ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(4)

REVIEW ARTICLE

A Review of Multi-Factor Authentication and Biometric Security in Online Banking

Dr. Nilesh Jain*
Associate Professor, Mandsaur University, Mandsaur
Department of Computer Sciences and Applications
Email- nileshjainmca@gmail.com

Received: 14-10-2025; Revised: 17-11-2025; Accepted: 20-12-2025

Abstract*— Digital banking has radically transformed the financial industry by increasing the speed, accessibility and efficiency of transactions and at the same time increased cyber terrorist threats. Single-factor authentication methods aren't good enough to protect sensitive banking data, so fingerprints and Multi-Factor Authentication (MFA) are being used more and more. This review delves into the history, applications, and integration of biometric authentication technologies, including behavioural biometrics, voice biometrics, facial and iris recognition, and fingerprint/face/iris scans. These technologies have seen a surge in usage within online banking in the past several years. An overview of recent literature shows that AI-based models, adaptive authentication, and risk-based models are enhancing the process of identity verification and reducing fraud. The comparative analysis demonstrates both advantages and disadvantages of the biometric and multifactor systems, identifying the issues associated with the usability and privacy, as well as the operational integration. The paper also marks such new trends as multimodal authentication, blockchain-enhanced verification, and AI-enhanced anomaly detection. Results point out that integrating AI and biometrics technologies into MFA systems can greatly increase user confidence, decrease cyber security risks, and boost the crypto-protective capabilities of digital banking architectures, which followed by smart, adaptive, and privacy-aware authentication frameworks.

Keywords*—Multi-Factor Authentication (MFA), Biometric Security, Online Banking, Digital Banking, Risk-Based Authentication.

INTRODUCTION

The fast growth of the online business has essentially redefined the international economy and the banking industry is the first in the digital revolution. The trend among financial institutions around the world is shifting their services to the web which allows their customers to conduct safe transactions [1], check on their account status, send and receive money and other financial products without leaving their homes. This advancement has been referred to as online or Internet banking that has created new levels of ease and availability diminishing reliance on physical bank departments and broadening financial accessibility [2]. Nonetheless, since such digital systems store significant amounts of sensitive financial data, they have also become a prime target by cybercriminals, which has created increased anxieties about data breaches, identify theft, and financial fraud [3][4]. Data confidentiality, integrity and authenticity have hence been a priority in ensuring trust in digital banking environments.

In the majority of online sources user authentication is the initial step to prevent the unauthorized access [5]. Historically, the most common solution has been Single-Factor Authentication (SFA) in which verification is based on a single component (a password, PIN or security question). SFA has become an easy target of phishing attacks, brute force, credential theft, and other social engineering [6], despite its simplicity and prevalence [7]. These loopholes put important financial information at the risk of fraudulent users and destroy the trust of the customers in the services of online banking.

MFA has become a key security upgrade in order to eliminate these weaknesses. MFA asks users to enter two or more autonomous credentials to verify, which normally includes something they know (techincal password or PIN), something they have (a token or card or a mobile device), and something they are (biometric characteristics). An approach to security that uses many layers, it significantly lowers the probability of unauthorised access even if one of the authentication requirements has been compromised [8].

Biometric authentication has become the most common method for several reasons. One of them is that it allows for the easy and fast verification of an individual's identification by comparing their distinct collection of physiological or behavioural attributes to a database. Besides its role in security, biometric authentication also makes user experience easier since it does not require one to memorize difficult passwords. Another game-changer in biometric authentication has been the incorporation of AI and ML into these systems, which has improved their pattern recognition, anomaly detection, and dynamic learning capabilities [9][10][11]. Intelligent models are capable of detecting spoofing, studying behavioral anomalies, and implementing reinforcing changes in real-time to the systems.

However, AI-based biometric technologies in the context of MFA have a number of barriers to implementation, such as privacy protection, the compatibility of the systems across different platforms, and ethical data usage [12][13]. Therefore, it is still necessary to create smart, dynamic, and privacy-aware authentication systems that enhance the confidence, safety, and reliability of a modern online banking infrastructure.

A. Structure of the paper

The paper structure is as follows: Section II provides a review of threats and vulnerabilities of online banking. The third section III is about Multi-Factor Authentication (MFA), its types, mechanisms, and challenges. Section IV entails biometric security and its usage in the banking industry. Section V is a literature review of MFA, biometrics and AI-driven frameworks. In Section VI, key findings and future research directions are given.

THREATS AND VULNERABILITIES IN ONLINE BANKING

Online banking is threatened by phishing, malware, and social engineering. Rather, the financial environment nowadays is being characterized more by how easily, conveniently, and quickly online banking can be performed. Through one or two clicks or taps, one can invest in financial instruments at the

comfort of their homes or anywhere they are. E-banking has introduced an unprecedented comfort and efficiency in the field of individual and business finance [14]. Digital revolution and government efforts to facilitate digitalization has been instrumental in changing the banking industry. The banks have taken advantage of the advancements in technology to offer a vast variety of online services to their customers. The services have not only enabled financial transactions but also promoted financial inclusion and people in remote locations can now get access to banking services through the services.

B. Key Features of Online Banking Systems

Online banking systems' newest capabilities are aimed at both individuals and companies:

- Account Management: A unified interface for managing many accounts, including the ability to see balances and transactions.
- Funds Transfer: Direct and easy money transfers between accounts at different banks or even other branches.
- Bill Payment and Subscription Management: Automation of bill and subscription payments helps to curb manual handling [15].
- Loan and Credit Services: Lend money, create credit accounts, and learn about budgeting.
- Investments: Manage portfolios and invest in securities directly while also receiving market insights. Such characteristics are backed by uncompromising security communication tools and identity validation systems to grant privacy and safety to the information of the users.

C. Types of online banking threats

The security of online banking systems is at risk from several attacks that exploit both technological and human errors. In this category and find insider fraud, credential theft, malware, MitM attacks, and phishing. When it comes to internet banking systems, these are some of the most common and dangerous dangers:

- **Phishing Attacks:** "Phishing" is shorthand for the practice of acquiring sensitive information (such as passwords or financial data) through fraudulent channels (email, SMS, websites, etc.). Emails masquerading as legitimate-looking websites or messages from organisations like banks are common vectors for phishing attacks. The illustration is seen in Figure 1.

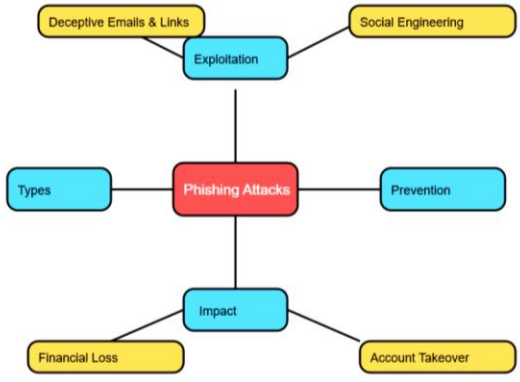

Fig.1.Phishing Attack Mindmap

- **Malware and Trojan Horses:** Malware and Trojan horses are evil software programs that aim to penetrate the computer of a user and in most cases, they do so using seemingly innocent downloads or file attachments. These programs can be installed to steal sensitive information, undermine the security of online banking session and even allow access to bank accounts without permission.
- **Denial of Service (DoS) Attacks:** DoS attacks interferes with online banking by flooding the systems with traffic that would render them usable [16]. Such attacks might cause financial losses to the banks and distrust of the customers.
- **Insider Threats:** Employees, independent contractors, or business associates of a bank pose a danger known as an insider threat if they are able to access confidential data or systems.
- **Man-in-the-Middle (MitM) Attacks:** An attacker can launch a MitM attack if he or she eavesdrops on or changes data in transit between a customer's bank and the server. Table I provides the comparison of the threats.

TABLE I. COMPARISON OF THREATS IN ONLINE BANKING[17]

Threat Type	Description	Mechanism	Impact	Example
Phishing Attacks	Phishing emails coerce recipients into giving over personal information.	Malicious emails, phoney websites	Financial loss, of user trust	COVID-19 phishing scams
Malware and Ransomware	Cyber malware that encrypts data and either demands payment to decrypt it or steals credentials.	Email attachments fake websites, keyloggers	Account takeover, service outages	Zeus Trojan
DDoS Attacks	overloads a bank's servers with traffic, making the platform unworkable.	Botnets, mass request flooding	Service outages, loss of customer trust	U.S. bank DDoS attacks (2012)
Insider Threats	Contractors or employees abuse their access to compromised data	Exploitation of internal access	Data breaches, reputational damage	Capital One breach (2020)
Man-in-the-Middle (MitM)	Attackers intercept communications to steal data or alter transactions.	Exploitation of unsecured connections	Data theft, financial fraud	Fake public Wi-Fi networks

D. Importance of Cybersecurity in Online banking

The risks posed by cyber threats have increased with the growth of online banking. Nowadays, cybersecurity is essential to maintaining operational integrity, regulatory compliance, and consumer trust. Online banking cybersecurity is essential because of the following reasons:

- **Protecting Customer Data:** Financial data, including account numbers, transaction history, and personal identities, is stored by online banking systems. Because fraud and identity theft might result from unauthorized access to personal data, adequate security is crucial.
- **Ensuring Transaction Integrity:** The financial transactions should be kept safe and undamaged in between the source and destination. Cybersecurity ensures that such transactions are not altered or intercepted by malicious users.
- **Maintaining Service Availability:** Cybersecurity risks like DDoS assaults can interfere with banking services,

rendering them inaccessible to clients. Availability is critical to consumer trust and service reliability [18].

- **Regulatory Compliance:** DDoS attacks and other cyber-security risks can interfere with banking services, rendering them inaccessible to clients. Availability is crucial for maintaining client trust and service reliability.

MULTI-FACTOR AUTHENTICATION (MFA) IN BANKING

The premise of multi-factor authentication (MFA) is to supply additional forms of authentication in order to strengthen security and facilitate the ongoing protection of critical infrastructure and services from unauthorised access. Most of the time, biometrics are utilised by MFA to automatically identify individuals according to their behavioural and biological traits [19]. This measure added an extra degree of security as users had to present identity, which is dependent on two or more different factors. Figure 2 illustrates the progression of authentication techniques that have been addressed.

Fig.2.Evolution of authentication methods from SFA to MFA

E. Types of Multi-Factor Authentication (MFA)

A way of verifying a login that requires at least two distinct pieces of evidence is called multi-factor authentication. Typically, three types of verification factors are recognised:

- **Type1**- something that the user possesses, such as code words, secret handshakes, PINs, passwords, or combinations. This covers whatever it is that is necessary to remember and subsequently type, speak, execute, or act upon [20].
- **Type2**- The user is cognisant of the fact that all of the products—including smart carts, cellphones, keys, and token devices—are tangible things. These token devices can, for example, calculate a response from a server-sent challenge number or produce a time-based PIN.
- **Type3**- Parts of the user's body that can be utilised for authentication include voice verification, palm scanning, face recognition, retinal and iris scans, fingerprints.

F. Factors Authentication

A vital line of defence against illegal access to any kind of data, service, or equipment is authentication, whether it's online or offline. During authentication, the user provides the system with x to confirm their identification. If F(x) is greater than or equal to y, the system checks the user's identify by comparing it to a stored number.

- **Single factor authentication (SFA):** A username and password combo is the gold standard of authentication. for example, requiring a password or PIN verification from the user [21]. Combinations of capital and lowercase letters, numbers, and symbols make compose a robust password. An attacker would have a harder and harder time deciphering the combination shown above as the password strength grows (see image 3).

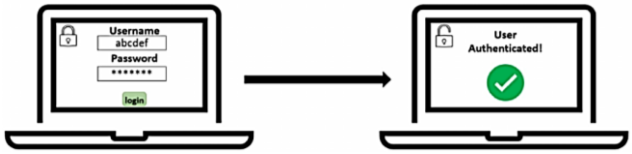

Figure.3: Single factor authentication

- **Two-factor authentication (2FA):** Several security concerns led to the conclusion that SFA could not give sufficient protection. Figure 4 demonstrates the process of two-factor authentication (2FA), which increases security by combining representative data (password/username combination) with an extra kind of identification, such as a personal ownership factor, which might involve a secure token utilising a OTP.

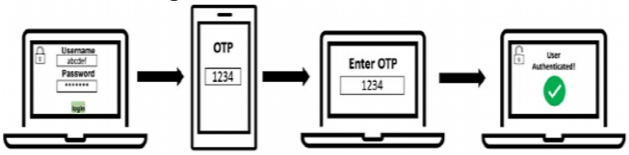

Figure.4: Two- factor authentication

- **Multi factor authentication (MFA):** MFA often makes advantage of the user's unique biological characteristics, including iris or fingerprint scans, which are usually produced and used with a high degree of accuracy. By combining at least three distinct kinds of credentials, as shown in Figure 5, a higher level of security may be provided to prevent unauthorized access to computer equipment and other important services.

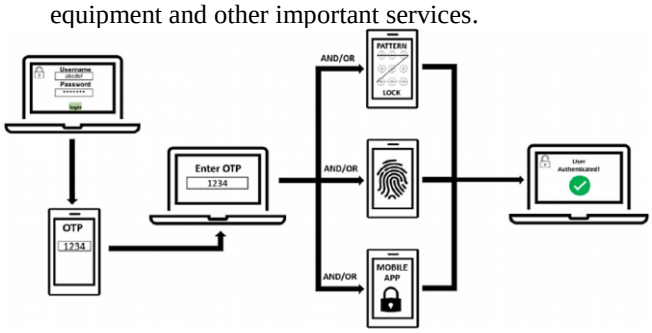

Figure.5: Multi factor authentication[22]

G. MFA Operation Challenges

The integration of cutting-edge technology has always presented developers and administrators with formidable obstacles. Figure 3 shows the main difficulties. Prioritising user input is essential when updating to multi-factor authentication and strong identification. Since most of the obstacles are actually opportunities and possible advantages, adopting and implementing MFA solutions requires a careful and comprehensive plan.

- **Usability:** There are three ways to look at the majority of authentication-related usability issues:
  - Task efficiency— Time required for system login and registration.
  - Task effectiveness— The login attempt attempts to establish a connection to the system.
  - User preference— Personal preference of the user about the authentication method.
- **Integration:** The majority of consumer MFA systems are still hardware-based. In general, a business can gain much from combining physical and IT security, including increased security as well as increased efficiency and compliance. Convergence is not that easy, though. Upgrading the physical access systems, integrating heterogeneous system components, and integrating the IT and physical security teams are related challenges.
- **Security and Privacy:** such as communication routes, sensors, data storage, and processing equipment. All of those are often open to a broad variety of assaults at various levels, such as replay attempts and attacks by

adversaries. In order to enable and preserve privacy, security is therefore an essential instrument. Consequently, start by attacking the input device itself.

- **Robustness to Operating Environment:** The biometric systems, primarily fingerprinting, were not meeting the "robustness" criteria from the start, even if the security and privacy issues are entirely overcome. The main reason for this was that the operational testing were conducted in a controlled laboratory environment instead of a real-world landscape. Consider speech recognition: it worked like a charm in a peaceful atmosphere, but in busy cities, it couldn't verify the user's identity [23].

BIOMETRIC SECURITY IN BANKING

Biometrics is the measurement and examination of specific physical or behavioral traits that are unique to individuals that have become eminent in different sectors. The innovative use of biometrics in banking has recently emerged as a prime area for academic inquiry. Biometric identification offers a new methodology over the old modes of identification using passwords or identification cards because biometric characteristics cannot be tampered with as far as theft, replication, purchase, or forgery are concerned [24]. This increased degree of trust has created much interest in implementing the biometric solutions in the banking sector, which can be regarded as a big leap in enhancing security and reliability.

H. Applications of Biometrics in Banking

The biometric technologies have transformed the banking industry by offering very secure and convenient ways of identifying the customers. They allow banks to increase security, decrease fraud, and automate other financial services. The most significant uses of biometrics in banking include the following:

- Customer Authentication – Biometric biometrics like fingerprint, facial, or iris identification is becoming a popular procedure used by banks to safely identify a customer whenever they log into a mobile application, online banking portal, or even branch kiosk. Traditional passwords and PINs, which are easy targets for hackers, see a decline in usage as a result [25].
- ATM Security – Biometric ATMs enable consumers to use their accounts without the use of physical cards, or via fingerprints, palm veins, or facial recognition. This greatly minimises the threats of card skimming, PIN stealing and unauthorized withdrawals.
- Fraud Detection and Prevention – Biometric verification is an additional security layer to high-value transactions, as it validates the identity of the customer in real time [26]. Banks are able to identify and avert fraudulent activities by keeping a check on unsuspected behaviors and by cross matching biometric data.
- Secure Payment Authorization – Biometric verification can be performed in the form of fingerprints, facial recognition, or vocal recognition enabling customers to make digital payments, online transfers, and contactless transactions. This guarantees the security of payments as the transaction can only be approved by the account holder.
- Remote KYC and Onboarding – Biometric systems allow the banks to be able to remotely check the identity of new customers on account opening and KYC compliance. It minimizes the amount of paperwork, reduces the need to visit a branch, as well as guarantees safe onboarding even in digital-first or remote banking conditions.

I. Use of Biometric Technology in Transactions

The banking industry is rapidly adopting biometric authentication due to its dependability, enhanced security, and simplicity. Biometric identifiers (fingerprints, face recognition, voice, iris scan, etc.) are extremely difficult to replicate, unlike traditional passwords or PINs. Biometric authentication of logins and authorization of transactions is being becoming more and more supported in modern banking applications and offers their users a more streamlined experience and lowers the possibility of identity theft considerably. Even in the event that a device is compromised, transaction cannot be made without a biometric match by the unauthorized users. Moreover, the biometric systems provide easier way to a user who might experience trouble with passwords such as the elderly or with lower literacy [27]. The biometric solutions are also extended to wearable gadgets and smart kiosks that have facial recognition features, which are more convenient and useful.

Biometric technology is a very important layer of security as digital banking grows to ensure that sensitive financial information is not accessed by unauthorized persons. A number of financial service providers and several banks around the world have applied smart banking practices that incorporate the use of biometrics [28]. Take Apple Pay as an example. It utilises Face ID and Touch ID to guarantee that only the owner of the device may authorise contactless payments. Biometric-enabled ATMs and kiosks are being adopted in multiple countries, allowing users to complete secure transactions without traditional cards or PINs. Improved security, a better customer experience, and more equitable access to digital financial services are all outcomes of biometric integration into banking procedures.

J. Types of Biometrics system

Global need for information security and security legislation has led to biometric identification technologies becoming more widespread in everyday life. For this reason, multimodal biometrics technology has become popular since it can solve many of the fundamental problems with traditional, single-modal biometric systems. A variety of biometric authentication methods, each utilizing one or more databases, are used to analyze specific articles. Figure 6 depicts the various biometric system types. In security, biometric authentication is the most effective method of identifying and confirming an individual. This kind of biometric authentication should be the main emphasis of this review:

- Face recognition: Face recognition is a technique that verifies or identifies a person based on their facial features. People can be recognized by face recognition software in real time or in pictures and videos. Computer algorithms are used by facial recognition software to recognize distinctive traits on an individual's face.
- Fingerprint identification: Among various biometric technologies, fingerprints are currently regarded as one of the most traditional and widely used. The valley, or empty area between the ridges, represents the low, shallow part of the friction ridge coat [29]. The friction ridge skin's elevated, peaky part shows a pattern of black lines. The minute, which is the position and orientation of ridge termini and bifurcations (splits) along a ridge route, is used to identify it.
- Iris Recognition: Iris recognition is a biometric technique for personal identification that makes use of distinct patterns in the ring-shaped region of the eyeball that encircles the pupil. Irises are a great biometric verification method because each one is unique to a person. Iris Recognition is a digital camera method that uses

specialised hardware. The camera takes a high-resolution image of an individual's iris by combining visible and near-infrared light. By using Recognition of Iris, the camera is able to focus on the eye and pinpoint its many features, including the pupil, iris, eyelids, and lashes.

- Speaker Recognition: Speaker recognition refers to the act of automatically identifying the speaker by analysing speaker-specific information present in speech waves. This technology verifies people's identities. Identification and verification of speakers are two kinds of speaker recognition. Finding out which of the registered speakers a specific speech came from is what speaker identification is all about. One way to confirm or deny a speaker's identity is through speaker verification.
- Gait Recognition: It is interesting though true that every human being has his or her style of walking. Gait recognition is not employed actively due to problems such as the requirement of large databases[30], less convenient patterns, etc. however, the study is still active.
- Ear Recognition: People are increasingly concerned with biometric recognition as technology advances. The human ear is a goldmine of data when it comes to passive person recognition. It seems like an excellent prospective solution because the ear is visible, taking pictures is simple, and the ear's structure does not change greatly over time. One of the most important biometrics that is gaining popularity is ear biometrics.
- Hand Scanning: The human hand, especially the palm, possesses certain characteristics that can be utilized for personal identification, according to biometrics research. The dimensions of the palm and fingers (width, thickness, and length) are part of these characteristics. These features are used in many commercial systems for various purposes.

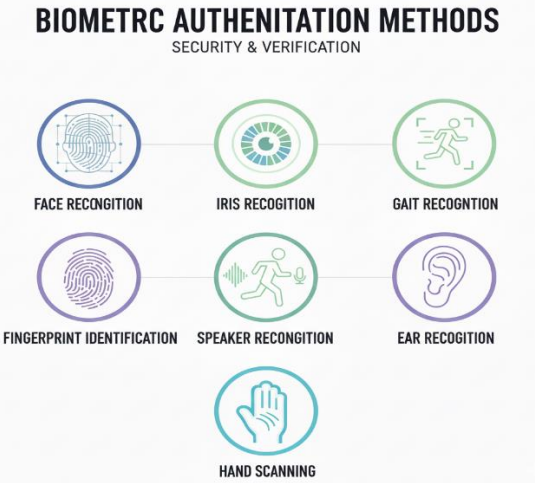

Figure.6: Type of Biometrics System

LITERATURE REVIEW

This section emphasizes recent research on MFA, biometric security, and AI-based authentication systems in digital banking, as well as demonstrate how they address the issues of user verification, fraud prevention, system reliability, and the enhancement of cybersecurity throughout internet-based financial services.

Pandey, (2025), introduces a Multi-Factor Authentication (MFA) framework that is AI-enabled so that cloud security can be improved through the application of AI methods of conducting behavioral analysis, detecting anomalies, and making dynamic decisions. Based on real world data, this framework identifies user behavior, device attributes and surrounding data used to assess authentication requests in real time. The outcomes of the implementation show that there is a tremendous increase in the accuracy, detection of threats and the user conveniences as the un-authorised access is minimised and security is ensured [31].

Gunalan *et al.*,(2025), proposals a new way to resolve this problem by introducing a dynamic Web site authentication system with TOTP validation. The system enables websites to enroll safely with a central authentication server, which produces unique TOTP codes, which the user can validate to ascertain the authenticity of the website. On registering a website, the owners are provided with a secret key which is used to calculate an TOTP code that expires after every 30 seconds. The proposed project focuses on easy to verify systems and key management systems to insure users against phishing attacks [32].

Kumar *et al.*,(2025), includes a synopsis of recent advances in behavioural biometrics, including methods that utilise ML algorithms to evaluate and understand behavioural data. It also discusses the constraints, including privacy issues and the reliability of algorithms, that prevent large-scale use, behavioral biometrics using technologies to enhance security and privacy protections like passwords and tokens are not effective in preventing such changing threats to enhance authentication systems hence, the use of behavioral biometrics has become a feasible step. Behavioral biometrics uses the idiosyncratic human behavior like typing rhythms and touchscreen gestures to continuously authenticate user identities with high precision and low levels of user friction [33].

Sriman *et al.*,(2024), evaluates the benefits and drawbacks of various biometric methods, such as behavioural biometrics, facial recognition, fingerprints, iris scans, and voice recognition, among others. The study emphasises the importance of a robust security strategy in addressing spoofing attacks, privacy concerns, and multimodal integration. The through analysis takes into consideration some of the key issues like accuracy, ease of use and susceptibility to fraudulent activities and its strengths and weaknesses are well balanced. More research and development is urgently needed to solve privacy and security problems; the study also explores the many biometric modalities and the progress of multimodal authentication systems [34].

Samonte *et al.*,(2024), explores the use of several algorithms, including caller ID verification, voice biometrics, two-factor authentication, and authentication based on blockchain. It covers the pros and cons of several technologies with an emphasis on a multi-layered security system to strengthen defences against advanced cyberattacks. For a more in-depth look at the challenges and successes, the report delves into industry-specific modifications and pilot initiatives. Ways forward for digital banking security research in terms of practical applications, user acceptability, and the integration of cutting-edge technology [35].

Pramila and Shukla,(2023), an ML-based risk-based authentication solution that suggests a multi-server architecture. Most of the existing research on adaptive authentication has concentrated on the technique alone, without considering its potential utility in a multi-server scenario. In a multi-server system, user data is more readily available for predicting on the first login, therefore this research aims to evaluate the user's risk at that point [36].

Table II presents the overview of the MFA, Biometric-based security, and AI-based authentication systems in online banking, the research focus, methodology, the main findings, the identified limitation or drawbacks, and the perspective of the research.

TABLE II. COMPARATIVE REVIEW OF MULTI-FACTOR AUTHENTICATION, BIOMETRICS, AND AI-DRIVEN FRAMEWORKS IN DIGITAL BANKING SECURITY

Reference	Study On	Approach	Key Findings	Limitations	Future Directions
Pandey (2025)	AI-enabled MFA for cloud security	AI-driven behavioral analysis, anomaly detection, dynamic decision-making	Improved accuracy, stronger threat detection, enhanced user convenience	Computational overhead; need for diverse datasets	Broader adoption of AI-MFA in real-time systems
Gunalan et al. (2025)	Dynamic website authentication	TOTP for site verification	Reduced phishing risks, improved trust between user and server	Dependence on secure key management; usability constraints	Expanding deployment in e-commerce and banking
Kumar et al. (2025)	Behavioral biometrics	ML algorithms for typing rhythm, touchscreen gestures, behavioral traits	Continuous identity verification, high accuracy, low user friction	Privacy concerns; algorithmic bias and reliability issues	Wider adoption with privacy-preserving AI techniques
Sriman et al. (2024)	Biometric authentication methods	Review of fingerprints, iris, facial, voice, and multimodal biometrics	Comprehensive strengths/weaknesses; emphasized multimodal integration	Vulnerability to spoofing; high implementation costs	Development of robust multimodal systems with privacy safeguards
Samonte et al. (2024)	Multi-layered authentication in digital banking	Caller ID, voice biometrics, 2FA, blockchain	Layered approach enhances resilience against advanced attacks	Sector-specific constraints; limited user adoption	Research into user acceptance and real-world deployments
Pramila & Shukla (2023)	Risk-based authentication in multi-server environment	ML-based adaptive authentication framework	Risk estimation improves login security	Limited real-world implementation; narrow scope	Extension to broader adaptive MFA across cloud and IoT environments

CONCLUSION AND FUTURE WORK

Multi-Factor Authentication (MFA) and biometrics aim to provide a major breakthrough in the protection of online banking systems in the face of emerging cybersecurity threats. The discussion shows that the integration of AI-based biometric recognition and multifactor systems can significantly increase the reliability of authentication, fraud detection, and trustworthiness of users. Facial, fingerprint and behavioral recognition are biometric modalities offer greater assurance than traditional password-based systems and convenience and security in financial transactions. Nevertheless, there are still a number of issues, such as privacy protection, interoperability across platforms, and the need to balance user convenience and strict security. To deal with these issues, it is necessary to design transparent and adaptive authentication models that can learn user behavior and adapt to the changing threat patterns in real time. Further study is needed on decentralized and privacy-preserving authentication systems that implement blockchain in recording immutable identities and apply federated learning to train AI models safely. The advent of multimodal verification systems that are sensitive to context and utilize biometric, behavioral and environmental information has the potential of transforming digital banking security. Regulatory compliance, ethical data processing, and inclusivity should be stressed as well to guarantee a high level of adoption. Ultimately, the convergence of AI, biometrics, and cryptography will define the next generation of secure, intelligent, and user-centric online banking ecosystems.

REFERENCES

[1] S. B. Shah, "Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection," in *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, 2025, pp. 1–7.

[2] V. Prajapati, "Exploring Machine Learning Models for Fraud Identification Through Credit Cards in Financial Market," in *2025 Global Conference in Emerging Technology (GINOTECH)*, 2025, pp. 1–6.

[3] H. Kali, "Optimizing Credit Card Fraud Transactions identification and classification in banking industry Using Machine Learning Algorithms," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 11, pp. 85–96, 2024.

[4] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," pp. 101–110, 2025.

[5] J. Mishra, B. B. Biswal, and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, 2025, pp. 431–436.

[6] N. A. Karim, O. A. Khashan, H. Kanaker, W. K. Abdulraheem, M. Alshinwan, and A.-K. Al-Banna, "Online Banking User Authentication Methods: A Systematic Literature Review," *IEEE Access*, vol. 12, pp. 741–757, 2024.

[7] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in *2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST)*, 2025, vol. 1, pp. 1–6.

[8] J. Williamson and K. Curran, "The Role of Multi-factor Authentication for Modern Day Security," *Semicond. Sci. Inf. Devices*, vol. 3, no. 1, pp. 16–23, May 2021.

[9] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, 2025.

[10] N. Malali, "Exploring Artificial Intelligence Models for Early Warning Systems with Systemic Risk Analysis in Finance," in *2025 International Conference on Advanced Computing Technologies (ICoACT)*, 2025, pp. 1–6.

[11] A. J. Rahul Dattangire, Ruchika Vaidya, Divya Biradar, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, 2024, pp. 1–6.

[12] V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions : A Case Study Using Real-Time Data Streams," vol. 3, no. 4, pp. 149–157, 2023.

[13] B. R. Ande, "Autonomous AI Agents for Identity Governance: Enhancing Financial Security Through Intelligent Insider Threat Detection and Compliance Enforcement," in *Data Science and Big Data Analytics*, vol. 56, D. Mishra, X. S. Yang, A. Unal, and D. S. Jat, Eds. Springer, Cham, 2025.

[14] V. C. -, "Threats in Online Banking," *Int. J. Multidiscip. Res.*, vol. 6, no. 1, pp. 1–8, 2024.

[15] K. S. Patange, M. I. UL Huq, and P. S. Bhambhani, "A Study On Impact Of Digital Banking On Customers Satisfaction," *Int. J. Res. Publ. Rev.*, vol. 6, no. 3, pp. 3015–3021, Mar. 2025.

[16] M. C. J. -, M. H. B. -, and M. A. S. -, "Enhancing Biometric Security with Artificial Intelligence: A Cutting-Edge Approach," *Int. J. Sci. Technol.*, vol. 16, no. 1, pp. 1–25, 2025.

[17] F. Jimmy, "Cybersecurity Threats and Vulnerabilities in Online Banking Systems," *Int. J. Sci. Res. Manag.*, vol. 12, no. 10, pp. 1631–1646, Oct. 2024.

[18] A. Chakraborty, "Cyber Security Threats In Indian Banking Sector And Implementation Of AI As A Preventive Measure," vol. 14, no. 4, pp. 83–91, 2024.

[19] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," *Digit. Heal.*, vol. 9, Jan. 2023.

[20] S. Rajarajeswari and M. A. M. Stella, "a Review of Authentication and Authorization Methods," *Int. J. Comput. Sci. Inf. Technol. Res.*, vol. 7, no. 3, pp. 78–83, 2019.

[21] M. K. Sukeerthi, B. S. Vaishnavi, J. A. Raju, S. S. Shetty, and M. H. Ali, "Real-Time Cyber Attack Prediction Using ML Algorithms," *Int. J. Res. Publ. Rev.*, vol. 6, no. 7, pp. 4905–4911, 2025.

[22] M. Papathanasaki, L. Maglaras, and N. Ayres, "Modern Authentication Methods: A Comprehensive Survey," *AI, Comput. Sci. Robot. Technol.*, vol. 2022, pp. 1–24, Jun. 2022.

[23] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, “A survey on multi-factor authentication for online banking in the wild,” *Comput. Secur.*, vol. 95, p. 101745, Aug. 2020.

[24] M. Marani, M. Soltani, M. Bahadori, M. Soleimani, and A. Moshayedi, “The Role of Biometric in Banking: A Review,” *EAI Endorsed Trans. AI Robot.*, vol. 2, Aug. 2023.

[25] P. M. A. B. Estrela, R. de O. Albuquerque, D. M. Amaral, W. F. Giozza, and R. T. de S. Júnior, “A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications,” *Sensors*, vol. 21, no. 12, p. 4212, 2021.

[26] J. Chase, “Predictive Modeling for High-Value Audience Identification in Financial Services,” *Int. J. Innov. Res. Technol.*, vol. 12, no. 2, pp. 4145–4152, 2025.

[27] R. Kumari and A. Gupta, “Smart Banking System : The Fusion Of AI And Biometrics In Secure Transactions,” vol. 13, no. 6, pp. 267–272, 2025.

[28] I. Velásquez, A. Caro, and A. Rodríguez, “Authentication schemes and methods: A systematic literature review,” *Inf. Softw. Technol.*, vol. 94, pp. 30–37, Feb. 2018.

[29] A. Babich, “Biometric Authentication . Types of biometric identifiers,” 2012.

[30] H. Ali and S. Shaikh, “Comprehensive Review on Different Types of Biometrics and the Impact of Pandemic on Biometric Security,” vol. 3, no. 2, pp. 70–79, 2024.

[31] P. Pandey, “AI-Enabled Multi-Factor Authentication (MFA) Systems for Private and Public Cloud Security,” in *2025 International Conference on Electronics and Renewable Systems (ICEARS)*, 2025, pp. 886–889.

[32] M. C. Gunalan, B. K, M. Hayden, M. H. R, and R. S, “Dynamic Website Authentication Using Time-Based One-Time Password (TOTP) for Enhanced Security,” in *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 2025, pp. 1–2.

[33] N. V. Kumar, K. Bonagiri, B. Thilakavathi, S. Banumathi, I. G. S, and P. K, “Cybersecurity and Behavioral Biometrics: Advancements, Challenges, and Future Directions in Authentication Systems,” in *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, 2025, pp. 898–903.

[34] J. Sriman, P. Thapar, A. A. Alyas, and U. Singh, “Unlocking Security: A Comprehensive Exploration of Biometric Authentication Techniques,” in *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2024, pp. 136–141.

[35] M. J. C. Samonte, J. K. Callejo, D. C. N. Lumbera, and J. C. B. Ocaya, “Mitigating Vishing in Digital Banking Through Caller Authentication and Verification Technologies,” in *2024 14th International Conference on Software Technology and Engineering (ICSTE)*, 2024, pp. 102–108.

[36] R. M. Pramila and S. Shukla, “An Architecture for Risk-Based Authentication System in a Multi-Server Environment,” in *2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA)*, 2023, pp. 1–5.