

Biometric Technology in Automated Teller Machines Adoption

Dr. K. Bharatha Babu

Associate Professor, Department of ECE
Anand Institute of Higher Technology
Chennai, Tamil Nadu, India.

Abstract The banking industry is constantly improving its services but using biometrics in ATMs has never been a viable option since data is scarce and the full potential of this mechanism has not been realized. Researchers emphasized biometric technology, stating that an in-depth investigation was conducted to discover the many forms of biometric technology that lead to and fit the concept of future banking. The main finding of the reviewers leads to the high potential of biometric as a security aspect in achieving an ideal future banking solution through a comparison of biometrics, where fingerprint biometrics has an average of more than 50% compatibility and flexibility of implementation and benefits compared to face image, iris recognition, voice recognition, and vein pattern. Another criterion that determines whether face and iris recognition can be a possibility or a replacement for fingerprint recognition, according to previous evaluations, is the intricacy, which makes efforts to steal this sort of security solution almost difficult. Biometric technology has shown to be a technology capable of guiding any bank toward achieving their intended future banking ideal. This paper will examine the use of biometric technologies in ATMs and the gaps that exist in achieving ideal future banking.

Keywords— Teller Machine (ATM), Biometric Technology, and Future Banking are some of the terms used in this article.

1. INTRODUCTION

From the service counter to the Automated Teller Machine to Online Banking and now mobile banking, the bank has evolved. This demonstrates that the financial industry is improving year after year and is following the cashless society trend. When there is a new presence of technology and a user's convenience demand, this evolution happens [1]. There is a problem and a danger at every step of development, which is why security architecture is such a high need to safeguard the company. For a few years, online bank applications have been more popular. Users who have a bank account may manage it with ease using technology such as a personal computer or a smartphone with internet access. Checking account balances, conducting transactions, and paying debts have become easier and more convenient with these electronic gadgets, all with a single click, regardless of place or time.

Viruses such as trojan horses and worms are prevalent. Trojan Horse can sneak up on users and collect their credentials, which it subsequently sends to a hacker. Worms, on the other hand, multiply and consume infrastructure resources, eventually shutting down the system when it reaches a critical level. Another hazard to the banking sector is a denial of service (DoS). This threat degrades the performance of a computer or network, causing it to fail to operate properly, and it

may be used by attackers to diminish the application's availability. This attack does not compromise the bank's hardware, but it has a significant impact on users since it exploits the server's resources to overwhelm it and prevent people from accessing the website.

The attacker floods the server with these many random targets, causing a server overload and reducing the website's accessibility. As previously stated, an application is deemed secure if it maintains Confidentiality, Availability, and Integrity. The security of the data is linked to confidentiality. In the case of a bank application, the data of the bank's customers should be kept private between the bank and the consumer. To avoid data leakage, transaction data kept on the server should not be accessed by other parties and must be properly guarded from attackers. When initiating a transaction or purchasing anything online, for example, customers are more likely to use a debit or credit card as a payment method.

This form of payment will be recorded, recorded in transaction history, and a receipt will be given. To prevent attackers from undermining the user's credentials and information, it should be encrypted. The capacity of an application to be online and functioning for a long period of time, or for the majority of the time, is referred to as availability.

Because users will use the programme for transactions at any time, it should be available 24 hours a day, seven days a week. Denial of Service attacks should not be allowed to harm the system since they will reduce the application's availability. In terms of banking application integrity, data should be consistent and correct throughout the process, as well as up-to-date and legitimate. Data, such as transaction history, cannot be changed without the permission and concern of the person in control. If there is a hazard or risk, backups should be accessible as a point of restoration.

2 FUTURE BANKING PROCESS EVOLUTION

With the advancement of technology, the banking industry has developed an application to ensure the integrity of each electronic device. For example, smartphone users have access to a banking programme called "mobile banking," which is simple to use and accessible to everyone. This programme performs the same functions as a banking application on a computer, but it is simpler and more handy for consumers who like the promise of availability. The word "e-banking" is now often used to refer to banking applications. Hardware, software, network, and users will be the most important aspects of this application. When an application delivers a good user interface and experience, it is deemed successful. Since a result, the application should follow the CIA (Confidentiality, Integrity, and Availability) guidelines, as the banking industry must be safe and prepared for any risk or attack that might negatively impact their company and undermine user trust [2]. [3]. With the present pace of technological advancement, the danger and hazard to the banking business is enormous. Low knowledge of e-banking is one of the dangers that has the greatest effect on users [4][5]. Users should be taught how to distinguish between a legal banking website and a scam one.

The modern banking system is based on the quality of information and service provided. In a system, information quality refers to the system's relevance, correctness, timeliness, and sufficiency. In the banking industry, information is regarded as critical data, and each piece of information gathered is precious. The quality of information influences end users' banking decisions, since technology plays an essential part in data maintenance [6]. The bank's business operations will be harmed as a result of the data's unavailability, resulting in user dissatisfaction with the banking service.

Another feature of the present systematic banking service procedure is service quality. Service quality refers to the level of help offered by the information system and information technology departments to users in troubleshooting their problems. Reference [7] stated emphatically that service quality has a direct impact on end-user experience. Users are dissatisfied because of the slow response and faulty system. Internet banking and mobile banking, for example, should be accessible 24 hours a day, seven days a week since customers may conduct transactions at any time.

Furthermore, system quality and trust are part of the present banking system's systematic procedure. The reaction speed, user interface reliability, and simplicity of use are all indicators of system quality. Reference [6] acknowledges that the system's user interface has a significant influence on consumers' willingness to utilise it. Users should not be confused or find it difficult to utilise the system if the user interface is designed to be user pleasant. User satisfaction will increase as a result of the convenience of usage. The system's security and privacy, as well as client information, should be maintained on a regular basis to ensure that end users' faith is not destroyed, since trust is critical for banks to continue operating. Figure 1 depicts the banking industry's present systematic approach.

Future Banking is an evolution of the current banking model, in which each bank has its own vision and purpose to achieve. One of the future banking ideas is Blockchain technology, which enables other parties to utilise the service supplied without jeopardising security and authority concerns [11]. The block, also known as nodes, in a blockchain architecture, as illustrated in figure 2, will evaluate whether a transaction performed by a user is genuine and determine if it needs to be preserved in the blockchain. This is a way that gives transparency to the IT team by allowing them to discover money laundering in the bank by employing any payment method through system in transaction. The consensus layer [3] will make the decisions. The governance layer works as a pattern reader for physical human engagement with the system, while the computing interface provides for extra blockchain technology capability.

2.1 Adoption of Automated Teller Machines (ATMs) in Future Banking

Since the shift to online and mobile banking, ATMs are now the preferred method of withdrawing and depositing funds. Users prefer to utilise online and mobile banking since the majority of services are accessible on both platforms and can be conducted at any time and from any location. Nonetheless, this user group is particularly susceptible to assaults such as phishing, ransomware, and other forms of malware. According to [8,] e-banking fraud has reached the status of a worldwide concern, with financial sectors

reporting 90 percent of attempted intrusions. According to [9], which agrees with [10], the banking industry has the largest cybercrime problem among the other key and necessary sectors as of August 2018, as seen in figure 3.

Figure 3 depicts the many forms of cyberattacks that the banking industry and other key services are subjected to. Phishing is one of the most prevalent cyberattacks, in which attackers masquerade as bank agents and utilise online or phone conversations to lure consumers into a trap. According to reference [12], phishing is targeted at random individuals, and most older people would fall for these traps since they are unaware of the attacks. With new technology being developed every year, phishing has progressed to many levels, including man-in-the-middle, misleading, and pharming assaults, which subsequently incorporate malware and mostly target users who utilise online and mobile banking as a payment method. Figure 4 depicts the global growth in phishing assaults, while Figure 5 depicts the different kinds of payment systems that are targeted by phishing attacks.

When it comes to the obstacles that online and mobile banking confront, cyberattacks on ATMs are unusual. Reference [10] reported that ATMs have their own issues, such as user-friendliness, where people prefer ATMs over online and mobile banking owing to the difficulty of learning ATM pin codes, the need to renew ATM cards when they expire, and lengthy lineups at ATMs. In comparison to the challenges that plague online and mobile banking, ATMs are more secure, and their potential for Future Banking is unbounded. Another feature that contributes to the ATM's future banking potential is the ability to incorporate new technologies.

2.2 Biometrics in Automated Teller Machines

Biometrics is becoming a must since it can address issues such as illegal transactions. According to reference [1,] the worldwide market is ready to invest in biometrics as a security authorization solution in order to limit the number of hack attempts on the banking industry. Fingerprint and facial images are the most prevalent and well-respected biometric technologies that have been or are being used in online and mobile banking. According to [14][16][17], fingerprint biometrics will be in short supply as additional complexity-based biometrics are added, making hacking and unauthorised attempts more difficult.

The complexity and waiting time for consumers will be minimised if fingerprint biometrics are used in ATMs [7][13]. Every fingerprint has a unique pattern that cannot be readily hacked, making it an excellent substitute for ATM pin entry. Not to mention that biometric technology may be adaptable if upgrades are necessary, and that fingerprints can be simply saved in an Image Processing Database.

Researchers discovered that an iris scanner is the best option for improving reliability and accuracy when compared to other biometric futures [14]. According to [15], owing to circumstances such as illuminations, genetic inheritance, and unique health conditions, everyone's iris has different size. To strengthen the representation of the iris picture that will be used to compare in the database whether it matches the users, a method called normalisation is performed to capture the iris image and filter out irregularities like as lighting and expanded pupil size.

3 CONCLUSION

In a nutshell, the researchers have identified the essential strength of biometrics technology and advocate its use in ATMs. However, while predicting is just mentioned, the study articles do not define the exact method or how it affects future banking. The most recent biometric technology has the ability to integrate with blockchain technology, but grasping the knowledge has proven difficult due to the need for more information to understand the entire process and how it can provide Confidentiality, Integrity, and Availability in the banking sector (CIA). There are other future banking concepts that were not included, such as green banking, humanising banking, and cordless banking, since these papers focused primarily on blockchain technology. Overall, many forms of common biometrics technologies that may be used in ATMs have been found, and this knowledge is useful for future study.

REFERENCES

- [1] 'Biometrics as a means of information security in the banking sector digitalization', 105(Iscde), pp. 264–269. Bakunova, T. V., Trofimova, E. A., and Lapteva, E. V. ISCDE-19.2019.50, doi: 10.2991/iscde-19.2019.50.
- [2] 'Technology Infrastructure Management in Banks 2020 - Agenda for the Future', 6(1), pp. 416–423. Bala, R.
- [3] 'A comprehensive literature analysis of blockchain-based applications: Current state, categorization, and outstanding concerns', Telematics and Informatics, Elsevier, 36(May 2018), pp. 55–81, Casino, F., Dasaklis, T. K., and

- Patsakis, C. tele.2018.11.006. doi:
10.1016/j.tele.2018.11.006.
- [4] Effort expectation, performance expectancy, social influence, and enabling circumstances as predictors of behavioural intentions to use ATMs with fingerprint identification in Ugandan banks, Catherine, B. N. et al. (2017), Global Journal of Computer Science and Technology, 17(5), pp. 5–23.
- [5] 'Offline mobile based OTP technology for business IOT enabled architecture in banking cash logistics and atm operations', International Journal of Advanced Research in Engineering and Technology, 11(1), pp. 61–69, Denis, L. et al. IJARET.11.1.2020.009, doi:
10.34218/IJARET.11.1.2020.009.
- [6] U. Dixit (2018), IOSR Journal of Business and Management, pp. 2319–7668, 'Cryptography-Security in E-Banking'. www.iosrjournals.org is a good place to start.
- [7] Customer data security and theft: a Malaysian organization's experience, Information and Computer Security, 27(1), pp. 81–100, Mohd Aizuddin Zainal Abidin, Anuar Nawawi, A. S. A. P. S., Mohd Aizuddin Zainal Abidin, Mohd Aizuddin Zainal Abidin, Mohd Aizuddin Zainal Abidin, Mohd Aizud
- [8] 'Prospective solution to bank card system using fingerprint,' Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018, (July), pp. 898–902. Muley, A. and Kute, V. (2018) 'Prospective solution to bank card system using fingerprint,' Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018, (July), pp. 898–902. The number to look for is 10.1109/ICISC.2018.8398930.
- [9] N. O. Ogini, N. O. Ogini, N. O. Ogini, N. O. Ogini, N. O. Ogini, N. O. Ogini, N. O. Ogini, N. O. Ogini, N. O. Ogini Issues and difficulties of internet banking (Ogini, Nicholas Oluwole, 2018).
- [10] 'Smart Intelligent ATM Using LABVIEW,' Padmavathi, M., and Nagarajan, R. (2017), International Journal of Emerging Technologies in Engineering Research (IJETER), 5 (5). www.ijeter.everscience.org is a good place to start.
- [11] 'On blockchain and its integration with IoT: Challenges and Opportunities,' by A. Reyna et al.
- [12] 88(2018), pp. 173–190 in Future Generation Computer Systems.
<https://doi.org/10.1016/j.future.2018.05.046>
- [13] 'Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation,' International Journal of Information Management, S. K. and Sharma, M. (2019).
- [14] Elsevier, pp. 65–75 in 44(July 2018), doi:
10.1016/j.ijinfomgt.2018.09.013.
- [15] Olga et al. (2019), CEUR Workshop Proceedings, 2422, pp. 100–110, 'Modeling the process of counteracting fraud in e-banking'.
- [16] C. Zhixia et al. (2018), Asian Economic and Financial Review, 8(5), pp. 571–585, 'Green banking for environmental sustainability-present state and future agenda: Experience from Bangladesh'. Journal.aefr.2018.85.571.585. doi: