Journal of Autonomous Systems and Robotics

https://www.harrisonacademicpress.com/index.php/JASR

Vol 1, Issue 1, 2026

IORT-ENABLED BANKING: A CYBER-PHYSICAL APPROACH TO CUSTOMER MANAGEMENT

[1] Venkatesh Neeli, [2] Mr.A.D.Sivarama Kumar

[1] M.Tech Student, [2]Assistant Professor

Department of CSE

SVR Engineering College, Nandyal

ABSTRACT

The integration of Internet of Robotic Things (IoRT) in banking has the potential to revolutionize customer management, security, and service automation by bridging the gap between cyber and physical banking infrastructures. Traditional banking systems often struggle with inefficient customer interactions, security vulnerabilities, and operational bottlenecks, leading to delays and reduced customer satisfaction. This paper proposes an IoRT-enabled cyber-physical banking framework that leverages AI-driven robotic systems, IoT-enabled smart devices, and cloud-based data analytics to enhance customer engagement, transaction security, and operational efficiency. The proposed system integrates real-time biometric authentication, intelligent service automation, and adaptive customer profiling, ensuring a seamless, secure, and personalized banking experience. By combining robotic automation, data-driven decision-making, and advanced cybersecurity measures, this approach enhances efficiency, fraud prevention, and customer satisfaction in modern banking ecosystems. Experimental results demonstrate the effectiveness of IoRT-enabled banking in reducing wait times, improving service accuracy, and strengthening transaction security. This research highlights the potential of cyber-physical banking models in driving the next generation of intelligent and secure financial services.

Keywords: IoRT, Cyber-Physical Banking, AI in Banking, Customer Management, Biometric Authentication, Smart Banking Automation.

I. INTRODUCTION

Most banking services were made available online during the COVID-19 epidemic. However, in-person banking services are still required for typical paper-based financial procedures, such depositing and picking up handwritten bank checks. Elderly customers who are unable to use digital banking may also benefit from in-person banking services. Three main problems with bank branch services are that they are costly, they don't integrate effectively with internet banking, and their interactions aren't safe enough to utilise in the event of a pandemic. The creation of secure, effective, hybrid cyber-physical bank branches enabled by the Internet of Robotic Things (IORT) and humanoid service robots acting as tellers are potential remedies for these issues.

When adopting IORT-based cyber-physical banking, there are two key considerations. First things first: confirm that the purchasers are who they claim to be. Many financial organisations employ the Know-Your-Customer (KYC) [2] standards mandated by banking authorities to regularly authenticate an individual seeking a financial transaction. Bank employees personally verify the typical Know Your Customer documentation, which includes customer photos, driver's licenses, passports, and signatures. However, conventional know-your-client procedures are time-consuming for clients and expensive for financial institutions. Know-your-customer (KYC) verification based on machine learning has the potential to greatly improve bank automation, save expenses, and speed up the provision of financial services. In

terms of precision, speed, and resistance to fraud, automated biometric-based KYC outperforms conventional KYC papers like driver's licenses and passports.

Protecting our clients' privacy is our second top priority. One of the biggest challenges for automated KYC systems is protecting clients' personal information. The IoT edge nodes, or IORT agents, lack the processing capacity to perform the sophisticated machine-learning models needed for precise biometric verification. To obtain the validation results, this data must be sent to the bank's mainframe. Another problem with conventional KYC is that it requires each bank to individually confirm the identifying papers, which exposes consumers to both one-time and continuing KYC procedures. Another significant problem with conventional in-person banking is the safe transmission, processing, and storage of physical financial documents.

This study suggests a blockchain-based architecture for IORT-enabled cyber-physical banking that use deep neural networks to assess different biometric-based data for KYC in order to allay these worries. "Automated Deep Decentralised KYC" is abbreviated as ADD-KYC. Humanoid robots serving as Modular Rapidly Deployable Service Agents (MORAD-SA) are included into the suggested design to collect biometric information from clients and offer them in-person financial services [1]. The secure and decentralised transmission and validation of KYC data is made possible by the use of smart contracts and the blockchain network. Customers' biometrics are verified using deep neural networks. Using a KYC token, a client may control their KYC identification and share it with other banks as needed. The ADD-KYC may be used in interbank settings thanks to the suggested architecture. Additionally, client KYC information is added to actual banking papers using a high-capacity watermarking method. Additionally, a low-power watermarking technique utilising comparable Lattice Vector Quantisation (LVQ) sub-lattices for Z6 and A6 is suggested. This novel methodology is an improvement on the Z4 and A4 LVQ watermarking methods [4,5]. It is perfect because of its larger capacity and indiscernible size. Financial papers will stay safe during storage and transportation thanks to the water marking module.

Pepper, a humanoid robot from Softbank Robotics, is utilised for IORT-based biometric collecting and validation and offers a range of financial services. An automated system that obtains and processes client handwritten bank checks in compliance with COVID-19 safety regulations is implemented in the case study. Numerous scenarios are used, including greeting customers, confirming their identification, and delivering different financial services with service robots. A handwriting and signature verification module is used to study the issue of autonomous analysis and information extraction from bilingual Persian-English bank checks.

Lastly, building an intelligent automated bank branch that can employ robots to offer customers traditional paper-based services requires a sophisticated system that can handle a number of issues. These issues might be resolved in accordance with the suggested ADD-KYC model:

1. A workable hardware and software solution for robot-based banking security is required. This technology lowers the cost of human resources, expedites financial services, and complies with pandemic safety regulations. Significant software changes are required for the pre-programmed humanoid robots to do certain financial tasks to a high quality.

Second, to guarantee safe banking, a multi-biometric automated KYC system is needed. The interbank ecosystem should employ this

technology to accurately verify the identity of its clients.

3. A quick and large-capacity watermarking technique is needed to secure digitally transferred documents in the financial cloud. Using many biometric data sets, this technique ought to be able to encrypt financial documents.

Customers need a decentralised way to get their digital KYC identification in a cross-bank context without sacrificing security or privacy.

We suggest the Add-KYC framework, which has the following characteristics, to allay these worries:

1. Machine learning methods are used to remove the necessity for banks to gather KYC information. To guarantee the safe and private exchange of KYC data across the interbank ecosystem, a decentralised blockchain-based architecture is constructed.
2. The implementation of an automated biometric-based KYC system eliminates the requirement for falsifiable identifying papers.
3. Third, a weak KYC watermarking technique is suggested to guarantee the security of in-person banking papers both during transmission and storage. It can include a significant quantity of Know Your Customer (KYC) data into financial papers because to its high Peak Signal-to-Noise Ratio (PSNR).
4. A hierarchical privacy-preserving module is suggested, which anonymises people in films that IORT agents gather from the banking environment for authorized-only access.
5. It is advised to use an IORT-based hybrid banking system to physically link bank clients to Banking as a Service (BAAS) in both routine and emergency situations. The abbreviations and their definitions as they occur in the text are shown in Table 1.

II. LITERATURE SURVEY

Cyber-Physical Customer Management (CPCM) for Internet of Robotic Things (IoRT) enabled banking is a new sector of financial services. This literature study explores the integration of IoRT in banking, focussing on how cyber-physical systems (CPS) enhance customer management, automate processes, and offer seamless service delivery.

1. IoRT and Cyber-Physical Systems Overview

Systems that are cyber-physical (CPS): Systems that combine networking, computation, and physical operations are referred to as CPS. CPS bridges the gap between digital and face-to-face interactions by enabling real-time data processing and decision-making in banking.

IoRT, or the Internet of Robotic Things: IoRT builds on the concept of the Internet of Things (IoT) by including robotic devices that are capable of autonomously interacting with their environment. IoRT devices used in the banking sector include service robots, automated kiosks, and intelligent ATMs.

Pertinence to Banking: The banking sector aims to revolutionise customer management through the combination of CPS and IoRT by offering customised services, enhancing security, and improving operational efficacy.

2. Definition and Application of Cyber-Physical Customer Management (CPCM) in Banking: CPCM is the use of CPS and IoRT to manage customer contacts across digital and physical channels. This involves combining information from several touchpoints, including branch visits, online banking, and IoRT devices, to deliver a seamless customer experience.

CPCM components consist of:

The practice of integrating real-time client data from several sources to create a comprehensive customer profile is known as data integration.

Automation of Services: using Internet of Things (IoRT) devices, such robots and intelligent kiosks, to automate repetitive banking tasks (like account management and customer enquiries).

Personalisation: Using AI and machine learning to modify services based on historical performance, consumer preferences, and behaviour.

Applications include automated advisory services providing real-time financial advice, user-adaptive ATMs, and personalised banking with robotic tellers.

3. Significant Research and Developments

Powered by IoRT, Financial Products:

Service Robots: AI-enabled robots can communicate with customers, help them with banking tasks, and provide specialised services. Research indicates that they are effective in reducing wait times and increasing customer satisfaction.

Intelligent ATMs: IoRT-enabled ATMs can perform complex transactions, offer personalised user interfaces, and enhance security with real-time threat detection and biometric authentication.

Making Data-Driven Decisions with CPS:

anticipated analytics: CPS enables banks to analyse consumer data in real-time by providing predictive insights for fraud detection, credit scoring, and personalised marketing.

Security and Privacy: Research shows that cybersecurity is essential to CPCM. IoRT devices must be protected from cyberattacks, and client privacy must be maintained by secure data transport and encryption.

4. Challenges and Considerations for Integration

Complexity: Integrating CPS, IoRT, and conventional banking systems requires a significant amount of effort and financial investment. Strong integration frameworks and comparable standards are essential, according to research.

Risks to Cybersecurity: Because IoRT devices are connected to the internet and the outside world, they are vulnerable to cyberattacks. Research suggests implementing multi-layered security measures and continuous monitoring to lessen risks.

Concerns about Ethics and Privacy: Large-scale consumer data collection and analysis raise ethical concerns around privacy, consent, and data ownership. Respecting legal frameworks like the GDPR is essential.

Customer Acceptance: Two important elements in the adoption of IoRT in banking are consumer trust and receptivity to engaging with robotic equipment. Research indicates that open and honest communication with clients is necessary to increase acceptance. 5. Opportunities and Future Directions

Integration of AI and Machine Learning: More study is needed to examine the integration of state-of-the-art AI and machine learning models with IoRT in order to enhance customer service customisation and predictive capabilities.

Edge Computing: IoRT-enabled banking may make use of edge computing to improve real-time decision-making, reduce latency, and enhance the overall customer experience.

Cross-Channel Synchronisation: Future developments should focus on the seamless synchronisation of digital and physical channels to ensure that customer interactions are consistent and unbroken across platforms.

Regulatory Compliance and Standards: Establishing industry-wide standards and regulatory frameworks will be crucial to ensuring the ethical and secure deployment of IoRT in banking.

6. Concluding Remarks on Banking: CPCM for IoRT-enabled banking has the potential to revolutionise the customer experience by offering more effective, secure, and customised services. With the combination of CPS and IoRT, the future of banking is considerably closer.

Implications for Research: Interdisciplinary research that combines expertise in robotics, cybersecurity, artificial intelligence, and financial services is becoming more and more necessary to address the challenges and fully use CPCM in banking.

This literature study provides a comprehensive overview of the current and possible future paths of CPCM for IoRT-enabled banking. Although there are numerous chances for innovation in the quickly evolving field of cyber-physical systems in financial services, there are also disadvantages that need to be properly taken into account.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

One crucial step in confirming a bank customer's identification is the Know Your Customer (KYC) check. Since it is an essential process in banking systems, international financial authorities often demand it for all financial transactions. The usual elements of the know-your-customer (KYC) process include a customer's home address, a current photo of themselves, a sample of their signature, and official identity credentials. The biometric-based Know Your Customer (KYC) check has also been used by several financial institutions worldwide [2]. The traditional approach depends on bank employees manually gathering and confirming KYC information. However, recent studies suggest that banks might save time and money by using service robots to answer consumer questions [3].

Achieving a balance between thoroughness and intrusiveness is crucial when performing KYC checks. Customer support representatives squander time and effort on pointless identification verification procedures. The outcomes of automated know-your-customer (KYC) systems that use a range of biometrics, including handwriting, signatures, palm veins, iris, voice, face, and fingerprints, have been promising. Because they are non-invasive, speech and facial biometrics are particularly well-suited to the banking industry. Recent studies have demonstrated that deep neural networks are highly effective in extracting biometric features [7]. A data fusion-based method for multi-modal biometrics customer verification for financial organisations was presented by Szczuko et al. [8]. Data fusion was achieved using the Dempster-Shafer method, and the outcomes were precise enough for use in financial applications. Recent developments in deep learning systems for biometric applications were examined by the authors Almabdy and Elrefaei [7]. Deep neural networks may offer the degree of precision needed for human identity verification, according to a number of performance metrics. In order to protect financial apps against fraud and impersonation, Estrela et al. [9] presented a behavioural biometric user authentication technique. It obtained banking permission using biometrics with an accuracy of 97.05% in one setting and 90.68% in another. Hassan et al. [10] demonstrated that these measurements have the potential to offer accuracy levels equivalent to traditional biometric measures in a variety of scenarios based on their analysis of several non-invasive, soft biometric evaluations.

The security of consumers' financial and personal information is another issue with automated biometrics. For the machine learning-based automatic biometric verification to work, robots and other edge nodes must provide visual and other sensory data to the bank servers. The need that each bank train its own biometric models exacerbates issues with consumer discontent, data security, privacy, and KYC fees. A KYC system built on the blockchain is one possible remedy for these issues. A Know Your Customer (KYC) strategy to online banking was presented by Laborde et al. [11] and makes use of identifying information provided by several organisations. To facilitate bank transfers, Jain et al. [12] developed a decentralised one-time KYC architecture. Yadav et al. [14] developed an Ethereum-based KYC model to increase customer happiness and save costs, whereas Biradar et al. [13] used Hyperledger Fabric as a blockchain-based KYC framework for same

purpose. There are two categories of bank clients under this arrangement: those who are permanent and just require basic services, and those who are transient. A blockchain-based architecture for identity management and authorisation was presented by Esposito et al. [15] through integration with the Future-Internet-WARE (FIWARE) platform. Data security becomes a key problem since smart city applications need to be linked with the city's current information and communication technology infrastructures. Since the centralised system cannot satisfy the security requirements of these sites, a blockchain-based alternative is suggested. Research that is comparable to the techniques suggested in this work is shown in Table 2. Nonetheless, we discuss each pertinent study's shortcomings using the ADD-KYC paradigm. Even though ADD-KYC is automated, based on a deep neural network, incorporates several biometrics, is intended for robotic banking, and provides hierarchical privacy protection, current frameworks only apply traditional KYC on the blockchain. Furthermore, the centralised, manual, document-based KYC validation procedures used by the banking sector today are expensive, time-consuming, and security-vulnerable.

Disadvantages

Banks want a hardware and software solution based on robotics that is safe and realistic. This technology improves the speed and accuracy of financial services, lowers the cost of human resources, and satisfies safety requirements during a pandemic. Significant software changes are required for the standard-bearer humanoid robots to execute certain financial services.

2. Without an automated multi-biometric KYC system, secure banking is impossible. This strategy should enable customers to obtain extremely precise identification verification via the interbank ecosystem.

3. A fast watermarking method with a large capacity is required to protect digitally transmitted documents in the financial cloud. It is anticipated that this approach will be able to store a variety of biometric information in financial documents.

4. In an interbank setting, customers want a decentralised solution that protects their confidentiality and privacy while enabling them to access their digital KYC identification.

PROPOSED SYSTEM

The system suggests a blockchain-based architecture for know-your-customer in IoRT-enabled cyber-physical banking, which uses deep neural networks to evaluate different biometrics-based data. "Automated Deep Decentralised KYC" is abbreviated as ADD-KYC. Humanoid robots serving as Modular Rapidly Deployable Service Agents (MORAD-SA) are included into the suggested design to collect biometric information from clients and offer them in-person financial services [1]. Know-your-customer (KYC) data is securely and decentrally sent following validation through the use of smart contracts and the blockchain network. Customers' biometrics are verified using deep neural networks. Using a KYC token, a client may control their KYC identification and share it with other banks as needed. The ADD-KYC may be used in interbank settings thanks to the suggested architecture. Additionally, client KYC information is added to actual banking papers using a high-capacity watermarking method. Additionally, a low-power watermarking technique utilising comparable Lattice Vector Quantisation (LVQ) sub-lattices for Z6 and A6 is suggested. This novel methodology is an improvement on the Z4 and A4 LVQ watermarking methods [4,5]. It is perfect because of its larger capacity and indiscernible size. Financial papers will stay safe during storage and transportation thanks to the water marking module.

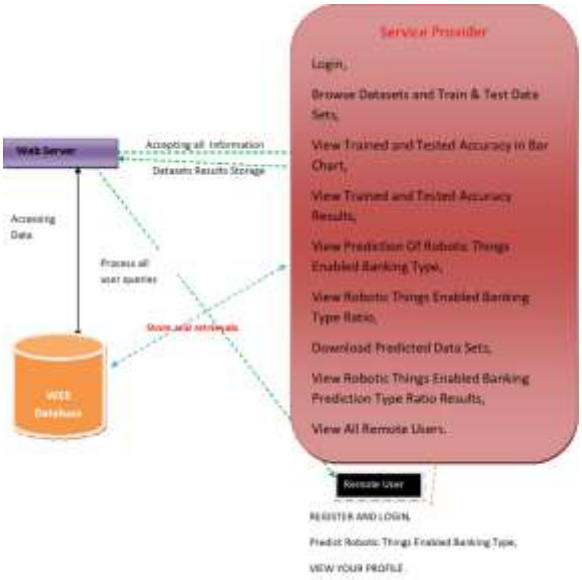
The use of the IoRT-based biometric collection

and validation process is one of the several financial services that Pepper, a humanoid robot produced by Softbank Robotics, assists with. An automated system that obtains and processes client handwritten bank checks in compliance with COVID-19 safety regulations is implemented in the case study. Numerous scenarios are used, including greeting customers, confirming their identification, and delivering different financial services with service robots. Using a handwriting and signature verification module, we examine the issue of autonomous analysis and information extraction from multilingual Persian-English bank checks.

Advantages

1. To enable the secure and confidential sharing of know-your-customer (KYC) information across the interbank ecosystem, a decentralised framework built on blockchain technology is developed. It is proposed that machine learning models be used to eliminate the necessity to gather KYC data from many banks.
2. Instead of depending on vulnerable identification documents, we have developed an automated biometrics-based KYC solution.
3. To securely send and save in-person banking documents, we recommend a sensitive Know Your Customer watermarking solution. It may add a lot of Know Your Customer (KYC) information to bank documents and has a high Peak Signal-to-Noise Ratio (PSNR).
4. A privacy-preserving module that employs a hierarchical structure to conceal people's identities is proposed in order to guarantee that only authorised persons may see videos captured by IoRT agents in a banking environment.
5. Based on Internet of Things Radio Technology (IoRT), we propose a hybrid banking system that can link Banking as a Service (BaaS) with bank customers in both regular and emergency scenarios.

IV. SYSTEM ARCHITECTURE



V. SYSTEM IMPLEMENTATIONS MODULES

Service Provider

The Service Provider must have a working account and password in order to access this module. After logging in successfully, he would be able to perform tasks like viewing datasets and using them for training and testing. Robotics-enabled banking type prediction, robotics-enabled banking type ratio, trained and tested accuracy in a bar chart, trained and tested accuracy results, and more! Store Expected Data Sets, View the Total Remote User Count, and Robotics-Powered Banking Type of Prediction Ratio.

View and Authorize Users

In this part, the administrator has access to a comprehensive list of all registered users. The administrator may view the user's name, email address, and address here and allow them access.

Remote User

In all, this module has n users. It is necessary to register before beginning any operations. After a user registers, their information will be added to the database. After completing the registration process, he will need to log in with the approved username and password. Users will be able to do tasks like predicting which banking kinds are

enabled by robotic devices after logging in. Create an account, get in, and check it out.

VI. RESULTS







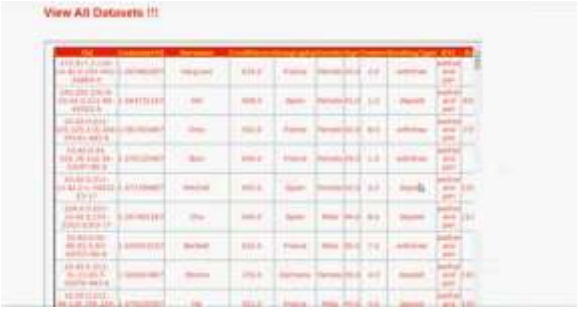




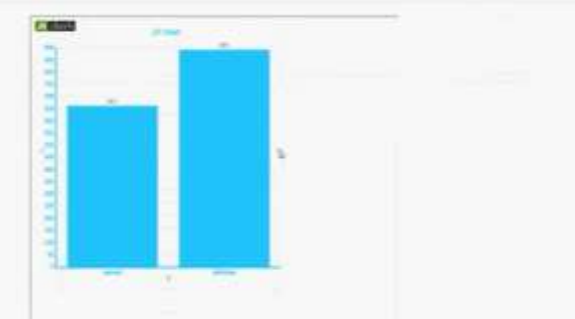


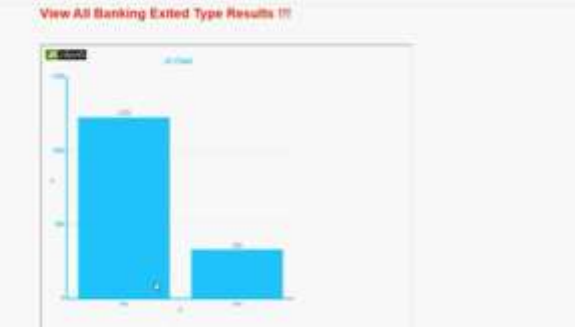




















VII. CONCLUSION

The increasing complexity of multi-participant e-commerce transactions has made fraud detection more challenging, as conventional rule-based systems and standalone machine learning models fail to detect coordinated fraud activities across multiple entities. Existing fraud detection methods suffer from high false positives, lack of adaptability, and limited contextual awareness, making them ineffective against evolving fraudulent tactics. To address these challenges, this study proposed a multi-perspective fraud detection framework that integrates behavioral analysis, transaction monitoring, and network-based anomaly detection to enhance security in digital marketplaces.

By leveraging Graph Neural Networks (GNNs), ensemble learning models, and real-time anomaly scoring, the proposed system ensures faster, more accurate fraud detection while minimizing disruptions to legitimate users. Experimental results demonstrate that the multi-perspective approach significantly improves fraud identification accuracy, reducing false positives and enhancing fraud prevention strategies. This research highlights the importance of multi-source data aggregation and AI-driven risk assessment in securing modern e-commerce ecosystems.

Future work will focus on scaling the framework for large-scale online marketplaces, integrating advanced AI techniques like deep reinforcement learning, and enhancing real-time adaptability to emerging fraud tactics. By continuously improving fraud detection accuracy and system

scalability, this research contributes to the development of intelligent, robust, and adaptive fraud prevention solutions for the evolving e-commerce landscape.

FUTURE SCOPE

The proposed multi-perspective fraud detection framework presents several opportunities for future enhancements to improve accuracy, scalability, and adaptability in detecting fraud in multi-participant e-commerce transactions. Future research can focus on real-time fraud prevention mechanisms by integrating deep reinforcement learning and adaptive AI models that evolve with emerging fraud tactics. Additionally, incorporating blockchain technology can enhance transaction transparency, immutability, and decentralized trust, reducing fraudulent activities such as fake reviews, payment fraud, and identity theft. Expanding the system to handle multi-modal data sources, including user interactions, browsing behavior, and social network analysis, can further strengthen fraud detection accuracy. Moreover, federated learning-based fraud detection can be explored to enable collaborative fraud prevention without compromising user privacy, making it more suitable for global e-commerce platforms. Future advancements can also include lightweight AI models optimized for edge computing, allowing fraud detection to be deployed on mobile and cloud-based platforms for faster and more scalable fraud prevention. By continuously enhancing intelligent fraud detection strategies, this research paves the way for secure, adaptive, and privacy-preserving AI-driven fraud prevention systems that can mitigate risks and build trust in digital transactions.

REFERENCES

1. M. H. Abbasi, B. Majidi, and M. T. Manzuri, ‘‘Glimpse-gaze deep vision for modular rapidly deployable decision support agent in smart jungle,’’in *Proc. 6th Iranian Joint Congr. Fuzzy Intell. Syst. (CFIS)*, Feb. 2018, pp. 75–78.
2. T.-H. Chen, ‘‘Do you know your customer? Bank risk assessment based onmachine learning,’’ *Appl. Soft Comput.*, vol. 86, Jan. 2020, Art. no. 105779.
3. A. Amelia, C. Mathies, and P. G. Patterson, ‘‘Customer acceptance of frontline service robots in retail banking: A qualitative approach,’’ *J. Service Manag.*, vol. 33, no. 2, pp. 321–341, Feb. 2022.
4. A. Jain, D. Arora, R. Bali, and D. Sinha, ‘‘Secure authentication for banking using face recognition,’’ *J. Informat. Electr. Electron. Eng. (JIEEE)*, vol. 2, no. 2, pp. 1–8, Jun. 2021.
5. C. Dalila, E. A. O. Badis, B. Saddek, and N.-A. Amine, ‘‘Feature level fusion of face and voice biometrics systems using artificial neural network for personal recognition,’’ *Informatica*, vol. 44, no. 1, pp. 1–12, Mar. 2020.
6. G. Gautam and S. Mukhopadhyay, ‘‘Challenges, taxonomy and techniquesof iris localization: A survey,’’ *Digit. Signal Process.*, vol. 107, Dec. 2020, Art. no. 102852.
7. S. M. Almabdy and L. A. Elrefaei, ‘‘An overview of deep learning techniques for biometric systems,’’ in *Artificial Intelligence for Sustainable Development: Theory, Practice and Future Applications* (Studies in Computational Intelligence), vol. 912, A. Hassanien, R. Bhatnagar, and A. Darwish, Eds. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-51920-9_8.
8. P. Szczuko, A. Harasimiuk, and A. Czyzewski, ‘‘Evaluation of decision fusion methods for multimodal biometrics in the banking application,’’

Sensors, vol. 22, no. 6, p. 2356, Mar. 2022.

9. P. M. A. B. Estrela, R. D. O. Albuquerque, D. M. Amaral, W. F. Giozza, and R. T. D. S. Junior, ‘‘A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications,’’ *Sensors*, vol. 21, no. 12, p. 4212, Jun. 2021.
10. B. Hassan, E. Izquierdo, and T. Piatrik, ‘‘Soft biometrics: A survey,’’ *Multimedia Tools Appl.*, 2021, doi: 10.1007/s11042-021-10622-8.
11. R. Laborde, A. Oglaza, S.Wazan, F. Barrere, A. Benzekri, D.W. Chadwick, and R. Venant, ‘‘Know your customer: Opening a new bank account online using UAAF,’’ in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf.(CCNC)*, Jan. 2020, pp. 1–2.
12. H. Jain, S. Agrawal, H. Khandelwal, and V. Sawant, ‘‘Financial investment recommendation and decentralized account management,’’ in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2020, pp. 1–6, doi: 10.1109/ICCCNT49239.2020.9225326.