Authentication To M-Banking Users

P. Ushahsree
Dept. of Computer Science
Geethanjali College of Engineering and Technology
Hyderabad, India
Ushashree.sgs@gmail.com

P. Preeti
Dept. of Computer Science
Geethanjali College of Engineering and Technology
Hyderabad, India
Preeti.preetu11@gmail.com

Abstract— **Mobile banking (also known as m-banking) has revolutionized the banking industry with new business models to offer convenient self-service banking options to their customers. Mobile banking has become an attractive target for attackers. Even though many security measures are taken with current mobile services, some threats against mobile devices such as physical theft or penetration from the remote side are still unsolved. In this paper we discuss about how security to the M-banking users can be provided by using the techniques that verify a user by examining his physiological and/or behavioral attributes through the direct measurement of certain properties.**

Index Terms: **M-Banking; Authentication; Biometrics; Neural Network; Capacitive and Resistive touch.**

I. Introduction

Mobile technology is disrupting every industry, with the full potential still not yet fully understood. It is not just about smart phones or handheld devices, but also includes other technologies such as robotics and sensors. Businesses should not silo mobile in their marketing, but should consider how to integrate mobile in all the media channels that they use. With the wide expansion of mobile telecommunication technology into the business world, mobile banking has become the most popular and promising method in the banking industry. Convenient, efficient and effective mobile banking is the main way for banks to attract more customers, so security is the utmost for mobile banking service development.

In spite of these security threats in mobile banking, it is difficult to use the same sort of security measures as PC-based online banking (Internet banking) because of the limits of a mobile device which are battery life, computing power, and bandwidth availability. For this reason, suitable security measures for mobile banking are needed desperately.

In this paper, we proposed authentication procedure for proactive prevention mobile. Most mobile banking users employ fingers or a stylus pen for input, because many mobile devices have adopted touch screens as their input medium. In this regard, we noticed that user’s usage patterns can be measured as user’s input patterns such as the input duration-time, finger pressure level and physical touch dimension on the touch screen. These measurements are consistent and distinct from those of other users. These features of quantified user’s input patterns can be used to identify users and detect an illegal transaction by an attacker. A user’s authentication information such like a password can be easily leaked to an attacker. However, even when an attacker holds all the rights of a user for mobile banking, our method can help to detect illegal transactions by analyzing the differences in input patterns between the original user and an attacker.

Recently, biometric authentication methods for mobile devices have drawn keen attention. Fingerprints, hand geometry, facial recognition, iris scanning and voice prints are the well-known biometric authentication methods. In particular, a mobile device, which is equipped with a camera, a microphone, and a touch screen, facilitates multimodal biometric authentication..

.

II. Literature Survey

Mobile banking implements the same login method, PIN authentication. Before conducting a transaction, a client is required to login with a PIN (some systems may also require their users to input a valid identification), and only a valid PIN code will grant the client access to the service.. During authentication, the user presents the Password, and the system verifies the user by checking its validity. Alternative mechanisms are biometric-based authentication and token-based authentication. Biometric-based techniques verify a user by examining the user‘s physiological and/or behavioral attributes through the direct measurement of certain properties. And, token-based methods verify a user by validating the authenticity of an object that the user presents or holds, such an object is typically known as a token.

Biometric authentication is a method in which initially the user biometric details are collected such as finger print, iris scanning and are stored in the database. So when the user logs in with the biometric input value it is compared with the stored database value if the pattern matches he is allowed to access the account. In this method there is no need for the user to remember his or her password. As the biometric values change from person to person it can be used for identification and verification, which is deemed as advantageous. Although biometrics is unique, not all biometric authentications are perfect; some biometrics can be forged. The accuracy of iris verification is much greater than fingerprints. It is advantageous because iris images can be acquired from the individuals without physical contact and forgeries, such as artificial irises, are easy to detect common, they have been put into practical use. Using biometrics for authentications appears to be a usable form of security Furthermore; biometric authentication requires devices with a biometric sensor. Most mobile phones on the current market are not equipped with a biometric sensor; as a result, this verification scheme is not suitable for mobile banking authentication.

A token is a piece of data created by server, and contains information to identify a particular user and token validity. The token will contain the user's information, as well as a special token code that user can pass to the server with every method that supports authentication, instead of passing a username and password directly. Token-based authentication is a security technique that authenticates the users who attempt to log in to a server, a network, or some other secure system, using a security token provided by the server. An authentication is successful if a user can prove to a server that he or she is a valid user by passing a security token. The service validates the security token and processes the user request.

This is a authentication method in which the user personal information is stored and accordingly the authentication to the user is provided. In this method basically the user should remember his own details and they are stored in the database while logging into the account a question regarding his personal information is asked if the answer matches with the existing details then authentication is provided**.**

A graphical password is a secret in an imagery form. A human user inputs the secret into an authentication system with the aid of visual cues, graphical inputs, and output devices. The techniques of graphical authentication can be classified into three main categories: Locimetric, Drawmetric and Cognometric. Locimetric (or location-based) authentication is a technique where the system provides an image as a memory cue and relies on precise position recall to authenticate. Drawmetric authentication involves the user drawing a simple outline of a password on a grid during enrolment, and the authentication is consisted of reconstruction of the enrolled sketch. Cognometric authentication is by far the most researched area in graphical authentication, and it is widely recognized by its simplicity to design and to implement. The process requires a user to identify a series of recognized password images amongst a larger set of decoy images; if the set of correct images are identified the user is authenticated.

Gesture movements are used as one of the input for authentication. In an attempt to create PIN-less authentication environments, researchers have designed methods that use gestures for pairing devices. an authentication scheme by shaking a device. Their authentication scheme is based on a user authenticating his/her device when using a public terminal by mimicking a sequence of gestures that is generated by the device and displayed on the terminal. Their authentication method requires a user to hold the pairing devices tightly together and shake the devices for a short period.

In this paper we propose a method that distinguishes the differences between an original user's usage pattern and an attacker's usage pattern. If the same account is used by radically different profiles an alert is flagged to human customer relationship executive who will then call the original user for confirmation.

III. AUTHENTICATION METHOD

Touch screens are the main interface device for a smart phone because of its small size and difficulty to attach physical input devices like a keyboard and mouse. Therefore, mobile banking users use a finger as a part of the body to input (touch and scroll-wheeling) in the process of the transaction. In this case, a user's input pattern such as an input duration time, finger-pressure level are considered as one of the types of biometric authentication information. This information, which would be based on fundamental human characteristics, could be used not only for checking whether or not a person exists, but also for verifying a user's identity.

Based on research carried out by many people, we proposed a novel authentication method using a user's input pattern, for preventing mobile e-financial accidents. There is difference in input patterns among mobile banking users because each user has unique biometric features. Thus, by analyzing a user's input pattern, financial institutes can detect illegal transactions by attackers who are not the original user, even when the user's authentication information for transactions in mobile banking is intercepted by attackers.

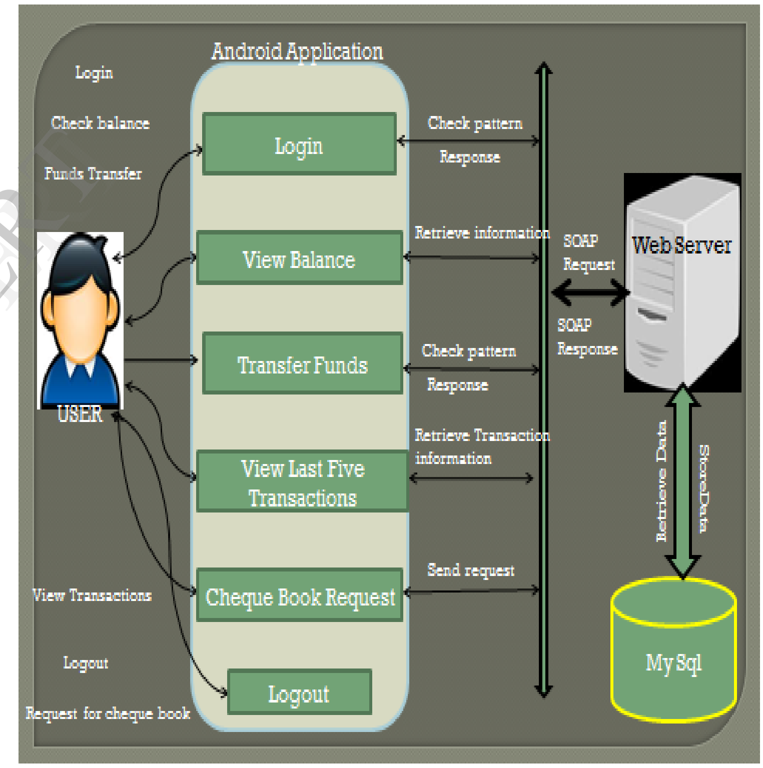
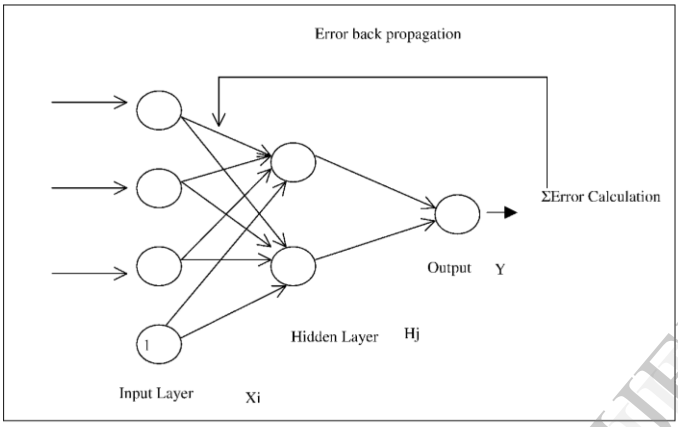


Fig 1 Architecture

In the above figure we stress on three tiers a user, System and database. Whenever user logs in for the first time for mobile net banking, the user credentials are retrieved to check whether the user is an authorized user or not, after that it will ask to enter the new password then the details are stored in database. The password which is re entered four times at that time only the network will analyze the user input pattern i.e.; typing speed, Pressure level, order in which the fields are entered, and then the details are stored in database. So after that whenever he gives the details or logs on to the system then the system will checks the current pattern of the user and compares that the existing user input patterns. If the user input pattern is matched it will identify the user is authenticated otherwise we will provide the security question. Finally when he is able to answer the question then he is directed to the home page of the website else an alert is sent to the human customer relationship executive who calls the original user for a confirmation

We use the Back Propagation Network (BPN) to train user input patterns. BPN, by using Least Squares Method (LSM), is the most widely used neural network algorithm in pattern recognition. As BPN has a better fault tolerance capacity than other algorithms for training. It is difficult for a person to always input in the same way that a machine would. Thus, noisy input values could rarely be included in user input patterns. BPN, however, is able to reduce a training error on account of its superior fault-tolerance, even though some noise is contained in the data.



Notes: The weight connecting node *i* in the input layer to node *j* in the hidden layer is denoted by *Wji*, and the weight connecting node *j* to the output node is represented by *Vj*

Fig 2 Back Propagation Network

An Architecture of BPN, three layer networks with one hidden layer is shown in Fig 2.Neural networks is taken as the backend and then training to the system is provided. In the training phase, as advance preparations, initially the user's input pattern data are collected, and then this data stored in a database for training. Next, user's input pattern is standardized by training several times with the collected data. After training the system depending on the input we decide, whether a requested transaction is the original users or an attacker's. If the input pattern of the requested transaction is not similar to one already registered by training, then a security question is asked so as to counter check for the authentication.

IV. Conclusion

The mobile environment has developed at a fast pace and more people are switching to smart phones which resemble older PCs. however, mobile banking continues to suffer from a high risk of incidents under restricted security measures by device resource constraints and the limit of existing biometric authentication methods. In this Paper an authentication approach based on the behavioral elements of humans has been proposed which to a certain extent can resolve the issues encountered in the M -Banking. In the immediate future, we foresee that the mobile environment and device techniques will have more diversity and developing an application that is scalable.

REFERENCES

[1] Hojin Seo & Huy Kang Kim Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium ;pages 382 – 387 ; May2011

[2] jwis2009.nsysu.edu.tw/location/paper/AuthenticationMethodsforUSIM-basedMobileBankingService.pdf

[3] jwis2009.nsysu.edu.tw/location/paper/AuthenticationMethodsforUSIM-basedMobileBankingService.pdf

[4] Liang Xie, Xinwen Zhang, Jean-Pierre Seifert, and Sencun Zhu, "pBMDS : A Behavior-based Malware Detection System for Cellphone Devices," WiSec'10, 2010, pp. 37-48.

[5] Jay I. Miinnix, "Fault Tolerance of the Backpropagation Neural Network Trained on Noisy Inputs," IEEE Neural Networks, 1992, pp. 847-852

[6] http://www.netaro.info/~zetaka/publications/papers/awasee-MobileHCI03.pdf