SECURED TRANSACTIONS IN INTERNET BANKING THROUGH BIOMETRICS IDENTIFICATION

R.Vasuki, G. Angeline Prasanna*

Abstract

In technological era, Internet banking is the most inevitable one for various banking services. Banking activities enhanced its flexibility with the help of information technology also improves the quality-of-service, delivery of service, reduction of transaction cost, anytime anywhere service demand for customers. In view of the expanding range of banking services, the customer identification is the foremost in authentication procedure. Phishing Spoofing Plastic card-the new technology has increased fraudulent usage in online transactions, resulting in security. The major concern in online banking is security. Since present authentication system such as password, OTP generations are not sufficient in providing high level security. Biometric scan be added with the traditional method in order to improve the security of customer when performing e-payments.

Keywords: Internet, banking, Authentication, Biometrics, Security.

I INTRODUCTION

Expansion of information technology provides new face to the banking sector. Traditional banking system, physical presence of the user plays the major role while the banking activities. It consumes more time and also not flexible to all the necessary actions. In the earlier days, all the banks are adapted the internet and mobile services for their customer usage. It makes tremendous change in the banking sector. Common people can easily access their own accounts for their regular banking activities. E-banking allow the users to access the transactions anytime anywhere in virtual concept via Bank websites and Mobile apps.

In the course of Online opening of accounts needs to address the following challenges [1]:

- Authentication
- Secrecy of customer's account
- Non repudiation

II ONLINE TRANSACTIONS WITH BANKER

The banks providing Internet banking service, at present are only willing to accept the request from the customer for opening of accounts. The accounts are opened only behind proper physical introduction and verification. This is the purpose of proper identification of the customer and also to avoid duplication in accounts as also money laundering activities that might be undertaken by the customer. All over the world for internet banking followed the principal of 'Know your customer'.

Terminologies in internet-banking:

1. Data integrity: It ensures the user information cannot altered by unauthorized user. Effective tools need to ensure the accuracy and soundness of data.

2. Data privacy: Due to open nature of internet resource anyone can monitor or read customers account details, personal information and password via special program 'sniffers'. Confidentiality extends beyond data transfer in the network storage systems.

3.Authentication: Identifying the right user is the essential step for any online transactions. It is the process of identifying the person, machine or other entity.

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

4.Access control: One of the mechanisms to control the access and its facilities even the customer to extern their access.

5.IP Spoofing: It is a kind of cyber-attack. Change the source address for the purpose of masquerade another system.

6.Non repudiations: Digital signature introduce the concept non repudiation that means anyone cannot deny the message except sender and receiver.

Authentication factor:

It is the piece of information to identify the person

1.Things you know: It confirms the users' credentials through the username and password.

2.Things you are: Persons physical and behavioral modalities are taken for the authentication purpose.

3.Things you have: It may be either tokens or smart phones.

Existing Security methods[2]

Phase 1: First factor authentication

- Login details
- Captcha: i)image captcha, ii)audio captcha

Phase 2: Second factor authentication

One –Time Password generation.

OTP is sent to the users registered phone number or email. In general OTP is secure and safe which is not attacks like impersonation, phishing and malware-based reply attacks. OTP cannot be reused after sometime.

Two-Factor Authentication used in the existing system which was 'Something you have and you know'.

Issues in Online Banking [3]

Online fraud is a universal phenomenon that is frequently evolving in order to abuse security gaps.

1. Privacy breach: Database need to keep carefully.
2. Security breach: Customer personal, official data have a chance to steal through illegal activities.
3. Man-in-the middle attack and man-in-the browser attacks.

Risks of Verifying Identity without Biometrics

Conventional mechanisms for identity verification are becoming archaic as technology continues to go forward. As advancement in technology and AI capabilities are becoming smarter, hackers finding more and more new ways to hack internal systems and make confusion. They focus to undermining the conventional mechanisms on user-id and passwords to protect digital identities. Compromising the personal recognition through biometrics leads to detrimental of the business. This leads a major security risk for companies who haven't adapted the advanced biometric technology solution.

Biometrics is the identification technique to recognize the humans based on their physical and behavioral characteristics. It is the branch of Computer security to authenticate the right person. Authentication system verifies the identity of the user for access control to the system.

III NEED OF BIOMETRICS

Protects the system and data from the unauthorized person. It used to authenticate and authorize a person using the question "Are you the same you are claiming to be?" or "Do I know you". One-to-one matching and comparisons help to increase the reliability of the persons identification procedure.

Why biometrics?

- It cannot be borrowed, forgotten or stolen.
- Prevents from masquerade
- Remove Multiple identities
- Defenses against Digital spoofing attack.

Biometrics Authentication Technologies[4]

1. Fingerprint Scanner: This is one of the commonly used biometric technologies. Even, smart phone also used as a personal identification marker for the individual. It captures the person fingerprint through fingerprint scanner. Patterns on human fingers are analyzed in detail which was already stored in the database.

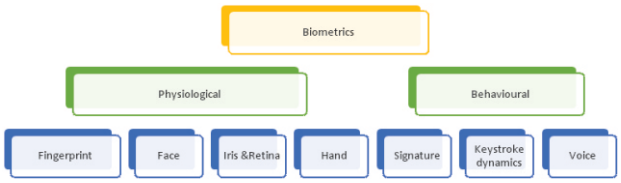

Fig.1. Fingerprint Scanner

2.Face recognition: It can verify users at ATM, online& mobile banking. This type of confirmation is dependent on the user'senvironment such as the lightning or positioning of the face. It analyse the facial contour to identify the individual.

3.Iris and Retina scan: One another method for scanning individuals Iris and retina for the verification purpose.

4.Hand Geometry: It is based on the palm and fingerprint structure. It is inclusive of fingers width, length of the fingers ,thickness of the palm area and surface area of person's hand.

5.Behavioural characteristics: Analyse the way of how the individual handle the system, style of keystroke dynamics, handwriting, GIAT and voice. It can help to assess a person identity.

STEPS TO VERIFY THE IDENTITY[5]

Enrollment: User enrolls their identity with the help of input devices like camera, scanner.

Extraction: With the help various algorithms captured images converted into templates and stored in the database for future verification.

Verification: Verification is the process of matching between stored template and liveness input.

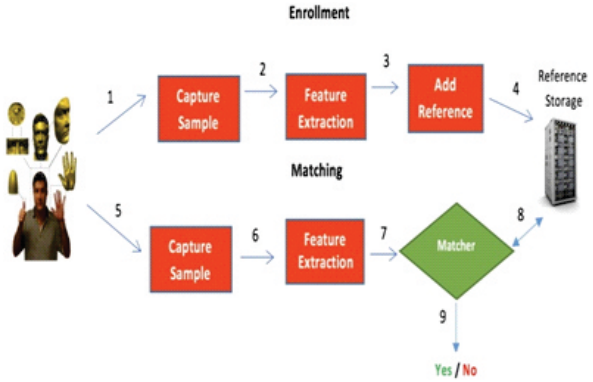

Fig.2.Verification Process

IV BIOMETRICS SECURITY FEATURES[6]

Multi-factor authentication

To make hacking into customer accounts nearly impractical, companies use employing multi-factor authentication or MFA—an additional layer of security to protect data, incorporating biometric identification methods along with the OTP.

Safe and simple internet banking

Many of the private banks all over world implement the Touch-id method to verify their clients to simple and secure online banking services.

Future of card payments

Famous card payments system started to implement the biometrics payment cards. In a single scan of the consumer fingerprint on the card sensors involved in purchases.

Driving financial inclusion

Biometrics fingerprint and Iris scanning involved at the time of payment process in the commercial companies, educational institution and factories etc.

Role of enrollment

Since identity is central to an effective biometric payment card strategy, accurate and safe enrollment through means such as smart phone, apps or physical attendance is essential.

The Bottom-Line

Increasing cybercrime activities and payment threat has need significant method to get secure and robust financial services without using cash.

Customers are willing to use biometrics authentication for their payments. Smart phones make this comfort zone to the user.

Limitations and issues[7]

1. Time consuming.
2. Need Mass database.
3. Biometrics is visible to everyone. It may not be private even if we have.
4. To make duplicate templates are simple, while you enter your identity in the machine. Silicon fingerprint caps are easily available in market.

Feature Extraction[8]

In this proposed system insists the importance of Multi Factor Authentication System (MFA) with One-time Password for stringent security.

V CONCLUSION

The biometrics security is far better compare to existing one. As banks combines biometrics with common password, they can bring MFA technology that's now considered the secure method from a way on security in high level. Before applying this concept in banking sector need to validate how it works well in the Third-party add-on products.

REFERENCE

[1] https://www.rbi.org.in/SCRIPTs/PublicationReportDetails.aspx?UrlPage=&ID=243#ch5

[2] https://retail.onlinesbi.com/retail/login.htm

[3] https://desklib.com/document/ethical-legal-and-social-issues-of-online-banking/

[4] A. Sedik et al., "Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities," in IEEE Access, vol. 9, pp. 94780-94788, 2021, doi: 10.1109/ACCESS.2021.3088341.

[5] Muntaheen ASM, Shaker MA (2021) Biometric Authentication in Mobile Banking. Am J Comput Sci Eng Surv Vol. 9 No. 1:18.

[6] Tsai, CH., Su, PC. The application of multi-server authentication scheme in internet banking transaction environments. Inf Syst E-Bus Manage 19, 77–105 (2021).

[7] Chien-Hua Tsai & Pin-Chang Su, 2021. "The application of multi-server authentication scheme in internet banking transaction environments," Information Systems and e-Business Management, Springer, vol. 19(1), pages 77-105, March.

[8] J. Jayanthan, N. K. Priya, S. P. Kumar, and K. Sangeetha, "Facial Recognition Controlled Smart Banking", IJRESM, vol. 4, no. 3, pp. 185–187, Apr. 2021.