A Qualitative Review of ZKP and Biometrics in DID Systems

Presented By: Sthembile Ntshangase

Other authors : Kedimotse Baruni, Harvest Ngobeni, Lesego Moatshe and Nomalisa Ndhlovu

02 December 2025

science, technology & innovation
Department:
Science, Technology and Innovation
REPUBLIC OF SOUTH AFRICA

CSIR
Touching lives through innovation
80th anniversary

Table of contents

Introduction

3

Importance of Protecting Data in the Current and Future Era

Problem Statement

5

Problem Statement

- Challenges of Centralized Identity
- Decentralized Identity Frameworks
- Zero-Knowledge Proofs for Privacy
- Biometric Authentication

Proposed Solution

7

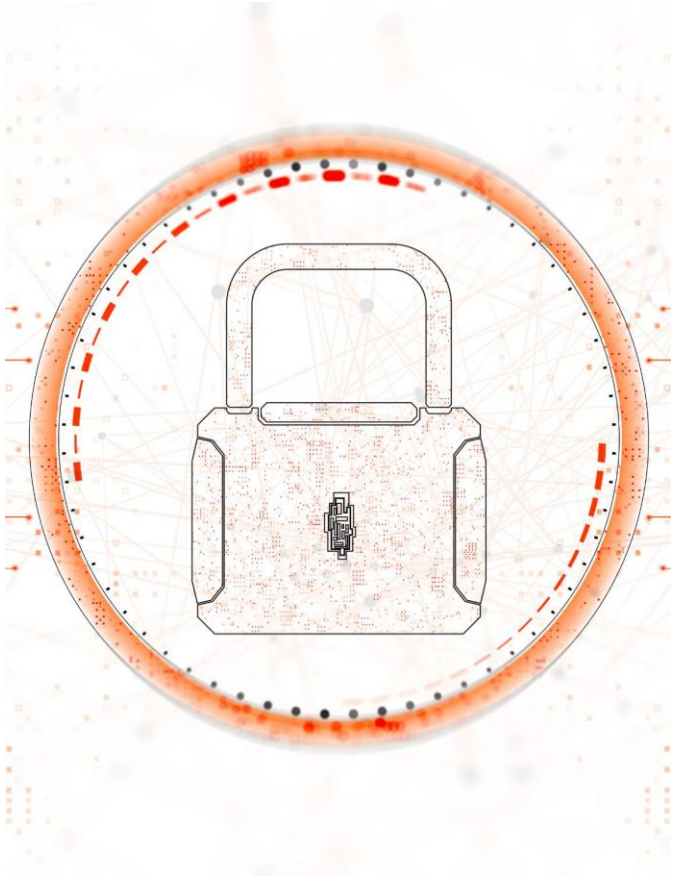
Solution

Integration of Advanced Technologies	• The system integrates decentralized identity, zero-knowledge proofs, and biometric authentication for secure identity management.
Research Objectives	• Designing a system architecture that enhances security and builds user trust through combined technologies.
Methodology and Validation	• Qualitative analysis and experimental validation are used to assess existing frameworks and the proposed model.
Expected Outcomes	• Anticipated benefits include stronger resistance to identity theft, enhanced privacy, and compliance with standards.

Existing Frameworks and Technologies

- Decentralized Identity Evolution
- Zero-Knowledge Proofs
- Biometric Authentication
- Integration Challenges

.



Methodology

10

Research Design and Approach

- Qualitative Research Approach
- System Architecture Design
- Data Collection Sources
- Evaluation and Iteration

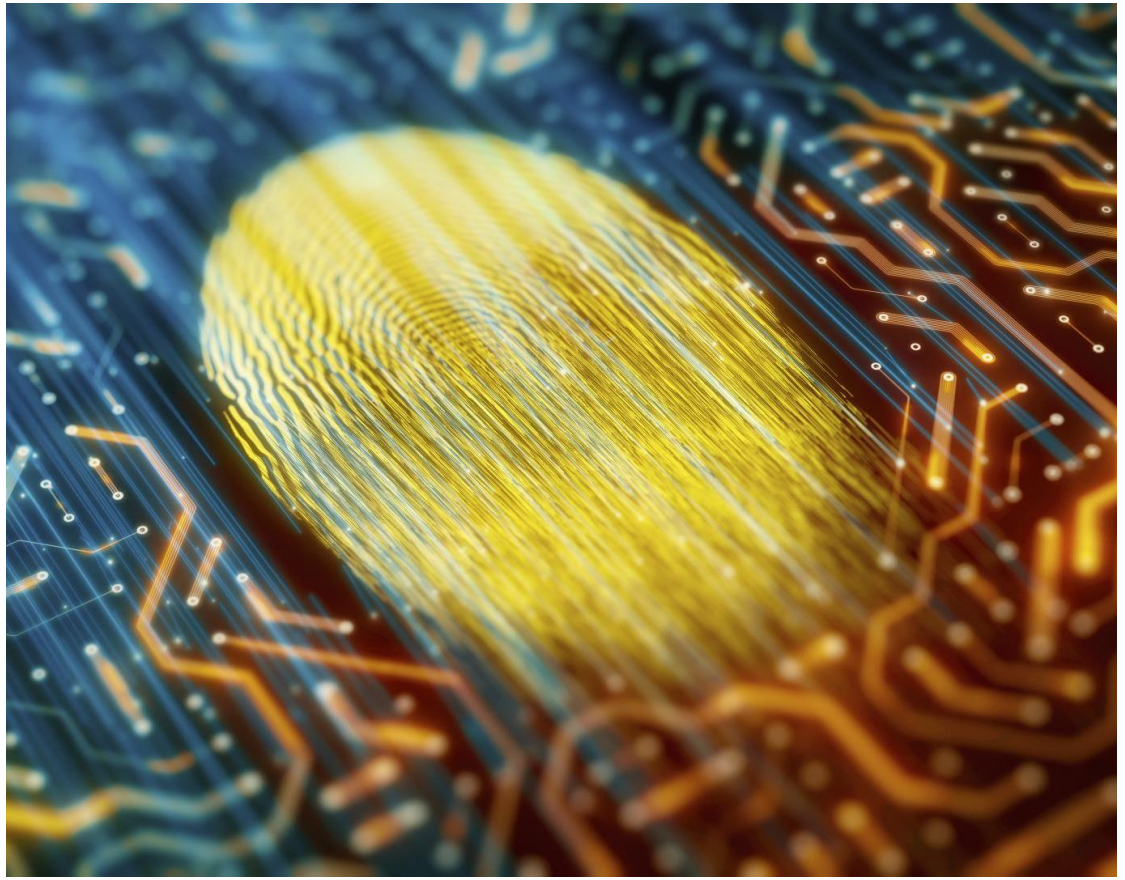
Results & Discussion

Results & Discussion

Methods	Problems Addressed	Application/Sectors	Regulations
ZKP-DID	Identity theft and fraud	Finance, Healthcare, Voting, Supply Chains	GDPR, KYC, AML
ZKP-DID	Privacy preservation	Healthcare, Education	GDPR
Bio-DID	Data breach risks, streamlined verification, user control & self-sovereignty	Identity Management Systems in Healthcare and Education	GDPR
ZKP-DID	Privacy preservation and scalability using zk-SNARKs	Finance (DeFi), Health, Governance & Public Services	Not specified
ZKP-DID	Privacy preservation, data breach risks, excessive data requests and misuse	Identity Management Systems	Novel three-party oversight ensuring complete regulatory coverage
ZKP-DID	Privacy preservation	Banking, Digital Identity Management, Healthcare	Not specified
BioZK-DID	Privacy preservation, security (Sybil attacks), scalability	Healthcare, Finance, E-commerce, Identity Management	Not specified
Bio-DID	Privacy preservation, security	Identity Management Systems	GDPR
BioZK-DID	Privacy preservation, security	e-Health	Not specified
ZKP-DID	Privacy preservation	Healthcare, Finance, Education	Not specified

Findings and Analysis

- Reviewed System Integration
- Enhanced Security and Privacy
- Challenges and Scalability
- Practical Applications



Recommendations

Future Enhancements and Applications

- Improving Protocol Efficiency
- Advanced Biometric Technologies
- Data Security and Privacy
- Practical tests, Interoperability and Applications

Conclusion

Summary and Implications

Research Contributions

The study highlights integrating decentralized identity, zero-knowledge proofs, and biometrics for secure identity management.

Addressing Challenges

This integration tackles vulnerabilities and data exposure issues in traditional centralized identity systems.

Broader Implications

The research impacts sectors needing robust identity verification, promoting secure and user-centric digital ecosystems.

Future Research Needs

Ongoing research is essential to refine identity systems amid evolving technology and regulations.

Thank you

Questions/Comments