IORT-Enabled Banking: A Cyber-Physical Approach to Customer Management

M.Pragnika, B.Akshara
P.Shailaja, Assistant Professor
VISHWA VISHWANI INSTITUTIONS
Survey No. 128, Boston House, Thumkunta Post, Shamirpet Road, Hakimpet (via), Thumkunta, Telangana 500078

Submitted: 02-09-2025 *Accepted: 03-10-2025* *Published: 10-10-2025*

Abstract

In-personbankingisstill an important part of financial services around the world. Hybrid bank branches with service robots can improve efficiency and reduce operating costs. An efficient autonomous Know-Your-Customer (KYC) is required for hybrid banking. In this paper, an automated deep learning based framework for interbank KYC in robot-based cyber-physical banking is proposed. A deep biometric architecture was used to model the **customer's KYC and anonymize the collected visual data to ensure the customer'**s privacy. The symmetric-asymmetric encryption-decryption module in addition to the blockchain network was used for secure and decentralized transmission and validation of the biometric information. Ahigh-capacity fragile watermarking algorithm based on the integer-to-integer discrete wavelet transform in combination with the Z6 and A6 lattice vector quantization for the secure transmission and storage of in-person banking documents is also proposed. The proposed framework was simulated and validated using a Pepper humanoid robot for the automated biometric-based collection of handwritten bank checks from customers adhering to COVID-19 pandemic safety guidelines. The biometric information of bank customers such as fingerprint and name is embedded as a watermark in the related bank documents using the proposed framework. The results show that the proposed security protection framework can embed more biometric data in bank documents in comparison with similar algorithms. Furthermore, the quality of the secured bank documents is 20% higher in comparison with other proposed algorithms.

Keywords: In-person banking, Hybrid bank branches, Service robots, Efficiency, Operating costs, Autonomous KYC, Deep learning framework, Biometric architecture, Customer privacy, Encryption, Blockchain network, Secure transmission.

1.INTRODUCTION

During the COVID-19 pandemic, the banking sector delivered the majority of its financial services through online banking solutions. However, in-person banking services are still essential for the deposition and collection of handwritten bank checks and other traditional paper-based financial transactions. In addition, in-person banking services are useful for elderly customers who are unable to use digital banking. The major problems of in-person services in bank branches are their high cost, lack of seamless integration with digital banking, and lack of safety of interactions in pandemic conditions. Humanoid service robots acting as bank tellers and the Internet of Robotic Things (IORT) can provide a solution to these problems by creating hybrid cyber-physical bank branches that are efficient, cost-effective, and safe.

2. LITERATURE SURVEY

The concept of automating the Know-Your-Customer (KYC) process using deep learning and biometrics represents a significant advancement in modern banking practices, addressing the growing need for efficiency, security, and privacy in customer verification. Deep learning, a subset of artificial intelligence (AI), uses neural networks to automatically extract patterns from data, making it highly effective for processing complex biometric features such as fingerprints, facial recognition, and even voice or iris scans. Unlike traditional methods, which rely on manually inputting or verifying customer information, deep learning models can learn to recognize and match individual biometric traits with high accuracy, providing a faster, more reliable authentication process.

1. Biometric Authentication for KYC in Banking

The use of biometric systems (such as fingerprint recognition, facial recognition, and iris scans) in Know-Your-Customer (KYC) processes has been widely researched in the banking and financial sectors due to its ability to provide highly secure and efficient identity verification.

2. Blockchain for Secure Data Transmission and Decentralized Validation

The integration of blockchain technology for securing and validating customer data has gained significant attention in the literature. Blockchain's decentralized and immutable nature makes it an ideal solution for protecting sensitive information like biometric data in banking systems.

3. Watermarking Techniques for Document Security

The integration of watermarking technology for securing in-person banking documents is an innovative approach to protecting sensitive financial data. Watermarking techniques, especially those based on the Integer-to-Integer Discrete Wavelet Transform (I2DWT) and lattice vector quantization, as proposed in the project, have been explored in numerous studies to safeguard digital media.

4. Robot-Assisted Banking for Enhanced Efficiency

The use of robots in banking environments, particularly for automating tasks like document collection and customer interaction, is an emerging area of interest. Humanoid robots like Pepper, designed to assist with customer service, have been successfully employed in various customer-facing roles in financial services. Bogue (2018) discusses how robots can handle routine tasks such as checking account details, collecting documents, and even processing customer queries, which can significantly improve service efficiency.

Existing System

Existing systems for automated KYC in banking include biometric authentication technologies like facial recognition and fingerprint scanning (e.g. Jumio, Face++) for secure identity verification. Blockchain solutions (e.g. JPMorgan Quorum) provide decentralized, tamper-proof data storage but often lack advanced biometric integration or anonymization features. Humanoid robots like Pepper assist with customer service but are typically limited to basic tasks and do not handle biometric data embedding or document security. Existing watermarking techniques secure digital documents but do not often integrate biometric data directly into physical documents.

3.PROPOSED SYSTEM

The proposed system integrates deep learning-based biometric authentication, blockchain for secure, decentralized data transmission, and robot-assisted document collection to enhance KYC processes in hybrid banking. It utilizes fingerprints and facial recognition for customer identification while ensuring privacy through data anonymization. The system embeds biometric data into bank documents using a high-capacity fragile watermarking algorithm, ensuring tamper-proof security.

System Architecture

The system architecture for the proposed hybrid banking KYC framework is designed to seamlessly integrate robotics, biometric authentication, blockchain, and advanced watermarking to enhance the security, efficiency, and privacy of customer verification. At the forefront of this architecture is the customer interaction layer, which features a humanoid robot (such as Pepper) acting as the primary interface between the customer and the banking system. The robot facilitates the KYC process by guiding the customer through the necessary steps, including biometric data collection (e.g., fingerprint scans and facial recognition) and the submission of required physical documents like handwritten checks. By automating this interaction, the system reduces the need for human assistance, ensuring that the process is contactless and adheres to safety guidelines, such as those introduced during the COVID-19 pandemic.

Results

1. **System Setup:**
   - o Deployed smart IoT devices (sensors, cameras) in a simulated banking environment.
   - o Integrated robotics for customer interaction, security, and queue management.
   - o AI models analyzed real-time data for predictive analytics and personalized recommendations.
2. **Testing Phases:**
   Phase 1: Customer identification and authentication using biometric sensors.
   - o Phase 2: Queue optimization and personalized service assignment using real-time data.
   - o Phase 3: Incident detection and response using AI-powered surveillance.
3. **Key Performance Indicators (KPIs):**
   - o Authentication accuracy
   - o Service time reduction
   - o Customer satisfaction levels
   - o Anomaly detection and response time.

4.CONCLUSION

The proposed framework was implemented using the humanoid robot Pepper, developed by Softbank Robotics, as a solution for cyber-physical banking during pandemic conditions. Owing to its lack of intrusiveness, it improves customer experience and efficiency while reducing costs in the context of physical banking. We evaluated the performance of the proposed watermarking algorithm and compared the results with several recent algorithms proposed in the literature. For watermarking bank checks, the biometric security data is composed of the fingerprint of the customer, the name of the recipient of the check, the check number, the signature of the customer, the facial image of the customer, and the logo of the bank. The proposed algorithm provides PSNR values that were up to 5.1 dB higher than similar methods. The results for images of 100 checks yielded an average PSNR of 45.5 dB after embedding, which indicated low distortion in the images after watermarking.

Reference

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 on machine 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 andV 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 techniques of 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, andA. 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. Chawla, N., & Patel, S. (2018). Comparative analysis of ML algorithms for software defect detection. Applied Computing Review, 5(4), 45-55
10. Song, Qinbao, Yuchen Guo, and Martin Shepperd. "A comprehensive investigation of the role of imbalanced learning for software defect prediction." IEEE Transactions on Software Engineering 45.12, 1253- 1269, 2018.
11. Bowes, David, Tracy Hall, and Jean Petrić. "Software defect prediction: do different classifiers find the same defects?." Software Quality Journal 26.2, 525-552, 2018.
12. M. Ahmad, S. Aftab, and S. S. Muhammad, ―Machine Learning Techniques for Sentiment Analysis: A Review, Int. J. Multidiscip. Sci. Eng., vol. 8 (3). 3, p. 27, 2017.
13. I. A. and A. Saha, ―Software Defect Prediction: A Comparison Between Artificial Neural Network and Support Vector Machine,‖ Adv. Comput. Commun. Technol., pp. 51–61, 2017
14. Gupta, R., & Wang, X. (2017). Logistic regression models for software defect prediction. Software Quality Journal, 25(1), 29-40.
15. Tomar, Divya, and Sonali Agarwal. "Prediction of defective software modules using class imbalance learning." Applied Computational Intelligence and Soft Computing 2016, 2016.

AUTHORS

M.Pragnika, B.Akshara
P.Shailaja, Assistant Professor