Significance of Biometric User Authentication and Authorization for Mobile Banking System

Gajendra Sharma

Department of Computer Science and Engineering, Kathmandu University Dhulikhel, Nepal

Abstract: *Biometric Authentication uses human physical and behavioral characteristics such as, fingerprints, retina, iris, face, vein, ear structure, voice, handwriting, typing rhythm etc to recognize and verify identity of individual. Combination of two or more such characteristics can be used to enhance accuracy and reliability. Modern smart phones have capability for capturing most of the human characteristics. The biometric information is stored in bank's server in encrypted form which is used to verify mobile banking user's identity over secured communication channel.*

Research Question

The research questions are:

Research Question 1: What are the issues in current mobile banking?

Research Question 2: How biometric authentication method can enhance customer trust in mobile banking?

Literature Review

Mobile banking service is provided by bank and financial institution worldwide. People use mobile banking for financial transactions (electronic bill payments, utilities payments and funds transfers etc), using a mobile device and mobile banking application. With the advent of electronic payment technologies the world is moving rapidly towards cashless society. Mobile banking is one of the most rapidly growing means of payment worldwide today. The numbers of mobile banking users cross 2 billion in 2018 which represents about 40% of world adult population [1]. According to annual report 2018 published by Nepal Rastra Bank, the number of mobile banking users has grown by more than 93% than last year[2]. The availability & affordability of smart mobile devices and network helps mobile banking to be grown up rapidly. With the ease of banking through mobile devices has brought many kinds of threats and security issues like authentication, integrity, confidentiality and non-repudiation. Today mobile banking system uses PIN (Personal Identification Number) and password based authentication which is risky and not secure. To deal with such kind of issues biometric authentication is required. Today's mobile devices have face recognition, voice recognition, fingerprint readers and iris scanning capability.

Biometric Authentication

1) Physical
    a. Fingerprint Recognition
    b. Face Recognition
    c. Eye Scanning
2) Behavioral
    a. Signature
    b. Keystroke Recognition
    c. Speech Recognition

a. Fingerprint Recognition

Fingerprint based biometric authentication is the oldest approach [3] with mature and proven technology. The fingerprint comprises of ridges and valleys [4] that form distinctive patterns (such as loops, swirls and arches). Everybody has unique finger print pattern which is analyzed by scanning the fingers. Each fingerprint has curves, bifurcations and deltas. Based on the set of these characteristics unique person is identified. Fingerprint matching techniques can be placed into two categories:

- Minutiae-based
- Correlation based.

b. Face Recognition

Face image is captured and digital representation of captured image [4] is calculated based on some features of the face (such as the upper ridges of the eye sockets, areas around the cheekbones, sides of the mouth, nose shape and the relative position of these features relative to each other) [3]. For authentication new image is taken and compared with digital code of stored image. It is cheaper technique but facial expression, lighting condition may affect authentication process.

c. Eye Recognition

There are two methods:

- Retinal Recognition

    Laser scanning of retina is done to analyze the blood vessels configuration of the acquired retinal picture [3]. This blood vessels configuration is unique for each eye [4].

- Iris Recognition

  Scanning of eyes is done using normal camera and the acquired image is analyzed. There are 266 different spots in eyes (such as furrows and rings) [3]. The iris patterns make people unique.

d. Signature

The signature analysis is one of the oldest methods for authentication. The parameters that are recorded and analyzed for the authentication are the shape of the signature, the time taken to do it, the stroke order and the pen pressure [3]. The computation of these parameters in the system provides to a unique authentication method.

e. Keystroke Recognition

It is not expected to be unique to each individual but it offers sufficient biased information for identity verification [3]. Keystroke can be a behavioral biometric authentication method if some individual is observed for longer time span, then one may expect to have typical typing patterns.

f. Speech Recognition

Microphone is used for voice recording. The recorded audio signal is computed by using some frequency analysis of the voice [3]. It is less accurate biometric authentication methods than other biometric means. The vocal characteristics depend on the vocal tract, mouth, nasal cavities and the other mechanisms of the human body [4]. The speech recognition system asks the user to pronounce a phrase and the voice is then processed and stored in the system, later the system asks for the same phrase and compares with the stored voiceprints.

Anil K. Jain et all refers that biometric authentication system is the automation recognition of individual based on physical and biological characteristics. In absence of robust system it can be vulnerable and risky. He presented an overview of various biometric template protection schemes with their advantages and limitations in terms of security, revocability, and impact on matching accuracy [6].

V Prasathkumar, Brindha, V.E. presented a high speed fingerprint authentication algorithm, with improvement in ridge and valley structures of input fingerprint images based on the estimated local ridge orientation and frequency [7].

Daesung Moon ; Sungju Lee ; Seunghwan Jung ; Yongwha Chung, presented PKI-based authentication where the private key is protected by fingerprint. To maintain the privacy and security measures, the fingerprint data was stored in user-carry device such as a smart card or a USB token rather than database [8].

Nemanja Macek, Mlan Milosavljevic, Agor Franc, Zlatogor Minchev, Milan Gnjatovic, Branimir Trenkic proposed a system which stores, transmits and verifies biometric templates in encrypted form. Encryption keys are stored on bank's authentication servers, once the user is authenticated; the communication between the client and the server is encrypted. Iris scanning is done by smart phone camera, further calculating the Hamming distance and that is done over the Smartphone having fingerprint readers. Thus XOR biometrics is obtained [9].

Methodologies

Research Question 1: The literature review provides the security issues. For this purpose a basic mobile bank transaction model is built and then added with security risks in the model. To identify various kinds of risks is one of the important issues for mobile banking transaction.

Research Question 2: Fingerprint, iris and Face recognition are suitable biometric mechanism as compared to other biometric means like voice, signature etc. The availability of affordable technology and communication infrastructure fingerprint, iris and face recognition are helpful means of biometric authentication mechanism to increase security level and improve trust.

Model

Biometric Authentication is being popular day by day because of the number of login credentials that a person has. This technology allows user to use single sign-on concept to get rid of forgetting user ID and password/PIN. Multimodal biometric authentication is useful because of ease of use and confidentiality, authenticity & non-repudiation.

As time passes on changes in biometric features of a person arises. These changes should be addressed and the system database should be updated frequently.

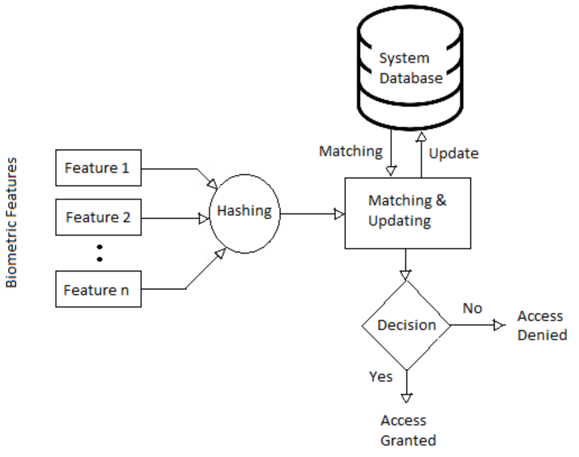

Figure 1: *Cognitive model for biometric authentication*

Conclusion & Future Works

Biometric authentication method in mobile banking can help to reduce various fraudulent activities. This help to increases reliable and secured transaction mechanism. It also helps to increases the trust and faith in user and service provider. One or combination of more than one biometric means can be used to enhance user authentication in mobile banking. As time passes on, there will be many instances of biometric matching factors stored in system database. An algorithm can be deduced to find best match.

References

[1] https://www.juniperresearch.com/press/press-releases/digital-banking-users-to-reach-2-billion Website accessed on 2019.04.10

[2] https://www.nrb.org.np/bsd/reports/Annual_Reports--Annual_Bank_Supervision_Report_2018-new.pdf Website accessed on 2019.04.28

[3] Mule Sandip, H.B.Mali "Review on Biometric Authentication Methods", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 11, November 2015

[4] C.B. Tatepamulwar, V.P. Pawar, H.S. Fadewarr, "Biometric Recognition: A Literature Review" National Conference on Innovations In IT and Management, 2014

[5] Gaurav Ogale, Pranita Hatte, Anand Sutar, Pratik Chaudhari, Prof.A.M. Wade, "Survey on Biometric Authentication in Mobile Banking", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 1, January 2017

[6] Anil K. Jain, Arun Ross, Salil Prabhakar, "An Introduction to Biometric Recognition" Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[7] V Prasathkumar1 , Mrs. V. Evelyn Brindha, "Personal Authentication using Fingerprint Biometric System" International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014

[8] Daesung Moon ; Sungju Lee ; Seunghwan Jung ; Yongwha Chung, "Mutual Authentication using Fuzzy Fingerprint Vault" International Conference on Computational Intelligence and Security IEEE Xplore: 29 January 2007

[9] Nemanja Macek, Mlan Milosavljevic, Agor Franc, Zlatogor Minchev, Milan Gnjatovic, Branimir Trenkic "Secure Mobile Banking Biometric Authentication" The 9th International Conference on Business Information Security (BISEC-2017), 18th October 2017, Belgrade, Serbia