Securing Individual's Identity using ZKP: Proposed System Architecture

Sthembile Ntshangase[1] , Kedimotse Baruni[2], Siphelele Myaka[3] and Oyena Mahlasela[4]

[1] The Counsil for Scientific and Industrial Research, 0001, Pretoria, South Africa,
[2] smlambo@csir.co.za, [3]kbaruni@csir.co.za,
[4]smyaka@csir.co.za, [5] omahlasela@csir.co.za

Abstract. Digital identity with biometrics is the future of how individuals will be identified in this digital era. Although there are current solutions that provide digital identity, the research reveals that traditional solutions lack security for biometric data, making them vulnerable to biometric data breaches, and data lost with difficulties to recover. This study discusses the importance of protecting our identities, as identity theft is increasing rapidly due to the rise of identity verification online. A comprehensive review on protecting identity using biometrics and Zero Knowledge Proofs has been conducted. A novel biometric system architecture based on Zero Knowledge Proofs has been proposed, ensuring that verification of an identity is performed without exposing biometric data. This architecture also includes a reference data engine for updating biometrics data in case of a breach, to improve security and overcome challenges faced by traditional biometric systems. The proposed architecture can be used to secure identities while preserving privacy.

Keywords: Identity, Security, Privacy, Biometrics, Zero Knowledge Proofs.

1 Introduction

Identity is a collection of unique characteristics that can be traced back and recorded or captured to distinguish and recognize individuals [1]. Identity can be authenticated using three factors: "*something a person knows*: a password or security question "*something a person has*: a token, smartcard, ID card, or cryptographic key, "*something a person is*: biometric data, such as a fingerprint or facial scan [2]. As compared to passwords and smart cards, biometric data is considered more secure as it cannot be misplaced or forgotten [3]. Biometric authentication uses unique biological characteristics like fingerprints, iris patterns, or facial features to verify identity [3]. However, it faces challenges like centralized storage, privacy concerns, data misuse, and lack of transparency due to proprietary algorithms and lack of scrutiny [4]. In addition, stolen biometric data can be challenging to recover [5]. These issues hinder its widespread use in access control, mobile devices, online authentication, and financial transactions.

Traditionally, individuals and organizations relied on conventional paper documents as a means of proving their identities, this practice is quickly becoming outdated due to technological improvements. People nowadays need to prove their identity remotely, online and digitally.

The issues surrounding identifying and verifying the identity of an individual or entity and organizations have gained significant attention from governments, organizations, and federal criminal units worldwide due to the persistent rise in identity theft and related crimes. Identity theft is a costly and widespread issue. The victim of the crime not only bears a heavy financial and psychological cost, but the organizations involved in the crime also suffer a financial blow [6]. Once an identity has been stolen, fraudsters can use it to access the victim's email accounts, open credit card accounts, perform transactions and apply for loans [7]. The victims of identity theft/fraud spend time recovering their identity.

There is a need for securely protecting each form of identity during identity capturing verification and identification to guard against identity theft. Security in digital identity helps maintain trust in the online system. Users are more likely to engage in digital services if they know their identities are secured and kept private.

The demand for security and privacy in managing digital identities has become critical in this digital world. The challenge of user security and privacy in identity authentication has thus been the subject of numerous works.

Hence, it's critical to ensure that identity is protected and secured when used online. This can be done by utilizing applications that offer enhanced identity information security and privacy [8]. This includes applications that encrypt sensitive data (identity information), use multi-factor authentication and secure protocols for data transfer and communication [8]. Cryptographic approaches such as homomorphic encryption [9], ring signature [10], secure multiparty computation [11], and Zero-Knowledge proof (ZKP) [12] are currently introduced in the identity field to solve those challenges. The first three methods cannot verify sufficient transactions/information without revealing sensitive information. ZKP is an interactive protocol that convinces a verifier that the prover possesses certain data without revealing any private information, including identities. It does not require a complex public key and repeated use does not help malicious users gain useful information [13]. ZKP can also be useful for anonymous identity verification applications such as voting, secure digital asset exchange, secure remote biometric authentication, and secure auctions [14].

In this work, presented is the proposed biometric system architecture that can be used to protect the identity of an individual using biometrics and ZKP. The overview of this work is as follows: Section 2 presents the background of this study with an emphasis on the importance of securing our identity, Section 3 presents a literature review for the related research works and market analysis based on biometrics and ZKP solutions, Section 4 presents the proposed system

architecture, towards a secure identity system. Section 5 represents the results and discussion, then Section 6 concludes the study.

2. Background

1.1 Authentication factors in identity

Identity authentication is the process of verifying and confirming the identity of an individual by providing unique information or data from different layers of identity. This unique information forms part of authentication factors which include passwords (what you know), tokens (what you have), ID badges (what you have), or biometric data (what you are). In digital and physical authentication, provided information is usually compared with what is known. For example, in physical authentication, the traffic officer can verify if you have a valid driver's license produced by the Department of Transport. With digital authentication, to access an online service, one will have to provide valid previously registered credentials. with stored data to verify the user's identity. This helps reduce fraud and adds security to data and information. Authentication is different from identification, which is explained in the next section [15].

Multi-factor authentication is a security method that grants access to a service or application after verifying identity with multiple factors. It protects systems against intruders, as traditional methods are vulnerable. Current systems use two-factor authentication, biometrics, or token devices, but require high-cost hardware equipment for small and medium companies [16].

1.2 Identification and Verification

Identification is a process where an identity claimer is determined if his/her identity exists and belongs to the claimer [17]. Three main parties are required, the claimer/owner of the identity, the identity and identifier system, which can be a tool or person. During the process of identification, a tool or person makes use of provided identity information to prove that the identity belongs to the claimer. The results indicate whether the claimer's identity was successfully identified or not. For example, identification using username, password and biometrics involves the process where a username, password and biometrics need to be previously linked and stored so that during the identification, these factors can be compared to what the user is providing. Corresponding username, password and biometrics are searched through a database, if this combination exists, it means the user is identified.

Identity verification is the process where an individual claims an identity, and that identity is compared to what is provided by the user to prove if the identity is for that person [3]. This process includes three parties,

owner/claimer, identity, and verifier (which can also be a person or a tool. For example, if using biometrics, ID card, and username, an individual can claim to be the owner of the username and ID card. The verification process will compare the biometrics of an individual, with the biometrics corresponding to the claimed ID card and username. If they match, it will mean the individual is successfully verified.

1.3 Biometrics

Biometrics is a technology used for identifying and controlling individuals based on their unique physical and behavioral characteristics, often under surveillance. Biometrics has by far proven to be an effective solution for many of the security challenges that are prevalent in most of the technical fields in this Digital era [18] The use of biometrics is increasing each day as modalities like faces, fingerprints, palm vein irises, hand geometry and voices are unique. This makes them an effectual blockade to cyber criminals trying to underhandedly impersonate individuals [2]. Generally, a biometrics system has two processes, first-time interaction with the system (registration), identification and verification. During registration biometric images are captured, processed, features get extracted and then stored in the database as a template. This template is then linked to an individual on the database. During verification or identification, biometric image is captured, processed, features get extracted and compared with the template that was stored during the registration.

1.4 ZKP

Zero Knowledge Proofs(ZKP) are mathematical techniques that verify information without revealing data, which makes this concept important of privacy and security of identifiable credentials and biometrics [12]. This concept is mostly used for enhancing technologies and cybersecurity, particularly in verifying the identity of individuals and protecting sensitive data on public services [14]. ZKPs can be used in the authentication and access control fields to ensure that sensitive information such as passwords, smart cards and biometrics is not revealed during verification and identification. This results in secure authentication techniques.

Biometrics and ZKP when used can protect user data and ensure privacy. Keyless, an information security organization, uses a Zero-Knowledge platform to verify users' identities without knowing their biometric template [19]. This system complies with regulations like GDPR and uses biometric templates for a unique hardware device. Mastercard, a biometric card company, uses ZKP to verify digital copies of biometric data without revealing the biometric data.

However, it does not change the issuer's ability to contest transactions if biometric authentication fails. Mastercard has joined a tech industry initiative called Fast Identity Online, which generates an encrypted passkey stored in a device and can only be accessed through biometrics [20]. The biometric

identification scheme (BIS) uses Zk-SNARK technology to reduce communication overheads and protect the fingerprint template from disclosure. The BIS framework explains the process of collecting fingerprints, extracting and processing features, and providing authentication results.

2 Literature Review

2.1 Current research works where ZKP and biometrics are used together

In this section, different current research works are discussed. This is to provide collective information that can assist organizations that are in the process of implementing ZKP-based systems. Details review of what has been done in this field can be found in the previous publication [21].

The work of Tagne *et al* [22] proposes a 3-factor authentication (namely password, smart card and biometrics) technique based on the concept of ZKP. This technique uses the concept of digital signature (DS) to authenticate the identity of the sender or the signer within a single communication. Since DS uses asymmetric encryption, a one-way hash of the user's identity is created and then signed using the private key.

Sarier proposed an identity management system for the smart industry using IoT, using ZKP protocol to protect biometric data during authentication [23]. This method prevents data transfer across connected devices and stores biometric data in a secure database during enrollment, ensuring no transmission during authentication or verification.

Liu. *et al*. presented a secure remote biometric-based authentication scheme using chaotic map Zero-Knowledge for crowdsourcing on the Internet of Things (IoT), [24]. Their approach allows the server to gateway node to remotely authenticate all authentication factors and participate in key agreements without transmitting or storing sensitive information. This scheme offers low computation and communication overheads, making it attractive for limited resources and battery power on devices. Liu. *et al.*, in the following years, also proposed a new ID-MAKA scheme for mobile cloud computing, which combines remote biometric-based authentication, single sign-on, and center-less authentication [25]. They designed a ZK-token based on Elliptic Curve Cryptography (ECC) and cryptographic hash function, introducing fuzzy extractor technology and ZKP technology into their scheme. This improves usability, scalability, and security compared to other existing solutions.

A light-weight biometric authentication method using ZKP and artificial intelligence was presented in [18]. This method operates based on binary representation of biometric instances, such as fingerprints and iris. The Support

Vector Machine and Multi-layer Perceptron Neural Network were chosen for fingerprint-based and iris-based authentication capabilities.

In [26] Hugde *et al*, proposed a multi-factor authentication scheme for vehicular cloud computing, using biometrics and ZKP for secure user identity authentication. This method provides good privacy preservation, prevents adversaries from tracing vehicles, and is cost-effective compared to similar existing schemes. Zhang *et al*. proposed BioP-TAP, an identity authentication protocol based on cancelable biometric and Physical Unclonable Function (PUF), which enables two-way authentication between users and servers [27] The method includes biometric template protection to preserve user privacy. Gaba *et al*. presented a novel mutual authentication method based on ZKP protocols, which uses key agreement protocol to ensure secure applications in IoT and critical healthcare [28]. The protocol withstands major security threats and offers anonymous and untraceable communication in public channels.

Mao *et al*. presented Biometric Authentication ZKP (BAZKP), an alternative biometric-based authentication method that combines biometric technology with a ZKP protocol to verify users while maintaining anonymity [29] BA-ZKP satisfies completeness, soundness, and Zero-Knowledge, and provides reliable and secure authentication. Guo *et al*. proposed a zero-knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARK) biometric identification scheme to address privacy protection against theft or loss of biometric data [30]. The proposed scheme reduces communication overhead and protects the fingerprint template from disclosure, making it a cost-effective and efficient solution for large-scale practical applications.

Song *et al*. studied ZKP of knowledge (ZKPoK), a zero-knowledge protocol that allows a prover to prove to a verifier without revealing any secret information [31] This method is not specifically used in biometrics. Alikhani *et al*. discussed an experimental zero-knowledge protocol with two separated verifier-prover pairs, ensuring security through special relativity [32]. This protocol works at short and long distances in about one second, demonstrating its practical potential for identification tasks and Blockchain applications like cryptocurrencies or smart contracts.

Presented in Table *1* is the summary of related works where ZKP and biometrics are used. This research shows that more research is still required to be done on how to protect biometrics data using ZKP. Most articles were considering fingerprints, and some the combination of both fingerprints and face or iris. Based on the research done, there is no architecture presented that can be applied in different systems to Incorporate the use of ZKP to protect biometrics data. Thus, the contribution of this paper is to look at the architecture of biometrics systems without using ZKP and propose a system architecture with the use of ZKP.

Table 1: Identified Studies on Biometrics and ZKP.

Ref	ZKP Protocol	Biometric/iDENTITY used	Application
[23] and [33]	ZKPoK protocol of Representation of Committed Value described in [34]	Fingerprints	Blockchain-based Identity Management System
[24]	ZKP proposed by Schnorr [35]	Fingerprints and face	Application of crowdsourcing Internet of Things
[25]	ZKP proposed by Schnorr [35]	Fingerprint and the face	Identity-based mutual authentication
[18]	Chaum-Pedersen protocol which is one of the interactive ZKP protocols [36]	Fingerprints and iris	Privacy-preserving biometrics fingerprint authentication scheme
[26]	Zero Knowledge protocol [37]	Not specified	Multi Factor Zero Knowledge Proof Authentication
[27]	ZKP proposed by Schnorr [35]	Face	Identity authentication protocol based on cancelable biometric and Physical Unclonable Function (PUF) namely BioP-TAP
[28]	Proposed a new protocol based on Zero Knowledge Proofs Protocol from [38] and [39]	Not specified	Internet of Healthcare applications (IoHA)

2.2 Traditional Biometrics System Architecture

Traditional systems for protecting identity lack security and privacy. Shown in **Fig. 1** is the traditional biometric system with four subsystems. The data acquisition subsystem, signal processing subsystem, data storage subsystem, and comparison subsystem are the four steps that make up the architecture of a biometric system. The primary function of the data acquisition subsystem is to record biometric information utilizing biometric sensors and scanners, like cameras or fingerprint scanners. After it has been obtained, the biometric data must be transferred from the data acquisition subsystem to the signal processing subsystem, leaving a gap that identity thieves could use to their advantage. The signal processing subsystem bears the responsibility of processing and obtaining pertinent features for use in the compilation of reference biometric data. Where in the composition of the reference data must be sent to the data storage subsystem to be used for comparison.

Nevertheless, biometric data storage devices are susceptible to damage, biometric tampering, and biometric theft. The reference and query biometric features are compared and matched by the biometric comparison subsystem, which then makes decisions depending on the outcomes of the matching. However, spoofing, replay, biometric tampering, and biometric data reuse make biometric data vulnerable during comparison. It indicates that the traditional biometric data architecture has shortcomings that could lead to identity theft

because there is a lack of data protection and privacy. ZKP can be integrated with a biometric system to guarantee data security and privacy.

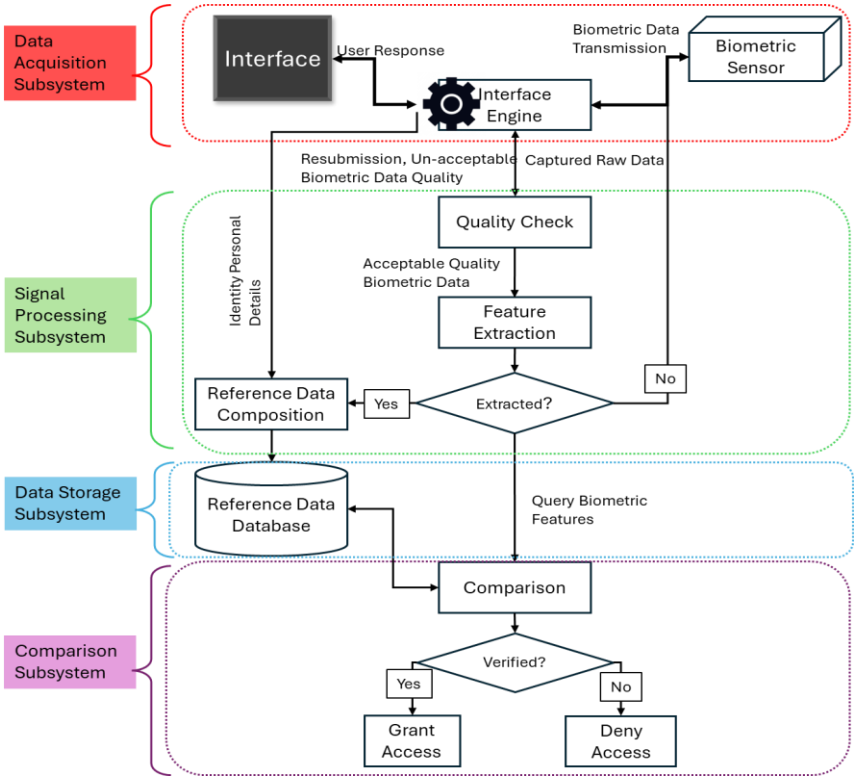

Fig. 1. Traditional Biometric System Architecture.

3 Proposed System Architecture of a Secure Identity using Biometrics and ZKP

This study focuses on using unique constant features of biometrics to protect and strengthen the identity of an individual and make use of ZKP to secure and preserve the privacy of identity. Biometrics are very linked to who we are, they act as an umbrella for our identity. ZKP also adds another layer of protection for our biometrics and identity. Without ZKP, our identity can be exposed to identity theft, misuse and unauthorized usage of identity after a data breach that can be difficult to control or fix.

The proposed architecture depends on capturing biometrics features and storing a challenge generated from these features, without revealing the exact values of features. This improves the security and privacy of biometrics data. Even in case of a data breach, the challenge can be updated using a different

pattern, for the same biometrics features, Instead of storing actual features, a challenge generated from extracted features is presented. To make this method even more secure, the challenge on the database is updated every time there is a successful verification. This means a new biometric-based challenge will be created and stored in the database by replacing the existing one.

This architecture is made of five subsystems, Data Acquisition Subsystem, Signal Processing Subsystem, ZKP-based feature Extraction, ZKP-Based Data Storage Subsystem and ZKP-Based Verification Subsystem, as illustrated in **Fig. 2**. The first subsystem is the same as in the traditional biometrics system. The Data Acquisition Subsystem captures biometric data from users using sensors to detect and record biometric traits like fingerprints, ear images, and faces, converting them into digital formats.

Signal Processing Subsystem involves quality check, normalization and data cleaning. Captured raw data must be assessed for quality before feature extraction to improve the extraction of accurate features. Various image quality assessment tools are available, such as the National Institute of Standards and Technology (NIST) Image Quality Checker for fingerprint biometrics data, NIST Fingerprint Image Quality (NFIQ) 2 for optical and ink fingerprint images, Face Analysis Technology Evaluation Quality performance scores for face and ear images, and specific libraries like OpenBR and OpenCV for face image quality. The Iris Image Quality Assessment framework is commonly used for iris recognition quality assessment, evaluating factors like focus, pupil dilation, and image resolution [40].

ZKP-Based Feature Extraction involves the process of extracting features from biometric images of good quality. These features need to be constant throughout the lifetime of a biometric. Studies already defined constant biometric features, in this research existing algorithms are used to extract constant features. Additionally, this subsystem involves the process of generating a challenge from extracted features. This challenge is then passed into a ZKP-proof generator method to generate proofs, and then hashed and sent into the database so that it can be linked with other identity information. Both proofs and hashed challenges are stored in a database. ZKP-Based Data Storage Subsystem is where data is stored and it involves ZKP reference data engine to perform proof selection and corresponding data selection that's required during verification.

On a ZKP-Based Verification Subsystem, the proofs stored on the database and from query biometric data are compared. The prover requests for the challenge, and the verifier sends back the challenge. The system on the prover side will generate the response based on the challenge from the captured biometric data. The proofs should give the same value if they are generated for the biometrics of the same person. The results can be verified or not. If successfully verified, access can be granted to the user. While the user is using the system, s/he can be asked to update their details.

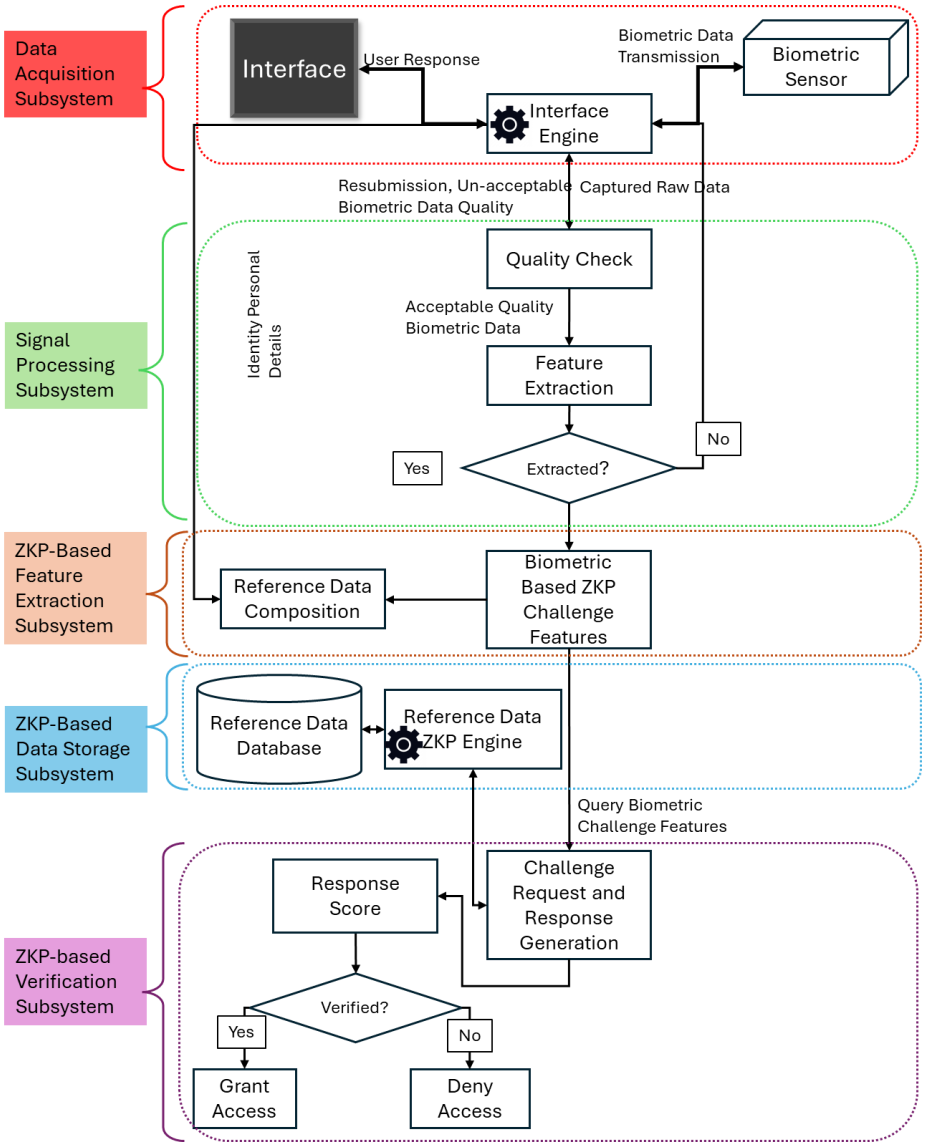

Fig. 2. Proposed Biometric system Architecture.

4 Results and discussion

The proposed system focuses on enhancing the security of identity by combining traditional methods with a new approach, as summarized in **Table 2**. Both systems the traditional and proposed, use the same sensors and methods for biometric data acquisition and signal processing. After signal processing, biometrics features are then extracted. The proposed method generates a

challenge and a hash value after feature extraction, which depends on biometric data features. The system does not directly store biometric features but generates proofs and challenges, along with other linked identity information. The verification subsystem compares proofs that are generated and stored from the process of registration, ensuring no biometric data is exposed.

Table 2: Comparison of traditional and proposed biometric system architecture.

Subsystem	**Traditional System**	**Proposed System**	**Comments, security of identity**
Data Acquisition Subsystem	Yes	Yes	Both traditional and proposed architecture include data acquisition using the same sensors and methods.
Signal Processing Subsystem	Yes	Yes	Both traditional and proposed architecture include biometric data processing using the same tools and procedures.
ZKP-Based Feature Extraction	No	Yes	Traditional methods extract features based on the existing algorithms and store those features for later verification. With the proposed method, after feature extraction, a challenge is generated together with a hash value, that is later will be used during verification.
ZKP-Based Data Storage Subsystem	No	Yes	With traditional methods, biometric data features are stored. The proposed method does not store biometric features directly but generates proofs and a challenge, together with other linked identity information.
ZKP-Based Verification Subsystem	No	Yes	The proposed architecture is based on comparing the proofs generated from registration and verification challenges. With this method, no biometric data is exposed.

The proposed system ensures that biometrics data is never directly exposed, significantly reducing the risk of data breaches. This is because ZKP allows one party to prove to another that they know a piece of data without revealing the data itself. This means the system can verify a user's identity without ever exposing the actual biometric data. In addition, since ZKP involves generating new proofs for each verification, replaying old data is ineffective. This ensures that the proposed system complies with the General Data Protection Regulation, and NIST-SP 800-63-3 which emphasizes the protection of biometric data.

Traditional biometric systems store and transmit biometric data, which can be vulnerable to theft. With the use of ZKP, only proofs are shared during verification not actual data. This ensures that the proposed system comply to the ISO/IEC 24745 that emphasize that biometric data is securely stored and transmitted. With the proposed system, data breaches and identity theft will be challenging for criminals. This is because by not storing actual biometric data, the system reduces the risk of data breaches. In addition, without access to actual biometric data, attackers cannot impersonate users.

Moreover, many regulations require the protection of personal data, including biometrics data. ZKP ensures that biometrics data remains confidential, as only proof of validity is shared, not the data. In addition, ZKP enables secure verification processes without requiring trust in the verifier, which is crucial in future decentralized technologies and applications.

5 Conclusion

This study presented the importance of protecting our identity in the digital world. As technology evolves, identity theft is also increasing at a very high rate. It is thus important to invest in solutions that will strengthen the security of an individual's identity while preserving privacy. To achieve that, it is crucial to understand what forms the identity. In this study, five layers of identity were presented, primary, secondary, tertiary, organizational and cultural. These layers lead towards an implementation of a secure identity, by investing more effort in the crucial layers based on the sensitivity of the data involved in that particular layer.

A comprehensive literature review on existing works where identity is protected using biometrics and ZKP has been conducted. The outcome indicated that traditional solutions, even if some incorporate the use of ZKP, there is a lack of security for biometric data, which is the primary layer of an individual's identity. These systems are vulnerable to biometric data breaches that are not easy to resolve since once biometric data is stolen, it cannot be replaced by a different biometric since a person owns only one biometric. Based on the conducted desktop market analysis, there are existing technologies where biometrics-ZKP are used, such as Biometric Identification Scheme, Mastercard, and Keyless.

A novel biometric system architecture based on ZKP has been proposed. This architecture ensures that ZKP challenges and proofs are generated from biometrics data, and stored for later verification, without exposing biometric data. This architecture also includes a reference data engine to enable the challenges and proofs to be updated when needed. This improves the security of the stored identity and overcomes the challenges faced by traditional biometric systems in case of data breach.

However, to implement ZKP solutions, or integrate them with current systems, individuals typically need a strong background in mathematics, cryptography, security awareness, experience, problem-solving skills in ZKP and computer science. ZKP experience includes practical experience with ZKP protocols such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge). Familiarity with ZKP libraries and frameworks such as zk-SNARK libraries in various programming languages can be advantageous.

References

[1] J. Blue, J. Condell, and T. Lunney, "A Review of Identity, Identification and Authentication," *International Journal for Information Security Research*, vol. 8, no. 2, pp. 794–804, 2018, doi: 10.20533/ijisr.2042.4639.2018.0091.

[2] V. Carmel and D. Akila, "A survey on biometric authentication systems in cloud to combat identity theft.," *Journal of Critical Reviews*, vol. 7, no. 03, pp. 540–547, 2020.

[3] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for Internet-of-Things Security : A Review," pp. 1–26, 2021.

[4] J. M. Morrow, "Legislative Recommendations on Biometric Security and Privacy Jurisprudence," University of Southern Maine, 2024.

[5] M. Gomez-Barrero and J. Galbally, "Reversing the irreversible: A survey on inverse biometrics," *Comput Secur*, vol. 90, p. 101700, 2020.

[6] O. Ogbanufe and R. Pavur, "Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection," *Int J Inf Manage*, vol. 62, no. October 2021, p. 102432, 2022, doi: 10.1016/j.ijinfomgt.2021.102432.

[7] C. Virmani, "Analysis of cyber attacks and security intelligence: Identity theft," *Indian J Sci Technol*, vol. 13, no. 25, pp. 2529–2536, 2020, doi: 10.17485/ijst/v13i25.580.

[8] O. A. Fayayola, O. L. Olorunfemi, and P. O. Shoetan, "Data Privacy and Security in It: a Review of Techniques and Challenges," *Computer Science & IT Research Journal*, vol. 5, no. 3, pp. 606–615, 2024, doi: 10.51594/csitrj.v5i3.909.

[9] C. Marcolla *et al.*, "Survey on Fully Homomorphic Encryption, Theory, and Applications," *Proceedings of the IEEE*, vol. 110, no. 10, pp. 1572–1609, Oct. 2022, doi: 10.1109/JPROC.2022.3205665.

[10] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings 7*, Springer, 2001, pp. 552–565.

[11] A. C. Yao, "Protocols for secure computations," in *23rd annual symposium on foundations of computer science (sfcs 1982)*, IEEE, 1982, pp. 160–164.

[12] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture," *Proceedings of the 23rd USENIX Security Symposium*, pp. 781–796, 2014.

[13] N. Yusuf, K. A. Marafa, K. L. Shehu, H. Mamman, and M. Maidawa, "A survey of biometric approaches of authentication," *International Journal of Advanced Computer Research*, vol. 10, no. 47, pp. 96–104, 2020, doi: 10.19101/ijacr.2019.940152.

[14] X. Sun, F. Richard Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, "A Survey on Zero-Knowledge Proof in Blockchain," *IEEE Netw*, vol. 35, no. 4, pp. 198–205, 2021, doi: 10.1109/MNET.011.2000473.

[15] F. Wang *et al.*, "Identity authentication security management in mobile payment systems," *Journal of Global Information Management (JGIM)*, vol. 28, no. 1, pp. 189–203, 2020.

[16] B. O. ALSaleem and A. I. Alshoshan, "Multi-factor authentication to systems login," in *2021 National Computing Colleges Conference (NCCC)*, IEEE, 2021, pp. 1–4.

[17] D. J. Haas, *Personal Identification: Modern Development and Security Implications*. CRC Press, 2024.

[18] Q. N. Tran, B. P. Turnbull, M. Wang, and J. Hu, "A Privacy-Preserving Biometric Authentication System With Binary Classification in a Zero Knowledge Proof Protocol," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 1–10, 2021.

[19] "Keyless | Why Keyless | The world's first privacy-preserving biometrics." Accessed: May 31, 2024. [Online]. Available: https://keyless.io/why-keyless

[20] Mastercard, "Accepting the Mastercard ® Biometric Card Processing points for acquirers and payment," 2021. Accessed: Oct. 28, 2024. [Online]. Available: https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/smb/other/biometric-card-merchant-acceptance-guide-global-jan21.pdf

[21] C. S. Ntshangase, K. Baruni, O. Mahlasela, and S. S. Mgaga, "Secure suthentication using zero knowledge proofs and biometrics: A review," in *THREAT 2023 CONFERENCE PROCEEDINGS*, K. Pillay and B. Watson, Eds., Government Academy Industry, 2024, pp. 66–75. [Online]. Available: http://creativecommons.org/licenses/by/4.0/

[22] E. Fute Tagne, E. Tonye, A. Z. Tsague, E. T. Fute, and A. El Amraoui, "DS-NIZKP: A ZKP-based Strong Authentication using Digital Signature for Distributed Systems," *Article in International Journal of Computer Science and Information Security*, no. July, 2018.

[23] N. D. Sarier, "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management," *Comput Secur*, vol. 105, p. 102243, 2021.

[24] W. Liu, X. Wang, and W. Peng, "Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things," *IEEE Access*, vol. 8, pp. 8754–8767, 2020, doi: 10.1109/ACCESS.2019.2962912.

[25] W. Liu, X. Wang, W. Peng, and Q. Xing, "Center-less single sign-on with privacy-preserving remote biometric-based ID-MAKA scheme for mobile cloud computing services," *IEEE Access*, vol. 7, pp. 137770–137783, 2019.

[26] N. Hegde and S. S. Manvi, "Mfzkap: Multi factor zero knowledge proof authentication for secure service in vehicular cloud computing,"

in *2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*, IEEE, 2019, pp. 1–6.

[27] H. Zhang, W. Bian, B. Jie, and S. Sun, "BioP-TAP: An efficient method of template protection and two-factor authentication protocol combining biometric and PUF," *Journal of Intelligent & Fuzzy Systems*, vol. 43, no. 4, pp. 4317–4333, 2022.

[28] G. S. Gaba, M. Hedabou, P. Kumar, A. Braeken, M. Liyanage, and M. Alazab, "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare," *Sustain Cities Soc*, vol. 80, p. 103766, 2022.

[29] X. Mao, Y. Chen, C. Deng, and X. Zhou, "A novel privacy-preserving biometric authentication scheme," *PLoS One*, vol. 18, no. 5, p. e0286215, 2023.

[30] C. Guo, L. You, and G. Hu, "A Novel Biometric Identification Scheme Based on Zero-Knowledge Succinct Noninteractive Argument of Knowledge," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/2791058.

[31] Y. Song, J. Zhang, X. Huang, W. Wu, and H. Yang, "Statistical zero-knowledge and analysis of rank-metric zero-knowledge proofs of knowledge," *Theor Comput Sci*, vol. 952, p. 113731, 2023.

[32] P. Alikhani *et al.*, "Experimental relativistic zero-knowledge proofs," *Nature*, vol. 599, no. 7883, pp. 47–50, 2021.

[33] N. D. Sarier, "Privacy Preserving Biometric Authentication on the blockchain for smart healthcare," *Pervasive Mob Comput*, vol. 86, p. 101683, 2022.

[34] M. H. Au, W. Susilo, and Y. Mu, "Proof-of-Knowledge of Representation of Committed Value and Its Applications."

[35] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Advances in Cryptology—CRYPTO'89 Proceedings 9*, Springer, 1990, pp. 239–252.

[36] D. Boneh and V. Shoup, "A graduate course in applied cryptography," *Draft 0.5*, 2020.

[37] Q. Nguyen, M. Rudoy, and A. Srinivasan, "Two factor zero knowledge proof authentication system," *Spring 2014 Project*, pp. 1–11, 2014.

[38] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali*, 2019, pp. 203–225.

[39] C. Hazay and Y. Lindell, "A note on zero-knowledge proofs of knowledge and the ZKPOK ideal functionality," *Cryptology ePrint Archive*, 2010.

[40] The National Institute of Standards and Technology, "Biometric Quality," NIST. Accessed: Jun. 01, 2024. [Online]. Available: https://www.nist.gov/programs-projects/biometric-quality