NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Special Issue – 1, 2024
E – ISSN – 2583-7559

Zero-Knowledge Proof Approach for DNA STR Profile Security using Blockchain: A Framework for Enhancing Genetic Privacy

Arunkumar P
Research Associate,
Department of Computer Science and Engineering,
National Institute of Technology, Puducherry

Suresh S
Assistant Professor,
Department of Computer Science,
Banaras Hindu University, Varanasi

Surendiran B
Associate Professor,
Department of Computer Science and Engineering,
National Institute of Technology, Puducherry

V Sankaranarayanan
Sr. Analyst/Sr. Scientist,
Forensic Science Laboratory,
Government of Puducherry, Puducherry

***Abstract* — Genetic research has significantly advanced with the utilization of DNA Short Tandem Repeat (STR) profiling, playing a pivotal role in forensic investigations and medical studies. However, the surge in genetic data usage has sparked concerns about the privacy and security of individuals' genetic information. In response to these challenges, this paper introduces a pioneering framework that integrates zero-knowledge proofs and blockchain technology to enhance the security of DNA STR profiles. The primary objective of this study is to establish a secure and privacy-preserving environment for the comprehensive management of DNA STR profiles. The proposed framework combines the cryptographic guarantees of zero-knowledge proofs with the decentralized and tamper-resistant nature of blockchain technology to enable secure transactions involving DNA STR profiles. This cryptographic technique allows parties to validate the authenticity of information without exposing the actual data, ensuring privacy during data interactions. Blockchain technology is leveraged for the creation of a decentralized and distributed ledger that stores DNA STR profiles for tamper proofing. Smart contracts play a crucial role in enforcing security policies within the blockchain network. These contracts automate the execution of predefined rules, such as access control and data sharing permissions. Additionally, a consensus mechanism is implemented within the blockchain network to ensure agreement among network participants on the validity of transactions. A detailed pseudo algorithm is introduced in the research paper, outlining the step-by-step processes involved in securing DNA STR profiles using zero-knowledge proofs and blockchain. The proposed framework not only addresses current challenges in genetic privacy but also establishes a foundation for the future development of secure genetic databases.**

Keywords—Genetic Privacy, DNA STR Profiling, Zero-Knowledge Proofs, Blockchain Security, Cryptographic Privacy in Genetic Data

I. Introduction

In the era of advanced genetic research, the utilization of DNA Short Tandem Repeat (STR) profiling has emerged as a cornerstone in various domains, ranging from forensic investigations to medical studies. The intricate nature of genetic data, particularly DNA STR profiles, has underscored the need for robust security measures to safeguard individuals' privacy. As the volume and significance of genetic information continue to surge, concerns regarding unauthorized access, data tampering, and overall security breaches have become paramount.

To address these pressing challenges, this research introduces an innovative framework that strategically merges two cutting-edge technologies: zero-knowledge proofs and blockchain. The primary aim is to elevate the security of DNA STR profiles, ensuring not only their confidentiality but also the integrity of genetic information. This endeavor becomes increasingly critical as genetic data evolves into a fundamental asset for scientific research, personalized medicine, and criminal investigations.

A. Objective of the Study

The central objective of this study is to establish a secure and privacy-centric environment for the comprehensive management of DNA STR profiles. With the proliferation of genetic data across diverse domains, the imperative to fortify privacy measures has become indispensable. The proposed framework operates at the intersection of cryptographic privacy and the decentralized, tamper-resistant attributes of blockchain technology, presenting a holistic solution to the security conundrum associated with genetic information.

B. *Key Components of the Framework*

The framework is anchored in four key components, each contributing to the overarching goal of fortifying DNA STR profile security:

1) Zero-Knowledge Proof Integration: This component harnesses the cryptographic prowess of zero-knowledge proofs to facilitate secure transactions involving DNA STR profiles. Zero-knowledge proofs empower parties to validate the authenticity of genetic information without exposing the actual data, thereby preserving the privacy of individuals during data interactions.

2) Blockchain-based Storage: Leveraging the decentralized and tamper-resistant characteristics of blockchain, the framework establishes a distributed ledger for the storage of DNA STR profiles. This not only ensures transparency and accountability but also bolsters the immutability of genetic data, safeguarding it against tampering and unauthorized access.

3) Smart Contracts for Security Policies: Smart contracts are introduced to automate and enforce security policies within the blockchain network [1]. By embedding predefined rules related to access control and data sharing permissions, these contracts act as vigilant guardians, permitting only authorized entities to interact with genetic data.

4) Consensus Mechanism: Ensuring the integrity of genetic information, a consensus mechanism is employed within the blockchain network [2]. This mechanism fosters agreement among network participants regarding the validity of transactions, thwarting potential malicious activities and preserving the overall security of DNA STR profiles.

In the subsequent sections, the research provides a detailed pseudo algorithm, outlining the intricacies of securing DNA STR profiles using zero-knowledge proofs and blockchain. Covering a spectrum of processes – from user registration to termination procedures – the algorithm serves as a comprehensive guide to the secure management of genetic data within the proposed framework.

In conclusion, this research sets forth a pioneering approach to fortify the security of DNA STR profiles, ensuring a harmonious coexistence of cryptographic privacy and blockchain transparency. The framework not only addresses the prevailing challenges in genetic privacy but also lays a robust foundation for the future development of secure genetic databases. As the research progresses toward implementation, it is poised to make significant contributions to the evolving landscape of genetic data security, establishing new benchmarks for privacy and integrity in genetic research and forensic applications.

II. RELATED STUDY

The work [3] discusses various issues related to cybersecurity and privacy in the context of DNA sequencing, genomic data sharing, and bioinformatics. It highlights vulnerabilities and potential cyber-attacks in bioinformatics tools and genomic databases, emphasizing the need for better security measures. The article also introduces the concept of cyberbiosecurity and proposes methods to protect sensitive genomic data. The study includes a software security analysis of open-source bioinformatics tools and databases, identifying common vulnerabilities.

The research paper [4] discusses the benefits and privacy concerns of sharing genetic data, the challenges and risks associated with sharing genetic data, the importance of adaptability in federal regulations for sensitive data, the implications of genetic data privacy regulations in the United States, the need for more protection of patient and consumer genetic data, the privacy concerns surrounding the collection, storage, and sharing of genetic data, the impact of the General Data Protection Regulation (GDPR) on data privacy, and the Genetic Information Non-discrimination Act of 2008 (GINA) and other laws protecting genetic privacy.

The authors in their work [5] explores the concept of relational privacy in the context of genetic data and the right to privacy. It discusses the challenges of applying a relational model of privacy within the existing human rights framework and the implications for non-consenting members of a biological group. The article suggests that a relational model of privacy could address individualistic framing, group impacts, and networked privacy harms. However, practical concerns and compatibility with existing laws, such as the GDPR, are also discussed.

The research paper [6] discusses the challenges and solutions for maintaining privacy in genomic data sharing. It covers various privacy attacks, auxiliary information used by adversaries, and popular direct-to-consumer genetic testing companies. The paper also provides an overview of privacy-preserving techniques such as data security, encryption, secure computation, data anonymization, and differential privacy. It emphasizes the importance of protecting genetic data and the need for advancements in privacy protection methods and regulations

The contribution of authors [7] discusses the challenges and solutions related to privacy protection in the field of genomic data. It covers topics such as re-identification experiments, privacy-preserving computation, secure genome matching, differential privacy, information leaks in genome-wide association studies, and more. The work highlights the need for privacy protection in genomic testing and data alignment processes and proposes solutions using encryption, secure computation protocols, and privacy-preserving algorithms. It also addresses the challenges in secure storage, sharing, and querying of genomic data.

The paper [8] discusses a privacy-preserving method called Varlock for masking and unmasking alleles in genomic data. The method allows for the secure storage and sharing of sequenced genomic data while protecting sensitive information. The study validates the effectiveness of Varlock using publicly available population data and clinical exomes.

The paper [9] covers various topics related to genetics, genomics, privacy, and data protection. It discusses genetic testing, data privacy, machine learning, and the use of genomic data in research. It also addresses regulations and ethical considerations related to genetic information.

The article [10] discusses the susceptibility of existing privacy protection models for genomic data to re-identification methods. It calls for the development of more robust protection strategies and highlights the need for formal anonymity protection schemas. The research concludes that current methods do not guarantee the protection of data subjects' identities and suggests directions for future research in genomic data privacy protection.

This contribution [11] discusses the challenges and approaches to protecting privacy in genomic data sharing. It covers various methods such as data perturbation, cryptographic protections, and legal protections. The lack of a national*(i)*data privacy policy in the United States is highlighted, along with the implications for the use of genomic data in research and non-research settings. The text also discusses privacy and security concerns related to genomic data sharing, potential attacks and protections against them, and the legal and regulatory aspects of genomic privacy. Additionally, it provides comprehensive lists of references and resources related to privacy in genomic data sharing.

The authors here [12] discusses the complexities of considering biological family members as data subjects under the European data protection framework, particularly in the context of processing genetic data. It explores the challenges and potential conflicts that may arise when biological family members exercise their data subject rights, such as the right to information, access, erasure, and restriction of processing. The passage also highlights the difficulties in balancing the competing interests of different stakeholders and suggests the need for the European Data Protection Board (EDPB) to provide guidance and updated guidelines on genetic data processing.

III. Conceptual Framework

In the ever-expanding landscape of genetic data security, the conceptual framework introduces two pivotal elements: Blockchain Technology and its integration with Zero-Knowledge Proofs. This synergy aims to establish an immutable and decentralized ledger for securely storing DNA Short Tandem Repeat (STR) profiles. The first layer of the proposed framework focuses on the encryption and decryption of DNA STR profiles using zero-knowledge proofs. This cryptographic technique allows entities to prove knowledge of specific genetic information without revealing the actual sequence. In the realm of genetic data security, zero-knowledge proofs emerge as a powerful cryptographic tool, offering a groundbreaking approach to enable verification of genetic information without divulging the actual DNA sequence. This conceptual framework is rooted in the fundamental principle of zero-knowledge proofs, which allows one party, known as the prover, to convince another party, the verifier, of the truth of a statement without revealing any information about the statement itself.

A. *Zero Knowledge Proof*

Zero-knowledge proofs operate on the concept of demonstrating knowledge of a particular piece of information without disclosing the information itself [13]. In the context of genetic information verification, this means that an entity can prove the accuracy or authenticity of genetic data without revealing the specific DNA sequence. This cryptographic technique ensures that sensitive genetic information remains confidential, addressing the growing concerns related to genetic privacy.

1) *Key Components and Mechanisms*

- Cryptographic Commitments: To initiate the zero-knowledge proof process, a cryptographic commitment is established. The prover commits to a specific genetic statement without revealing its content. This commitment is analogus to sealing information in a secure envelope.

- Challenges and Responses: The verifier then presents challenges to the prover, seeking proof of knowledge regarding the genetic information. The prover responds to these challenges, providing evidence of possessing the required knowledge.

- Verifiable Consistency: Through a series of interactions, the prover convinces the verifier that they possess the accurate genetic information without disclosing the actual DNA sequence. The process ensures verifiable consistency without compromising the confidentiality of the underlying data.

2) *Application to Genetic Data*

In the specific context of genetic information verification, zero-knowledge proofs can be applied to authenticate the accuracy of DNA STR profiles. The prover, often an individual or a system holding genetic data, aims to prove the validity of the DNA sequence without exposing the sequence itself. This is particularly relevant in scenarios such as medical research, where researchers may need to validate the authenticity of genetic information without compromising individual privacy.

3) *Benefits and Implications*

The following are the benefit of Zero Knowledge Proof implementation.

- Enhanced Privacy: Zero-knowledge proofs provide a robust solution for enhancing privacy in genetic data transactions. Individuals can share genetic information for research or diagnostic purposes without exposing the intricacies of their DNA sequences.

- Secure Data Interactions: The framework ensures secure interactions between entities, allowing genetic data to be verified for accuracy without the need to disclose the raw genetic information. This is especially critical in environments where confidentiality is paramount.

- Compliance with Regulations: The application of zero-knowledge proofs aligns with evolving data protection regulations, addressing concerns related to informed consent and privacy rights in the genetic domain.

B. *An Immutable and Decentralized Ledger for DNA STR Profiles using Block Chain*

Blockchain, originally designed as the foundational technology for cryptocurrencies, has transcended its initial purpose and found applications in various domains. In the context of genetic data security, blockchain serves as an immutable and decentralized ledger, providing a secure and transparent framework for storing DNA STR profiles.

Immutability: Each transaction or entry in the blockchain is cryptographically linked to the previous one, creating a chain of blocks. Once a block is added, it is nearly impossible to alter or delete the information within it [14]. This immutability ensures the integrity and authenticity of the stored DNA STR profiles.

Decentralization: Unlike traditional centralized databases, blockchain operates on a decentralized network of nodes. Each participant in the network has a copy of the entire blockchain, promoting transparency and eliminating the risk of a single point of failure [15]. This decentralized architecture enhances the security of DNA STR profiles by reducing vulnerability to unauthorized access.

Transparency and Traceability: The transparent nature of blockchain enables all participants to view the entire transaction history [16]. This transparency, coupled with cryptographic hashes and consensus mechanisms, ensures the traceability of every change made to DNA STR profiles, enhancing accountability and trust.

C. *Integration of Zero-Knowledge Proof with Blockchain Technology*

The integration of blockchain technology with Zero-Knowledge Proofs presents a formidable solution to privacy concerns associated with genetic data. Zero-Knowledge Proofs, as explained in the previous section, allow entities to verify genetic information without disclosing the actual DNA sequence. Here's how the integration unfolds:

Cryptographic Commitments on Blockchain: Genetic data, represented by DNA STR profiles, is cryptographically committed to the blockchain. This involves creating a secure and verifiable commitment to the information without revealing its content. The commitment is analogous to sealing the genetic data within a secure digital envelope.

Zero-Knowledge Proofs for Verification: When verification of genetic information is required, Zero-Knowledge Proofs come into play. The prover, holding the genetic data committed to the blockchain, can interact with the verifier using zero-knowledge proofs to substantiate the accuracy of the information without exposing the raw DNA sequence.

Smart Contracts for Automated Verification: Smart contracts, self-executing pieces of code within the blockchain, can automate the verification process. They define the rules and conditions under which genetic information can be accessed or verified. This not only ensures accuracy but also enforces predefined security policies.

Consensus Mechanism for Security: The consensus mechanism within the blockchain network plays a crucial role in maintaining security. It ensures that any changes or verifications made to DNA STR profiles are agreed upon by the majority of participants, preventing malicious activities and unauthorized alterations.

D. *Benefits and Implications of Integration*

Enhanced Security and Privacy: The integration of zero-knowledge proofs with blockchain establishes a secure and private framework for managing DNA STR profiles. It addresses concerns related to unauthorized access, tampering, and privacy breaches.

Transparent and Auditable Transactions: The transparent and auditable nature of blockchain transactions, coupled with zero-knowledge proofs, creates a robust system where the verification of genetic data can be conducted with transparency and accountability.

Decentralized Trust: The decentralized architecture of blockchain builds trust by eliminating single points of failure. This distributed trust ensures that DNA STR profiles remain secure, even in the absence of a central authority.

IV. PROPOSED FRAMEWORK

In order to address the critical challenges associated with genetic data security, the proposed framework introduces a comprehensive set of components, each playing a vital role in ensuring the confidentiality, integrity, and controlled access to DNA Short Tandem Repeat (STR) profiles. The below table Table 1. Represents the layers of the proposed framework and its key features and Operational Mechanisms.

TABLE I. MULTI-LAYERED SECURITY FRAMEWORK CONCEPTS

Layers	**Key Features**	**Operational Mechanisms**
Data Encryption and Decryption Layer	1. Proving Knowledge without Disclosure: Zero-knowledge proofs for proving possession of genetic information. 2. Two-Way Encryption: DNA STR profiles encrypted with zero-knowledge proofs. 3. Decryption with Authorization: Authorized entities decrypt DNA STR profiles using cryptographic keys.	1. Zero-knowledge proofs generate cryptographic evidence for possession of specific DNA STR profiles. 2. Two-way encryption renders profiles unreadable without cryptographic keys. 3. Authorized entities decrypt using cryptographic keys and zero-knowledge proofs.
Block Chain Storage Layer	1. Immutable Transactions: DNA STR profiles recorded as immutable transactions. 2. Distributed Storage: Profiles distributed across blockchain nodes. 3. Cryptographic Hashing: Cryptographic hashes link blocks for secure connections.	1. DNA STR profiles recorded as immutable transactions on the blockchain. 2. Distribution across multiple nodes prevents single points of failure. 3. Cryptographic hashes secure and link blocks for transparency and integrity.
Smart Contract and Access Control Layer	1. Access Control Rules: Smart contracts define rules for accessing genetic data. 2. Automated Execution: Smart contracts automatically execute actions based on access control conditions. 3. Auditability: Transparent smart contracts allow easy auditing.	1. Smart contracts define rules and conditions for accessing genetic data. 2. Automated execution ensures access control based on predefined conditions. 3. Transparent nature allows for easy auditing of access control actions.
Consensus Mechanism Layer	1. Secure Validation: Validators chosen for block creation based on cryptocurrency holdings. 2. Reduced Energy Consumption: PoS known for energy efficiency compared to PoW. 3. Incentive for Honest Behavior: Validators incentivized to act honestly for financial gain.	1. Validators selected based on cryptocurrency holdings and willingness to stake. 2. PoS offers energy-efficient alternative to traditional PoW mechanisms. 3. Financial incentives drive validators to act honestly and secure the network.

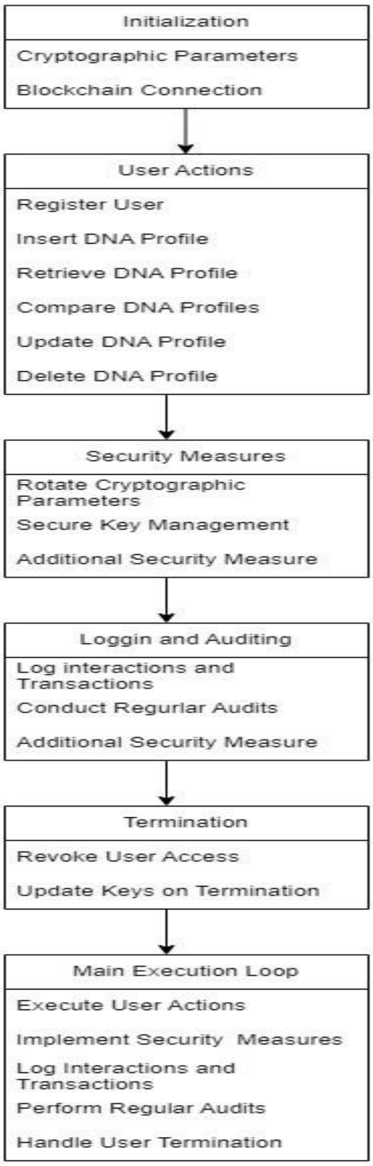

Fig. 1. DNA STR Profile Security Framework Flowchart

The proposed framework presents an integrated approach to genetic data security, leveraging the strengths of zero-knowledge proofs and blockchain technology. By combining cryptographic privacy with decentralized and transparent storage, the framework addresses the challenges of genetic data confidentiality, integrity, and controlled access. As we delve into the subsequent sections of this paper, we will explore the detailed algorithms, implementation strategies, and potential implications of deploying this framework in real- world scenarios.

The Fig. 1 reprsents the diagrammatic view of the proposed Multi layered Security mechanism.

V. NOVEL ALGORITHM

In this section, we present the pseudocode for the security procedures for DNA STR profile system. The proposed Algorithm outlines the key steps involved in user registration, record insertion, retrieval, comparison, and various security measures. The algorithm is designed to safeguard DNA profiles using a combination of cryptographic techniques and zero-knowledge proofs. For better understanding the proposed algorithm is explained in parts.

```
# Initialization
Initialize cryptographic parameters
Establish a secure blockchain connection
```

This section covers the initialization of cryptographic parameters and the establishment of a secure connection to the blockchain network.

```
# User Registration
Function register_user():
    private_key, public_key = generate_key_pair()
    store_user_keys_in_database(user_id, private_key,
public_key)
    create_blockchain_account(user_id, public_key)
```

In the user registration section, a user-specific key pair is generated, stored in the database, and an account for the user is created on the blockchain.

```
# Record Insertion
Function insert_dna_str_profile(user_id, dna_profile):
    encrypted_profile = encrypt_dna_profile(dna_profile,
user_public_key)
    proof_insertion =
generate_zkp_proof_insertion(dna_profile, encrypted_profile,
user_private_key)
    add_data_to_blockchain(user_id, encrypted_profile,
proof_insertion)
```

This section describes the process of inserting a DNA STR profile into the system. The DNA profile is encrypted, a zero-knowledge proof is generated, and both are stored on the blockchain

# Record Retrieval

```
Function retrieve_dna_str_profile(user_id):
    encrypted_profile, proof_retrieval = retrieve_data_from_blockchain(user_id)
    verify_zkp_proof_retrieval(encrypted_profile, proof_retrieval, user_public_key)
```

The retrieval section explains how to retrieve a DNA STR profile from the blockchain, verify the zero-knowledge proof, and use the retrieved data

# Record Comparison

```
Function compare_dna_str_profiles(user_id1, user_id2):
    encrypted_profile1, proof_comparison1 = retrieve_data_from_blockchain(user_id1)
    encrypted_profile2, proof_comparison2 = retrieve_data_from_blockchain(user_id2)
verify_zkp_proof_comparison(encrypted_profile1, encrypted_profile2, proof_comparison1, proof_comparison2)
```

This section details the comparison of two DNA STR profiles stored on the blockchain. It retrieves the data and verifies zero-knowledge proofs for the comparison.

# Proof Verification

```
Function verify_zkp_proof_insertion(dna_profile, encrypted_profile, private_key):
Function verify_zkp_proof_retrieval(encrypted_profile, proof_retrieval, public_key):
Function verify_zkp_proof_comparison(encrypted_profile1, encrypted_profile2, proof_comparison1, proof_comparison2):
```

This section includes functions for verifying zero-knowledge proofs associated with insertion, retrieval, and comparison.

# Updates and Deletions

```
Function update_dna_str_profile(user_id, new_dna_profile):
    encrypted_profile = encrypt_dna_profile(new_dna_profile, user_public_key)
    proof_update = generate_zkp_proof_update(new_dna_profile, encrypted_profile, user_private_key)
    update_data_on_blockchain(user_id, encrypted_profile, proof_update)
Function delete_dna_str_profile(user_id):
    proof_deletion = generate_zkp_proof_deletion(user_private_key)
    delete_data_from_blockchain(user_id, proof_deletion)
```

This section introduces functions for updating and deleting DNA STR profiles on the blockchain.

# Security Measures

```
Function rotate_cryptographic_parameters():
Function secure_key_management():
Function additional_security_measures():
# Logging and Auditing
Function log_interactions_and_transactions():
Function conduct_regular_audits():
```

This section outlines security measures to enhance the overall system security. Functions for rotating cryptographic parameters, implementing secure key management practices, and additional security measures are included.

# Termination

```
Function terminate_user(user_id):
    revoke_user_access(user_id)
    update_keys_on_termination(user_id)
```

This section provides a function for terminating a user's access. It revokes the user's access and updates keys associated with the terminated user.

# Main Execution

```
If __name__ == "__main__":
    register_user()
    insert_dna_str_profile(user_id, dna_profile)
    retrieve_dna_str_profile(user_id)
    compare_dna_str_profiles(user_id1, user_id2)
    update_dna_str_profile(user_id, new_dna_profile)
    delete_dna_str_profile(user_id)
    rotate_cryptographic_parameters()
    secure_key_management()
    additional_security_measures()
    log_interactions_and_transactions()
    conduct_regular_audits()
    terminate_user(user_id)
```

The main execution section checks whether the script is being run as the main program. If so, it executes a sequence of tasks, including user registration, profile insertion, retrieval, comparison, updates, deletions, security measures, logging, audits, and user termination

VI. Discussion

This section discuss about the potential advantages, limitations and challenges of the proposed framework.

A. *Advantages of the Proposed Framework*

The presented framework for DNA STR profile security offers several advantages. Firstly, the integration of zero-knowledge proofs ensures that sensitive genetic information remains confidential during interactions. The cryptographic techniques utilized allow entities to prove knowledge of specific

DNA STR profiles without disclosing the actual sequence, enhancing user privacy. Additionally, the use of blockchain as a decentralized and immutable ledger enhances the security and transparency of genetic data. Immutable transactions and distributed storage across multiple nodes in the blockchain network prevent tampering and provide resilience against single points of failure.

B. *Limitations and Potential Challenges*

While the proposed framework is robust, it is essential to acknowledge its limitations and potential challenges. One challenge involves the computational overhead associated with zero-knowledge proofs, which may impact system performance. Balancing the trade-off between enhanced security and computational efficiency will be crucial. Moreover, ensuring widespread adoption of blockchain technology within the genetic data ecosystem may face resistance and regulatory hurdles. Standardizing protocols for interoperability and addressing legal and ethical concerns will be critical for the framework's successful implementation.

VII. Conclusion

In conclusion, the presented framework for DNA STR profile security, integrating zero-knowledge proofs and blockchain technology, makes significant strides in addressing key challenges in genetic data protection. The framework's key contributions lie in its ability to ensure confidentiality through zero-knowledge proofs, allowing secure verification without revealing the actual genetic sequence. Leveraging blockchain provides an immutable and decentralized storage solution, reinforcing the integrity and transparency of DNA STR profiles. The potential impact of this framework on genetic privacy is substantial, offering a robust and privacy-preserving infrastructure for storing and managing genetic data. By emphasizing access control, tamper resistance, and user-centric privacy measures, the proposed framework lays the foundation for a more secure and privacy-enhanced landscape in genetic data management.

Acknowledgment

The authors express their gratitude to Directorate of Forensic Science Services (DFSS), New Delhi for the EMR Project grant to conduct this study as part of funded project titled “Gene Databank for Forensic Investigation in India” .

References

[1] H. Taherdoost, “Smart Contracts in Blockchain Technology: A Critical Review,” Information, Feb. 13, 2023. https://doi.org/10.3390/info14020117

[2] S. X. Zhou, K. Li, X. Liu, J. Cai, W. Liang, and A. Castiglione, “A Systematic Review of Consensus Mechanisms in Blockchain,” *Mathematics*, May 11, 2023. https://doi.org/10.3390/math11102248

[3] S. Arshad, J. Arshad, M. M. Khan, and S. Parkinson, “Analysis of security and privacy challenges for DNA-genomics applications and databases,” Journal of Biomedical Informatics, vol. 119, p. 103815, Jul. 2021, doi: 10.1016/j.jbi.2021.103815.

[4] K. Harbord, “Genetic Data Privacy Solutions in the GDPR,” Texas A&M Law Review, vol. 7, no. 1, pp. 269–297, Oct. 2019, doi: 10.37419/lr.v7.i1.6.

[5] R. Á. Costello, “Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?,” Human Rights Law Review, vol. 22, no. 1, Jan. 2022, doi: 10.1093/hrlr/ngab031.

[6] L. Bonomi, Y. Huang, and L. Ohno-Machado, “Privacy challenges and research opportunities for genomic data sharing,” Nature Genetics, vol. 52, no. 7, pp. 646–654, Jun. 2020, doi: 10.1038/s41588-020-0651-0.

[7] M. Akgün, A. O. Bayrak, B. Ozer, and M. Ş. Sağıroğlu, “Privacy preserving processing of genomic data: A survey,” Journal of Biomedical Informatics, vol. 56, pp. 103–111, Aug. 2015, doi: 10.1016/j.jbi.2015.05.022.

[8] R. Hekel, J. Budis, M. Kucharik, J. Radvanszky, Z. Pös, and T. Szemes, “Privacy-preserving storage of sequenced genomic data,” BMC Genomics, vol. 22, no. 1, Oct. 2021, doi: 10.1186/s12864-021-07996-2.

[9] Marie Oestreich and Dingfan Chen, “Privacy considerations for sharing genomics data,” EXCLI Journal , vol. 20, Jul. 2021, doi: http://dx.doi.org/10.17179/excli2021-4002.

[10] B. A. Malin, “An Evaluation of the Current State of Genomic Data Privacy Protection Technology and a Roadmap for the Future,” Journal of the American Medical Informatics Association, vol. 12, no. 1, pp. 28–34, Oct. 2004, doi: 10.1197/jamia.m1603.

[11] Z. Wan, J. W. Hazel, E. W. Clayton, Y. Vorobeychik, M. Kantarcioglu, and B. A. Malin, “Sociotechnical safeguards for genomic data privacy,” Nature Reviews Genetics, vol. 23, no. 7, pp. 429–445, Mar. 2022, doi: 10.1038/s41576-022-00455-y.

[12] T. Kuru and I. de M. Beriain, “Your genetic data is my genetic data: Unveiling another enforcement issue of the GDPR,” Computer Law & Security Review, vol. 47, p. 105752, Nov. 2022, doi: 10.1016/j.clsr.2022.105752.

[13] P. Alikhani *et al.*, “Experimental relativistic zero-knowledge proofs,” *Nature*, Nov. 03, 2021. https://doi.org/10.1038/s41586-021-03998-y

[14] F. Hofmann, S. Wurster, E. Ron and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, Nanjing, China, 2017, pp. 1-8, doi: 10.23919/ITU-WT.2017.8247004.

[15] J. Zarrin, H. W. Phang, L. B. Saheer, and B. Zarrin, “Blockchain for decentralization of internet: prospects, trends, and challenges,” Cluster Computing, May 15, 2021. https://doi.org/10.1007/s10586-021-03301-8

[16] A. Badhwar, S. Islam, and C. S. L. Tan, “Exploring the potential of blockchain technology within the fashion and textile supply chain with a focus on traceability, transparency, and product authenticity: A systematic review,” Frontiers in blockchain, Feb. 20, 2023. https://doi.org/10.3389/fbloc.2023.1044723