ENHANCING CUSTOMER AUTHENTICATION IN BANKING USING IRIS BIOMETRIC TECHNOLOGIES

Ms. SUNITHA M.E
Assistant Professor,
Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – asunitha2022@gmail.com

Mr. GOPINATH. S
Student,
Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – asunitha2022@gmail.com

Abstract -- The Banking and Secure Transactions Using Fingerprint and Iris Recognition System is designed to enhance financial security by integrating biometric authentication into banking operations. The system enables users to register using their Voter ID, personal details, bank account information, fingerprint, and iris scan, generating a unique card number upon successful enrolment. During authentication, users verify their identity through a combination of card number, password, and biometric data, ensuring a high level of security. The system supports both inner transactions (self-transfers) and outer transactions (transfers to other accounts), maintaining confidentiality and integrity throughout each process.

I. INTRODUCTION

The Banking and Secure Transactions Using Fingerprint and Iris Recognition system ensures highly secure and seamless financial transactions by integrating biometric authentication. The project focuses on eliminating vulnerabilities associated with traditional authentication methods by requiring users to register with their Voter ID, bank details, fingerprint, and iris scan to obtain a unique card number. During login, users must validate their biometric credentials before accessing account information and performing inner (self) and outer (external) transactions.

Admin oversee user accounts, transaction records, and system management to maintain security and operational efficiency. The system provides enhanced protection against fraud, identity theft, and unauthorized access, ensuring a reliable and scalable banking solution for financial institutions.

II. BACKGROUND AND MOTIVATION

Traditional banking authentication methods such as passwords, PINs, and ATM cards are increasingly vulnerable to cyberattacks, identity theft, phishing, and unauthorized access. As digital banking services continue to expand, ensuring secure and reliable customer authentication has become a major challenge for financial institutions. Biometric technologies have emerged as an effective solution because they rely on unique physical characteristics that are difficult to duplicate or steal. Among various biometric methods, iris recognition is considered one of the most accurate and secure due to the uniqueness and stability of iris patterns in every individual.

The motivation for using iris biometric technology in banking comes from the growing need for stronger security, faster authentication, and improved customer convenience. Unlike fingerprints or facial recognition, the iris remains stable throughout a person's lifetime and can be captured without physical contact, making it highly hygienic and reliable. Iris-based authentication reduces the risk of fraud, unauthorized transactions, and identity impersonation while enhancing trust in banking systems. Additionally, with the rise of online banking, mobile banking, and automated teller machines, banks require advanced authentication systems that can provide both security and efficiency.

This project focuses on enhancing customer authentication in banking using iris biometric technologies to improve security measures and user experience. The system aims to integrate iris recognition into banking applications for secure login, transaction verification, and account access. By implementing this technology, banks can minimize security breaches, strengthen customer identity verification, and support the development of smarter and safer digital banking environments.

III.NOVEL APPLICATIONS OF IRIS BIOMETRIC

Iris biometric technology has evolved beyond traditional security systems and is now being applied in several innovative fields due to its high accuracy, reliability, and resistance to forgery. In the banking sector, iris biometrics can be used for secure ATM authentication, mobile banking login, online transaction verification, and contactless payment systems. Customers can access their accounts quickly and securely without remembering passwords or carrying physical cards, thereby improving both convenience and security.

In healthcare, iris recognition is used for patient identification, medical record management, and secure access to healthcare systems. It helps prevent identity fraud and ensures that patient information remains confidential. In airports and border security, iris biometrics enables faster passenger verification, automated immigration clearance, and enhanced surveillance systems. Governments also use iris recognition in national identity programs, voter registration, and welfare distribution systems to eliminate duplicate identities and improve transparency.

Educational institutions and corporate organizations have adopted iris biometric systems for attendance monitoring, access control, and employee authentication. In smart homes and Internet of Things (IoT) environments, iris recognition can provide personalized and secure access to devices and services. Furthermore, iris biometrics is increasingly being integrated with artificial intelligence and cloud computing technologies to support real-time authentication, remote verification, and advanced cybersecurity applications. These novel applications demonstrate the growing importance of iris biometric technology in creating secure, efficient, and intelligent digital systems across multiple industries.

IV. ROLE AND POTENTIAL

Role:

- Customer/User

  The customer is the primary user of the system who registers and authenticates using iris biometric data. Customers can securely access banking services such as account login, ATM transactions, fund transfers, and balance inquiries through iris

verification.

- BankAdministrator

  The bank administrator manages the overall system operations, customer records, and biometric database. The administrator is responsible for monitoring authentication activities, maintaining system security, updating customer information, and handling access permissions.

- System Administrator

  The system administrator maintains the technical infrastructure of the iris biometric system. Their role includes software installation, server maintenance, database management, system updates, backup management, and ensuring proper integration between biometric devices and banking applications.

- Security Officer

  The security officer monitors suspicious activities, fraud attempts, and unauthorized access within the banking system. They analyze authentication logs, ensure compliance with security policies, and take preventive actions against cyber threats and identity fraud.

- Biometric Device Manager

  The biometric device manager handles the installation, configuration, and maintenance of iris scanning devices used in banks and ATMs. They ensure that scanners function accurately and efficiently for smooth customer authentication.

- Database Manager

  The database manager securely stores and manages customer biometric templates, transaction details, and authentication records. They ensure data privacy, backup, recovery, and protection against data breaches or unauthorized modifications.

Potential:

Iris biometric technology has significant potential to transform the banking sector by providing highly secure, fast, and reliable customer authentication. Since every individual has a unique iris pattern that remains stable throughout life, iris recognition offers greater accuracy compared to traditional authentication methods such as passwords, PINs, and cards. This reduces the risk of identity theft, fraud, and unauthorized account access.

One major potential of iris biometrics is in enhancing digital banking security. Customers can securely access mobile banking, internet banking, and ATM services using iris verification without needing to remember multiple passwords. The technology also supports contactless authentication, improving hygiene and convenience in banking operations.

Iris biometric systems can improve operational efficiency by reducing transaction time, minimizing human errors, and automating customer verification processes. Banks can use this technology for secure fund transfers, account opening, loan verification, and high-value transaction approvals. It also helps financial institutions comply with strict security and identity verification regulations.

In the future, iris biometrics has the potential to integrate with artificial intelligence, cloud computing, blockchain, and Internet of Things (IoT) technologies for advanced cybersecurity solutions. The adoption of iris recognition can support the development of smart banking systems that are more secure, user-friendly, and efficient. As cyber threats continue to increase, iris biometric technology is expected to play a vital role in strengthening trust and safety in modern banking environments.

V. INNOVATIVE INTEGRRATION

Innovation integration in iris biometric banking systems refers to the combination of advanced technologies with iris recognition to create secure, intelligent, and efficient banking solutions. By integrating modern innovations such as artificial intelligence (AI), cloud computing, blockchain, Internet of Things (IoT), and machine learning, banks can enhance customer authentication and improve overall banking security.

Artificial intelligence and machine learning can be integrated with iris biometric systems to improve recognition accuracy, detect fraudulent activities, and analyze customer authentication patterns in real time. Cloud computing enables secure storage and fast processing of biometric data, allowing customers to access banking services from multiple locations and devices efficiently.

Blockchain technology can be used to protect biometric records through decentralized and tamper-proof storage mechanisms. This ensures transparency, data integrity, and protection

against unauthorized modifications. Integration with IoT devices and smart ATMs allows customers to perform secure contactless transactions using iris verification, improving convenience and user experience.

Mobile banking applications can also integrate iris biometric authentication for secure login, transaction approvals, and digital payment verification. Furthermore, combining iris recognition with multi-factor authentication methods enhances security by adding additional verification layers. These innovations help banks reduce cyber risks, improve operational efficiency, strengthen customer trust, and support the development of modern smart banking systems.

VI. RECENT ADVANCEMENT

Recent advancements in iris biometric technology have significantly improved the accuracy, security, and efficiency of authentication systems, especially in the banking and financial sectors. Modern iris recognition systems now use artificial intelligence (AI) and deep learning algorithms to enhance pattern recognition, improve matching speed, and reduce authentication errors. These technologies help banks provide faster and more reliable customer verification services.

One major advancement is the development of liveness detection technology, which can identify fake or duplicated iris images and prevent spoofing attacks. Companies such as Mantra Softech recently achieved advanced iris liveness certification for dual-eye iris scanners, improving security against fraudulent access attempts.

Another important development is the integration of iris biometrics with digital payment systems and wearable devices. The National Payments Corporation of India (NPCI) introduced biometric and wearable-based authentication methods for secure UPI payments, supporting contactless and seamless banking transactions. In addition, companies like Ant International have introduced iris-authenticated smart glasses for secure digital payments and augmented reality commerce applications.

Cloud computing and blockchain technologies are also being integrated into iris biometric systems for secure storage, decentralized identity management, and faster authentication processing. Researchers are further improving multi-factor authentication systems by

combining iris recognition with smart cards, facial recognition, and PIN-based security to enhance cybersecurity protection.

Recent studies also confirm the long-term stability and reliability of iris recognition systems, even for children and large-scale identity programs, making iris biometrics suitable for national identification and banking applications. Furthermore, the global iris recognition market is rapidly expanding due to increasing demand for secure digital banking, e-payment systems, and fraud-resistant authentication technologies.

VII.CHALLENGES

Despite its high accuracy and security, iris biometric technology faces several challenges in banking and other authentication systems. One major challenge is the high implementation cost. Installing iris scanners, maintaining biometric databases, and integrating the technology with existing banking infrastructure require significant investment, which may be difficult for smaller financial institutions.

Another challenge is environmental and image capture issues. Poor lighting conditions, reflections from eyeglasses, eye movement, and low-quality cameras can affect the accuracy of iris image acquisition. Customers with eye diseases, injuries, or contact lenses may also experience difficulties during authentication.

Privacy and data security concerns are also important challenges. Since biometric information is highly sensitive and unique to each individual, unauthorized access or data breaches can create serious security risks. Banks must ensure strong encryption, secure storage, and strict privacy policies to protect customer biometric data.

User acceptance and awareness can also affect the adoption of iris biometric systems. Some users may feel uncomfortable sharing biometric information due to fear of surveillance or misuse of personal data. In addition, technical failures, system downtime, or false rejection cases may reduce customer trust and satisfaction.

Another significant challenge is spoofing and cyberattacks. Although iris recognition is highly secure, attackers may attempt to use fake iris images or advanced hacking techniques to bypass authentication systems. Therefore, banks must continuously update security mechanisms such as liveness detection and multi-factor authentication.

Finally, integrating iris biometric systems with existing banking platforms, ATMs, and

mobile applications can be technically complex. Proper training, maintenance, and regular system upgrades are necessary to ensure smooth and secure operation.

VIII. CONCLUSION

Iris biometric technology has emerged as a highly secure, accurate, and reliable solution for enhancing customer authentication in the banking sector. Traditional authentication methods such as passwords, PINs, and ATM cards are increasingly vulnerable to fraud, cyberattacks, and identity theft, creating a strong need for advanced security mechanisms. Iris recognition provides a unique and stable biometric feature that significantly improves user verification and reduces unauthorized access.

The integration of iris biometrics with modern technologies such as artificial intelligence, cloud computing, blockchain, and IoT has further strengthened banking security and operational efficiency. It enables secure access to digital banking services, contactless transactions, real-time authentication, and fraud prevention while improving customer convenience and trust.

Although challenges such as implementation cost, privacy concerns, environmental limitations, and system integration exist, continuous advancements in biometric technologies are helping overcome these issues. Features like liveness detection, multi-factor authentication, and encrypted biometric storage enhance the overall reliability and safety of iris-based systems.

In conclusion, iris biometric technology has great potential to transform modern banking by providing stronger authentication, improved cybersecurity, and smarter financial services. As digital banking continues to expand, the adoption of iris recognition systems is expected to play a vital role in building secure, efficient, and customer-friendly banking environments.

IX.REFERENCE

[1] Cheng Wang and Hangyu Zhu. Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services. VOLUME 19, pp. 301 - 315, 2022.

[2] OMER MELIH GUL, MICHEL KULHANDJIAN, BURAK KANTARCI , AZZEDINE TOUAZI ,CLIFF ELLEMENT AND CLAUDE D'AMOURS. Secure Industrial IoT Systems via RF Fingerprinting Under Impaired Channels With Interference and Noise. VOLUME 11, pp 26289 - 26307, 14 March 2023.

[3] Yanming Zhu , Xuefei Yin and Jiankun Hu. FingerGAN: A Constrained Fingerprint Generation Scheme for Latent Fingerprint Enhancement. VOLUME 45, pp. 8358 - 8371, 13 January 2023.

[4] XINRUI GONG, XIANGLONG YU, XIAOFENG LIU AND XIQI GAO. Machine Learning-Based Fingerprint Positioning for Massive MIMO Systems. VOLUME 10, pp. 89320 - 89330, 18 August 2022.

[5] UMER RASHID, SAMRA NASEER, ABDUR REHMAN KHAN, MUAZZAM A. KHAN, GAUHAR ALI, NAVEED AHMAD AND YASIR JAVED. Sampling Fingerprints From Multimedia Content Resource Clusters. VOLUME 11, pp. 141640 - 141656, 14 December 2023.

[6] A. S. Yaro, F. Malý, and K. Malý, ‘‘Improved indoor localization performance using a modified affinity propagation clustering algorithm with context similarity coefficient,’’ IEEE Access, vol. 11, pp. 57341–57348, 2023.

[7] Y. Zhu, X. Yin, and J. Hu, ‘‘FingerGAN: A constrained fingerprint generation scheme for latent fingerprint enhancement,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 7, pp. 8358–8371, Jul. 2023.

[8] A. B. V. Wyzykowski and A. K. Jain, ‘‘Synthetic latent fingerprint generator,’’ in Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. (WACV), Waikoloa, HI, USA, Jan. 2023, pp. 971–980.

[9] D. Ko, M. Kim, K. Son, and D. Han, ‘‘Passive fingerprinting reinforced by active radiomap for WLAN indoor positioning system,’’ IEEE Sensors J., vol. 22, no. 6, pp. 5238–5247, Mar. 2022.

[10] M. E. M. Gonzales, L. C. Uy, J. A. L. Sy, and M. O. Cordel, ‘‘Distance metric recommendation for k-means clustering: A meta-learning approach,’’ in Proc. IEEE Region 10 Conf. (TENCON), Nov. 2022, pp. 1–6.