, WAP-Gateway, Double Encryption Model , Biometric Techniques, Miniture Matching, AES.

I. INTRODUCTION (HEADING 1)

Mobile commerce has exploded in the last five years. In fact, Bank of America predicts US$67.1 billion in purchases will be made from mobile devices by European and US shoppers in 2015.1 Several factors are driving this rapid growth of m-commerce. Another driving factor is consumer demand for applications for buying and selling goods and services, as well as for online banking and bill payment. Nowadays, most banks and brokerage firms provide mobile apps for their customers to support online banking and trading. The final factor is the rapid adoption of online commerce due to stronger security practices. For example, authentication techniques that use multiple factors or out-of-band verification are common practices now. A variety of m-commerce products and services have thus emerged. These include mobile money transfer, mobile ATM, mobile ticketing, content (video and audio) purchase and delivery, and location-based services (local discount offers). New applications are also developing quickly. Mobile payments can be made directly inside of a mobile app running on a smartphone.

Superiority of M-Commerce

M-commerce defined as “the delivery of electronic commerce capabilities directly into the hands, anywhere, via wireless technology”. The M-commerce means purchase from everywhere and it is much easier than E-commerce. E-commerce means purchase from home or 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. The users expect immediate response and provide the exact result based on context. M-Commerce occurs through the use of wireless devices such as cell phones, pocket PC's, and PDAs. It allows a user to purchase goods and services on the move, anytime, and anywhere

Mobile Wins PCS

M-Commerce is becoming a larger part of the internet commerce experience. Juniper Research performed a study that predicted that by 2009, global M-Commerce revenue will exceed 88 billion dollars. A Morgan Stanley report found that in 2005 there was 19.5 billion dollars in M-Commerce transactions. These included revenue from people buying ring tones, cell phone personalization, games, and services. With the large amount of revenue potential, companies are quickly moving into the mobile marketplace.. In many countries of the world it is more likely that an individual will have a cell phone rather than a computer with internet connectivity. McKinsey research firm reported that in 2005, there was an estimated 85% penetration rate for mobile phone usage in Europe but in Asia there were over 310 million mobile devices .The Morgan Stanley research report mentioned earlier shows that in many areas of the world the number of mobile users exceeds the number of PC users. These scenarios are highly attractive to companies because it provides an opportunity to expand their customer bases. This means there is a potential to reach millions of new customers and expand on revenues.

Mobility

The biggest benefit that M-Commerce provides to consumers is mobility. As long as their mobile device network is in range then M-Commerce transactions can be made. In order to meet these demands, cell phone companies across the world are continually upgrading their networks and increasing the speed and bandwidth of these networks.

Scope of the Project

It enhances the security of the trusted device and minimizes the possibility of security breach in Authentication scheme. Provides greater amount of security in M-Commerce transactions such as Location Based Services, Mobile Ticketing, Mobile Shopping, Mobile Financial Services, Mobile Marketing, Mobile Entertainment and so on. For promotion of mobile transaction among users a secure M-Commerce Architecture has been built, providing three way security like user authentication, merchant authentication, message authentication and building a complete solution for M-Commerce applications.

II. EXISTING SYSTEM

In our system the entire PIN can be obtained if the external network is cracked so that third party can easily enter. Authentication of user and merchant is totally under Absence. Security is not assured. So that our customer details will be sent to financial Institutions. The customer selects the product which he wishes to buy and the product Details will be sent directly to the customer where the customer chosen product can easily been traced in the existing system. Due to external network damage it is easy to acquire Someone's PIN number. Biometric feature extraction algorithm used in our system failed to produce accurate results. Lack of security for M-Commerce applications.

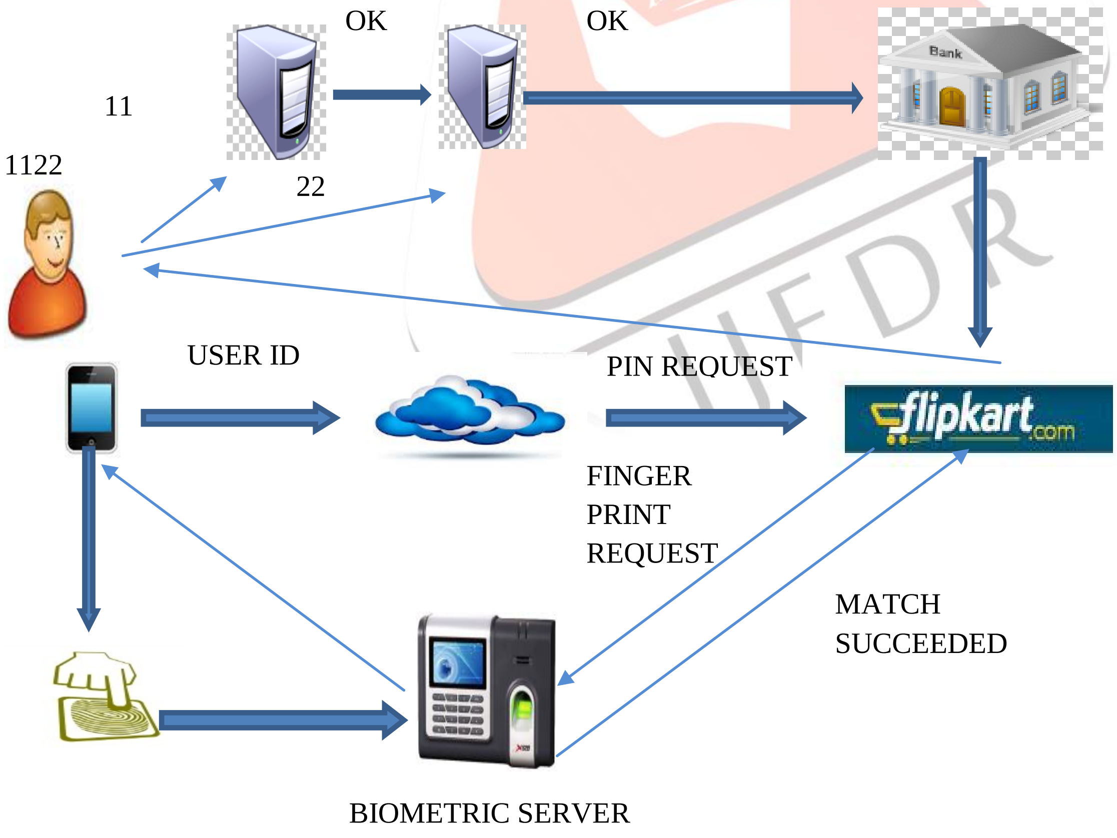
III. PROPOSED SYSTEM

The proposed application improves user authentication by a number of techniques as mentioned below

- Biometric server – Finger Print extraction
- Finger print feature extraction – MINITURE MAPPING
- Reversible data hiding – DWT ALGORITHM
- PIN distribution architecture
- Research on implementing effective encryption

algorithms among RC4, AES, TWO FISH, SHA.

System Architecture



Module Description

The entire system is been divided into a number of modules for their detailed description.

- Finger Print Identification

- Data Hiding Technique
- Finger Print Extraction
- Finger Print Comparison
- PIN Distribution

Finger Print Identification

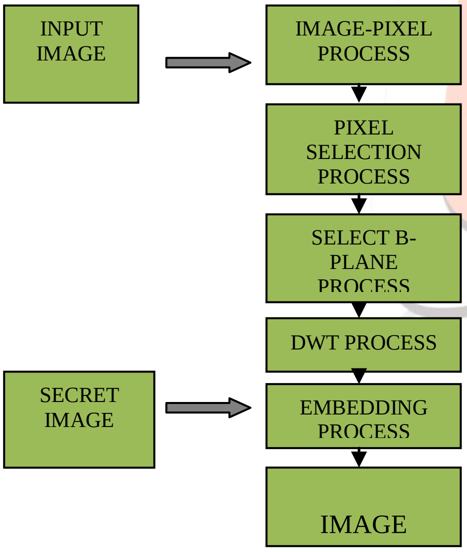
It is the method of identification using impression made by minute ridge formation or patterns found on finger tips. No two persons have exactly same arrangement of ridge patterns, due to distinctiveness, compactness and compatibility Minutiae based representation is used. Uniqueness of fingerprint is determined by local ridge characteristics and their relationship because it is an infallible means of personal identification.

Data Hiding Technique

Reversible data hiding is a technique where the original cover can be losslessly restored after the embedded information is extracted. The user finger print is transferred to the biometric server in a secure way using DWT algorithm. DWT stands for **DISCRETE WAVELET TRANSFORM**. DWT is used to improve data-hiding capacity and retain good stegno - image quality. The secret message is inserted directly into the pixels. Our proposed method is to embed secret data into the coefficients after quantizing and rearranged in the quantization factors using wavelet filter for a cover image, and to recover the original image.

DWT ALGORITHM:

Step 1: Read IMAGE.
Step 2: Convert to PIXELS.
Step 3: Select cover IMAGE.
Step 4: Convert to any single PlaneProcess.
Step 5: For that Plane convert to DWT Process
Step 6: Select Secret Image.
Step 7: Embed that Secret Image with Key
Step 8: Write Image
Step 9: Reconstruct IMAGE.



Finger Print Extraction

Minutiae points are the locations where a ridge becomes discontinuous. A ridge can either come to an end, which is called as termination or it can split into two ridges, which is called as bifurcation. A number of techniques is been carried over in minutiae based finger print extraction. First stage is to find the centre point which is of region of interest and then cropping is carried out. After that Binarization is an effect which converts grayscale image to binary image by fixing the threshold value, pixel value above and below threshold value are said to be '0' and '1'. Binary image is thinned using Block filter to reduce thickness of all ridge lines to single pixel width to extract minutiae points effectively. It does not changes the location and orientation and provides accurate estimation of minutia points.Thining preserves outermost pixels by placing white pixels at boundary of image Dilation and erosion are used to thin the ridges.

MINUTIAE ALGORITHM

Finger print recognition based on

local ridge feature where markings

are carried out accurately and false

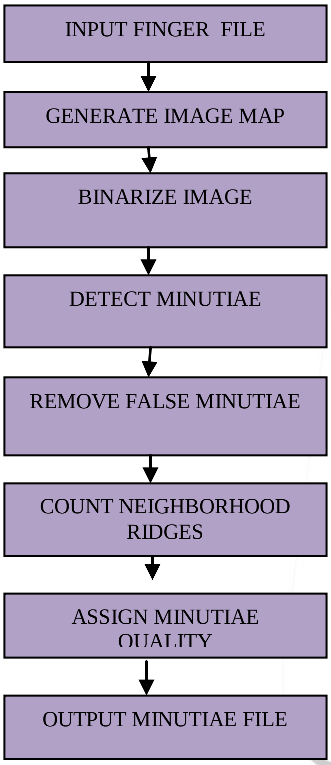
ones are rejected.

T,Q :Feature Vector where each element is minutiae point).
(location, orientation , quality of neighbor).

X,Y : Minutiae location.

Teta : Minutiae angle

m,n : Number of minutiae points in T,Q.



Finger Print Comparison

After minutia extraction the location and angles are derived. The termination lying outside the boundary are not said to be considered as minutia points which is been calculated by using crossing number. Crossing number is half the sum of difference between intensity values of 2 adjacent pixels. Finger prints of customers will be recorded on a database for personal identification said to be known as the reference database. Minutiae-based fingerprint matching system usually returns the number of matched minutiae on both query and reference fingerprint and uses it to generate similarity scores. When two fingerprints have a minimum of 12 matched minutiae, they are considered to have come from the same. So the minutiae based comparison gives the accurate results in user authentication. Matrix format is used for efficient matching in minutiae.

PIN Distribution

After the user is said to be authenticated, the request for PIN number is been sent. AES stands for Advanced Encryption Standard which is a symmetric encryption algorithm used for PIN distribution where there is no intrusion of third party. PIN number is said to be a sensitive data of the customer which need to be handled carefully. The decryption of the encrypted text is possible only if we know the correct password and in addition same key is used for encryption and decryption. PIN distribution and transactions are carried out in android to deliver electronic commerce capabilities via wireless technology.

AES Algorithm

1. Key—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

- Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

- Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- Add Round Key

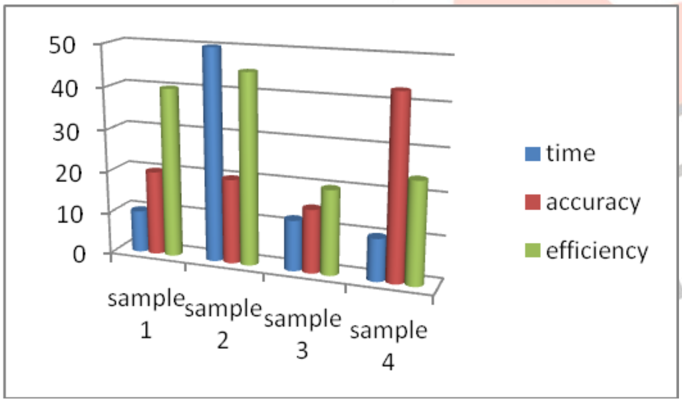
4. Final Round (no Mix Columns)

- Sub Key
- Shift Rows
- Add Round Key

.

IV. SIMILARITY MEASURES

AES key expansion algorithm is used to derive 128 bit round key for each round from the original 128 bit encryption key First four bytes of encryption constitute to word w0 and so on and the algorithm expands word into a 44-word key schedule
Four words of round key for final round. In Minutiae matching the local ridges is clearly identified and given more importance unlike in gabor filter algorithm.



Complexity

Calculation time may exceed due to the number of rows and columns in shifting in PIN Distribution.As we are using Minutiae matching algorithm calculation is made faster because there’s no need to scan each data set at every time while processing.

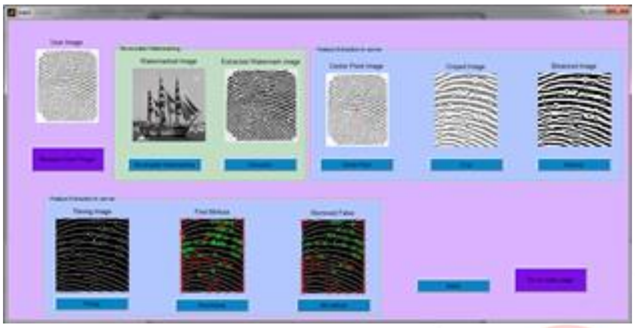
Related Work

A number of studies had been made on M-Commerce to provide User authentication, Merchant as well as Message authentication. In data hiding technique DWT shows robustness and imperceptibility when compared to DCT, where original image is extracted without any distortion and additionally frequency and time domains are obtained. In encryption technique AES is chosen to be the best as it performs ten times faster than DES, 3 DES algorithms and the same key is used both for encryption and decryption techniques. For finger print feature extraction some fingerprints are collected and stored in the database , upon matching the query and the representative template the person is said to be authenticated or not. The algorithm called Minutiae mapping is superior when compared to other algorithms because in minutia the local ridges is given more importance as the edges of the person be the same, but the ridges vary.

V. RESULT

The wavelet transformation is a mathematical tool that can examine an image in time and frequency domains. Discrete Wavelet Transform is simple and fast transformation approach that translates an image from spatial domain to frequency domain. The main requirements of data hiding is imperceptibility and robustness which will be gained in DWT when compared to DCT. The Capacity is also more in DWT.

Minutiae mapping is a finger print extraction technique where complex features can be expresses as a combination of ridge ending and bifurcation. It takes lesser time to run where in Fuzzy Logic the program has to run for each individual patient and so it provide high Performance, Scalability and timely execution. The ridge type, number, spatial relation ridge lines, shape of fingering is obtained from global features. More matched yield higher similarity score when two finger print have minimum 12 matched Minutiae. The below Figure shows the number of processes that takes place while finger print feature extraction in the Biometric Server.



AES algorithm is used for PIN distribution. It is a symmetric encryption algorithm protecting secrecy of message . Encryption is about 10 times faster than DES. The same key is used for both encryption, decryption techniques and so there is no intrusion of third party.

VI. CONCLUSION

In spite of the limitations of a mobile device, the user authentication scheme is highly effective and provides immense security. The merchant’s authentication makes sure the customer is transacting with the right person. Effective fingerprint feature extraction algorithms Minutiae Maps is implemented for user authentication. The user information i.e., Fingerprint is sent to the biometric server in a secure way using data hiding technique. For data hiding we have implemented Discrete Wavelet Transform (DWT) for security. PIN distribution is made effective by Double Encryption technique with the use of AES Algorithm.

VII.ACKNOWLEDGMENT

The fingerprint boundary of persons can be similar, but the ridges will be different. Minutia based representation matching will be accurate and in rare case mismatch occurs and in such situation we can choose an algorithm which enhances accuracy both in identity and time consumption. The authors would like to thank the editors and reviewrs for their constructional comments and suggestions that help improving quality of paper.

REFERENCES

[1] Chang-Lung Tasi , Chun-jung chen, “Secure OTP and Biometric Verification Scheme”, 2012 IEEE , DOI 10.1109.

[2] Davide Maltoni, “Handbook of Fingerprint Recognition”, Springer Science & Buisness Media,2005.

[3] John Chrillo, “Implementing Biometric Security” –Wiley Red Books, May 9, 2003.

[4] Jerry Gao , Vijay Kulkarni, Lee Chang, “Barcode Based Mobile Payment”, 2009 IEE, DOI 10.1109

[5] Sameer Singh, Maneesha Singh, Chid Apte “Pattern Recognition and Image Analysis” Springer Part II.

[6] Sugata Sanyal , Ayu Tiwari, “Secure Electronic Transaction Specification”, MAY 2011, Journal in Advance sciences.

[7] Wen-Chen Hu, “Handheld Computing for Mobile Commerce” Information Science Reference, April 9, 2010

[8] Wan S. Yil , Woong G02,Dongho Won1, “Secure Authentication Protocol with Biometrics”, 2010 IEEE , VOL 2.