Secure OTP and Voice Authentication by using KIVOX Mobile software scheme for Mobile Banking

Dr.B.Vanathi
Professor& Head Department of CSE
SRM Valliammai Engineering College
Chennai, India
mbvanathi@gmail.com

K.Shanmugam
Assistant Professor, Department of CSE
SRM Valliammai Engineering College
Chennai, India
Shanucan87@gmail.com

***Abstract*—In a mobile commerce process, user authentication is major fact. In existing system one time password (OTP) and Fingerprint Authentication is used for user verification. In this paper Multi factor authentication is used. Multifactor authentication consists of knowledge-based authentication (user ID and password), one time password (OTP), and Fingerprint and Voice authentication. First Multifactor process is user login with their user ID and password.Server to verify the userID and password. If the user password is not correct, the server rejects the transactions. User ID and password is correct go to the next transaction. Second process is, Finger image is send to the server.If finger print image is verified by fuzzy logic and find out the threshold level. Threshold level is 60-99%, OTP is generated by server. Third process is, Server sends the OTP to the user by using QR code with encrypted form by user mobile device password. Encryption is done by AES 256 bit algorithm. User find the OTP by QR code reader in have the android mobile. This is already built the QR reader Application in mobile so easily find out the OTP. User decrypts the OTP by using mobile device password. Final process is verifying the user voice authentication by server using KIVOX Mobile software. . KIVOX Mobile software provides a platform for the use of simple, short voice authentication that is accurately detected 99.9% of the time. Therefore, Multi factor authentication is provided the greater security and confidentiality, Data integrity is achieved in mobile banking Transaction**

Keywords— M-commerce, QR code ,Fingerprint, KIVOX mobile software

I. INTRODUCTION

Today we are living in digital kingdoms having computer 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. Firstly hacking, from the internet any one can hack the username and password and the result is third person gets access to owner account. As anyone is not with twenty four hours on the Internet, i.e. access bank website, it takes some time to know that your account get hacked and third one can get transfer the money to his own account. Secondly, every time one has to carry laptop or PC with you. So for this issue secured payment applications on mobile device i.e. M-commerce is proposed.

Today is the era of mobile, everyone having the mobile in his hands, instead of using the laptop or PC, mobile is the best option to use for the banking purpose. The next generation of banking applications won't be on desktops or mainframes but on the small mobile devices we carry every day. Secured e-banking on the mobile is the latest issue for all mobile users. 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 in that 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 [1]. 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.) [2], 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 [3].

Fingerprint is probably the most used for biometric authentication. It is also likely to be the oldest biometric in use. There is archeological evidence that fingerprints as a form of identification have been used at least since 7000 to 6000 BC by the ancient Assyrians and Chinese. However, biometric authentication is not the silver bullet for secure authentication. We cannot use fingerprint biometrics everywhere instead of passwords or Tokens. Nothing is perfect, and fingerprint biometric authentication methods also have their own shortcomings. Spoofing of biometric systems for misappropriation of biometric data is a realistic security threat. The consequences hereof can be very severe, because biometric characteristics in principle cannot be changed, unless biometric are used in a revocable way. In order to fake a fingerprint, one needs an original first. The hack is to create an artificial finger using a mold that is manufactured using the legitimate user's actual finger. This type of attack is not really usable in real life as people are usually wise enough not to give their fingers as a mold material. However, this hack demonstrates that the scanner can be fooled using a gelatine finger instead of a live finger and can be taken further in technology. Latent fingerprints are nothing but fat and sweat on touched items. Thus to retrieve someone else's fingerprint (in this case the fingerprint you want to forge) one should rely on well tested forensic research methods.In a propose work using voice authentication. Voice authentication is verified by KIVOX Mobile software.

II. RELATED WORK

A. *KIVOX Voice authentication software*

KIVOX Mobile is a Software Development Kit (SDK)[4] which enables on-device secure speaker verification. It can be easily integrated in authentication applications for smartphones and other embedded platforms. KIVOX is AGNITIO´s technology for strong speaker authentication solutions [5].

Enrolment and matching are done locally. There is no need for network connections or voice transmissions. As a result, authentication can be done anywhere [4].

Users can select a pre-defined passphrase or choose its own (in any language) to create a Biometric Voice Print (BVP) which can later be used for verification. KIVOX Mobile only requires three simple steps to start securing your mobile transactions [4].

1) Teach your phone to recognize your voice by speaking intoit;

2) Authorize any App powered by KIVOX technology to use yourvoiceprint;

3) Pay, log-in, unlock, and authenticate yourself to conduct multiple transactions - simply by speaking.

KIVOX Mobile offers a successful detection rate of more than 99.5%, with a false acceptance rate of less than 0.1%. On top of this, with the use of AGNITiO's proprietary patented anti-spoofing technology, KIVOX Mobile detects up to 97% of replay attacks, as well as many other spoofing attacks such as cut-and-paste. The protection is achieved as part of the verification attempt, without the need for any additional steps such as liveness detection [4] [5].

B. *QRCode*

QR Code is a two-dimensional symbol [6]. It was invented in 1994 by Denso, one of major Toyota group companies, and approved as an ISO international standard (ISO/IEC18004) in June 2000. This two-dimensional symbol was initially intended for use in production control of automotive parts, but it has become widespread in other fields. Now QR Code is seen and used every day everywhere in Japan for the following reasons [6].

- Several characteristics superior to linear bar codes: much higher data density, support Kanji/Chinese character, etc.
- It can be used by anybody free of charge as Denso has released the patent into the public domain.
- Data structure standard is not prerequisite for current usages.
- Most mobile phones in Japan equipped with cameras that enable reading of QR Codes can access Internet addresses automatically by simply reading a URL encoded in the QR Code.

C. *QR-code characteristics*

Additional to the characteristics for two-dimensional symbols [6] such as large volume data (7,089 numerical characters at maximum), high-density recording (approx. 100

times higher in density than linear symbols), and high-speed reading. QR Code has other superiority in both performance and functionalities aspects.QR-code characteristics as shown in Fig. 1.

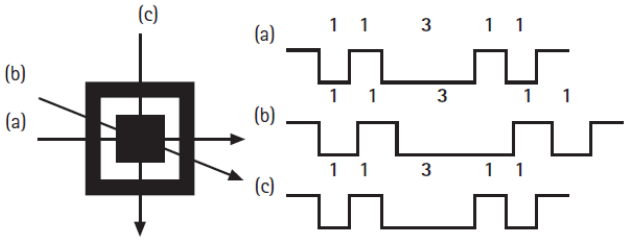

Fig. 1. QR-CODE characteristics [6]

A: All-Direction (360°) High-Speed Reading

B: Resistant to Distorted Symbols

C: Data Restoration Functionality

D. The QR Code Structure

QR Code is a matrix type symbol with a cell structure arranged in a square [6] and this structure as shown in figure 6. It consists of the functionality patterns for making reading easy and the data area where the data is stored. QR Code has finder patterns, alignment patterns, timing patterns, and a quiet zone [6].

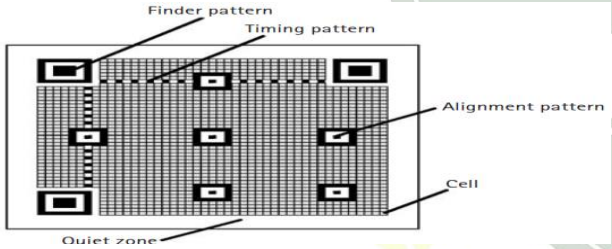

Fig. 2. QR-CODE STRUCTURE [6]

1) Finder Pattern: A pattern for detecting the position of the QR Code. By arranging this pattern at the three corners of a symbol, theposition, the size, and the angle of the symbol can be detected. This finder pattern consists of a structure which canbe detected in all directions (360°)[6].

2) Alignment Pattern: A pattern for correcting the distortion of the QR Code. It is highly effective for correcting nonlinear distortions. The central coordinate of the alignment pattern will be identified to correct the distortion of the symbol. For this purpose, a black isolated cell is placed in the alignment pattern to make it easier to detect the central coordinate of the alignment pattern[6].

3) Timing Pattern: A pattern for identifying the central coordinate of each cell in the QR Code with black and white patterns arranged alternately. It is used for correcting the central coordinate of the data cell when the symbol is distorted or when there is an error for the cell pitch. It is arranged in both vertical and horizontal directions[6].

4) Quiet Zone: A margin space necessary for reading the QR Code. This quiet zone makes it easier to have the symbol detected from among the image read by the CCD sensor. Four or more cells are necessary for the quiet zone[6].

5) Data Area: The QR Code data will be stored (encoded) into the data area. The data will be encoded into the binary numbers of '0' and '1' based on the encoding rule. The binary numbers of '0' and'1' will be converted into black and white cells and then will be arranged. The data area will have Reed-Solomon codesincorporated for the stored data and the error correction functionality.

E. Biometric authentication in mobile commerce

Wan S. Yi, et al, proposed the fingerprint user authentication in mobile commerce [9]. This proposed system provides the high risk of loss, high authentication factor and low computation time. Disadvantages of this system consists of not focused on the finger print matching threshold level ,finger print minutiae matching and pattern matching algorithm is not concerned. Finger print image is send to the biometric server. The way in which to found the user is authenticated person? What the solution of poor image finger print quality? And how to analyze the user fingerprint image? Are not focused and do not provide solution to these question in this paper. Mangala Belkhede,et al (2012) proposed[1] the online transaction by using fingerprint mechanism on android system. An advantage of in this Proposed System focused on the finger print image is how to analyze? That means fingerprint image is analyzed by using fuzzy logic at the server side but not focused on the threshold level(100%,60-99% or below 60%).Chang-Lung Tsai Chun-jung chen,Deng-jie Zhuang (2012) proposed the Onetime password(OTP) and unique biometric based finger authentication for mobile banking in mobile commerce. Disadvantages of this system do not provide the security at transmission level. Biometric verification process is not focused. Based on these disadvantages leads to the proposed level. Dr.B.Vanathi,K.Shanmugam et.al Proposed the more security in mobile commerce transaction process[7].

F. Finger print analysis by using Fuzzy logic

K.shanmugam, Dr.B.Vanathi proposed the biometric finger print mechanism to secure the mobile payment also provides the security at the transmission level [8]. Existing work uses fuzzy logic for comparing the user finger print image but it does not focus on the threshold level. So In this proposed work, it uses fuzzy logic and if the fingerprint matching percentage is in the range of 60-99%, in this case a onetime password (OTP) is automatically generated at server side. Else the system will ask some security questions that are already stored in the database system during registration process. If the OTP is correct, SMS Authentication is generated and User is captured the Short message from the server. By using the SMS authentication, only valid users will receive the SMS from the authentication server. After getting the SMS, a user can acknowledge the choices (Yes/No). When the authentication server receives "YES" it knows that the user is valid and that the user has approved their initiated transaction otherwise denied the transaction. SMS confirmation is a final approval to their initiated online payment transactions. The security of the system also depends on the security of the messages sent by SMS and WAP. Fingerprint image and messages are encrypted and protected with RC4 algorithm by using Double encryption model. Based on proposed work consists of OTP and SMS authentication is to be provided in

60-99% threshold level of user finger print matching percentage in mobile payment user authentication process.SMS authentication is provided in the transaction in threshold level is 100%.

III. PROPOSED PROCEDURE FOR MOBILE BANKING

In current situation, Mobile banking process by using OTP for transaction process is initiated as the client side presents the request of transaction application. The server side generates the OTP and send to the client mobile phone. After then, user enter the correct OTP in particular transaction web page of mobile banking for user authentication purpose.so in this method easily trace out the OTP by external hackers.

In this paper, OTP is generated by the server and send the OTP by using QR-code and also Encrypt the OTP by using RC4 algorithm and send to the user. So more secure authentication is achieved by proposed work.

Multifactor authentication is providing by proposed idea. It consists of username and password, Fingerprint authentication, OTP send by using QR-code in server side and Voice authentication.

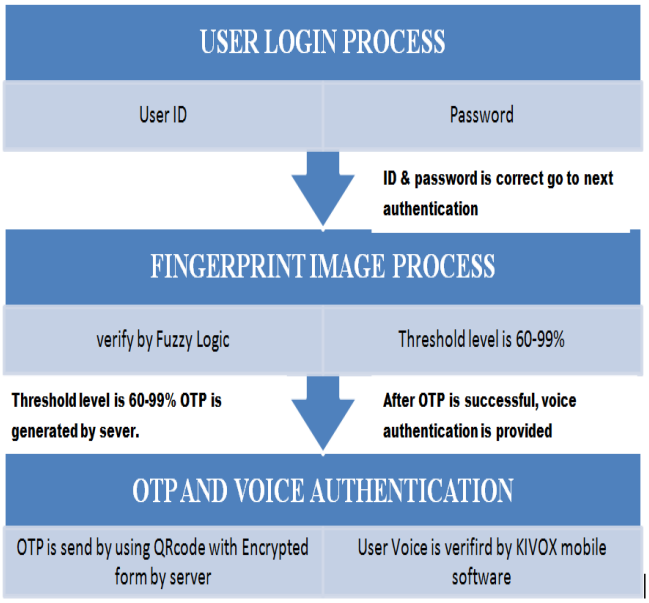

Fig. 3. Mobile banking Process

The detailed procedure of using secure mobile banking process through mobile phone is as the following.

Step1: user login with their user ID and password.

Step 2: Server to verify the userID and password.If the user password is nor correct,the server rejects the transactions.User ID and password is correct go to the next transaction.

Step 3: After login process,User Fingerprint image is send to the server.Server verify the fingerimage by stored finger image data in database.Verification process done by fuzzy logic.Finger image threshold level I found ou by fuzzy logic. Threshold level is 60-99%, in this case OTP is generated by the server.

Step 4: OTP is send to the user by using QR code with encrypted form by mobile device password. Encryption is done by AES 256 bit algorithm. User find the OTP by Qr code reader in have the android mobile. This is already built the QR reader Application in mobile so easily find out the OTP.user decrypts the OTP by using mobile device password.

Step 5: OTP is send to the server by user.OTP is verified by server.

Step 6: After OTP is verified, Voice authentication is provided.Voice(particular phrase) is send to the server.Server verifried the voice by KIVOX Mobile software. KIVOX Mobile software provides a platform for the use of simple, short voice authentication that is accurately detected 99.9% of the time.

Step 7: Server side will compare the voice data is identical to the user.If the answr is yes,the user can perfrom the transaction services.Other vice ,the server side will reject the transaction.

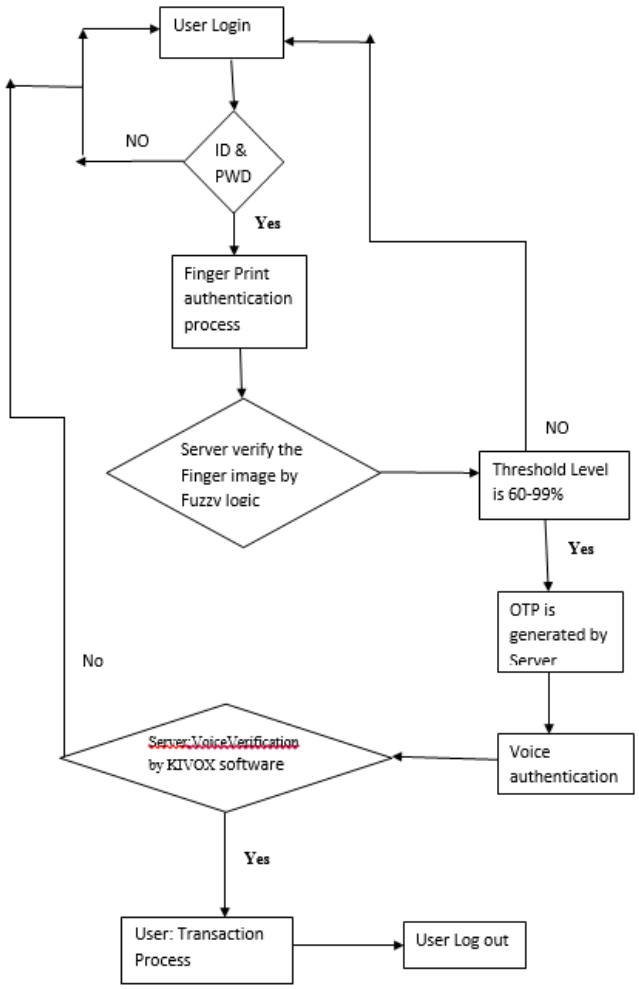

Fig. 4. Proposed mobile banking process in flow chart

CONCLUSION

User authentication provides the assurance that the communicating entity is claimant person. User authentication is done by secure OTP, Finger print authentication and Voice authentication by KIVOX software. Fingerprint image is used instead of ordinary image like as peacock, lion, and Tiger picture so more security and confidentiality is occurred. Multifactor authentication is available in a proposed system.AES 256 bit algorithm is used for encryption

process.AES 256 bit block cipher algorithm provides the more security then stream cipher algorithm. Service provider improve the quality and quantity by using gender classification (male or Female) from the user fingerprint image implementation as a future work.

REFERENCES

[1] Mangala Belkhede*, Veena Gulhane**, Dr. Preeti Bajaj*** "Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach" ISBN 978-89-5519-163-9,Feb. 19~22, 2012 ICACT2012.

[2] Fahad Al-harby, Rami Qahwaji, and Mumtaz Kamala "Secure Biometrics Authentication: A brief review of the Literature"

[3] Uday Rajanna Ali Erol George Bebis" A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion" Springer-Verlag London Limited 2009

[4] http://www.agnitiocorp.com/products/commercial/speakerverification

[5] http://www.agnitio-corp.com/products/commercial/voice-recognition-software

[6] Tan jin soon,Overview of the QRcode,synthesis journal 2008.

[7] Dr.B.Vanathi,K.Shanmugam, Dr.V.Rhymend Uthairaj, Enhancing Secure Transaction And Identity Authentication Method Based On Mixed Fingerprint, Hmac Techniques nd Qr-Code In M-Commerce, Australian Journal Of Basic Applied Sciences, ISSN: 1991-8178, January 2015, Pages: 149-164.

[8] K.SHANMUGAM, DR.B.VANATHI, Fuzzy logic implementation of fingerprint mechanism for secure transaction and identity authentication in M-commerce, International Journal of Recent Advances in Engineering and Technology(IJRAET),ISSN:2347-2812,volume-2,Issue-2,2014.

[9] Wan S. Yi1, Woong Go2, Dongho Won1, Jin Kwak2∗, SecureAuthentication Protocol with Biometrics in an M-CommerceEnvironment, Information Security Group, SungkyunkwanUniversity, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea {wsyi, dhwon}@security.re.kr.