Secured E-Banking System using Artificial Intelligence

R. Augustian Isaac [1], Prakhar Chaturvedi [2], Pradip Gareja [3], Rohan Grover [4]
[1] Asst. professor, Dept. of CSE, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[2, 3, 4] Student, Dept. of CSE, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.

Abstract – The issue of design and security is very predominant in any financial and business organization, especially such organization as a bank. Therefore, we intend to aid in security of the bank by bringing in an Artificial intelligence system that involves an individual to get an access to some items using face and voice recognition security system. This AI system is not just a normal password lock system that require a user to insert password and gain access to some items, it is a system that has an administrative authentication. In addition, with this kind of security authentication system we intend to implement, a highly secured AI feature, which enables the user with assured and highly secured transactions using their personal frame. Here an individual have to provide the face and voice authentication, which uses different algorithms, and is read by the AI server for clarification and verification. From this project, we hope to build an alternative and highly verified security for banks.

Index Terms – Face recognition with Artificial Intelligence, Voice recognition, Biometric, Login System, OTP.

1. INTRODUCTION

In today's drastically developing society, the network and information technologies are redesigning and trendsetting the traditional business activities and asset circulation models. Mostly all the products and services are available online while other activities like business activities are involved in the E-banking or E-commerce. Due to swift technological developments, traditional trading is being transformed into new trading. Online stores are fast rising based on the technologies of mobile, tablets and PCs along with the Internet of Things.

Despite fast expanding E-banking transaction volume, interviews, past year data shows that all the participants of E-banking does not find themselves happy at electronic transactions and benefits from online banking. Further, privacy and security are becoming the most concerned issues with online shopping experiences, considering rising threats from virtual cyber space, transferring of large amount of data at once, location based information, and limited account security. As a result, new improvement at E-banking architectures, models, techniques and services are in urgent need.

E-banking drivers around the world, from giant businesses such as Reliance, Amazon, to make huge amount of business deals use only online banking transactions.

Based on comprehensive research and inspired by regular work and concerns, the only OTP use is old trend and use of voice detection and face detection has shown beneficial in different platforms such as i-phones, echo speaker by amazon that made to apply on E-banking system.

In this paper, an overall presentation of the proposed E-banking system is provided. Section 2 will discuss the related work and importance of E-banking security improvement. Section 3 will describe the architecture and working process of E-banking security system. Section 4 will conclude the paper.

2. RELATED WORK

With the advancement of the technologies and emerging crimes in the field of cybersecurity, related to banking systems has shown a tremendous need of upgradation in the virtual transaction security system of E-banking that affect the lives of people.

In the existing model, there are methods, which were implemented to protect the E-banking security system, such as one-time password, alphanumeric based login and transaction password, which has gone to old tradition for E-banking model after 1990's.Present days E-banking resulting as failure model due to no upgradation with the time.

2.1 Importance of E-banking security improvement

A report released by the payment company FIS, stated that the 18 percent of the Indian customer reported a fraud last year which is much higher in comparison to other countries. Also, many incidents previous years has proved that this existing model is not that much safer and secured for people. Many attacks has been introduced in cybercrime for current model. The common attack included as follows:

1. Brute force attack: In this attck the criminal will form all several possible combinations to find password.
2. Dictionary attacks: These attacks are based on different dictionary of password, which are generated based on the phrases that can be used in the passwords.
3. Shoulder surfing attacks: The criminal looks over the shoulder of the user and memorize the password.

Regarding the mentioned above attacks there is a need for more secure and robust E-banking model that to be simple, publicly-accepted, dynamic and resistant to attackers in order to be applied to E-banking channels.

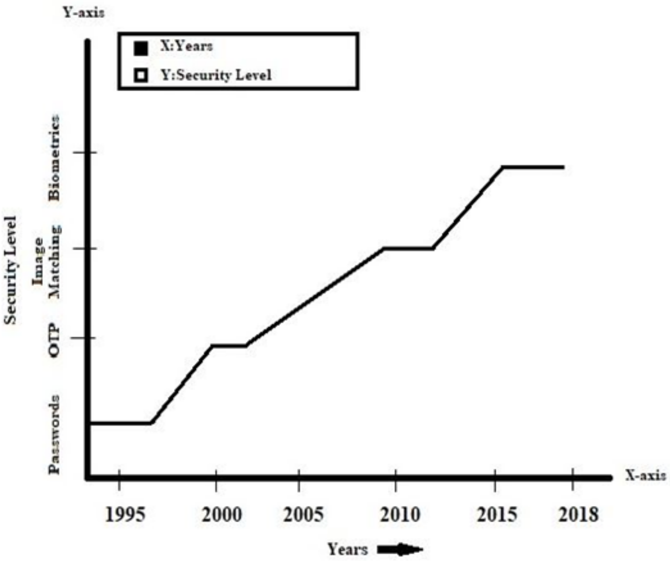


Fig. 2.1 Existing E-banking Security Level

In the above given figure 2.1, the existing security level in E-banking is given according to the respective years. At the initial stage, when E-banking was first introduced only password was used as a method of security, which was not at all profitable for the users. As the attacks explained above were introduced until that period by the cybercrime to hack the E-banking password. So, new technologies were introduced in the need to protect it. Such as OTP (One-Time-Password) using mobile SMS was introduced which results in increasing the security level but mobile started soon Image matching was introduced by some banks to increase more security. Later some virtual banks like Paytm payment bank implements biometric using mobile touch sensors, which bring some increment in the E-banking security level but not up to the level that required by the user with the introduction of new technologies.

3. PORPOSED MODELLING

After various introduction of security level in mobile with upgraded technology such as face detection, fingerprint, iris detection results its uses in mobile screen locks, various application securities and drawback is the removing of the various locks with some technique such as formatting.

Looking to the mobile security that can be easily hacked has alerted the model of security that need to be changed and implemented with the banking and finance system with the time.

Now, moving from OTP based security to artificial intelligence security that has shown new model for providing security in the field of E-banking system such as face recognition and voice recognition i.e. one level ahead of previous safety level.

3.1. Architecture diagram and Working

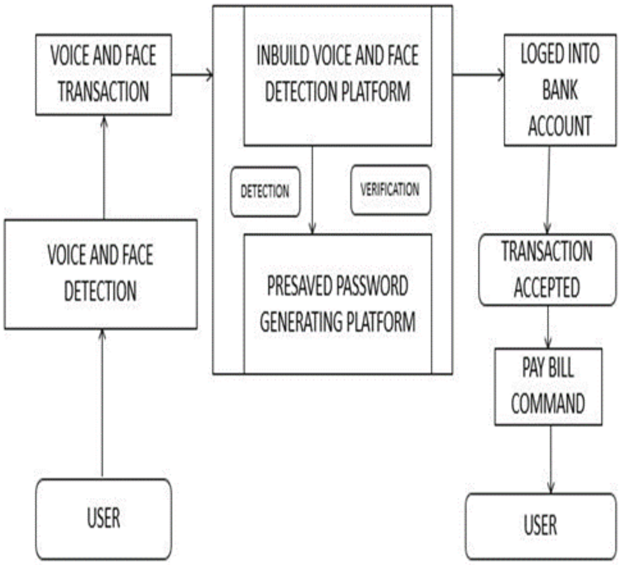


Fig. 3.1, Proposed Model Architecture

In the figure 3.1, we have proposed a peer to peer security level system of E-banking using voice detection and face detection technologies. Here, peer to peer means that this model will operate for sender and receiver both. Firstly, the sender enter its credentials with face detection or voice detection for login into the E-banking page. Then a transfer is made using the face and voice recognition from senders side. Now the transfer is initiated and need to be authorized by the receiver end. Here, the receiver is notified for the transaction completion. Until the authentication is not successful from receiver's end, the transfer is completed. In this way the E-banking is made secured from the both senders and receiver's end.

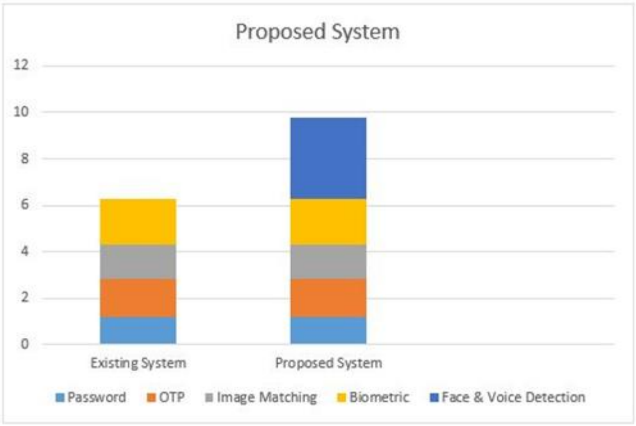


Fig. 3.2, Existing vs Proposed System

In the above given figure 3.2, existing vs proposed system bar graph is given. This graph explains how the security level that was provided in the existing model and security level that is proposed in the system is different. By providing the latest technologies such as face detection and voice recognition to the existing model can bring a sudden changes in online banking and transaction security.

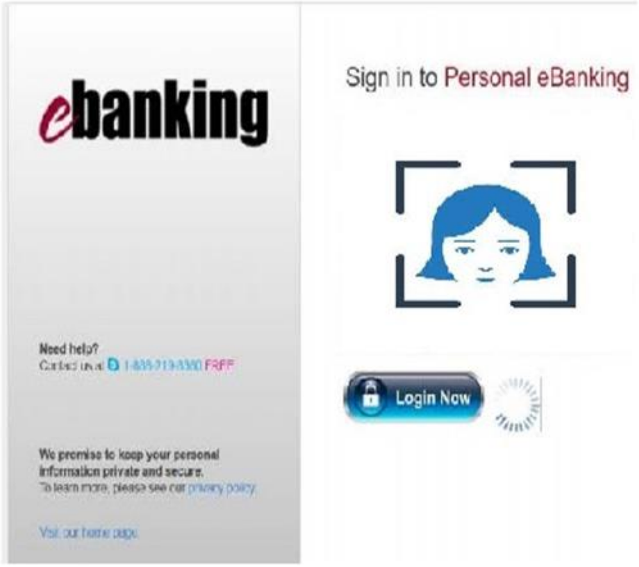
3.2. Proposed technologies

By looking into the problems that the users are facing currently due to large amount of frauds and crime technologies in the online banking and transaction security, a more secured upgradation is provided by using the following methods:

3.2.1. Face detection

This method is possible using the camera, and in today's developing world, every user have a smartphone or laptop in which it is inbuilt. The user just has to keep his or her face in front of the camera, which will recognize the face that must be provided during the setup process. Face detection method is purely based on the recognition of human eye, nose, mouth and face boundaries. The camera is used to create a systematic picture or pattern of human face, encrypts it into a special algorithm and the convert it into a biometric template, which is then saved in a special database or server. Ayonix's 3D Face recognition is impermeable to environmental influences and it is completely contactless. The present state of technology is free from manipulation and works with living tissue of human only.

3.2.2 Voice Recognition


ebanking
Sign in to Personal eBanking
Need help?
Contact us at 1-888-213-8380 FREE
Login Now
Visit our home page

We promise to keep your personal information private and secure.
To learn more, please see our privacy policy.

Fig. 3.3. Login page using Face Detection

In this, a voice recognition software is used, in which the user has to speak up his or her secret phrase or message. This software store that voice and phrase in a database in the form of text for future login purpose. Every human has unique voice just as fingerprint so no fraud can be made. This helps in making the login more fast and robust. To making it possible an inbuilt mic is use in which user will speak the secret message, which is converted into text by the system and is match with the database. Using this it will also be easier to use the account more easily and securely.

In the above figure 3.3, a sample login page is given using face detection, which replace the password login. This made simple and secured login using face recognition.

4. CONCLUSION AND FUTURE SCOPE

In this paper, a full proof secured banking system was introduced for secured login and transactions using Artificial Intelligence Technologies to reduce frauds that occur during transactions or during password login. AI technologies like those that face recognition and voice detection system, which will help in making the existing banking system more secured and robust. We can also include biometric verification system for smartphone users to make it simpler by using just a finger impression or touch. This system not only meet practical use, but also promotes development in banking systems in real time for large amount transactions. In addition, this method is not only limited to use in electronic banking system but can also be implement in other password-based services.

REFERENCES

[1] Yinsheng Li*, Shuai Xue, Xu Liang, Xiao Zhu "I2I: A Balanced Ecommerce Model with Creditworthiness Cloud" in IEEE International Conference on e-Business Engineering in 14th issue, pp. 23 November 2017.

[2] G C Feng, Pong C Yuen and J H Lai "Virtual View Face Image Synthesis Using 3D Spring-based Face Model from A Single Image" in International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) in 14th issue, pp. 06 August 2002.

[3] Hyan-Soo Bae, Ho-Jin Lee, Suk-Gyu Lee "Voice Recognition Based on Adaptive MFCC and Deep Learning" in IEEE 11th Conference on Industrial Electronics and Applications (ICIEA) in 2nd issue, pp. 24 October 2016.

[4] Chang-Lung Tsai Chun-Jung Chen, Deng-Jie Zhuang "Secure OTP and Biometric Verification Scheme for Mobile Banking" in Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing issue 3rd, pp. 20 September 2012.

[5] Bilgehan Arslan, Ezgi Yorulmaz, Burcin Akca, Seref Sagiroglu "Security Perspective of Biometric Recognition and Machine Learning Techniques" 15th IEEE International Conference on Machine Learning and Applications in 2016 on, pp. 02 February 2017.

[6] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[7] C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.