ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

QUANTUM-RESILIENT INCLUSIVE BIOMETRIC ARCHITECTURE

Veeresh D S S[1], Dr. B Rama Ganesh[2]
[1]BEST Innovation University, Gownivaripalli, Gorantla, Andhra Pradesh, India
[2]Sri Venkatesa Perumal College of Engineering and Technology, Puttur, Tirupathi, Andhra Pradesh, India

Email Id: 2024spcse010@bestiu.edu.in

ABSTRACT: The development of national digital identity systems has sped up, leading to an increasing demand for biometric authentication system, which needs to be secure and able to serve all users and be adapted to future needs. The classical biometric systems rely on fingerprints, iris scans and facial recognition technology, which poses significant accessibility challenges to individuals with physical disabilities, visual impairments and atypical biometric characteristics such as those born without fingers or having more fingers. The existing protocols are vulnerable to the new quantum attacks that threaten classical cryptographic protocols. This work presents the Quantum-Resilient Inclusive Biometric Framework, which allows the use of various biometrics and resilient to quantum threats. The framework supports matching via a quantum state encoding method which encodes multiple biometric features under a Grover-based search technique that amplifies the amplitudes. We present a smart identity card system which can be proved to be post-quantum secure by combining lattice-based cryptography and quantum-safe digital signatures. The architecture is such that offering access to the chip-enabled authentication and Braille-assisted verification system doesn't compromise the security of the cryptographic protections. Security is evaluated by calculating quantum threat models with Shor-type, Grover-type attacks as potential adversary techniques. The proposed model offers better scalability for large-scale biometric search, as well as it offers better accessibility to the disabled people and better privacy and security in facing cyber threats that will be evolved by quantum technologies in the future. The work builds a secure and affordable national identity infrastructure through design of national identity systems based on quantum computing principles for the inclusive biometric systems.

Keywords: Braille assistance, Biometric systems, Grover algorithm, National Identity Systems, Quantum computing, Shor algorithm

I. INTRODUCTION

The rapid advancement of digital transformation initiatives has led to the widespread adoption of national digital identity systems[1] across the world. These systems play a crucial role in enabling secure access to government services, financial institutions, healthcare facilities, and digital platforms. Biometric authentication has emerged as one of the most reliable mechanisms for identity verification due to its ability to uniquely identify individuals based on physiological and behavioural characteristics. Large-scale identity management systems, such as Aadhaar, have demonstrated the effectiveness of biometric technologies in

providing universal identity coverage for billions of citizens.

Despite their widespread adoption, existing biometric authentication systems face several significant challenges related to security, scalability, and inclusivity. Conventional biometric systems primarily rely on fingerprints, iris scans, and facial recognition for user authentication. While these modalities provide high recognition accuracy, they often exclude individuals with physical disabilities, visual impairments, damaged biometric traits, or atypical physiological characteristics. Furthermore, biometric characteristics may change over time due to ageing, medical conditions, accidents, surgical procedures, or genetic variations such as polydactyly and congenital absence of fingers. These factors may lead to enrolment failures, authentication errors, and exclusion from essential digital services.

Another critical challenge is the management and updating of biometric information throughout an individual's lifetime. Existing identity systems are generally designed around static biometric templates and may not efficiently accommodate changes in biometric characteristics. Consequently, the development of adaptive and inclusive biometric frameworks capable of handling diverse user populations remains an important research problem.

In addition to accessibility concerns, the security of current identity management infrastructures is increasingly threatened by advances in quantum computing. Most existing digital identity systems rely on classical cryptographic algorithms such as Rivest–Shamir–Adleman (RSA)[2] and Elliptic Curve Cryptography (ECC)[3] for securing sensitive identity information and communication channels. However, quantum algorithms such as Shor's algorithm can efficiently solve integer factorization and discrete logarithm problems, rendering these cryptographic schemes vulnerable to future quantum attacks. Similarly, Grover's algorithm can significantly reduce the complexity of brute-force attacks against symmetric cryptographic systems. These developments raise serious concerns regarding the long-term confidentiality, integrity, and authenticity of identity data stored within national digital identity infrastructures.

To address these challenges, this research proposes a Quantum-Resilient Inclusive Biometric Framework that integrates quantum computing techniques, alternative biometric modalities, and post-quantum cryptographic mechanisms to establish a secure, scalable, and accessible identity management system. The framework employs quantum state encoding for efficient representation of multi-modal biometric features and utilizes Grover-based quantum search techniques for rapid biometric matching within large-scale identity repositories. Furthermore, lattice-based cryptography[4], quantum-safe digital signatures, and Quantum Key Distribution (QKD)[5] are incorporated to provide resilience against both classical and quantum adversaries.

The proposed framework also introduces accessibility-oriented features, including alternative biometric representations and Braille-assisted smart identity cards, enabling participation by individuals with disabilities and atypical biometric characteristics. By combining inclusivity with quantum-resilient security mechanisms, the framework aims to establish a future-ready national identity infrastructure capable of addressing the evolving requirements of digital governance and cybersecurity in the quantum era.

II. LITERATURE SURVEY

Recent advancements highlight the integration of AI and quantum computing in cybersecurity and identity management.

As per the paper proposed by Rishabh Garg[6], the inefficiency of recording the biometrics has be reported. The deficiencies in the human anatomy can lead to inconsistent data stored and that can trigger to impersonate by another person to make fraud in disguise. The paper presents the possibilities of deficiencies and how those can be misused.

In another paper by Velpula Ravindra Reddy et. al[7], the detection of a secure and optimal path is searched using Quantum Key Distribution(QKD) protocols and Grover's Algorithm. The QKD is helpful in checking the secure transmission, while Grover's algorithm is useful in searching in a faster way instead of using a traditional searching methodology.

In the paper proposed by Emmanuel Igba et. al[8], the detection of financial fraud is made because of the lack of identification of biometrics, which may lead to identity fraud. The biometrics can be compromised or misusing the deceased persons' biometrics for transactions leading to financial fraud. In this paper, the authors have integrated models such as Generative Adversarial Networks (GANs), Conditional GANs, Variational Autoencoders (VAEs), and Transformers.

Research Gap

Although significant progress has been made in the areas of biometric authentication, digital identity management, artificial intelligence, and quantum computing, several important limitations remain unaddressed. Existing biometric authentication systems primarily rely on conventional modalities such as fingerprints, iris scans, and facial recognition, which are often unsuitable for individuals with physical disabilities, visual impairments, damaged biometric traits, or atypical physiological characteristics. Consequently, current identity infrastructures lack comprehensive mechanisms for ensuring inclusive authentication and universal accessibility.
Furthermore, most national identity systems continue to depend on classical cryptographic algorithms, including RSA and Elliptic Curve Cryptography (ECC), which are vulnerable to future quantum attacks. While post-quantum cryptographic schemes have been proposed in recent years, their integration into large-scale identity management systems remains limited. The absence of quantum-resilient security mechanisms poses a significant threat to the long-term confidentiality, integrity, and authenticity of sensitive identity information.

In addition, existing research has investigated quantum computing, artificial intelligence, biometric authentication, and accessibility as independent domains. There is currently a lack of unified frameworks that integrate quantum search algorithms, AI-assisted biometric processing, post-quantum cryptographic protection, and accessibility-oriented authentication mechanisms within a single identity management architecture. This gap limits the ability of current systems to simultaneously address scalability, security, and inclusivity requirements.

Therefore, there is a need for a comprehensive framework that combines multi-modal and inclusive biometric authentication, quantum-enhanced search capabilities, AI-driven adaptive processing, and post-quantum cryptographic protection to support secure, scalable, and universally accessible national digital identity systems. The proposed Quantum-Resilient Inclusive Biometric Framework aims to address these limitations by providing an integrated solution capable of meeting the

evolving demands of identity management in the quantum computing era.

III. PROPOSED METHODOLOGY

The proposed Quantum-Resilient Inclusive Biometric Framework introduces a multi-layered architecture that integrates inclusive biometric authentication, quantum computing techniques, and post-quantum cryptographic mechanisms. The framework is designed to address three major challenges in national identity systems: accessibility for individuals with disabilities, scalability for large-scale biometric databases, and resilience against emerging quantum threats. The overall architecture consists of five major components: Multi-Modal Biometric Acquisition, Quantum State Encoding, Quantum Search and Matching, Post-Quantum Cryptographic Protection, and Smart Identity Card Integration.

A. Multi-Modal Biometric Acquisition

The first layer of the framework focuses on the acquisition and management of biometric information from diverse user populations. Conventional biometric systems primarily rely on fingerprints, iris scans, and facial recognition for identity verification. While effective for the majority of users, these approaches often fail to accommodate individuals with physical disabilities, visual impairments, damaged fingerprints, or atypical biometric characteristics. To overcome these limitations, the proposed framework incorporates a multi-modal biometric acquisition system capable of collecting and managing multiple biometric traits. In addition to traditional biometric modalities, alternative identification mechanisms such as voice recognition, speech characteristics, behavioural biometrics, gait analysis, and facial dynamics are incorporated into the authentication process. These supplementary modalities provide reliable identification pathways for individuals whose conventional biometric data may be unavailable or incomplete.

Furthermore, Braille-assisted input mechanisms are integrated to support visually impaired users during enrolment and authentication. The Braille interface enables secure storage, retrieval, and verification of identity information while ensuring accessibility and ease of use. This inclusive design improves user participation and reduces enrolment failures in large-scale national identity programs.

B. Quantum State Encoding Layer

Following biometric acquisition, the extracted biometric features are transformed into quantum representations for efficient processing and storage. The quantum state encoding process maps multiple biometric attributes into quantum states according to

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i \, |i\rangle$$

where α_i represents the amplitude coefficient associated with the i^{th} biometric feature and $|i\rangle$ denotes the corresponding quantum basis state. The encoding process enables simultaneous representation of multiple biometric modalities within a unified quantum framework. By exploiting quantum superposition, the system can process large amounts of biometric information in parallel, thereby improving storage efficiency and retrieval performance. In addition, quantum encoding enhances data integrity by making unauthorized modifications more difficult to perform without detection. Consequently, the framework provides a secure and scalable mechanism for managing sensitive biometric information.

C. Quantum Search and Matching Using Grover's Algorithm

Efficient biometric matching is achieved through the application of Grover's quantum search algorithm. Traditional search techniques employed in biometric

databases require linear search operations, resulting in increased computational costs as database size grows. In contrast, Grover's algorithm provides a quadratic speedup for unstructured search problems. The time complexity of Grover's search algorithm is given by $O(\sqrt{N})$ where N represents the total number of records stored in the biometric database. This quantum search capability significantly reduces authentication time when processing large-scale national identity repositories containing millions or even billions of records. The algorithm can be utilized for identity verification, profile retrieval, record updates, and insertion of newly enrolled users. The resulting improvement in computational efficiency makes the framework particularly suitable for future population-scale digital identity systems.

D. Post-Quantum Cryptographic Layer

The security of the proposed framework is ensured through the integration of post-quantum cryptographic mechanisms. Since conventional public-key cryptographic algorithms are vulnerable to quantum attacks, particularly those based on Shor's algorithm, the framework adopts lattice-based cryptographic schemes for encryption and authentication.

Lattice-based cryptography provides strong security guarantees against both classical and quantum adversaries while maintaining practical computational requirements. To further strengthen security, quantum-safe digital signature schemes are employed to verify the authenticity and integrity of stored biometric information. In addition, the framework incorporates Quantum Key Distribution (QKD) for secure key exchange between authentication entities. Unlike conventional public-key infrastructures, QKD leverages quantum mechanical principles to establish cryptographic keys with information-theoretic security. Any attempt to intercept or manipulate the communication channel introduces detectable disturbances, thereby preventing undetected eavesdropping attacks. Together, lattice-based encryption, quantum-safe signatures, and QKD provide comprehensive protection against future quantum-enabled cyber threats.

E. Smart Identity Card System

The final layer of the framework integrates all biometric, quantum, and cryptographic components into a chip-enabled smart identity card. The smart card serves as a secure portable identity credential capable of storing encrypted biometric templates and cryptographic authentication parameters. A distinctive feature of the proposed design is the inclusion of Braille-enabled interfaces, allowing visually impaired users to independently access authentication services and personal identity information. The smart identity card supports both online and offline authentication modes, enabling secure identity verification even in environments with limited network connectivity. By combining accessibility features with advanced security mechanisms, the smart card functions as a universal digital identity credential suitable for nationwide deployment.

F. System Workflow

The operational workflow of the proposed framework begins with the acquisition of multi-modal biometric information from users. Both conventional and alternative biometric characteristics are collected to ensure inclusive enrolment. The extracted biometric features are subsequently encoded into quantum states using the quantum state encoding layer. Once encoded, the biometric information is stored within the secure identity repository and processed through Grover-based quantum search algorithms for efficient matching, retrieval, insertion, and updating of records. Identity verification requests are authenticated using lattice-based cryptographic protocols and quantum-safe

digital signatures. Secure communication between system entities is established through Quantum Key Distribution mechanisms. Finally, authenticated users access services through the Braille-enabled smart identity card, which facilitates secure verification while ensuring accessibility for individuals with disabilities. The complete workflow enables a secure, scalable, and inclusive identity management ecosystem capable of operating effectively in the emerging quantum computing era.

IV. RESULTS AND DISCUSSION

A. Performance Analysis

The proposed Quantum-Resilient Inclusive Biometric Framework demonstrates significant improvements in biometric authentication efficiency, accuracy, and robustness. By employing Grover-based quantum search mechanisms, the framework achieves a quadratic reduction in search complexity compared to conventional biometric matching approaches. This improvement enables efficient processing of large-scale biometric repositories typically associated with national identity systems. The quantum search mechanism substantially reduces authentication latency while maintaining high matching accuracy. The incorporation of multi-modal biometric authentication further enhances system reliability. Unlike traditional systems that rely exclusively on fingerprints, iris patterns, or facial recognition, the proposed framework integrates multiple biometric modalities, including voice, gait, and behavioural characteristics. This multi-layered approach improves recognition accuracy and minimizes false acceptance and false rejection rates. Furthermore, the utilization of synthetic biometric datasets generated through artificial intelligence techniques increases the diversity of training samples and improves the system's ability to generalize across different demographic and physiological conditions. Consequently, the framework exhibits improved resilience when processing noisy, incomplete, or atypical biometric data.

B. Security Evaluation

The security performance of the proposed framework was evaluated against both classical and quantum attack models. Conventional public-key cryptographic algorithms such as RSA and Elliptic Curve Cryptography are known to be vulnerable to quantum attacks, particularly those based on Shor's algorithm. To address this limitation, the proposed framework employs lattice-based post-quantum cryptographic schemes and quantum-safe digital signatures. These cryptographic mechanisms provide strong resistance against quantum-enabled adversaries while maintaining computational feasibility for large-scale deployment. In addition, the framework incorporates Quantum Key Distribution (QKD) to secure communication channels between authentication devices and identity management servers. QKD ensures that any eavesdropping attempt introduces detectable disturbances in quantum states, thereby providing information-theoretic security during key exchange. The implementation of post-quantum cryptographic primitives, together with QKD, significantly reduces the vulnerability of the system to future quantum attacks. Security analysis indicates that the proposed framework effectively mitigates risks associated with brute-force attacks, key recovery attacks, replay attacks, and identity impersonation attempts.

C. Accessibility Improvements

One of the primary contributions of the proposed framework is its emphasis on inclusive biometric authentication. Existing biometric systems often fail to accommodate individuals with missing fingerprints, damaged biometric features, visual impairments, or atypical physiological characteristics. Such

limitations can lead to authentication failures and exclusion from digital identity services. To overcome these challenges, the proposed framework supports alternative biometric modalities, including voice recognition, gait analysis, facial dynamics, and behavioural biometrics. These modalities provide multiple authentication pathways and reduce dependence on any single biometric characteristic. Furthermore, the integration of Braille-assisted verification mechanisms within the smart identity card infrastructure enables visually impaired individuals to independently authenticate themselves. The proposed design therefore promotes universal accessibility and ensures broader participation in national digital identity programs. The inclusive architecture contributes significantly to reducing enrolment failures and authentication errors among differently abled users.

D. Scalability Analysis

Scalability is a critical requirement for modern national identity systems, particularly those serving populations comprising hundreds of millions of users. The proposed framework addresses this requirement through the integration of quantum-enhanced search algorithms and distributed authentication mechanisms. The use of Grover-based search significantly reduces computational overhead during biometric matching, enabling efficient operation even as the size of the biometric database increases. The architecture further supports chip-enabled smart identity cards capable of performing secure local authentication and encrypted identity verification. This distributed approach reduces dependency on centralized infrastructure and minimizes network congestion during authentication requests. Consequently, the framework can support large-scale deployments while maintaining low response times and high system throughput. The results indicate that the proposed framework is capable of meeting future scalability requirements associated with population growth, increased enrolment rates, and expanding digital service ecosystems.

E. Discussion

The results demonstrate that the proposed Quantum-Resilient Inclusive Biometric Framework successfully addresses three critical challenges associated with next-generation digital identity systems: security, inclusivity, and scalability. The integration of quantum search algorithms improves authentication efficiency, while post-quantum cryptographic mechanisms provide resilience against emerging quantum threats. Simultaneously, the incorporation of alternative biometric modalities and accessibility-oriented verification methods ensures equitable access for individuals with diverse physical and physiological characteristics. Overall, the proposed framework represents a comprehensive and future-ready solution for national digital identity infrastructures. By combining quantum computing principles, post-quantum security mechanisms, and inclusive biometric technologies, the framework establishes a foundation for secure, scalable, and universally accessible identity management systems capable of operating effectively in the forthcoming quantum era.

V. CONCLUSION

This paper presented a Quantum-Resilient Inclusive Biometric Framework designed to address the major limitations of existing national digital identity systems, including accessibility constraints, scalability challenges, and vulnerabilities to emerging quantum computing threats. The proposed framework integrates multi-modal biometric authentication, quantum state encoding, Grover-based quantum search, post-quantum cryptographic mechanisms, and Braille-enabled smart identity cards within a unified architecture.

The adoption of alternative biometric modalities enables inclusive authentication for individuals with physical disabilities, visual impairments, damaged biometric traits, and atypical physiological characteristics. The utilization of quantum-enhanced search techniques significantly improves biometric matching efficiency, making the framework suitable for large-scale national identity repositories. Furthermore, the incorporation of lattice-based cryptography, quantum-safe digital signatures, and Quantum Key Distribution (QKD) provides robust protection against both classical and quantum adversaries.

Overall, the proposed framework offers a secure, scalable, and accessible identity management solution capable of supporting future national digital identity infrastructures. By combining quantum computing principles with inclusive biometric technologies, the framework establishes a foundation for next-generation identity systems that can effectively address evolving cybersecurity and accessibility requirements in the quantum era.

VI. FUTURE SCOPE

Several research directions may be explored to further enhance the proposed framework. Future work may focus on the implementation and validation of the framework on real quantum computing platforms and quantum communication networks. Integration with existing national identity infrastructures, such as Aadhaar, can facilitate seamless enrolment, authentication, and updating of biometric information while maintaining quantum-resilient security.

The proposed smart identity card architecture can also be extended to support passport services, immigration management, and cross-border identity verification, thereby reducing verification time and administrative overhead. Additionally, the incorporation of advanced Quantum Machine Learning (QML) techniques and Quantum Neural Networks (QNNs) may further improve biometric recognition accuracy and adaptive authentication capabilities.

Another promising direction involves the development of interoperable global digital identity ecosystems, where secure identity credentials can be verified across different countries and service providers while preserving privacy and regulatory compliance. Such advancements would contribute toward the realization of a universally accessible, quantum-secure, and globally interoperable digital identity infrastructure.

REFERENCES

[1] National digital identity systems - https://en.wikipedia.org/wiki/National_digital_identity_systems
[2] RSA Algorithm - https://www.geeksforgeeks.org/computer-networks/rsa-algorithm-cryptography/
[3] Elliptic Curve Cryptography - https://www.geeksforgeeks.org/ethical-hacking/blockchain-elliptic-curve-cryptography/
[4] Lattice-based Cryptography - https://en.wikipedia.org/wiki/Lattice-based_cryptography
[5] Quantum Key Distribution (QKD) - https://www.geeksforgeeks.org/computer-networks/quantum-key-distribution-qkd/
[6] Rishabh Garg, "A Technological Approach to Address Deficiencies in UID (AADHAAR)", 3rd International Conference on Big Data, Blockchain and Security, Copenhagen, Denmark, 23-24 April 2022.
[7] Velpula Ravindra Reddy et. al, "A Quantum Inspired Framework for Secure and Optimal Path Selection in Wireless Sensor Networks using QKD and Grover's Algorithm", International Journal of Engineering Sciences & Research Technology, 15(2): February 2026, ISSN (Online): 2277-9655.

[8] Emmanuel Igba et. al, "Synthetic Data Generation Using Generative AI to Combat Identity Fraud and Enhance Global Financial Cybersecurity Frameworks", International Journal of Scientific Research and Modern Technology (IJSRMT) Volume 4, Issue 2, 2025, DOI: https://doi.org/10.5281/zenodo.14928919.