Advancing AI-Enhanced Financial Security: A Review of Facial, Voice, and Medical Biometrics for Identity Verification

Zhicong Chen[1]Alice Xiaodan Dong[2]Gareth William Peters[3]
Jennifer Chan[4]Weidong Huang[5]Chun-Cheng Lin[6]

***Abstract*— Identity verification is a critical component of financial data and systems security and privacy preservation, and is required by regulatory guidelines to ensure compliance with regulatory requirements and to aid in fraud prevention. With advances in artificial intelligence (AI), deep learning, and statistical methods, financial institutions are increasingly adopting multifactor authentication (MFA) that incorporates biometric-based approaches to perform authentication of identities for access to accounts, records or data and for verification of decision making and confirmation of actions.**

This paper presents a systematic review of current methodologies that utilize facial recognition, voice biometrics, and other data for identity verification in financial institutions. We explore the effectiveness and challenges associated with these approaches, highlighting recent developments in AI-driven models, deep learning architectures, and statistical techniques. In addition, we discuss the integration of multimodal biometric data and the decision and access systems that are developed for MFA approaches to improve security and accuracy. This review offers insights into the future of biometric identity verification in the financial sector.

Our findings suggest that the integration of multimodal data in financial applications could serve as a valuable avenue for future research and practical applications. In addition, investigating the role of biometric authentication in back-end systems is an important area worth further exploration.

Keywords — Biometrics, ID Verification, Artificial Intelligence, Financial Security

I. INTRODUCTION

As cyberattacks grow in frequency and sophistication, ensuring secure and reliable identity verification has become more critical than ever to safeguard financial systems. Identity verification supports secure access to data and records, authorizes transactions, and supports effective risk management. It also enables financial institutions to comply with regulatory frameworks while mitigating the threat of fraud and unauthorized activity.

Traditional methods, such as single factor authentication that has traditionally focused on document-based verification based on signatures or passwords, are becoming less effective against sophisticated threats. The development of IP address tracking, or pin verification systems based on authenticator apps or sms text messages has failed to act as the best standard of security in financial data/account access as threats improve in sophistication with malware on computers, such as IP masking and phone sim card jacking.

The 2020 Twitter breach demonstrated critical security failures when hackers compromised high-privilege internal accounts through social engineering, hijacking over 130 verified accounts to promote Bitcoin scams. This incident revealed systemic vulnerabilities in traditional access management, particularly overreliance on single-factor authentication and inadequate employee privilege controls. While Twitter responded by implementing MFA and least-privilege principles the financial sector remains exposed to similar risks.

With advances in artificial intelligence (AI), deep learning, and statistical techniques, financial institutions are moving towards biometric-based authentication, leveraging facial recognition, fingerprint scanning, and behavioral analytics to enhance security and streamline the verification process. This transition not only strengthens fraud prevention, but also improves the user experience by offering seamless and reliable identity authentication solutions. Industry reports [1] highlight the increasing risk of cyber threats and the need for robust digital ID verification in financial services. AI enhances security by automating identity checks, reducing fraud, and improving compliance and data privacy.

While identity verification methods are well-explored in engineering domains, their application within the financial sector remains relatively underdeveloped. This paper addresses this gap by presenting a systematic review of identity verification techniques

*This work was not supported by any organization

[1]Zhicong Chen, [2]Alice Xiaodan Dong and [5]Weidong Huang are with Transdisciplinary School, University of Technology Sydney, [3]Gareth William Peters is with Department of Statistics and Applied Probability University of California, Santa Barbara, [4]Jennifer Chan is with Faculty of Science The University of Sydney, [6]Chun-Cheng Lin is with Dept. of Industrial Engineering & Management National Yang Ming Chiao Tung University Zhicong.Chen-1@student.uts.edu.au
Xiaodan.Dong@uts.edu.au
garethpeters@ucsb.edu
jennifer.chan@sydney.edu.au
Weidong.Huang@uts.edu.au
cclin321@nycu.edu.tw

across key functional areas within financial institutions. It offers industry practitioners and researchers critical insight into how recent advances, particularly in artificial intelligence, are enhancing biometric-based authentication for tasks such as customer onboarding, transaction authorization, fraud detection, and regulatory compliance. Our findings suggest that the use of multimodal data in financial applications presents a promising area for future research and practical implementation.

II. Related Work - related review papers

Modern face recognition primarily employs CNN architectures, utilizing convolutional layers to extract hierarchical features enhanced by triplet loss optimization, particularly for financial liveness detection against Deepfake attacks [2]. The field of voice recognition has transitioned from Long short-term memory (LSTM) to Transformer models, leveraging self-attention mechanisms to capture temporal dependencies for voiceprint authentication and fraudulent call analysis. Lightweight models achieve optimal accuracy-efficiency balance through Neural Architecture Search, making them ideal for mobile payment applications [3].

The digital transformation of the financial sector has introduced new opportunities and challenges, particularly in identity verification. Parate et al. review the evolution and critical role of digital identity verification, with a focus on its importance in Know Your Customer (KYC) processes essential for maintaining the security and integrity of financial transactions in the digital age [4]. It highlights how emerging technologies are converging to redefine the future of digital identity verification in banking. However, it has not addressed the use of multimodal data in identity verification.

Biometric systems based on physiological and behavioral characteristics (such as fingerprints, irises, faces, veins, etc.) are widely used in the field of identity authentication due to their uniqueness and durability [5]. However, single-modal systems have limitations such as environmental sensitivity and spoofing attacks [6]. To address these issues, multimodal biometric systems have significantly improved recognition accuracy and anti-spoofing capabilities by using multiple features [7].

III. Review method

In order to minimize subjective bias in the screening process and maximize search efficiency, we have created a systematic search specification to guarantee the thoroughness and high caliber of the literature. The literature for this study is gathered from two databases: IEEE Xplore and Science Direct. Although the search methodology is comparable between the two, their built-in filtering techniques differ significantly, as shown below.

- Selection and combination of keywords: The retrieval formula is built from the views of machine learning and financial applications and it conducts extensive mining around biometric technology. The keyword system is organized into three dimensions. Keywords in each dimension are combined using the logical operator ”AND” and permit flexible collocation (for example, ”fingerprint recognition AND payment security”) to build highly relevant search algorithms to assure search accuracy and coverage.
  - Biometric Modalities: covers core terms including ”biometric”, ”facial”, ”fingerprint”, ”voice”, ”iris” and ”signature”;
  - Technical Approaches: including ”authentication”, ”multi-factor authentication” (MFA) and ”recognition”;
  - Financial Contexts: focus on practical application fields including ”payment”, ”banking” and ”finance”.
- Setting the time span: For the purpose of balancing the historical depth and academic frontier, we restrict the search period to 2015–2025. In order to capture the most important research findings and trends in technological evolution over the last ten years.
- Differentiated screening strategies of databases. Due to the differences in the literature collection preferences of different platforms, we have adjusted the filtering strategies in a targeted manner:
  - IEEE Xplore: This platform focuses on conference papers and journal documents in the field of computer science and engineering. In order to retain the diversity of technological exploration, we did not impose additional restrictions on the document type to avoid missing innovative research. The number of papers come out with 290 for total, but consider there were papers repeated in different keywords combine, exact number should be lower than this figure.
  - Science Direct: This platform focuses on natural sciences and social sciences, so we limit its document type to ”Research Articles” and narrow the subject range to ”Finance”, ”Economics” and ”Econometrics” to enhance the relevance of the results.

Among the 290 initially retrieved documents, a subset demonstrated no substantive relevance to the designated search terms. This lack of relevance encompassed, but was not limited to, the following: (1) papers whose central topics were

unrelated to the search criteria, (2) documents containing no meaningful connection to the key terms, or (3) studies discussing biometric technologies without any discernible applicability to the financial sector.

Following the application of the aforementioned screening strategy—which involved the removal of duplicate entries across search terms as well as irrelevant documents—45 publications were ultimately selected as the core references for this study. The research trends and key findings in this domain are synthesized in Figure 1, with further visualization supported by prior [8].

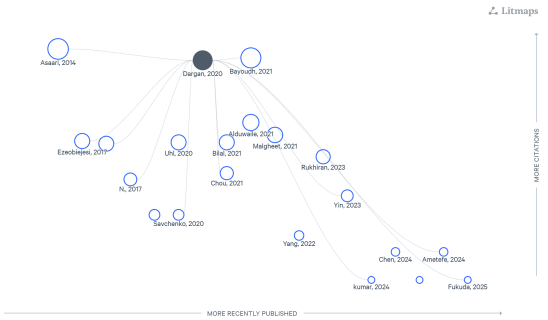

Fig. 1: An Overview of Scholarly Publications on Biometrics and Multi-Factor Authentication

IV. Categorization Method

The 45 documents mentioned above provide comprehensive insights into the application of biometric technology across both front end interfaces and backend security and the front and backend concept is frequently used in practical settings within the financial sector and that is why the classification structure happened. Given their detailed coverage of existing technological implementations, this section focuses on analyzing the current state of these technologies from this perspective.

Biometric technology is a key component of multi-factor authentication (MFA), combining independent verification factors to enhance security against threats like phishing and man-in-the-middle attacks. A summary of the articles reviewed, categorized into distinct functional areas and data types, is presented in Table 1.

A. Functionality

We systematically examine contemporary identity verification (IDV) methods and their applications across financial service functionalities from an implementation perspective. As illustrated in Figure 2, financial institution operations can be fundamentally categorized into front-end and back-end functionalities as illustrated in Figure 2.

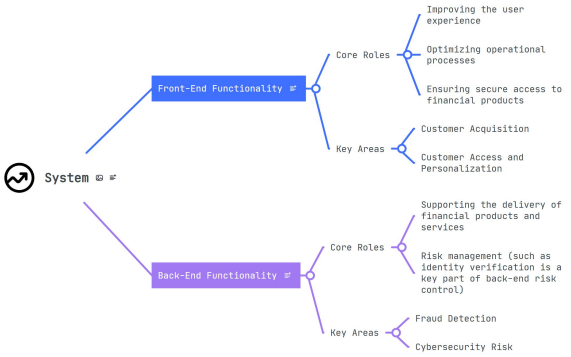

Fig. 2: The Role and Functions of Financial Institutions

1) Front-End Functionality: This encompasses customer-facing systems that enable interactions between users (customers, clients, employees) and digital financial services, particularly through biometric authentication systems. These solutions enhance user experience, operational efficiency, and secure access to financial products, with two primary applications:

- Customer Acquisition: Digital onboarding processes utilizing biometric authentication for identity verification and account creation. These technologies are becoming increasingly pivotal in shaping next-generation financial services [9].
- Customer Access and Personalization: Financial institutions employ biometric authentication to optimize secure access while improving user experience. Pre-transaction user verification, as demonstrated in prior research [10], proves particularly effective when implemented through biometric systems.

2) Back-End Functionality: Back-End Functionality in financial institutions refers to the operational infrastructure supporting financial services, where ID verification serves as a critical risk management component:

- Fraud Detection: Real-time analysis of transaction patterns and user behavior through advanced algorithms. ID verification ensures the legitimacy of individuals accessing services or executing transactions.
- Cybersecurity Risk: Implementation of strategies to identify, assess, and mitigate verification-related risks. This includes continuous security protocol monitoring and compliance with Anti-Money Laundering (AML) standards. The growing adoption of

biometric security solutions reflects their effectiveness against cyber threats [10].

B. Types of Data

Identity verification in the banking sector has evolved due to four major trends. First, multimodal biometric technologies have transformed security, with 97% better anti-spoofing capabilities than single-modal alternatives [11]. Second, the COVID-19 epidemic has increased contactless authentication acceptance by 300% [12], highlighting the necessity for sanitary authentication techniques. Third, technology developments such as Field-programmable gate array(FPGA) design and CNN algorithms have effectively addressed long-standing cost-effectiveness challenges [13]. Finally, advanced liveness detection integration enables compliance with regulatory frameworks such as Payment Services Directive 2(PSD2) had strong customer authentication (SCA) requirements [11]. These trends highlight the industry's emphasis on improving security and user experience, prompting a deeper exploration of biometric data applications and other data sources as illustrated in Figure 3.

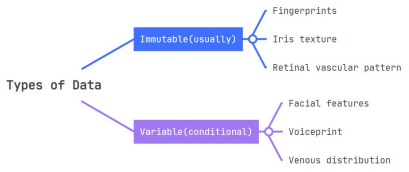

Fig. 3: Classification of Various Data Types

1) Facial image data: Facial recognition technology operates by capturing and analyzing the unique three-dimensional features of a human face, enabling precise biometric identification [14]. This technology synthesizes advanced methodologies from digital image processing, computer vision, pattern recognition, and artificial neural networks, driving its rapid evolution into a sophisticated and widely adopted solution.

- Enhanced Security in Identity Authentication: As a robust biometric verification tool, facial recognition significantly enhances identity authentication processes, balancing heightened security with unparalleled convenience. Despite ongoing data privacy concerns, its real-world utility is undeniable, spanning diverse applications from consumer-facing solutions—such as seamless smartphone unlocking and frictionless mobile payments [15] to enhance financial integrations. By replacing vulnerable physical cash transactions, the technology not only mitigates theft risks but also elevates transactional efficiency, fostering safer and more streamlined economic interactions [16].
- Reinventing Credit Card Security: Traditional authentication techniques, such as CVV codes and password input for credit cards, are still commonly used, although they are vulnerable to cyber attacks. In this instance, several facial recognition-based authentication solutions have emerged as an alternative. This research [17] offers an advanced system that uses FaceNet and multi-task convolutional neural networks (MTCNN) to build encrypted facial embeddings and perform real-time authentication using cosine similarity matching. This method not only improves security but also ensures that transactions run smoothly.

2) Voice Data: Speech recognition technology has advanced significantly in recent years, thanks to developments in natural language processing (NLP) and deep learning, and it is now widely employed in a variety of applications. Although speech recognition technology has advanced in consumer-oriented services such as smart assistants and voice search, its integration with financial payment systems remains difficult, limiting its full deployment and making it less widely used in the financial field than facial recognition.

- Accuracy and Security: Financial transactions necessitate unusually high accuracy and robust security due to the processing of sensitive user data such as bank accounts and passwords; nevertheless, present voice recognition systems have substantial difficulties in satisfying these expectations. The most significant of these challenges is noise sensitivity; performance loss in noisy situations significantly raises the risk of misinterpreting payment instructions and completing incorrect transactions [18]. Furthermore, while deep learning has enhanced voice recognition skills, the system still suffers with specific financial terms and different accent identification, raising dependability problems that limit its use in secure financial applications [19].
- Security Vulnerabilities: Multi-factor authentication (MFA) (which combines voice

and fingerprint recognition) can lessen hazards to some level and is increasingly being used. When paired with biometric information like a face or a fingerprint, it can give outstanding results. However, voice biometric recognition technology itself has inherent security flaws: on the one hand, recording playback and synthetic voice attacks may bypass the authentication system, which requires the use of advanced protection measures such as liveness detection [20]. On the other hand, the system also needs to deal with new threats such as the growing number of playback attacks and AI voice cloning, which forces security protocols to be continuously updated [21].

3) Others: In addition to the previously described facial images and spoken voice data, the biometric system incorporates additional modalities to enhance multi-factor authentication. These modalities include hand geometry, vein pattern recognition, DNA (deoxyribonucleic acid) matching, and gait analysis [5]. Among the various types of biometric data, three widely adopted methods—fingerprint recognition, iris recognition, and signature verification—are particularly noteworthy. The following section provides a concise overview of how these biometric technologies are implemented within the financial sector.

- Fingerprint recognition has become a very secure biometric verification method alongside facial recognition, and it is a fundamental component of multi-factor authentication (MFA) systems [22]. This technique gained traction after Citibank pioneered fingerprint payments in Singapore (2006), demonstrating how biometric cards might reduce fraud risks associated with standard payment systems [23].
- The iris's unique and unchanging properties make it the gold standard in biometric verification, providing substantially more dependability than fingerprint-based systems, which can degrade over time. Cutting-edge systems currently use convolutional neural network (CNN)-enhanced feature extraction algorithms to successfully overcome traditional illumination constraints, resulting in robust performance across a wide range of environmental circumstances [24].
- A signature based on the dual analysis of static graphical patterns and dynamic behavioral biometrics is a unique and powerful authentication mechanism for highly valued financial transactions. The post-pandemic digital transformation has highlighted the value of these systems, with optical character recognition (OCR) platforms automating the entire document life cycle management—from initial capture to final execution—while maintaining a full audit trail for critical infrastructure sectors such as power grid operations [25].

TABLE I: Summary of Categorization by Functionality and Types of Data

	Front-End Functionality	Back-End Functionality	Facial Image Data	Voice Data	Other Data
Kambampati et al. [20]	*		*		
Burkul et al. [26]	*		*		*
Dahiya et al. [17]	*	*	*		
Debas et al. [27]	*		*		*
Enriquez III et al. [12]	*			*	*
Chang et al.[28]	*	*			*
Moondra et al. [18]	*			*	
Barnwal et al. [29]	*			*	
Muhammad et al.[22]	*	*	*		
Nasution et al.[30]	*		*		
Yıldırım et al.[31]	*		*		*
Alkaldi et al.[32]	*	*	*		
Ismail et al. [16]	*	*	*		
Arepalli et al. [33]	*	*			*
Yang et al.[7]	*	*			*
Liébana-Cabanillas et al.[34]	*	*	*	*	*
Obi Ogbanufe and Dan J. Kim.[35]	*	*			*
Alay Nada and Al-Baity Heyam[36]	*	*	*	*	*
Alessandra Lumini and Loris Nanni[37]	*	*	*	*	*

V. Contribution

This paper systematically examines existing authentication methods to identify development trends and research opportunities in the financial domain. With the evolution of AI technologies, the vulnerability of single biometric authentication has become increasingly prominent. Studies have shown that facial image forgery technology based on generative adversarial networks (GANs) can effectively break through some face recognition systems. This situation highlights two key research directions: one is to improve encryption strength through multimodal biometric fusion, and the other is to build a dynamically evolving MFA system architecture. It is worth noting that there are significant differences in the application maturity of different biometrics. Taking voiceprint recognition

as an example, existing applications are mostly limited to auxiliary function scenarios, such as the payment assistance system for visually impaired users demonstrated in the literature [20]. Its potential as an independent authentication factor has not been fully explored. This provides a valuable breakthrough direction for identity authentication research.

Another important gap in the research perspective is the exploration of back-end systems. The existing literature focuses too much on front-end functions such as transaction processes, while neglecting the research and development of back-end core components such as credit assessment models and privacy protection mechanisms. Against the backdrop of the accelerated development of the digital economy, the construction of back-end systems for financial institutions has three strategic significances: ensuring the effectiveness of corporate risk control, optimizing the accuracy of user portraits, and strengthening data security protection. Especially in high-risk areas such as banking and insurance, a sound back-end system can not only effectively safeguard the interests of institutions, but also is an important guarantee for the security of customer assets and information.

VI. Conclusion

This article discusses the role and application of biometric technology in the financial field. Technology plays a role that can be summarized into two categories, namely functionality and data type. Functionality focuses on two categories, namely front-end applications and back-end applications. The type of data will affect the focus of the functionality. While front-end systems have seen significant advancements, back-end functionalities require further reinforcement. This includes implementing more sophisticated multi-factor authentication (MFA) protocols to ensure robust identity verification and prevent unauthorized access, thereby mitigating potential financial losses.

Biometric authentication key limitations require deeper analysis. Current vulnerabilities include AI voice spoofing attacks and performance degradation in noisy environments. Future development should explore: (1) advanced anti-spoofing techniques using multimodal verification, (2) robust noise-adaptive algorithms for real-world conditions, and (3) systemic integration beyond user interfaces into core financial infrastructure like transaction monitoring and risk assessment systems. These enhancements could significantly improve security while maintaining usability, particularly for high-value transactions and sensitive operations.

References

[1] A. Name, "Cyber security considerations for the financial services sector," KPMG, White Paper, 2025, accessed: 2025-03-28. [Online]. Available: https://kpmg.com/au/en/home/insights/2024/06/cyber-security-considerations-financial-services.html

[2] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," 2015.

[3] A. Baevski, H. Zhou, A. Mohamed, and M. Auli, "wav2vec 2.0: A framework for self-supervised learning of speech representations," 2020.

[4] S. Parate, H. P. Josyula, and L. T. Reddi, "Digital identity verification: Transforming kyc processes in banking through advanced technology and enhanced security measures," *International Research Journal of Modernization in Engineering Technology and Science*, 2023.

[5] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, p. 113114, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417419308310

[6] Y. Chandrasekran, C. R. Ramachandiran, and K. Chandrasekaran Arun, "Adoption of future banking using biometric technology in automated teller machine (atm)," in *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, 2022, pp. 1–4.

[7] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognition*, vol. 78, pp. 242–251, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0031320318300384

[8] Connected Papers, "Connected Papers - A visual tool to explore academic papers," 2025, accessed: 01-Apr-2025. [Online]. Available: https://www.connectedpapers.com/

[9] M. García, E. Venegas, SOTER, E. Aguilera, J. Panizo, C. Kelly, and D. Serrano, "Digital onboarding in finance: a novel model and related cybersecurity risks," *Open Research Europe*, vol. 1, p. 149, March 2022.

[10] H. U. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah, and F. Ali, "Role of authentication factors in fintech mobile transaction security," *Journal of Big Data*, vol. 10, 2023.

[11] V. Vassilev, A. Phipps, M. Lane, K. Mohamed, and A. Naciscionis, "Two-factor authentication for voice assistance in digital banking using public cloud services," in *2020 10th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, 2020, pp. 404–409.

[12] A. J. Enriquez III, G. E. H. Tuazon, E. D. Dimaunahan, and A. H. Ballado, "Development of a non-contact two-tier biometric security system for the dswd 4ps using iris recognition and speech recognition," in *2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2021, pp. 550–555.

[13] B. Rong and C.-H. Liu, "A fingerprint payment system based on fpga," in *2016 International Conference on Information System and Artificial Intelligence (ISAI)*, 2016, pp. 472–475.

[14] K. Bowyer, "Face recognition technology: security versus privacy," *IEEE Technology and Society Magazine*, vol. 23, no. 1, pp. 9–19, 2004.

[15] Q. Liu and E. M. Albina, "Application of face recognition technology in mobile payment," in *2022 IEEE 12th International Conference on RFID Technology and Applications (RFID-TA)*, 2022, pp. 217–219.

[16] S. Ismail and S. Ismail, "A preliminary study of cashless payment face recognition system development in malaysia," in *2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 2022, pp. 1–5.

[17] K. Dahiya, J. Goel, A. Kaushik, K. Rai, N. Jain, and A. Gambhir, "Evolving payment security: A facial recognition-based credit card reader with a multi-functional cascade neural network," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, vol. 5, 2024, pp. 1630–1634.

[18] A. Moondra and P. Chahal, "Voice feature extraction method analysis for speaker recognition with degraded human voice," in *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 2023, pp. 385–388.

[19] N. H. Tandel, H. B. Prajapati, and V. K. Dabhi, "Voice recognition and voice comparison using machine learning techniques: A survey," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2020, pp. 459–465.

[20] P. Kambampati, S. Rane, A. Shoeb, and R. Dhannawat, "Payv - payment voice: A platform using voice recognition to enable payment transactions," in *2024 Asia Pacific Conference on Innovation in Technology (APCIT)*, 2024, pp. 1–6.

[21] I. Samuel, F. A. Ogunkeye, A. Olajube, and A. Awelewa, "Development of a voice chatbot for payment using amazon lex service with eyowo as the payment platform," in *2020 International Conference on Decision Aid Sciences and Application (DASA)*, 2020, pp. 104–108.

[22] M. Sajjad, S. Khan, T. Hussain, K. Muhammad, A. K. Sangaiah, A. Castiglione, C. Esposito, and S. W. Baik, "Cnn-based anti-spoofing two-tier multi-factor authentication system," *Pattern Recognition Letters*, vol. 126, pp. 123–131, 2019, robustness, Security and Regulation Aspects in Current Biometric Systems. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167865518300588

[23] B. T. Dommaraju, D. S. Kondaveeti, S. Katta, V. N. Sai Akarsh Devanaboina, and N. L. Sowjanya Cherukupalli, "Fingerprint sensor based biometric payment cards," in *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, 2023, pp. 388–392.

[24] Q. Zhang, H. Li, Z. Sun, Z. He, and T. Tan, "Exploring complementary features for iris recognition on mobile devices," in *2016 International Conference on Biometrics (ICB)*, 2016, pp. 1–8.

[25] D. Xiaoping, G. Chun, and L. Tao, "Research on e-settlement system of centralized purchasing material based on optical character recognition technology and electronic signature technology," in *2018 China International Conference on Electricity Distribution (CICED)*, 2018, pp. 248–251.

[26] T. S. Burkul and S. Patil, "Exploring the intricacies of biometric atm operations, specifically focusing on the integration of fingerprint and facial recognition using deep learning techniques," in *2024 Third International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, 2024, pp. 1–7.

[27] E. A. Debas, R. S. Alajlan, and M. M. Hafizur Rahman, "Biometric in cyber security: A mini review," in *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2023, pp. 570–574.

[28] H.-M. Chang, S.-C. Lin, P. S. Chen, and Y.-H. Hung, "A verification protocol of mobile payment based on signature recognition," in *2015 International Carnahan Conference on Security Technology (ICCST)*, 2015, pp. 379–384.

[29] S. K. Barnwal and P. Gupta, "Evaluation of ai system's voice recognition performance in social conversation," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 2022, pp. 804–808.

[30] M. I. P. Nasution, N. Nurbaiti, N. Nurlaila, T. I. F. Rahma, and K. Kamilah, "Face recognition login authentication for digital payment solution at covid-19 pandemic," in *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, 2020, pp. 48–51.

[31] N. Yıldırım and A. Varol, "Android based mobile application development for web login authentication using fingerprint recognition feature," in *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, 2015, pp. 2662–2665.

[32] W. Alkaldi, N. AlRossais, S. AlAhmadi, H. AlOmran, N. AlSultan, and N. AlFulaij, "Masroofi: Saudi canteen payment system using face recognition technology," in *2024 15th Annual Undergraduate Research Conference on Applied Computing (URC)*, 2024, pp. 1–5.

[33] G. S. Arepalli, P. Bhavana, Y. V. S. Krishna, and C. Surendrababu, "Enhancing transaction security through iris recognition," in *2024 International Conference on Expert Clouds and Applications (ICOECA)*, 2024, pp. 684–688.

[34] F. Liébana-Cabanillas, Z. Kalinic, F. Muñoz-Leiva, and E. Higueras-Castillo, "Biometric m-payment systems: A multi-analytical approach to determining use intention," *Information Management*, vol. 61, no. 2, p. 103907, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378720623001556

[35] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decision Support Systems*, vol. 106, pp. 1–14, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923617302154

[36] M. AlRousan and I. Benedetto, "Multi-factor authentication for e-government services using a smartphone application and biometric identity verification," *Journal of Computer Science*, vol. 16, pp. 217–224, 02 2020.

[37] A. Lumini and L. Nanni, "Overview of the combination of biometric matchers," *Information Fusion*, vol. 33, pp. 71–85, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253516300446