Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
July 2024 5(7), 568–573

ENHANCING CYBERSECURITY IN BANKING THROUGH THE IMPLEMENTATION OF BIOMETRIC SYSTEMS: A SYSTEMATIC STUDY

Jayasree. L[1], Dr. B. Anuja Beatrice [2]

[1] Research Scholar, Department of Computer Applications Sri Krishna Arts and Science College
[2] Associate Professor, Department of Computer Applications, Sri Krishna Arts and Science College

ABSTRACT

Security systems in corporations, public spaces, consumer electronics, and private industry are becoming more interested in biometric authentication. Businesses, individuals, and organizations are using biometric security more and more to safeguard their online spaces from attackers and other malicious actors. The term "cyber security" describes the methods, approaches, and instruments used to protect software, computer networks, data, and network systems against potential online threats. The supply of financial services via the internet is known as "cyber banking." Internet banking has expanded along with the shift in the exchange of goods. Internet banking has occasionally experienced problems with security threats, despite its advantages. Biometric security uses behavioral and physical characteristics to authenticate people. It is the most dependable and efficient physical security technique for identity verification. Biometric authentication claims that an individual's unique physical or behavioral characteristics can be used to accurately identify them. To address these concerns, a number of safety measures have been put in place across the board for the Internet banking service. Cybercrime is pervasive throughout the world and represents a serious risk to the development of criminal or terrorist activity. These dangers have the potential to jeopardize both internal and external security if they are not addressed through a single authority. Unnoticed cybercrimes result in the loss of money and personal data. Attacks have previously been launched against information infrastructure and internet services. Hacker attacks and online fraud are just two instances of the frequent crimes involving computers. The Internet of Things, or IoT, is the most dependable platform for enabling pleasant, high-quality human existence. IoT has significantly impacted a number of application sectors. Since smart devices rely on wireless technology for data transit and are developing at a rapid pace, they are more susceptible to hackers. As a result, cybercrime is becoming more commonplace every day. Technology growth gives rise to artificial intelligence (AI)-based cybersecurity, which jeopardizes people's privacy, personal property rights, and public safety. The present study is an attempt to study systematically how the banking security can be impacted through the proper usage of biometric devices integrated with cyber security in banking domain.

Keywords: Security systems, biometric authentication, Cybercrime, artificial intelligence (AI)-based cybersecurity

Corresponding Author
Jayasree. L,
jayasreeanitha92@gmail.com

DOI
10.29121/shodhkosh.v5.i7.2024.3889

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

In today's hyper-connected digital landscape, where financial transactions occur seamlessly across borders and sensitive information traverses networks instantaneously, cybersecurity emerges as an indispensable shield guarding against a plethora of malicious cyber threats. Its paramount importance is particularly evident within the banking sector, where the stakes are high and the potential ramifications of security breaches are profound. Robust cybersecurity measures serve as the bedrock upon which trust and confidence are built among customers, investors, and stakeholders alike. By safeguarding against data breaches, fraud, and unauthorized access, cybersecurity not only protects the financial assets and integrity of banking institutions but also ensures the stability and resilience of the entire financial ecosystem.

Moreover, as the threat landscape continues to evolve with the emergence of sophisticated cyberattacks and vulnerabilities, the need for proactive and comprehensive cybersecurity strategies becomes increasingly imperative.
Investing in cybersecurity not only mitigates potential financial losses but also safeguards critical infrastructure, preserves customer privacy, and upholds regulatory compliance. Furthermore, effective cybersecurity practices bolster innovation and digital transformation within the banking sector by fostering a secure environment conducive to the adoption of emerging technologies such as cloud computing, artificial intelligence, and blockchain. Ultimately, by prioritizing cybersecurity as a fundamental pillar of their operations, banking institutions not only protect their own interests but also contribute to broader economic stability, societal trust, and sustainable growth in the digital age.
Biometric authentication methods, leveraging unique physical or behavioral characteristics of individuals such as fingerprints, iris patterns, voiceprints, or facial features, offer a highly secure and reliable means of identity verification. By incorporating biometric authentication into banking systems, institutions can significantly mitigate the risk of unauthorized access, identity theft, and fraudulent activities. Moreover, biometric authentication not only enhances security but also streamlines the user experience, eliminating the need for cumbersome passwords or PINs. This seamless and convenient authentication process not only boosts customer satisfaction but also bolsters trust in the banking institution. Furthermore, biometric-integrated cybersecurity measures play a vital role in compliance with regulatory standards and data protection laws, ensuring that sensitive financial information remains safeguarded against potential breaches. As cyber threats continue to evolve in complexity and sophistication, the adoption of biometric technology represents a proactive and forward-thinking approach to fortifying cybersecurity defenses within the banking sector. By embracing biometric-integrated cybersecurity solutions, banks can effectively safeguard their digital infrastructure, protect customer assets, and uphold the integrity of the financial system as a whole.

2. REVIEW FROM PREVIOUS STUDIES

According to Machap, Dr. K., & Marco (2023), there has been a notable surge in the adoption of mobile banking in the past two years. Globally, people favor mobile banking above traditional banking methods like ATMs and online banking. Hackers and cybercriminals are more likely to target mobile users when there are more concurrent mobile banking customers. In order to create a safe mobile banking system that makes use of facial recognition, the researcher made the decision to investigate the current mobile banking system. The security of the current mobile banking apps was the main focus of the study. The investigator performed reviews of the literature and analyses of current mobile banking apps to acquire more information for a more comprehensive comprehension of the subject. The developer additionally looked into the technological requirements and methods needed for this project. Upon collecting the results, it was found that over 50% of the participants said their mobile banking app did not enable biometric authentication at the moment. Some of the participants also mentioned that mobile banking fraud still occurs, and that they have either personally experienced it or know of others who have. As a result, this paper will investigate the security features of mobile banking systems offered by a number of reputable banks and financial institutions. Additionally, a comparison between the suggested last-step verification of facial recognition and the current last-step verification of OTP will be conducted. At the end, a suggested approach will be presented explaining why facial recognition is superior to OTP and how it may be incorporated into a mobile banking system to add a higher level of security. Keywords: MiTM, face recognition, biometric security, mobile banking, network security, and payment card industry data security standard.
According to Nesakumar, D., Suresh, T., &Mugilan, P. (2020), everyone uses ATMs to withdraw and transfer money. The application of a fingerprint recognition mechanism in the ATM system is the foundation of this study. We chose this to improve client security and facilitate simple transactions. Since every person has unique fingerprint details, this method will be more widely applicable. There is no need to continually carry your ATM card with you, nor is there any worry of losing it. It is found that fingerprint recognition technology outperforms and is safer than other technologies when compared to other ATM security systems already in use. This facilitates safe and simple transactions while upholding a user-friendly environment. One of the most promising technologies for electronic money transactions is this procedure. The need for quick and precise user identification and authentication has increased due to the expansion of the electronic transaction industry. The Automated Teller Machine (ATM) is a fantastic convenience for people to meet their financial needs. Notwithstanding the many benefits of this system, ATM fraud has recently grown in severity. This technique aids in reducing ATM theft and improper use by other parties. We suggested the technique to stop people from destroying or breaking the devices, threatening to deny transactions to ATM users and other users by using fake identities or masks.

A person's successful identity is a primary concern for any security authentication in a variety of applications, including banking, e-commerce, communications, and so on, according to research by Biradar, P. S., and Jatti, Dr. A. (2020). Multimodal biometric technology is among the greatest identification technologies for person identification and authentication when compared to the current password-based authentication. A system that employs two or more biometrics to identify a person is known as multimodal. In the paper, we offer a multimodal biometric system that incorporates an extraction method for safe authentication and has a unique methodology. The facial and thumb modalities are the two that the system uses. We extract features from both images using a Harris-based technique, selecting the most distinctive characteristics from each and fusing them together via concatenation. A cover picture is steganographically encrypted with the unique features that have been retrieved using a modulo operator-based approach. The recipient receives this encrypted data as an image file for authentication. The concealed features are decrypted and divided into face and thumb features at the receiving end. The pre-trained authorized person feature and these decrypted features are compared, and the individual's authorization or unauthorized status is determined using the multi-svm classifier result. The system's accuracy was calculated, and the results showed that it was accurate enough. By including a second secret key for encryption and decryption, the system can be made significantly more secure.

According to Manju, V., and Madhumathi, S. (2019), online banking services need to be more sensitive to security needs. With the advent of networks, cybercrime has become easier to commit for hacking purposes. As a result, in today's security environment, network security has emerged as a major concern. Without a doubt, Internet banking transactions need to be protected from security risks with many layers of safety. However, providers should address security concerns as part of their services. I've also heard a lot about security breaches, ID card fraud, credit card fraud, and hackers' and crackers' methods of stealing any logical password or pincode character. According to current work, identity can be converted into a username and used to grant access to a system. Since usernames might be misplaced or stolen, the authentication process is required to ensure that the intended user is who they say they are. The latest solutions to the safety and privacy problems are biometric based entire authentication and identity systems. The process of identifying an individual by analyzing their facial features or behavioral characteristics is known as facial recognition. A person's fingerprints, face, hand shape, voice, and iris biometric device are just a few examples of their biometric traits. Here, a facial biometric authentication system is implemented in real time to verify a person's identity for online banking. Our project's main goals are to create a completely functional face recognition system, a verification system, and an understanding of the important components of these important technologies, as well as the social environment system and performance elements. Additionally, offer a multiparty access solution that grants original account holders access capabilities, enabling multiple users to access the same accounts. According to experimental findings, the suggested solution offers a higher level of security for online transactions than the conventional cryptography approach now in use.

According to Deshmukh, P. (2017), the security of one-time passwords (OTPs) is essential because these days, these mechanisms are used to complete the majority of e-commerce transactions. OTP is used to thwart eavesdropping and replay attacks. One kind of assault against an isolated or network-connected computing environment is the replay attack, sometimes known as eavesdropping. The Rivest Shamir and Adleman (RSA) algorithm requires a key size of 2048 bits to achieve a security level of 112 bits, while Elliptic Curve Cryptography (ECC) requires a key size of 224–255 bits. Secret key storage is a problem with the majority of current security model implementations. Cryptographic keys are typically unbreakable in a secure manner and can be retrieved through brute force attacks or by guessing or social engineering. This turns into a weak lin k and causes integrity issues with private data in an extremely secure model. In order to overcome this further drawback, biometrics and cryptography are coupled to create a robust security model. This study proposes a more secure OTP system paradigm that combines fingerprint biometric authentication and electronic commerce. In addition, this approach offers more security with smaller keys than other popular public key crypto models. The cryptographic keys are created just when needed, thus there is no need to memorize or store them anywhere.

3. BIOMETRIC INTEGRATED CYBER SECURITY ARCHITECTURE

Biometric integrated cybersecurity for banking involves the amalgamation of biometric technologies with conventional cybersecurity measures to fortify security within banking systems. Here are the essential components:

1.Biometric Authentication: Incorporating biometric identifiers like fingerprints, iris patterns, facial recognition, voice recognition, or behavioral biometrics such as typing patterns for user authentication. This ensures that only authorized users gain access to banking systems or transactions.

2.Multi-factor Authentication (MFA): Combining biometric authentication with other factors like passwords, tokens, or smart cards to add layers of security. MFA guarantees that even if one authentication factor is compromised, the system remains secure.

3.Biometric Database Security: Implementing robust security measures to safeguard the biometric data stored in databases. This includes encryption techniques, access controls, and secure storage mechanisms to thwart unauthorized access or tampering.

4.Continuous Monitoring: Employing systems to continuously monitor biometric data and authentication attempts for any suspicious activities or anomalies. This aids in detecting and mitigating potential security threats in real-time.

5.Biometric Template Protection: Ensuring secure storage and transmission of biometric templates (digital representations of biometric data). Techniques such as template encryption, tokenization, and secure hashing are utilized to protect biometric templates from unauthorized access or misuse.

6.Integration with Security Information and Event Management (SIEM): Integrating biometric authentication logs and events with SIEM systems for centralized monitoring and analysis of security events. This enables proactive threat detection and response.

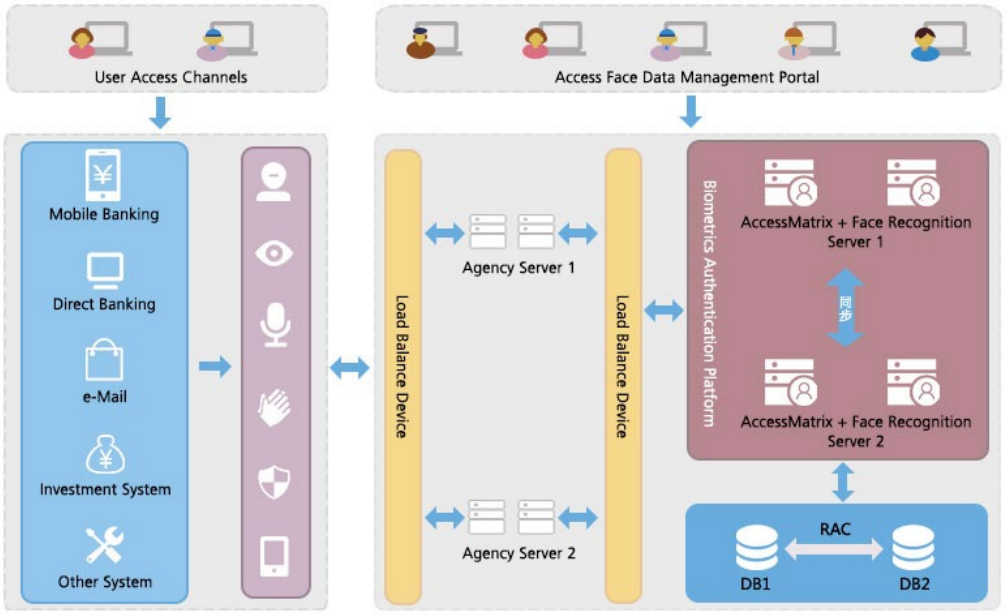
7.Regulatory Compliance: Adhering to relevant regulatory standards and guidelines such as GDPR (General Data Protection Regulation), PSD2 (Revised Payment Services Directive), and industry-specific regulations to safeguard the privacy and security of biometric data.

8.User Education and Awareness: Educating banking staff and customers about the significance of biometric security measures, best practices for biometric usage, and potential security risks associated with biometric authentication.

9.Secure Communication Channels: Employing secure communication protocols and channels for transmitting biometric data between devices and servers to prevent interception or tampering by unauthorized entities.

10.Biometric Device Security: Ensuring the security of biometric authentication devices like fingerprint scanners, iris scanners, or facial recognition cameras against physical tampering or hacking attempts.

ACCESS MANAGEMENT IN FACE DATA MANAGEMENT



Source: https://www.ibia.org/

4. FUTURISTIC ASPECTS OF BIOMETRIC IN BANKING

1.4.1 Biometric Wearables:

Wearable devices like smartwatches, augmented reality glasses, or even biometric-enabled jewelry could become standard in banking.These wearables would feature advanced biometric sensors capable of accurately identifying individuals based on unique physiological traits such as fingerprints, iris patterns, or even vein

patterns.Customers would enjoy the convenience of accessing their accounts or authorizing transactions with a simple gesture, tap, or glance at their wearable device.The integration of biometric wearables with banking systems would significantly enhance security by eliminating the need for passwords or physical cards, which can be lost, stolen, or hacked.

1.4.2.DNA Biometrics:

DNA-based biometrics represent the cutting edge of personal identification technology, offering an unparalleled level of uniqueness and security.Banks could potentially collect DNA samples from customers to create highly secure biometric profiles linked to their accounts. Authentication using DNA biometrics would involve analyzing DNA sequences to verify the identity of customers, ensuring virtually foolproof security. While still in the early stages of development, DNA biometrics hold immense potential for revolutionizing identity verification in banking, especially for high-security applications such as access to vaults or highly sensitive accounts.

1.4.3 Brainwave Authentication:

Brainwave authentication relies on analyzing the unique patterns of electrical activity in an individual's brain to verify their identity.EEG headsets equipped with advanced biometric sensors could capture and analyze these brainwave patterns for authentication purposes. Customers could authenticate banking transactions simply by wearing these EEG headsets, which would recognize their distinct brain activity patterns associated with authorization. Brainwave authentication offers a high level of security as brainwave patterns are highly individualized and difficult to replicate, making them ideal for secure banking applications.

1.4.4 Gait Recognition:

Gait recognition technology identifies individuals based on their unique walking patterns, which are determined by factors such as body structure, movement, and rhythm. Banks could deploy advanced cameras equipped with computer vision algorithms to analyze customers' gait patterns for authentication purposes. Customers would be able to authenticate transactions simply by walking in front of these cameras, eliminating the need for physical tokens or passwords.Gait recognition technology offers a non-intrusive and highly secure method of authentication, as gait patterns are difficult to mimic or spoof, making them ideal for preventing unauthorized access to banking systems.

1.4.5 Emotion Recognition:

Emotion recognition technology utilizes facial expression analysis or voice tone analysis to gauge individuals' emotional states.Banks could employ emotion recognition algorithms to detect signs of stress, anxiety, or deception during banking transactions. This technology could help identify instances of potential fraud or unauthorized access by detecting abnormal emotional states associated with fraudulent activities. Emotion recognition could also be used to personalize banking experiences based on customers' emotional states, offering tailored support or assistance when needed.

1.4.6 Blockchain and Biometrics:

Integrating biometric data with blockchain technology offers a highly secure and tamper-proof method of storing and verifying identity information. Biometric data such as fingerprints, iris scans, or facial recognition templates could be securely stored on the blockchain, accessible only through cryptographic keys owned by the individual. Blockchain-based biometric authentication systems eliminate the need for centralized databases, reducing the risk of data breaches and identity theft. Banks could leverage blockchain and biometrics to create self-sovereign identity solutions, giving individuals full control over their identity information and enhancing privacy and security in banking transactions.

1.4.7.AI-Powered Biometrics:

Artificial intelligence algorithms play a crucial role in enhancing the accuracy and reliability of biometric authentication systems.Machine learning algorithms can continuously analyze and adapt to users' biometric traits, improving the system's performance over time. AI-powered biometric systems can detect and mitigate sophisticated fraud attempts in real-time by analyzing patterns of behavior and identifying anomalies. These systems can also provide personalized recommendations and alerts based on users' biometric data, enhancing security and user experience in banking.

1.4.8 Biometric Cryptocurrency Wallets:

Biometric authentication adds an extra layer of security to cryptocurrency wallets, which are often targeted by hackers due to the irreversible nature of cryptocurrency transactions.Users can secure their cryptocurrency wallets with biometric identifiers such as fingerprints, facial recognition, or iris scans, making it virtually impossible for unauthorized individuals to access their digital assets.Biometric cryptocurrency wallets provide a convenient and secure way to manage digital assets, promoting mainstream adoption of cryptocurrencies in the banking sector.

1.4.9 Biometric ATMs and Branches:

Biometric authentication can transform the way customers interact with ATMs and bank branches, eliminating the need for physical cards or identification documents.ATMs and branches equipped with biometric scanners can authenticate customers using their fingerprints, iris scans, or facial recognition, providing a seamless and secure banking experience.Biometricauthentication enhances security by ensuring that only authorized individuals can access banking services, reducing the risk of card skimming, identity theft, and fraud.

1.4.10 Personalized Banking Experiences:

Biometric data can be leveraged to personalize banking experiences based on individual preferences, behaviors, and needs.Banks can use biometric authentication to tailor product recommendations, marketing offers, and customer support services to each customer's unique profile.Byanalyzing biometric data, banks can gain valuable insights into customers' preferences, risk profiles, and financial habits, enabling them to offer more targeted and relevant services. Personalized banking experiences enhance customer satisfaction, loyalty, and engagement, driving business growth and competitiveness in the banking industry.

5. CONCLUSION

In the rapidly evolving landscape of cybersecurity, where digital threats loom large and financial institutions are prime targets, the integration of biometric technology has emerged as a beacon of hope in the battle against cybercrime. With the proliferation of online banking, mobile payments, and digital transactions, traditional security measures such as passwords and PINs have proven vulnerable to exploitation by sophisticated hackers. In response, the banking sector has turned to biometric authentication – a cutting-edge solution that harnesses unique physiological or behavioral characteristics of individuals to verify identity with unparalleled accuracy. This in-depth exploration delves into the transformative potential of biometric-integrated cybersecurity within the banking industry, examining its underlying principles, technological advancements, implementation challenges, and the profound impact it holds in fortifying defenses against cyber threats. As financial institutions navigate the complex terrain of digital transformation, biometric authentication stands poised as a cornerstone of security, promising not only enhanced protection for sensitive financial assets but also a seamless and user-centric banking experience.

ACKNOWLEDGEMENT

None.

CONFLICT OF INTEREST

None.

REFERENCES

Machap, Dr. K., & Marco. (2023). Facial Recognition Authentication Adds an Extra Layer of Security to Mobile Banking Systems. Journal of Applied Technology and Innovation, 7(1), 2600–7304. Retrieved from https://www.researchgate.net/publication/368316674

Manju, V., &Madhumathi, S. (2019). Improving Net Banking Security with Face Recognition Based Bio-Metric Verification. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 82–91. https://doi.org/10.32628/cseit195335

Biradar, P. S., &Jatti, Dr. A. (2020). Face and Thumb Based Multimodal Bio-Metric Authentication using Harris Feature Extraction and Stenography. International Journal of Recent Technology and Engineering (IJRTE), 9(3), 550–555. https://doi.org/10.35940/ijrte.c4629.099320

Yadav, D., Malwe, D., Rao, Ks., Ku mari, P., Yadav, P., &Deshmukh, P. (2017). Intensify the security of One Time Password using Elliptic Curve Cryptography with Fingerprint for E-commerce Application. International Journal of Engineering Science and Computing (p. 5480). Retrieved from http://ijesc.org/

https://www.idenfy.com/blog/biometrics-in-banking/

https://appinventiv.com/blog/biometrics-technology-in-digital-banking/