www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

INTEGRATING CYBER-PHYSICAL SYSTEMS FOR CUSTOMER MANAGEMENT IN IORT-ENABLED BANKING ENVIRONMENTS

[1]D. SAIKRISHNA, [2]MADDI RAHUL
[1]Assistant Professor, [2]MCA Student
Department Of MCA Student
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

In-person banking still plays a big part in financial services all around the world. At hybrid bank offices, robotic service staff may boost output while reducing costs. An efficient autonomous Know-Your-Customer (KYC) system is necessary for hybrid banking. This study suggests a deep learning-based automated solution for interbank KYC in robot-based cyber-physical banking. A deep biometric architecture was employed to model the customer's KYC and anonymise the collected visual data in order to preserve their privacy. The biometric data was sent and validated in a secure, decentralised way using the blockchain network and the symmetric-asymmetric encryption-decryption module. A high-capacity fragile watermarking method based on the integer-to-integer discrete wavelet transform in conjunction with the Z6 and A6 lattice vector quantisation is also recommended for the secure transmission and storage of in-person financial documents. The proposed framework for automated biometric-based bank check collection of handwritten checks from customers in accordance with COVID-19 pandemic safety guidelines was simulated and evaluated using a Pepper humanoid robot. The proposed framework is used to watermark and integrate bank customers' biometric information, including their name and fingerprint, into the appropriate bank documents. The results show that the proposed security protection framework can incorporate more biometric information in bank documents than similar algorithms. Furthermore, the quality of the protected bank document is 20% higher than that of other proposed methods. The hierarchical visual information transmission and storage module, which hides people's identities in films collected by robots, may also satisfy the banks' privacy requirements. Taking everything into account, the proposed framework may offer a rapid, simple, and reasonably priced interbank solution for future in-person banking while adhering to security regulations and banking rules.

I. INTRODUCTION

During the COVID-19 pandemic, the majority of banking services were made accessible online. Yet, traditional paper-based financial operations, such as the depositing and pickup of handwritten bank checks, still need in-person banking services. Furthermore, in-person banking services may be helpful for elderly consumers who are unable to use digital banking. Bank branch services have three major flaws: they're expensive, they don't work well with online banking, and their interactions aren't secure enough to use during pandemics. Possible solutions to these problems include the development of safe, efficient, hybrid cyber-physical bank branches made possible by the Internet of Robotic Things (IORT) and humanoid service robots working as tellers.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

There are two important factors to think about while implementing cyber-physical banking based on IORT. First things first: make sure the buyers are who they say they are. In order to routinely verify a person requesting a financial transaction, many financial institutions use the Know-Your-Customer (KYC) [2] requirements that are enforced by financial regulators. The usual Know Your Customer paperwork includes things like passports, driver's licenses, client photographs, and signatures, all of which are manually verified by bank staff. But traditional know-your-client processes are costly for financial institutions and tedious for customers. Machine learning-based know-your-customer (KYC) verification may significantly enhance bank automation, save costs, and expedite the delivery of financial services. Automated biometric-based KYC is superior to traditional KYC documents such as passports and driver's licenses in terms of accuracy, speed, and fraud resistance.

Our second priority is ensuring the privacy of our customers. Protecting customers' personal information is a major challenge for automated KYC systems. The complex machine-learning models required for accurate biometric verification are computationally beyond the capabilities of IORT agents, which are the IoT edge nodes. Sending this data to the bank's mainframe is necessary to get the validation results. Constantly exposing customers to both one-time and ongoing KYC procedures is another issue with traditional KYC, as is the need for each bank to independently authenticate the identification documents. The secure transfer, processing, and preservation of tangible financial papers is another major issue with traditional in-person banking.

To address these concerns, this article proposes a blockchain-based architecture for IORT-enabled cyber-physical banking that uses deep neural networks to validate various biometrics-based data for KYC. The acronym for "Automated Deep Decentralized KYC" is ADD-KYC. The proposed design incorporates humanoid robots acting as Modular Rapidly Deployable Service Agents (MORAD-SA) to gather biometric data from customers and provide them with in-person financial services [1]. The use of smart contracts and the blockchain network allows for the safe and decentralized validation and transmission of KYC information. Deep neural networks are used to confirm the biometrics of the customers. A customer may keep their KYC identity under their control and share it with other banks as required using a KYC token. The proposed architecture makes the ADD-KYC usable in interbank environments. In addition, a high-capacity watermarking technology is used to incorporate client KYC information onto real banking documents. There is also a recommendation for a low-power watermarking method that uses similar Lattice Vector Quantization (LVQ) sub-lattices for Z6 and A6. This new method improves upon the previous ones, namely the Z4 and A4 LVQ watermarking techniques [4,5]. Its bigger capacity and lack of discernible size make it ideal. The water marking module ensures that financial documents will remain secure throughout transport and storage.

A variety of financial services are provided by Softbank Robotics' Pepper, a humanoid robot that is used for IORT-based biometric collection and validation. The case study presents an implementation of an automated system that retrieves and processes client handwritten bank checks in accordance with COVID-19 safety guidelines. A variety of situations are put into play, such as welcoming

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

clients, verifying their identity, and using service robots to provide various financial services. The problem of autonomous analysis and information extraction from multilingual Persian-English bank checks is investigated using a handwriting and signature verification module.

Finally, an advanced system capable of handling several concerns is required to construct an intelligent automated bank branch that can use robots to provide clients with traditional paper-based services. According to the proposed ADD-KYC model, these problems may be solved:

1. A practical software and hardware solution for banking security based on robots is necessary. This technology is compliant with pandemic safety laws, speeds up banking services, and reduces the cost of human resources. To do certain financial activities to a high standard, the pre-programmed humanoid robots need extensive software modifications.

Second, a multi-biometric automated KYC system is required to ensure secure banking. Client identities should be correctly verified by the interbank ecosystem with the use of this technology.

3. Securing digitally transmitted documents in the financial cloud requires a watermarking approach that is both rapid and has big capacity. This method should be able to encrypt financial documents using several biometric data sets.

Clients want a decentralized method to obtain their digital KYC identity in an interbank setting without compromising their privacy or security.

To address these concerns, we recommend the Add-KYC framework, which has the following features:

1. To eliminate the need for banks to collect KYC information, machine learning techniques are introduced. A decentralized framework based on blockchain is built to ensure the secure and privacy-preserving interchange of KYC information throughout the interbank ecosystem.

2. The need for falsifiable identification documents is eradicated with the introduction of an automated KYC system that relies on biometrics.

Third, to ensure the security of in-person banking documents during transmission and storage, a weak KYC watermarking approach is proposed. With its high Peak Signal-to-Noise Ratio (PSNR), it can include a large amount of Know Your Customer (KYC) data into financial documents.

4. Proposed is a hierarchical privacy-preserving module that, for authorized-only access, anonymizes individuals in films collected from the banking environment by IORT agents.

5. In both normal and emergency scenarios, it is recommended to employ a hybrid banking system based on IORT to physically connect bank customers to Banking as a Service (BAAS). Table 1 displays the abbreviations and their definitions as they appear in the text.

II. LITERATURE SURVEY

An emerging area of financial services is Cyber-Physical Customer Management (CPCM) for Internet of Robotic Things (IoRT) enabled banking. The integration of IoRT in banking is examined in this literature review, with a particular emphasis on the ways that cyber-physical systems (CPS) improve customer management, automate procedures, and provide seamless service delivery.

1. Overview of IoRT and Cyber-Physical Systems

Cyber-Physical Systems (CPS): CPS is the term for systems that integrate networking, computing, and physical processes. Real-time data processing and decision-making in banking are made possible by CPS, which closes the gap between digital and in-person encounters.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

Internet of Robotic Things (IoRT): By adding robotic devices that can interact with their surroundings on their own, IoRT expands on the idea of the Internet of Things (IoT). Intelligent ATMs, automated kiosks, and service robots are examples of IoRT equipment in the banking industry.

Relevance to Banking: By providing individualized services, boosting security, and increasing operational effectiveness, the banking industry hopes to transform customer management via the integration of CPS and IoRT.

2. In banking, Cyber-Physical Customer Management (CPCM)

Definition and Scope: Customer contact management across digital and physical channels using CPS and IoRT is known as CPCM. In order to provide a cohesive client experience, this entails integrating data from several touchpoints, such as branch visits, internet banking, and IoRT devices.

CPCM components include:

Data integration is the process of combining client information in real-time from many sources to provide a thorough customer profile.

Service Automation: Automating repetitive banking processes (e.g., account administration, client questions) with the use of Internet of Things (IoRT) devices, such as robots and intelligent kiosks.

Personalization: Adapting services according to past performance, preferences, and behavior of customers by using AI and machine learning.

Applications: Personalized banking with robotic tellers, user-adaptive ATMs, and automated advisory services with real-time financial guidance are a few examples.

3. Important Studies and Advancements

IoRT-Powered Financial Products:

Service Robots: AI-equipped robots are capable of interacting with clients, assisting them with banking procedures, and offering specialized services. Studies demonstrate their efficiency in raising customer satisfaction levels and cutting down on wait times.

Smart ATMs: With real-time threat detection and biometric identification, IoRT-enabled ATMs can execute intricate transactions, provide customized user interfaces, and improve security.

Using CPS to Make Data-Driven Decisions:

predicted analytics: Real-time customer data analysis by banks is made possible by CPS, which provides predicted insights for credit scoring, fraud detection, and customized marketing.

Security and Privacy: Studies highlight how crucial cybersecurity is to CPCM. Cyberattacks must be prevented on IoRT devices, and secure data transfer and encryption must be used to preserve client privacy.

4. Difficulties and Things to Take Into Account

Integration Complexity: It takes a lot of work and money to integrate CPS, IoRT, and traditional banking systems. Research emphasize the need of strong integration frameworks and compatible standards.

Cybersecurity Risks: IoRT devices are susceptible to cyber attacks since they are networked to the internet and the outside world. To reduce threats, research recommends putting in place multi-layered security mechanisms and ongoing monitoring.

Privacy and Ethical Issues: Large-scale consumer data gathering and analysis bring up moral questions about data ownership, permission, and privacy. Adherence to regulatory frameworks such as GDPR is crucial.

Customer Acceptance: Consumer trust and openness to interacting with robotic devices are key factors in the adoption of IoRT in banking. Studies show that in order to improve acceptability, there is a need for open and honest

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

communication with customers.

5. Prospects and Future Paths

Integration of AI and Machine Learning: To improve customer service customization and predictive capabilities, further research is required to investigate the integration of cutting-edge AI and machine learning models with IoRT.

Edge Computing: By enhancing real-time decision-making, cutting latency, and improving overall customer experience, edge computing may be used in IoRT-enabled banking.

Cross-Channel Synchronization: To guarantee that consumer interactions are constant and uninterrupted across platforms, future advances should concentrate on the smooth synchronization between digital and physical channels.

Regulatory Compliance and Standards: To guarantee the safe and moral implementation of IoRT in banking, it will be essential to create industry-wide standards and regulatory frameworks.

6. Final Thoughts on Banking: With more efficient, safe, and individualized services available, CPCM for IoRT-enabled banking has the potential to completely change the consumer experience. The future of banking is one that is much closer with the merging of CPS and IoRT.

Research Implications: To solve the difficulties and realize the full potential of CPCM in banking, there is an increasing need for interdisciplinary research that brings together knowledge in robotics, cybersecurity, artificial intelligence, and financial services.

An extensive overview of the present and potential future directions of CPCM for IoRT-enabled banking is given by this literature review. Cyber-physical systems in financial services are a rapidly changing field that has many opportunities for innovation, but there are drawbacks that must be carefully considered.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

The Know Your Customer (KYC) check is an essential procedure for verifying the identity of a bank customer. Global financial authorities routinely require it for all financial transactions since it is a vital procedure in banking systems. A customer's home address, a recent photo of themselves, a sample of their signature, and official identification documents are the standard components of the know-your-customer (KYC) procedure. Numerous financial institutions throughout the globe have also begun using the Know Your Customer (KYC) check that is based on biometrics [2]. The conventional method relies on bank workers manually collecting and verifying KYC data. But new research shows that banks may save money and time by utilizing service robots to handle customer inquiries [3].

It is critical to strike a balance between thoroughness and intrusiveness while conducting KYC checks. Customer service agents waste time and energy on unnecessary identity verification processes. Automated know-your-customer (KYC) solutions using a variety of biometrics, such as face, voice, iris, fingerprints, palm veins, handwriting, and signatures, have shown encouraging results. Facial and voice biometrics are especially well-suited to the banking sector because to their non-invasive nature. Research in the last few years has shown that deep neural networks excel in extracting biometric characteristics [7]. Szczuko et al. [8] introduced a data fusion-based approach to multi-modal biometrics client verification for financial institutions. The Dempster-Shafer approach was used to accomplish data fusion, and the results were accurate enough for use in financial applications. The authors Almabdy and Elrefaei reviewed recent advances in deep learning systems used

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

for biometric applications [7]. Several performance measures indicate that deep neural networks may provide the level of accuracy required for human identity verification. Estrela et al. [9] detailed a behavioral biometric user authentication method for usage in financial apps as a defense against impersonation and fraud. It used biometrics to get banking approval with an accuracy of 97.05% in one environment and 90.68% in another. Based on their examination of many non-invasive, soft biometric assessments, Hassan et al. [10] shown that these measures have the potential to provide accuracy levels comparable to standard biometric measures in various contexts.

Another concern with automated biometrics is the protection of customers' personal information and financial data. Robots and other edge nodes must provide visual and other sensory data to the bank servers so the automated biometric verification based on machine learning can function. Problems with customer dissatisfaction, data security, privacy, and KYC fees are made worse when each bank is required to train its biometric models individually. One potential solution to these problems is a blockchain-based KYC system. Laborde et al. [11] introduced a Know Your Customer (KYC) approach to internet banking that uses identifying information given by many organizations. Jain et al. [12] created a decentralized design for one-time KYC to ease transfers between banks. Hyperledger Fabric was employed by Biradar et al. [13] as a blockchain-based KYC framework for this purpose, while an Ethereum-based KYC model was established by Yadav et al. [14] to improve customer satisfaction and minimize expenditures. Under this arrangement, there are two types of bank customers: those who are temporary and just need basic services, and those who are permanent. Integrating with the Future-Internet-WARE (FIWARE) platform, Esposito et al. [15] introduced a blockchain-based architecture for authorization and identity management. Because smart city applications must be integrated with the city's preexisting information and communication technology infrastructures, data security becomes a major concern. A blockchain-based solution is proposed since the centralized system is unable to meet the security demands of these sites. Table 2 displays research that is similar to the methods proposed in this paper. However, we address the limitations of each relevant study in the ADD-KYC framework. Current frameworks just implement conventional KYC on the blockchain, despite the fact that ADD-KYC is automated, built on a deep neural network, uses several biometrics, is designed for robotic banking, and has hierarchical privacy protection. In addition, the current banking industry's centralized, manual, document-based KYC validation methods are costly, time-consuming, and security-vulnerable.

Disadvantages

Banks need a realistic, safe software and hardware solution based on robots. This technology meets the safety criteria during a pandemic while simultaneously reducing the cost of human resources and improving the speed and accuracy of banking services. In order for the standard-bearer humanoid robots to perform some financial services, substantial software modifications are necessary.

2. You can't have safe banking without an automated multi-biometric KYC system. Customers should be able to get very accurate identification verification from the interbank ecosystem thanks to this approach.

3. In order to secure digitally transferred documents in the financial cloud, a watermarking technique that is both quick and

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

has a high capacity is necessary. It is expected that this method can store various biometric data in financial papers.

4. Customers need a decentralized solution that safeguards their privacy and security while allowing them access to their digital KYC identity in an interbank environment.

PROPOSED SYSTEM

Using deep neural networks to assess various biometrics-based data, the system proposes a blockchain-based architecture for know-your-customer in IoRT-enabled cyber-physical banking. The acronym for "Automated Deep Decentralized KYC" is ADD-KYC. The proposed design incorporates humanoid robots acting as Modular Rapidly Deployable Service Agents (MORAD-SA) to gather biometric data from customers and provide them with in-person financial services [1]. By using smart contracts and the blockchain network, know-your-customer (KYC) information is safely and decentrally sent after validation. Deep neural networks are used to confirm the biometrics of the customers. A customer may keep their KYC identity under their control and share it with other banks as required using a KYC token. The proposed architecture makes the ADD-KYC usable in interbank environments. In addition, a high-capacity watermarking technology is used to incorporate client KYC information onto real banking documents. There is also a recommendation for a low-power watermarking method that uses similar Lattice Vector Quantization (LVQ) sub-lattices for Z6 and A6. This new method improves upon the previous ones, namely the Z4 and A4 LVQ watermarking techniques [4,5]. Its bigger capacity and lack of discernible size make it ideal. The water marking module ensures that financial documents will remain secure throughout transport and storage. One of the many financial services that Pepper, a humanoid robot manufactured by Softbank Robotics, helps with is the implementation of the IoRT-based biometric gathering and validation procedure. The case study presents an implementation of an automated system that retrieves and processes client handwritten bank checks in accordance with COVID-19 safety guidelines. A variety of situations are put into play, such as welcoming clients, verifying their identity, and using service robots to provide various financial services. We look at the problem of autonomous analysis and information extraction from multilingual Persian-English bank checks using a handwriting and signature verification module.

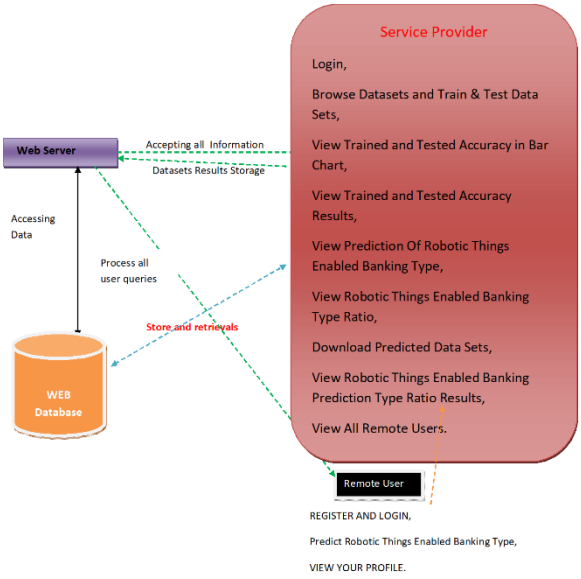
Advantages

1. A decentralized framework based on blockchain technology is created to facilitate the safe and private exchange of know-your-customer (KYC) data inside the interbank ecosystem. To do away with the need of collecting KYC data from various banks, machine learning models are suggested.
2. We have created an automated biometrics-based KYC system that does not rely on susceptible identifying papers.
3. We suggest a delicate Know Your Customer watermarking solution to safely transmit and save in-person banking papers. It has a high Peak Signal-to-Noise Ratio (PSNR) and can insert a lot of Know Your Customer (KYC) data into bank papers.
4. To ensure that only authorized individuals may view films taken in a banking environment by IoRT agents, a privacy-preserving module is suggested that uses a hierarchical structure to mask people's identities.
5. We suggest a hybrid banking system that is based on the Internet of Things Radio Technology (IoRT) that can connect Banking as

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

a Service (BaaS) with bank clients in both normal and pandemic situations.

IV. SYSTEM ARCHITECTURE



V. SYSTEM IMPLEMENTATIONS

MODULES

Service Provider

A valid username and password are required for the Service Provider to access this module. He would be able to do actions like browsing datasets and running tests and training on them when he successfully logs in. Prediction Of Robotic Things Enabled Banking Type, Robotic Things Enabled Banking Type Ratio, Trained and Tested Accuracy in Bar Chart, Results of Trained and Tested Accuracy, and More! Store Anticipated Data Sets, Check Out the Total Number of Remote Users, Robotic Things-Enabled Banking Prediction Type Ratio.

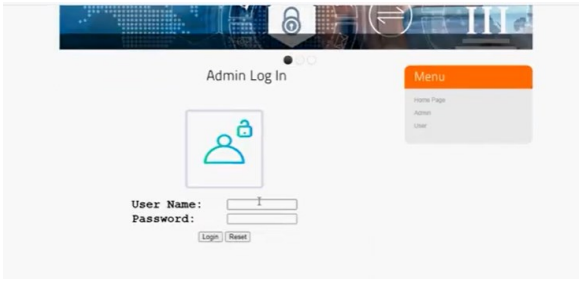
View and Authorize Users

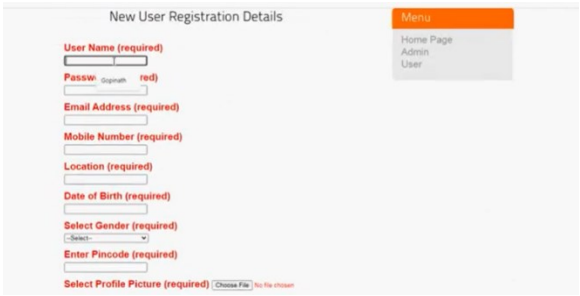
The admin can get a complete rundown of all registered users in this section. Here, the administrator may see the user's information (name, email, and address) and grant them access.

Remote User

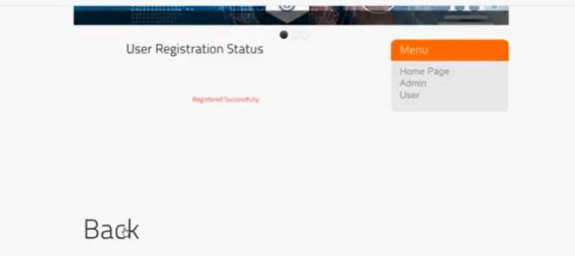
All all, there are n users in this module. Registration is required prior to performing any operations. Details will be entered into the database after a user registers. He will need to log in using the permitted username and password when registration is completed. After logging in, users will be able to perform things like predict which banking types are enabled by robotic things, REGISTER AND LOGIN, and Check Out Your Account.

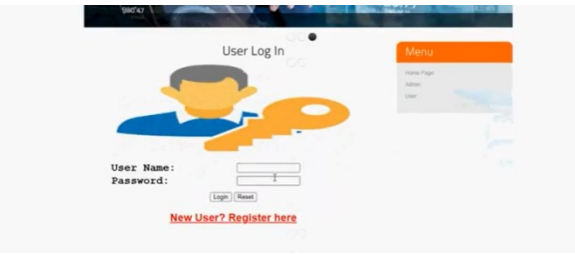
VI. RESULTS

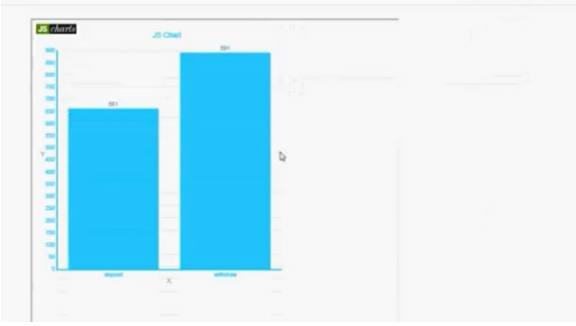


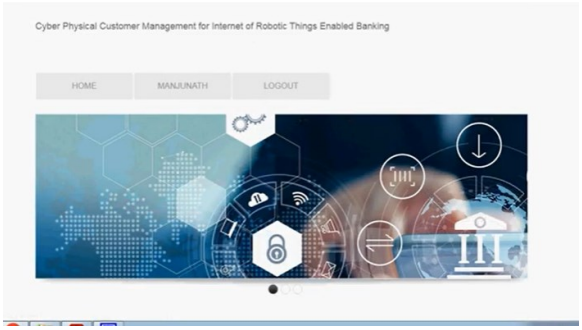


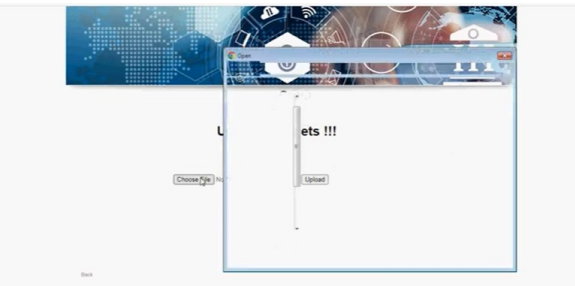
www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298



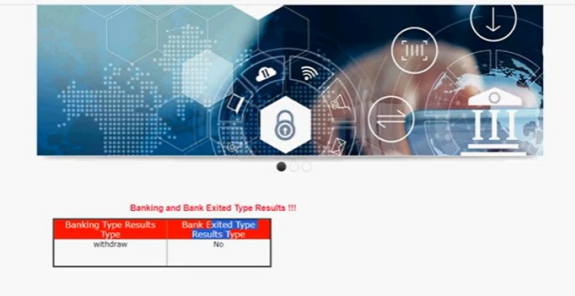


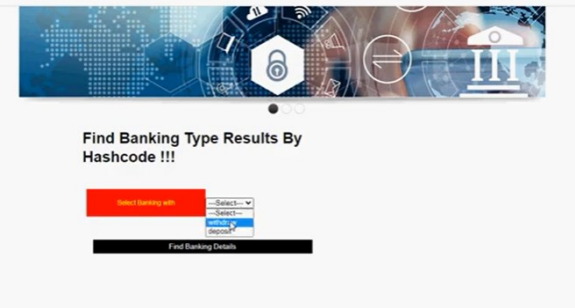


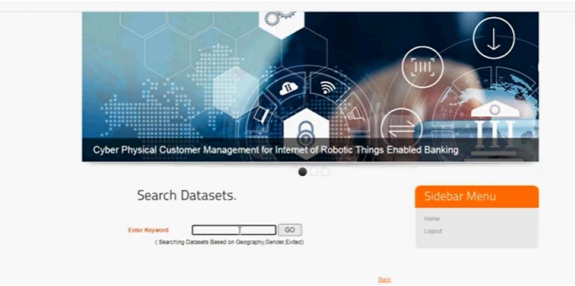




www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298







VII. CONCLUSION

The proposed framework was built using Pepper, a humanoid robot from Softbank Robotics, to manage cyber-physical banking in the case of a pandemic. Because it isn't intrusive, it improves customer satisfaction and efficiency while reducing costs in the setting of physical banking. We evaluated the performance of the proposed watermarking algorithm and compared the results with many recently proposed approaches from the literature. The customer's fingerprint, the recipient's name, the check number, the customer's signature, their facial image, and the bank's logo are the biometric security details that are used to watermark bank checks. The proposed methodology produced PSNR values that were up to 5.1 dB higher than similar strategies. The average PSNR for the 100 check photographs after embedding was 45.5 dB, suggesting that the watermarked images had minimal distortion. The results of the simulation showed how accurate the proposed framework was. The main flaw in the proposed design is that automated systems must be continuously supervised by humans in order to meet banking laws, which require 100% client satisfaction. Furthermore, the correctness of the proposed framework is limited in its current version. Because customer biometrics and bank environment characteristics vary so much, more model training is required. A solution for the provision of financial services during the COVID-19 pandemic is currently under development. In such cases, using human workers to do regular KYC checks and paper-based financial services presented a health risk to both customers and staff. Generally speaking, figuring out how to improve the client experience necessitates a careful examination of various banking environments and cultures. Extensive customer feedback collection and analysis are expected as future study phases after being deployed in several bank locations. Future studies on this subject might focus on improving the independence of contacts with bank customers and broadening the scope of financial services provided.

REFERENCES

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066298

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.