Privacy-Enhanced One-to-Many Biometric System Using Smart Contracts: A New Framework

1st Alec Wells
School of Computer Science
University of Sunderland
Sunderland, United Kingdom
alec.wells@research.sunderland.ac.uk

2nd Norbert Dajnowski
Department of Computer Science
York St John University
York, United Kingdom
n.dajnowski@yorksj.ac.uk

3rd Aminu Bello Usman
School of Computer Science
University of Sunderland
Sunderland, United Kingdom
aminu.usman@sundeland.ac.uk

4th John Murray
Faculty of Technology
University of Sunderland
Sunderland, United Kingdom
john.murray@sunderland.ac.uk

5th Basel Barakat
School of Computer Science
University of Sunderland
Sunderland, United Kingdom
basel.barakat@sunderland.ac.uk

***Abstract*—This paper presents a novel framework for one-to-many biometric systems by adapting decentralised storage over a centralised database solution, by leveraging smart contracts to address the concerns commonly associated with decentralised solutions. Smart contracts enforce strict privacy controls, enabling individuals to retain ownership and control over their biometric data on decentralised networks, while facilitating secure and efficient authentication, helping achieve the principles laid out by privacy by design. Biometric systems play a crucial role in identity verification and access control, but their deployment raises significant privacy challenges due to the sensitive nature of biometric data. Traditional approaches often involve centralised storage of biometric information, increasing the risk of data breaches and unauthorised access. We discuss the architecture, implementation, and benefits of our framework, highlighting its potential to enhance privacy and trust in one-to-many biometric systems across various applications.**

***Index Terms*—Authentication, biometric, blockchain, decentralisation, smart contract**

I. Introduction

Biometric authentication has become increasingly prevalent in recent years – being seen as a more secure form of authentication compared to its alternatives [1]. Biometric authentication relies on a system being able to verify a user, from them presenting a live biometric sample which is compared with a previous sample of the same biometric, that the user previously gave to the system during enrolment; if the two samples match – the user is verified.

Biometric authentication systems offer robust security applications across various domains by verifying individuals' unique physiological or behavioral characteristics. One significant application is in access control and physical security. Biometrics factors, such as fingerprints, iris patterns, or facial recognition, can grant or deny access to secure locations, buildings, or digital devices. By accurately identifying authorised personnel based on their unique biometric traits, these systems enhance security by reducing the risk of unauthorized access or identity fraud.

Another critical application lies in digital authentication and identity verification. Biometric authentication can be integrated into smartphones, laptops, and other electronic devices, offering a convenient and secure method for user authentication. For instance, fingerprint sensors or facial recognition technology can replace traditional passwords or PINs, mitigating the risk of unauthorized access to sensitive information or online accounts. This application is particularly valuable in sectors like banking, healthcare, and e-commerce, where protecting user data and preventing identity theft are paramount concerns.

Moreover, biometric authentication holds promise in enhancing border security and immigration control, since it helps identify individualals based on their biometric characteristics, facilitating an efficient and accurate screening processes at airports, seaports, and international borders. By comparing biometric data against centralized databases, authorities can quickly detect individuals with fraudulent identities or those on watchlists, bolstering national security measures.

A. One-to-many Biometric System

Many of the applications described above are what is known as a one-to-many biometric system, also known as an identification system. This is a type of biometric authentication system that compares a biometric sample provided by an individual, against a database of various biometric templates, often of other users, to determine the identity of the person.

A summary of the steps in a one-to-many voice biometric system is shown in Figure 1. First, a user provides their biove biometric as a signal by using a microphone. In the example of voice biometrics, the signal has to be pre-processed by converting the audio segments for speech recognition. Next, unique features are extracted to create a template representing each individual's biometric characteristics during feature extraction. The next step is the matching process, which utilizes sophisticated algorithms to quickly compare the provided sample's biometric characteristics against those stored prior in the database from when the user enrolled. The system can then make its decision, if a match is found within an acceptable threshold of similarity, the individual's identity is confirmed, and access is granted. Conversely, if no match is found, access is denied, ensuring secure and accurate identity verification.

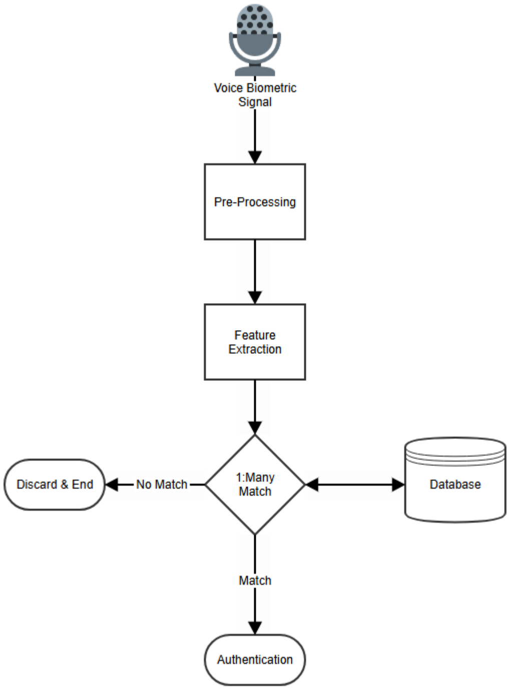

Fig. 1. Flowchart of a Voice One-to-many Biometric System

Currently most one-to-many biometric systems employ the use of a centralised database to store users' templates for controlling access to a system. However, centralised databases have several issues and vulnerabilities that can be exploited by malicious attackers. These include, introducing a single point of failure to the system, they can also suffer delayed responses due to traffic jams [2] and can be targeted by attackers with malicious intent. These concerns could partiality be alleviated by data being stored in a decentralised database, given that for these attacks to be performed, an attacker needs to have some knowledge of the database location so they can target the user's templates, of which a decentralised database could prove to be more secure.

A blockchain forms a decentralised database that is shared among several nodes across a computer network of which, allows for information to be stored electronically in a digital format, in a decentralised and secure fashion. Smart contracts are programs that are stored on a blockchain, which can be executed when certain conditions are met, such as to automate a workflow. As such, we seek to ask if we can utilise Ethereum blockchain's smart contract technology to host a decentralised application (DApp) for a biometric system constructed with the user's privacy in mind.

To design a system with the users privacy at the forefront it is important to follow a set of principles that underpin the most important aspects of designing a privacy concerning system, especially in a one-to-many system that searches a large databases for matches, which can pose a higher risk of privacy infringement that one-to-one-systems [3]. By integrating privacy protections into the design and implementation of biometric systems from the outset, developers can minimize the collection, use, and disclosure of sensitive biometric data, ensuring that individuals' privacy rights are upheld [4].

The paper is structured as follows, in part 2 we discuss the related work around biometrics and highlight the need for privacy preserving techniques and explore other prior implementations of blockchain technology in applications. In part 3 we cover the issues that proposing a framework such as this might have and the potential solutions to alleviate or remove these problems. In part 4 we showcase our proposed framework. We also illustrate the pseudo code behind the idea and highlight how it preserves user privacy, by following the privacy by design principles. Finally, in part 5 we conclude our findings and consider the future directions of a framework such as this.

II. Related Work

The human body provides many distinctive features suitable for providing samples to control access to a system. A biometric sample could be either a physical biometric or behavioural biometric. A physical biometric is a characteristic of the user, examples can include a fingerprint image, facial image, or iris scan. A behavioural biometric is an analysis of patterns the user does such as a keystroke pattern, voice biometric or signature analysis. While biometrics are considered more secure for authentication than other authentication factors like knowledge-based (pins, passwords, etc.) or ownership-based factors (credit cards, authenticators, etc.) biometrics still have their share of concerns. One such concern is that once a biometric is compromised, it is virtually impossible to change. As such, it is of the upmost importance to keep users' biometrics private and secure, especially in vulnerable positions such as its storage in databases.

As covered prior, centralised databases can introduce privacy and security concerns to biometric systems, such as introducing a single point of failure to the system, delayed responses due to traffic jams [2] and malicious users targeting the biometric templates. Attackers can target templates using attacks such as substitution and multiplicity attacks, to modify the templates contents or combine the users and attackers' templates together to spoof the biometric system to grant an attacker access [5].

To address these issues, studies have investigated the potential use of a decentralised database using the blockchain, allowing for the storage of encrypted template data with smart contracts. For example, Cunningham proposes the use of distributed ledger technology to allow access to patient's electronic health records, utilising Ethereum blockchain technology for its implementation of a "secure, trustless, and openly auditable environment" [6]. A solution such as this can alleviate the privacy concerns of using a centralised databases as digital data is instead stored across several nodes in a decentralised fashion. Not using a centralised database provides other advantages too, as blockchains are less vulnerable to infrastructure attacks such as denial-of-service attacks, replay attacks and Sybil attacks, as highlighted in the study [7] which proposes the use of a biometric blockchain framework to prevent these attacks in a vehicular, Ad-hoc Network.

The work in [8] highlights the need for privacy-preserving and decentralized identity management solutions amidst concerns over data centralization and security breaches. The proposed decentralized system aims to facilitate key management operations, including generation, backup, and recovery, while also introducing a decentralized identity verification protocol. Leveraging Shamir's Secret sharing scheme and blockchain technology, the digital wallet serves as a key component of the solution, addressing various security parameters. Similarly, we can adapt Ethereum's decentralisation to provide secure identity verification for our biometric authentication framework.

Blockchain technology and smart contracts can enhance privacy in biometric technology by decentralizing storage and access control of biometric data [9]. Each individual's biometric data can be securely stored on the blockchain, with cryptographic techniques ensuring its integrity and privacy. This decentralized approach ensures transparency, accountability, and privacy protection in the handling of biometric data, fostering greater trust in biometric systems, which is ideal for managing small data like keys to govern the access to a larger storage of data.

Existing biometric systems can also be adapted to use blockchain technologies quite easily. The study [10] identifies that the same techniques and algorithms used currently, can also be utilised in a blockchain solution and that blockchain solutions wouldn't always need complex smart contracts. This is because the minimum function needed is to manage storage and the blockchain architecture wouldn't suffer from scalability issues as the biometric process is performed off-chain. This provides confidence in applying blockchain solutions to a large amount of existing centralised use-cases.

Although blockchain solutions do propose its own unique challenges that have to be considered. For example, in a blockchain there is no way to identify who owns what data, hence measures will need to be taken to assure that data can securely retrieved. Papers such as [11] propose a solution to this using a protocol known as Biometric Blockchain, which incorporates biometric cues of individuals to identify creators and users in blockchain-based systems. The paper also acknowledges the risks that are proposed with a system such as this, as while the biometrics would be secure, it could expose the user's privacy. Hence, in a potential decentralised authentication solution, to preserve the users privacy, biometrics will need to be encrypted if they are to be stored in this way. This could be done using a Many Graph Embedding solution which was proposed in the study [12] which discovers discriminate patterns during facial recognition, allowing data to be stored on a block-based system while still preserving the user's privacy, though will vary based on the type of biometric data being stored.

In Cunningham's proof of concept, other problems with the solution were identified, such as the inefficiency and immaturity of the technology. Likewise, the study also notes that distributed ledger technology has the potential to add a significant degree of trust for systems - adding privacy and accountability [6]. This is important as in the modern discourse, the handling of data has become a contentious area, with scandals such as Cambridge Analytica acting as a catalyst for such discussion. The following fallout of such scandals has birthed the introduction of stricter data regulations such as Europe's GDPR (General Data Protection Regulation) as well as giving users a more astute awareness of the commodity of data, and a greater concern for how their data is handled, stored, and how they can keep their data private [13]. As such, when developing authentication systems with the interests of both the user and regulation expectations, it is important to keep the user's data safe and therefore private, the easiest way to do so is to follow a set of design principles such as Privacy by Design to show a commitment to this ideal [14].

Privacy by Design is built on 7 foundational principles for designers to follow in order build systems with users' privacy in mind, these are:

- **Proactive not Reactive; Preventative not Remedial:** Applications should choose to try prevent and anticipate breaches of privacy before they happen, rather than try reactively remedy privacy breaches.
- **Privacy as the Default Setting:** Settings that keep the user's data private should be on by default rather than require action from the user to protect their data.
- **Privacy Embedded into Design:** Privacy features should not be bolted on to the system and should be an integral part of the systems throughput.
- **Full Functionality – Positive-Sum not Zero-Sum:** The application should not compromise and take trade-offs, instead both privacy and security should be desired for a 'win-win' scenario.
- **End-to-End Security – Full Lifecycle Protection:** The users' data should be protected from its conceptualisation to its deletion, so no point of the system is vulnerable.
- **Visibility and Transparency – Keep it Open:** The operation of the application or architecture should be transparent in its operation and workings to verified users and providers.
- **Respect for User Privacy – Keep it User-Centric:** At all costs the interests of the individual are of the utmost importance with user-friendly design and strong privacy defaults.

Privacy by design principles emphasize embedding privacy considerations into the design and architecture of systems from their inception [15]. When applied to biometric technology, this means integrating privacy protections into every stage of biometric data processing, storage, and access. Smart contracts, as self-executing contracts with the terms of the agreement directly written into code, offer a powerful tool for implementing privacy by design in biometric systems [16]. By encoding privacy rules and access controls into smart contracts deployed on a blockchain, organizations can ensure that biometric data is handled in accordance with privacy regulations and user preferences. These smart contracts can automate consent management, data anonymization, and granular access control, giving individuals greater visibility and control over how their biometric data is used and shared.

Furthermore, smart contracts can facilitate transparency and accountability in biometric systems by recording all transactions and data accesses on the blockchain, providing an immutable audit trail. This transparency enhances trust among users and regulators, as they can verify that biometric data is being handled in a privacy-preserving manner [17]. By leveraging smart contracts to bridge the gap between privacy by design principles and biometric technology, organizations can build more trustworthy and ethical biometric systems that prioritize user privacy while still enabling valuable use cases such as identity verification and authentication.

III. Methods

A potential framework that utilises blockchain technology for a decentralised storage of templates, while promising, does have some potential issues that need to be addressed in order to be successful. Namely the two largest challenges of a solution such as this would be the gas prices and the publicness of blockchain technology.

A. Addressing Potential Gas Fees

One potential issue of a framework such as this could be the high price of network gas fees. These fees are required to cover costs of smart contract operations and keep stability across the network. Unfortunately, the larger the processing data, the larger the fees that will be accumulated. As such, to mitigate the gas fees, we propose extending our model to use IPFS for biometric data storage. Essentially, user's biometric data will be split into blocks of 256 kilobytes and assigned unique identifiers, these will then be encrypted and stored across the blockchain [18]. A design is introduced where Ethereum is engaged to provide automation of tasks through its smart contract technology, while IPFS decentrally hosts the system's sensitive data. Another advantage of such a design is its universal application, our public smart contract model is accessible to all network users, authorising it to be used by any developer for their DApps; provided that they require decentralised biometric authentication.

B. Addressing Blockchain Publicness

The other issue with a biometric authentication system that uses blockchain/IPFS, is that blockchain technology is publicly available. As such, one solution to address this is the use of the smart contract using Ethereum. The Ethereum smart contract will serve as a repository for storing pointers and encryption keys that grant access to biometric data on the IPFS blockchain.

The smart contract within the system will encompass two principal methods for biometric data: read and write. The presence of biometric data on the web application is transient, solely retained for the purpose of conducting necessary authentication comparisons. Once the comparisons are completed, the temporary data must be promptly cleared, facilitating the progression to the subsequent dataset. This stringent data management approach ensures the maintenance of optimal data security on the web application, both within the blockchain and outside of it.

Each application entity that interacts with the biometric smart contract is granted access only to the data they have initially stored, a validation enforced through wallet address verification. In addition to the write and read methods, the smart contract assumes the responsibility of safeguarding the privacy and tracking the IPFS biometric data pointers. To accomplish this, a distinct class structure should be employed, utilizing an array to store the relevant information.

IV. Proposed Framework

The model we propose in this study presents a one-to-many blockchain biometric authentication method based on privacy by design concepts, as shown in Figure 2. The Ethereum and IPFS blockchains will operate the fundamental functionality for our biometric method, employing Ethereum's smart contracts to keep records and process computations, while IPFS is used to decentrally store the biometric data.

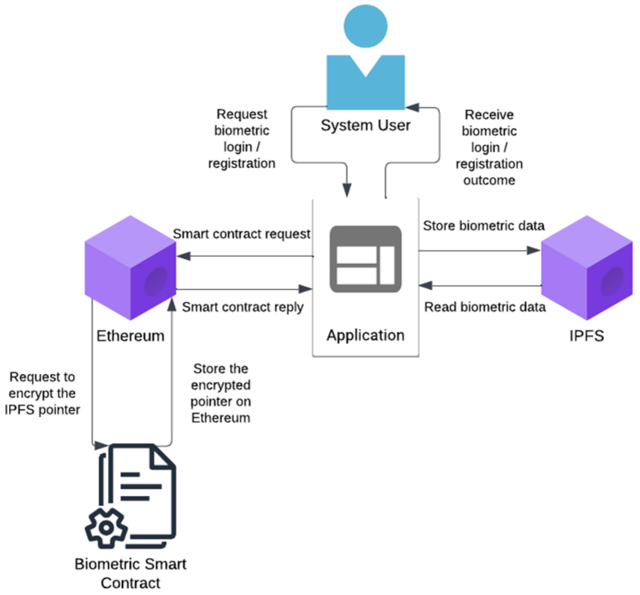
System User
Request biometric login / registration
Receive biometric login / registration outcome
Smart contract request
Smart contract reply
Store biometric data
Read biometric data
Ethereum
Application
IPFS
Request to encrypt the IPFS pointer
Store the encrypted pointer on Ethereum
Biometric Smart Contract

Fig. 2. System Architecture.

For this framework proof-of-concept, our system will be configured and evaluated on a virtual network utilizing

Ganache CLI. This approach is implemented to mitigate the high gas fees typically associated with Ethereum transactions from storing large amounts of data, which can be prohibitively expensive, by instead storing the user's encrypted biometric data on IPFS, where gas fees are minimal to none. Ethereum's smart contract technology is only employed to store minimal data such as the user's address, to authenticate the action of retrieving further sensitive biometric data from the IPFS storage. This approach ensures costs are kept minimal in comparison to storing all the user's data on Ethereum. Additionally, all biometric data stored on IPFS is encrypted prior to being visible to the public, ensuring that the proposed system's sensitive data is kept private, despite the publicness of blockchain technology.

Our utilisation of smart contracts via Solidity (a collection of code, its functions, and data that resides at a specific address on the Ethereum blockchain) helps achieve privacy by design principles. When a user is first enrolled the smart contract is compiled so that later when a user attempts to login, the smart contract is then checked to confirm that the user exists in the system and therefore their data, which is stored on IPFS, can only be accessed if that check is successful. Since smart contracts are inherently encrypted and are theoretically immutable, hackers should not be able to view data or manipulate this check by injecting their own malicious date. By having the smart contract, we are embedding preventative measures into the design of the system. These settings are on by default, rather than attempting to react to security breaches, achieving privacy by design principles.

The framework utilises Ethereum Virtual Machine (EVM) and InterPlanetary File System (IPFS) as a replacement for storing voice models in a centralised database to help achive privacy by design. With IPFS being a protocol for a decentralised network compromised of nodes, allowing us to pin data to, which are open and participatory - hence why we utilise a secure and encrypted smart contract to store the IPFS address of a user's data. EVM meanwhile is a blockchain platform that serves as the runtime environment for executing the smart contracts we utilise to store the users addresses. These in tandem act as a decentralised, secure storage method for our voice models, that retain the full functionality of a centralised database, though should provide a more secure storage.

A. Pseudo Code

The pointer storage method, as shown in Algorithm 1, serves the purpose of acquiring the user's biometric data. Once the data is obtained, it undergoes validation against a predetermined set of rules. Subsequently, the data is encrypted and transferred to the IPFS chain. Meanwhile, the Ethereum chain retains the URL, which can be considered as a secret access key.

In contrast to the previously described method, Algorithm 2 assumes the responsibility of retrieving the pointer from the IPFS chain. The code systematically scans the global array of pointers, aiming to identify any pointers associated with the user's wallet address. Upon finding a matching pointer, further steps are taken to validate and decrypt it using the user's encryption key. As a result of this process, the pointer becomes accessible, granting the user access to the biometric data for subsequent authentication purposes.

Algorithm 1: Pointer Storage Write Pseudo Code

```
Input: Wallet Address and IPFS Pointer
Function storePointer($address, pointer$):
    if validate(pointer) == True then
        $encryptedPointer \longleftarrow encrypt(pointer)$
        $pointerStorage \longleftarrow (address, encryptedPointer)$
        return $pointerStorage(secretKey)$
    end if
End Function
```

Algorithm 2: Pointer Storage Read Pseudo Code

```
Input: Wallet Address and Public Key
Function readPointer($address, secretKey$):
    if address in encryptedPointer then
        $pointer \longleftarrow decrypt(encryptedPointer, secretKey)$
        if validate(pointer) == True then
            return $Pointer$
        end if
    end if
End Function
```

B. Security of the Framework

A security analysis is performed to evaluate the effectiveness of how secure our proposed framework is, as well as identify and review the different impact factors introduced in our proposed solution.

- **Single point of failure:** In contrast to centralised systems, this framework eliminates single point of failure, providing enhanced robustness and reliability.
- **Data integrity:** Improved data integrity is introduced, since all blockchain transactions must be publicly validated on the network.
- **Encryption:** All data stored on the blockchain is encrypted to ensure user's privacy is maintained, and their credentials are inaccessible to other network users.
- **Transparency:** Blockchain's transparent nature provides a verifiable history of immutable transactions, and comprehensive audit trails.
- **Insider threat:** Prevents scenarios in which a system administrator or insider could maliciously tamper with user data.

C. Advantages & Use Cases

Centralised systems often pose a significant risk; by providing a single point of failure, susceptibility to a targeted attack, and lack of trust between the user and system operator. In contrast, a decentralised solution, such as the one in our proposed framework, offers enhanced security for biometric systems by distributing data across multiple nodes and preventing attackers from locating or having a specific target. This mitigates the risk of privacy infringement, especially in large one-to-many databases, through the integration of privacy by design principles.

However, the primary advantage of the framework we propose compared to other decentralised storage solutions, is the utilisation of both Ethereum and IPFS together to store a user's biometric data. This allows the solution to utilise the security provided by Ethereum's smart contract technology, while bypassing the high gas fees associated with storing data on Ethereum, as only a partial a amount of data is stored there. Also, despite the publicness of IPFS, the encrypted data that is stored there is only available with access to the secure smart contract, keeping the users privacy intact.

Our proposed framework has multiple use cases, particularly in industries that require enhanced security measures and biometric authentication. These include corporate and government facilities, where access to rooms and certain building areas can be controlled with biometric authentication. Furthermore, online applications like voting, healthcare, and general identity verification systems can benefit from our proposed solution as well.

V. Conclusion

The paper presents a framework for one-to-many biometric systems, leveraging blockchain technology and smart contracts to enhance privacy and security. By addressing the inherent challenges of centralised storage in traditional biometric systems, the proposed framework aims to decentralise the data storage and authentication processes, thus minimising the risk of data breaches and unauthorised access. Key challenges of decentralised solutions are also identified, such as high gas fees and the public nature of blockchain technology, while offering solutions to address these challenges.

The proposed framework utilises Ethereum smart contracts and the InterPlanetary File System (IPFS) to store biometric data in a decentralised manner. Smart contracts enforce strict privacy controls, allowing individuals to retain ownership and control over their data while ensuring secure authentication processes and we provide pseudo code to illustrate the implementation of the proposed framework, demonstrating how smart contracts can facilitate the storage and retrieval of biometric data securely. By embedding privacy by design principles into the architecture, the framework proactively addresses privacy concerns, providing a transparent and accountable system for biometric authentication.

Future research directions may involve further optimisation of gas fees, scalability considerations, and real-world implementations to validate the effectiveness of the proposed framework in diverse applications. Overall, the framework presented in this paper represents a significant step towards building privacy-preserving biometric authentication systems for the digital age.

References

[1] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja, "Comprehensive study of biometric authentication systems, challenges and future trends," *International Journal of Advanced Networking and Applications*, vol. 10, no. 4, pp. 3958–3968, 2019.

[2] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," 2018. ID: 1.

[3] A. K. Martin, *Envisioning Technology through Discourse: A case study of biometrics in the National Identity Scheme in the United Kingdom*. PhD thesis, London School of Economics and Political Science, 2011.

[4] E. Haber and A. Tamò-Larrieux, "Privacy and security by design: Comparing the eu and israeli approaches to embedding privacy and security," *Computer Law & Security Review*, vol. 37, p. 105409, 2020.

[5] G. S. Karimovich and K. Z. Turakulovich, "Biometric cryptosystems: Open issues and challenges," in - *2016 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–3, 2016. ID: 1.

[6] J. Cunningham and J. Ainsworth, "Enabling patient control of personal electronic health records through distributed ledger technology," *Stud Health Technol Inform*, vol. 245, pp. 45–48, 2018. pmid:29295049.

[7] A. Alharthi, Q. Ni, and R. Jiang, "A privacy-preservation framework based on biometrics blockchain (bbc) to prevent attacks in vanet," *Ieee Access*, vol. 9, pp. 87299–87309, 2021.

[8] R. Soltani, U. T. Nguyen, and A. An, "Decentralized and privacy-preserving key management model," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–7, IEEE, 2020.

[9] E. Barka, M. Al Baqari, C. A. Kerrache, and J. Herrera-Tapia, "Implementation of a biometric-based blockchain system for preserving privacy, security, and access control in healthcare records," *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, p. 85, 2022.

[10] O. Delgado-Mohatar, J. Fierrez, R. Tolosana, and R. Vera-Rodriguez, "Blockchain and biometrics: A first look into opportunities and challenges," in *Blockchain and Applications: International Congress*, pp. 169–177, Springer, 2020.

[11] B. Xu, T. Agbele, and R. Jiang, "Biometric blockchain: A better solution for the security and trust of food logistics," in *IOP Conference Series: Materials Science and Engineering*, vol. 646, p. 012009, IOP Publishing, 2019.

[12] R. Jiang, A. T. Ho, I. Cheheb, N. Al-Maadeed, S. Al-Maadeed, and A. Bouridane, "Emotion recognition from scrambled facial images via many graph embedding," *Pattern Recognition*, vol. 67, pp. 245–251, 2017.

[13] W. Presthus and H. Sørum, "Are consumers concerned about privacy? an online survey emphasizing the general data protection regulation," *Procedia Computer Science*, vol. 138, pp. 603–611, 2018.

[14] A. Cavoukian, "Privacy by design: The 7 foundational principles," *Information and privacy commissioner of Ontario, Canada*, vol. 5, p. 12, 2009.

[15] A. Cavoukian *et al.*, "Privacy by design: The 7 foundational principles," *Information and privacy commissioner of Ontario, Canada*, vol. 5, p. 12, 2009.

[16] L. S. Alotaibi and S. S. Alshamrani, "Smart contract: Security and privacy.," *Computer Systems Science & Engineering*, vol. 38, no. 1, 2021.

[17] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-enabled telehealth services using smart contracts," *Ieee Access*, vol. 9, pp. 151944–151959, 2021.

[18] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for ipfs," in *2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData)*, pp. 1499–1506, IEEE, 2018.