



Hybrid Authentication System: A Survey

Piyush A Ingole & Prof. Amit Welekar

¹Nagpur, India

²T.G.P.C.E.T.Nagpur, India

¹paingole4519@gmail.com

²welekar.amit@gmail.com

Abstract-

Enhancing Mobile Payment System By using Hybrid Authentication is used for making transaction such as doing payment, transferring funds/money, doing online transaction via android Smartphone platforms for prominent mobile payment. Mobile payment system work combines a pair of Smartphone for apparent transaction, Server and paying client. These devices are featuring hybrid authentication in this work to make a simpler and secure transaction than credit cards/atm cards/debit cards or other electronic payment cards. Hybrid authentication consists of Password authentication, QR code, Image authentication, psychometric authentication and signature authentication. This work offers simple but practical method for signature recognition, Discrete Wavelet Transform. Research shows that proposed work have developed a near real time computer system that can locate and track a subject head and then recognize the person by comparing authentication of known individual.

Keywords-

Android Development Kit, mobile payment, Hybrid authentication system.

[A]INTRODUCTION

The cell phone embedded with a Universal Subscriber Identity Module (USIM) card become the most widespread device that human being have ever created and brought along, global telecom operators are unexceptionally engaged in mobile payment service to share the ever-increasing electronic payment card market. The Universal Subscriber Identity Module is used to make video calls and local service portal giving you access to your phone bill. SIM stores user authentication information, Subscriber

information and storage space for text message. The mobile payment technology can be applied to public transportation's electronic ticketing, membership card, smart poster interaction, and car smart keys, official digital signature and soon [1]. The administrators work with end users to improve the quality and security, and network systems analysts. Administrators are responsible for maintaining equipment and monitor the security level to be maintain when user transaction between server and the client. The user interface of the mobile payment devices is designed as easy-to-use as possible and the personal security must be protected by hybrid authentication feature that is Password authentication, QR Code, Psychometric authentication, image authentication and signature recognition authentication[2].

According to a recent mobile communication world news article, and the security team at a large company ran a network password cracker and within 20 seconds, they identified about 80% of the passwords. Passwords that are hard to guess or break are often hard to remember. In Online based Application having few main advantage and many disadvantages when it comes to weak single-factor authentication, which are many more familiar with as the single static passwords still employed by most companies. Advantage is that static passwords are easy to remember. However, when different systems have different passwords are difficult to remember and may have to be written down, raising their vulnerability[3]. The many disadvantages of single static passwords include how easy they are to decipher. Studies showed that since user can only remember a limited number of passwords, they will write them down or will use the same passwords for different accounts. To solve the problems with traditional

username password authentication, many authentication methods, such as image authentication, QR code authentication, psychometric authentication, signature recognition authentication have been used [4].

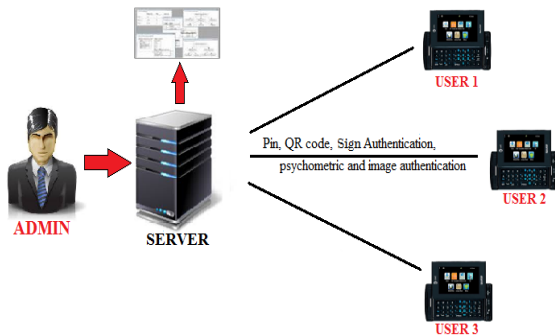


Figure. Mobile payment device by Hybrid authentication

[C] LITERATURE SURVEY

S. Yadav, P. Patil, M. Shinde, Priyanka Rane [1] Author propose another thought called Android Based mobile payment system using 3-factor authentication. These devices are featuring 3 types of authentication in this work to make a simpler and secure transaction than credit cards/atm cards/debit cards or other electronic payment cards. 3 type of authentication consists of Password authentication, USIM card authentication and biometric facial authentication. This work offers simple but practical method for face recognition, eigenvectors. Eigenvectors known as eigenfaces is the approach for recognition in face classification. These project are featuring 3 type of authentication USIM card authentication, bio metric face recognition by Eigen faces and password authentication.

H. B. Kekre, V. A. Bharadi, T. K. Sarode [2] Author propose another thought called Signature verification using vector quantization. Handwritten Signatures are one of the widely used bio metric traits for document authentication as well as human authorization. Different techniques have been implemented for Automatic Signature Recognition. In this we discuss the application of vector quantization to the problem of signature recognition. Vector quantization

methodology based is used here to detect intra and inter-class variations in signatures. Here we discuss a method for the code book generation; this method is fast and simple. We use the code book to generate a code vector histogram specific to the signature template. The spatial moments related to the code vectors are also calculated.

V.P. Bharadi, V. I. Singh [3] Author propose another thought called Hybrid Wavelets based Feature vector Generation from multi-dimensional Data set for On-line handwriting signature recognition. On-line handwritten Signature is one of the important behavioral bio metric traits. On-line signature have more information such as pressure levels, x, y, z parameters variations, Azimuth and Altitude of pen tip, when signatures are captured in real time with digitizer device due to this better accuracy can be achieved. In this a technique based on Hybrid Wavelets to extract texture features of Dynamic Handwritten (On-line) signature is proposed. Combine the advantage of transforms and Multi resolution analyses are flexible by hybrid wavelets.

Chin-seng Chua, Feng Fan, Yeong-Khing Ho [4] Author propose another thought called 3D Human face recognition using point signature. It can present a novel face recognition algorithm based on the point signature-a representation for free-form surfaces and treat the face recognition problem as a non-rigid object recognition problem. The rigid parts of the face of that one person can be extracted after registering the range data sets of faces having different facial expressions. To create a model library for efficient indexing rigid parts are used. For a test face, various models are indexed from the library and the most appropriate models are ranked according to their similarity with the test face. Verification can be quickly and efficiently identified of each model face.

Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., and Minkyu Choi [5] Author propose another thought called Biometric Authentication. Advances in the field of Information Technology also make Information Security an inseparable part of it. In order to deal with Authentication plays an



important role, security. This paper presents a review on the bio metric authentication techniques and some future possibilities in this field. In bio metrics, a human being needs to be identified based on some characteristic physiological parameters. A large variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such a schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. By using bio metrics it is possible to confirm or establish an identity.

S. Baker, I. Matthews and J. Schneider [6] Author propose another thought called Automatic construction of active appearance model as an image coding problem. The active Appearance Model (AAM) of automatic construction is usually posed as finding the location of the base mesh vertices in input image And to recognized proper image.

Reena Bajaj, Santanu Chaudhury [7] Author propose another thought called Signature Verification Using multiple neural classified. This paper is concerned with signature verification. There are three different types of global features have been used for the classification of signatures. In which one is Feed-forward neural network based classifiers have been used. These features are used for the classification and project moments and upper and lower envelope based characteristics. Output of these three classifiers is combined using a constructionist scheme. Combination of these feature based classifiers for signature verification is the unique feature.

A. Zimmer and L. L. Ling [8] Author propose another thought called A Hybrid On/Off Line Handwritten Signature Verification System. A new hybrid handwritten signature verification system where the on-line reference data acquired through a digitizing tablet serves as the basis for the segmentation process of the corresponding scanned off-line data. Local foci of attention over the image are determined through a self-adjustable learning process in order to pinpoint the feature extraction process. Both local and global

primitives are processed and the decision about the authenticity of the specimen is defined through similarity measurements.

[C] RELEVANCE OF WORK

In this work we are developing a pair of mobile payment device, server and a paying client, on Android-Based Smartphone platform for emerging mobile payment or electronic wallet services. Hybrid authentication in this work makes a simpler and secure transaction than traditional credit card or electronic payment card / Atm cards.

[D] HYBRID AUTHENTICATION FEATURE

In order to protect the transaction itself with the lowest risk, Hybrid authentication involves three different kinds of identification procedures:

1. What the paying client knows (e.g., password, PIN card)
2. What the paying client has (e.g., ATM card, Electronic card)
3. What the paying client characterizes (e.g., behavioral or signature feature)

Only mobile payment service based on the Android based Smartphone platforms can accomplishes all requirement of hybrid authentication factor easily. Android development kit uses eclipse software for developing authentication system. The authentication feature common authentication standard adopted by global mobile telecom operators for promotion of mobile payment service[5].

I. Password Authentication

Since passwords involve mouse input instead of keyboard input, it will not be practical to carry out dictionary attacks against this type of passwords. A password is word or string of characters used for user authentication to prove their identity. If password is valid it will grant permission to access resource. Password should most secret thing to kept away from public user. Password is usually known as pass phrase. The term pass code is used when



secret information is totally numerical. Such as PIN code known as Personal identification number.


II. QR Code authentication

QR code (abbreviated from Quick Response Code) is the trademark for a Type of matrix bar code (or two-dimensional bar code) first designed for the automotive Industry in Japan. A bar code is a machine readable option label that contains information about the item to which it is attached. A QR code uses standardized encoding of four types modes as alphanumeric, Numeric, binary, byte to efficiently store data passwords.

III. Image Authentication

Image authentication Password is a visual login technique that matches the capabilities and limitations of most handheld devices and provides a simple and intuitive way for users to authenticate. Besides user authentication, image authentication Password may also be used in other security applications where conventional passwords have been used traditional. While the solution is particularly well suited for handheld devices, it can also be used in a wide range of computing platforms. Users are select only one picture at the time of registration and images are easily remembered as compared to the traditional password system [6].

Username:

Password: 

IV. Signature Authentication

Signature authentication is a method of identifying yourself to a login server, instead of typing the password. Signature authentications are more secure and at the same time more flexible than conventional password authentication. In signature authentication uses a discrete wavelet transform technique are used. In DWT we used to measure the pressure and style of the

user at the time of registration user insert the sign and that pressure and style and handwriting will be store on database by the DWT technique [7]-[8].

[E] ANDROID DEVELOPMENT KIT

Android software development is the process by which new applications are created for the Android operating system. Applications are generally developed in Java programming language are used Android Software Development Kit (SDK). The Android software development kit (SDK) includes a comprehensive set of development tools. These include a handset emulator based on QEMU, a debugger, libraries, documentation, sample code, and tutorials. Current supporting development platforms include computers running Linux.

[F] IMPLEMENTATION METHODOLOGY

The Implementation methodology of enhancing mobile payment client device using hybrid authentication. The above figure show that the implementation module interactive with android operating system architecture, this work of implements application.

1. PIN (Password) authentication application to employ android based web kit library and web browser for PIN code authentication feature.
2. Other authentication application to inquire android based interface layer daemon and RIL module driver through telephone Manager Frame work for QR code and psychometric authentication.
3. Signature authentication application to apply open source Open CV library through Android Java Native Interface (JNI) for discrete wavelet Transform technique.

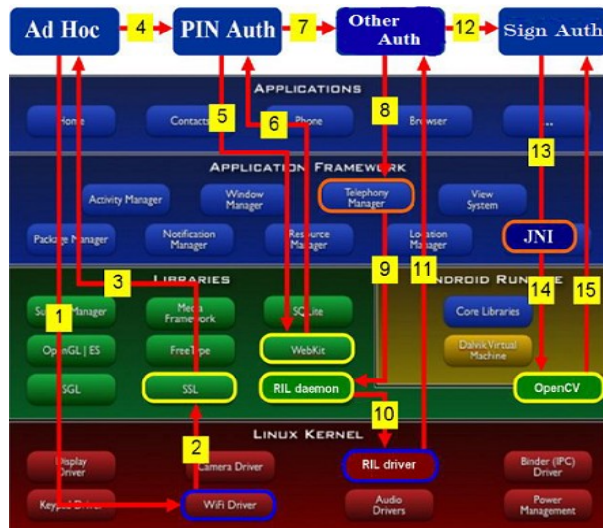


Figure. Implementation Methodology of Mobile payment device by Hybrid authentication[1]

[G] CONCLUSION

In information security, user authentication is the most critical of all the elements. The Android-Based mobile payment service using hybrid authentication can perform well and securely. In the near future, more multi factor authentication feature and virtual private networking features will keep being developed and integrated. We are going to cover all drawbacks of One Time Password (OTP) in this hybrid authentication. Researches made between 1996 to 2011 has shown that people tend to remember combinations of geometrical shapes, patterns, colours and textures better than alphanumeric characters that are meaningless to the user.

REFERENCES

[1] S. Yadav, P. Patil, M. Shinde, PriyankaRane “Android Based mobile payment system using 3-factor authentication”, IEEE Transaction on Mobile computing, VOL.15, NO. 3, MARCH 2014

[2] H. B. Kekre, V. A. Bharadi, T. K. Sarode, “Signature verification using vector quantization”, International Conference on Advance in computing and communication, Vol. 3, 2010

[3] V.P. Bharadi , V. I. Singh, ”Hybrid Wavelets based Feature vector Generation from multi -dimensional Data set for On-line handwriting signature recognition”, Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference.

[4] Chin-seng Chua, Feng Fan, Yeong-Khing, “3D Human face recognition using point signature”, IEEE International Conference on IEEE International Conference on Automatic Face and Gesture Recognition, 2000.

[5] Debnath Bhattacharyya, Rahul Ranjan, FarkhodAlisherovA.,andMinkyu Choi, “Biometric Authentication”, IEEE Transaction on Service, Science and Technology, VOL. 23, NO. 7, 2009

[6] S.Baker , I. Matthews, and J. Schneider, “Automatic Construction of active appearance models as an image coding Problem,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 26, pp. 1380–1384, Oct. 2004.

[7] Reena Bajaj, SantanuChaudhury, “Signature Verification Using multiple neural classified”, IEEE Transaction on Advance computing, Vol.3,2007.

[8] A. Zimmer and L. L. Ling, "A Hybrid On/Off Line Handwritten Signature Verification System", ICDAR, vol. 1, pp. 424-428, Aug. 2003.

[9] Google, “Android Developers,” [Online]. Available:<http://developer.android.com/index.html>