International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

ADVANCED TWO FACTOR AUTHENTICATION USING IMAGE PROCESSING

S. Jeyalakshmi[1], H. Vaitheeswaran[2], S. Vashanth[3], G. Vignesh kumar[4], S. Vijayan[5]

[1]*Asst. Prof, Dept. of Information Technology, Valliammai Engineering College, Chennai, Tamil Nadu*
[2,3,4,5]*B. Tech, Dept. of Information Technology, Valliammai Engineering College, Chennai, Tamil Nadu*

Abstract - *Mobile commerce is an emerging trend. Mobile commerce provides users to perform shopping, order food, m-payments, etc. These increasing trend leads to security threats. This paper is focused on users authentication and security. Existing system used for mobile payment services in handheld devices doesn't involve biometric authentication. Hence leading to misuse and confusion among m-commerce users, User authentication is performed by using fingerprint analysis invoking fusion of 2 algorithms namely Minutiae Maps (MM) and Orientation Map (OM). Also to enhance and provide more security we integrate IRIS recognition of the users. Fingerprints are the most used biometrics in mobile applications at recent but it has not been implemented in mobile transactions. This project implements the identification procedure. It matches one fingerprint among N fingerprints. It uses minutiae points based algorithms. In the enrollment step, the points are extracted from the print. Later on, during the authentication step, the points are matched. They are implemented using fingerprint enhancement and minutiae filtering. Then for IRIS recognition, K-NN classifiers are used. For effective encryption and decryption we implement the algorithms among RC4, AES, DES, 3DES. For PIN generation we are using PIN distribution technique and for message authentication purpose we are using more secured algorithm like SHA algorithm.*

Key words: K-NN Classifier, MM – Minutiae maps, OM-Orientation maps, PIN – Personal Identification Number

1. INTRODUCTION:

Online banking transaction is developing and mostly used by every merchant user in recent times. More than millions of customers using online transactions. Authentication is the only process to validate and verify the users. One time password (OTP) is the only security added in present time for authenticating users. As the users increases, intruders and security breaches also increases. To increase more security we can adopt our bio-metrics for the authentication. The main objective of this research project was to create a performing and accurate program for fingerprint identification. Also to enhance and provide security we integrate IRIS recognition of the users. For IRIS recognition, we used K-NN classifier algorithm. For effective encryption and decryption we are using the algorithms such as RC4, AES, DES, 3DES. For PIN generation we are using PIN distribution technique. Message authentication purpose, we are using more secured algorithm like SHA algorithm. I choose the subject of fingerprints because it involves different fields like pattern recognition, statistical tests, minutiae detection, performing algorithm programming. Fingerprint recognition stands for me as a stereotype in pattern recognition and detection. Techniques used in this field can be reused in other applications. Added to that, high security issues led to a lot of research on fingerprint recognition, meaning that the techniques we used are advanced.

2. OBJECTIVE

This project is proposed to provide greater security in online transactions.

- And our main motive is to minimize the possibility of security breach in Authentication scheme.
- Then to provide secure forwarding infrastructure and to provide useful privacy and secure public policy framework.
- Finally we had developed to enhance the confidentiality and integrity in online banking transactions.

3. RELATED WORK:

Online banking dealings were developing and largely employed by each people in gift year. Over scores of customer's victimization on-line transactions. Authentication is that the solely method to validate and verify the users. Only once secret (OTP) is that the solely security value-added in nowadays for authenticating users. Because the users will increase, intruders and security breaches conjointly will increase. To extend a lot of security we are able to adopt our bio-metrics for the authentication. We choose the topic of fingerprints as a result of it involves completely different fields: pattern recognition, applied mathematics tests trivialities detection, playacting formula programming. Fingerprint recognition stands on behalf of me as a stereotype in pattern recognition and detection. Techniques employed in this field will be reused in alternative applications. additional to it, high security issues diode to plenty of analysis on fingerprint recognition, For encryption and decryption we used different algorithms like RC4, AES, DES, 3DES. Thus finally we used Pin distribution algorithm for distributing the PIN. Thus, Our project

promotes and focuses on the users authentication in safe and secured way for safeguarding the users in bank transactions.

In [1] "A Brief Review of the Iris Recognition Systems for Developing a User-Friendly Biometric Application", IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017) by Jagadeesh N and Dr. Chandrasekhar M. Patil in 2017: A biometric system offers automatic identification of a human being based on the unique feature or characteristic which is being possessed by the individual. A number of biometric techniques exists in the current scenario, viz., finger print, iris, face, etc. The iris segmentation is one of the most dominant type used in all Aadhar card applications & has its own major applications in the field of surveillance as well as in security purposes. The performance of an iris recognition systems depends heavily on the feature extraction, histogram, and segmentation with normalization techniques.

In [2] "A Survey on Iris Recognition System", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016 by Sandeep Patil, Shreya Gudasalamani, Nalini C. Iyer in 2016: Biometrics recognition is the use of physiological and behavioral traits to identify an individual. Many biometric traits have been developed and are being used to authenticate the person's identity. Iris recognition systems are widely used and have been proved to be efficient at individual recognition with high accuracy and nearly perfect matching. the Iris images are gathered from the publically available Iris database The Iris feature of two eyes of same person are not similar making it more secured way of authentication compared to other Biometric recognition systems. The various stages of processing involved in the design of Iris recognition system are Localization of eye, Boundary segmentations of Iris and pupil, Normalization, Local feature extractions and Matching.

In [3] "Fingerprint Based Biometric ATM Authentication system", IEEE International Journal of Engineering Inventions, e-ISSN: 2278-7461, p-ISSN: 2319-6491, Volume 3, Issue 11 (2014) PP: 22-28 by Dhiraj Sunehra in 2014: Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The various features used are face, fingerprints, hand geometry, handwriting, iris, retina, vein and voice. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization. These unique fingerprint traits are termed "minutiae" and comparisons are made based on these traits.

In [4] "An improved algorithm for feature extraction from a fingerprint fuzzy image", by kamil surmacz*, khalid saeed, piotr rapta in 2013: Proper fingerprint feature extraction is crucial in fingerprint-matching algorithms. permanently results, different items of knowledge a couple of fingerprint image, like ridge orientation and frequency, must be thought of. it's usually necessary to boost the standard of a fingerprint image so as for the feature extraction method to figure properly. During this paper we tend to gift an entire (fully implemented) improved algorithmic program for fingerprint feature extraction, supported various papers on this topic. The paper describes a fingerprint recognition system consisting of image preprocessing, filtration, feature extraction and matching for recognition. The image preprocessing includes normalization supported mean and variation. The orientation field is extracted and physicist filter is employed to organize the fingerprint image for additional process

4. PROPOSED SYSTEM:

This project is mainly focused on Fingerprint recognition, IRIS recognition and PIN authentication. Thus fingerprint recognition provides more security for online transactions. Then IRIS recognition integration provides high security and avoid fake users. Thus two steps are done to perfectly validate the users and avoid fake users. The biometric image of the user is sent safely to biometric server via WAP gateway. Effective finger print extraction algorithm like OM, MM, Core point detection, Gabor filter, OCM are used and they are used to identify the fingerprint. IRIS recognition is implemented using K-NN classifier. PIN distribution technique are used to finally verify the users. We researched on implementing effective encryption algorithms among RC4, AES, DES.

5. SYSTEM ARCHITECTURE:

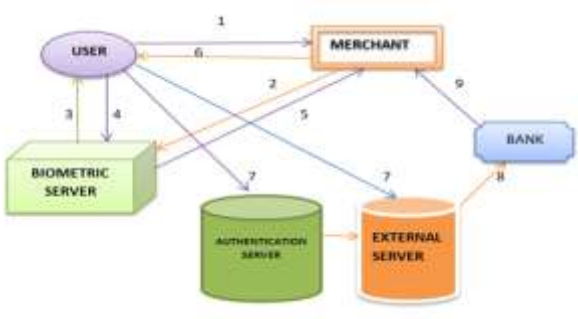

Fig- 1: System Architecture diagram

The above diagram clearly explains that the customer or user wants to purchase some products or items they should place the products in a cart and then wants to pay the appropriate amount for the product. Hence, The product merchant confirms the order. The merchant gateway invokes the biometric server for money transaction. Then the biometric server request the user to give the biometrics. As a

response the user gives the biometrics. They are acknowledged to the payment gateway merchant that the biometrics are given and they will intimate the user that are biometrics are taken as an input successfully, then they are authenticated with the help of the authentication server by the given inputs. If the authentication server fails the external servers are used to authenticate the users. Thus backup servers are known as external server. Thus finally, money gets transacted to the bank if biometrics placed are legitimate and matched with the appropriate user and are given to the appropriate merchant. Thus, the user was authenticated and transacted the money in a secured way. This will be very effective when compared to other authentication schemes.

6. METHEDOLOGY:

For implementation the entire system has been divided into the following modules:

- IRIS recognition
- Fingerprint recognition
- PIN distribution

A. IRIS recognition:

IRIS is recognized by KNN-classifiers. In pattern recognition field, KNN algorithm is one of the most important and secured non-parameter algorithms and it is a supervised learning algorithm. The classification rules are generated by the set of training samples itself without the need of any additional data. The KNN classification algorithm predicts the test sample's category according to the K training samples which are the nearest neighbors to the test sample, and judge it to that category which has the largest category probability. Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region so that it has fixed dimensions in order to allow comparisons. The detection inconsistencies between eye images are mainly due to the streching of the iris caused by pupil dilation from varying levels of illumination. The IRIS recognition module is described below as follows,

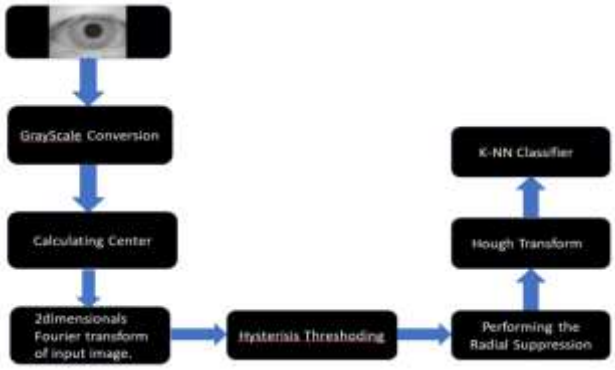

Fig – 2: IRIS recognition flow diagram

The described iris recognition process will be shown in fig.3 as below as follows,

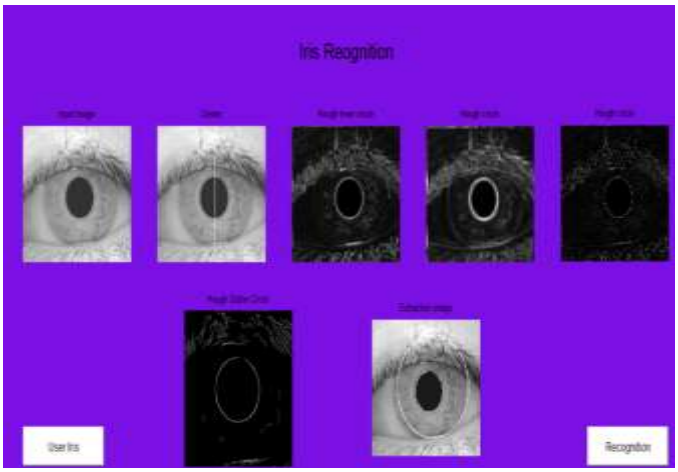

Fig - 3: IRIS recognition module

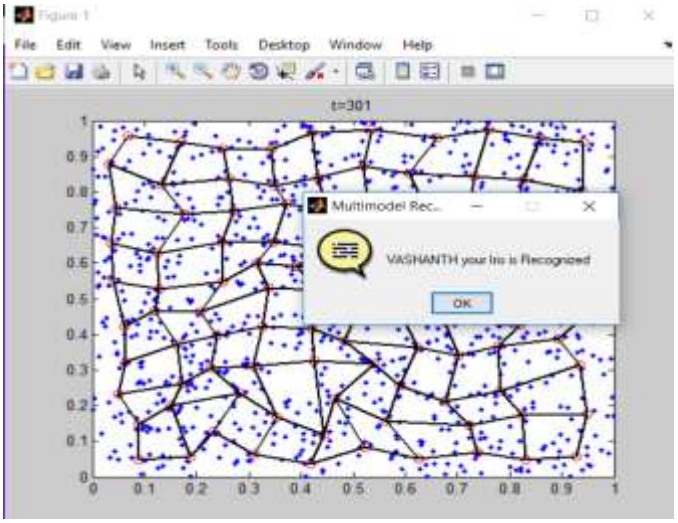

Fig – 4: Classification and recognition module

B. Fingerprint recognition:

The orientation info per pel is just required to enhance the fingerprint. This method is completed to extend the quality of the print by reducing the noise, filling some tiny gaps and enhancing the ridges and valleys. The Gabor filters are usually utilized in fingerprint identification algorithms. Histogram equalization improves distinction of the input image by uniformly distributing intensity levels on whole image manufacturing uniform bar chart. So new intensity values replaces all the previous intensity values manufacturing bright and increased image. Minutiae points are extracted throughout the enrollment process and so for every authentication. In an exceedingly fingerprint, they correspond to either a ridge ending or a bifurcation, there's a duality between the two kinds of minutiae: if the picture element brightness is inverted, ridge endings become bifurcations and contrariwise. The position of the detail

purpose is at the tip of the ridge or the valley. The orientation is given by the orientation of the arrow formed by the ridge or the depression. Steganography is the process of hiding a secret message within an ordinary message and the detection of hidden content is called as steganalysis. We propose an optimal discrete wavelet transform based steganography. First decomposition is done on a host image and the secret information is hidden by manipulating the transform coefficients of the decomposed image. After embedding, the stego image is subjected to various types of image processing attacks like Gaussian white noise, salt and pepper noise, blurring and sharpening. Experiments show that the peak signal noise ratio generated by the proposed method is better. The Fingerprint recognition is described as follows,

Fig – 5: – Fingerprint recognition module

C. PIN distribution:

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. Each part separately will be processed to produce the decimal sequence number. The PIN distribution is shown in Fig. 4.1.3.b. Recent 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.

Fig – 6: PIN seperation

Fig 7: PIN encryption

Fig – 8: PIN decryption

7. FUTURE ENHANCEMENT:

Advanced two factor authentication can be useful for banking in future. Now, fingerprints are mostly used and trending in all mobile phones, laptops, tablets. But iris recognition is developing step by step and now implemented in some mobiles. If they are implemented in every mobile phones then these authentication will helpful in banking sector and provides a better security with high performance and reduces the time of authentication. Since the finger print and iris are unique for every humans, they can be integrated and used in all the authentication purposes. This can be the perfect solution choice for the challenging security in banking sectors.

8. 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.

9. REFERENCES:

1. Jagadeesh. N, Dr. Chandrasekhar M. Patil, "A Brief Review of the Iris Recognition Systems for Developing a User-Friendly Biometric Application", International Conference on Energy, Communication, Data Analytics and Soft Computing, 2017

2. Sandeep Patil, Shreya Gudasalamani ,Nalini C. Iyer, "A Survey on Iris Recognition System", International Conference on Electrical, Electronics, and Optimization Techniques, 2016

3. Dhiraj Sunehra, "Fingerprint Based Biometric ATM Authentication system", International Journal of Engineering Inventions, Vol.4,Issue 11,2014.

4. K Amil Surmacz ,K Halid Saeed, P Iotr Rapta , "An improved algorithm for feature extraction from a fingerprint fuzzy image", IEEE Transactions on Pattern Analysis and Machine Intelligence VOL.43, Issue.3, 2013

5. Aayushi Mishra,Manish Mathuria, "Multilevel Security Feature for OnlineTransaction using QR Code & Digital Watermarking", International Conference on Electronics, Communication and Aerospace Technology,2015