Generating an Iris-based Seed for Key-pairs in a Blockchain Platform

Marco Fiore, Federico Carrozzino, Gianvito Coppola, Gianni Guariglia, and Marina Mongiello

Original scientific article

***Abstract*—Authentication is a critical concern in cybersecurity, and the challenge of combining security with ease of use remains a pressing issue. Biometric authentication methods, particularly iris recognition, leverage unique physical characteristics to confirm identity, presenting an effective solution to enhance security over traditional password systems. However, the management of sensitive biometric data requires privacy measures to protect user information from potential misuse. This work proposes a novel Blockchain-based system that utilizes biometric data, specifically iris scans, as a seed for generating cryptographic key-pairs. By employing feature extraction and hashing techniques, the system ensures that sensitive biometric information is neither stored centrally nor accessible in its original form, thereby preserving user anonymity and privacy. The architecture is designed to distribute fragmented biometric data across multiple nodes in the Blockchain, enhancing scalability and security. The system's functionality is validated through extensive testing scenarios that demonstrate its reliability and robustness in various operational conditions. This research highlights the potential of combining Blockchain technology with biometric authentication to create secure and privacy-preserving identity management solutions, paving the way for applications in sectors such as finance, healthcare, and secure voting systems.**

***Index Terms*—Blockchain, key-pair generation, iris scan, biometric.**

I. Introduction

The rise of Blockchain technology has introduced a revolutionary change in how data and transactions are stored and validated, shifting from centralized databases to decentralized and distributed networks. Blockchain's intrinsic properties, such as transparency, immutability, and decentralization [1]–[3], have paved the way for secure and tamper-resistant systems across various sectors, even when it comes to Internet of Things (IoT) devices with low memory and performance [4] and their usage in critical scenarios [5], [6]. Among the critical aspects of blockchain applications is identity management [7], which is typically handled through the generation and management of key-pairs (private and public keys) [8]. However, the growing demand for higher levels of security in the face of sophisticated cyber threats necessitates an advanced approach to key generation and management [9], [10].

In parallel, biometric authentication systems have become increasingly prevalent due to their unique ability to identify individuals based on intrinsic physical characteristics [11], [12]. Biometrics, such as fingerprints, facial recognition, iris scans, and combinations of them [13], offer a highly secure alternative to traditional password-based systems by utilizing characteristics that are unique to each individual and difficult to replicate [11]. Yet, despite their advantages, biometrics introduce challenges regarding privacy and data security, particularly when it comes to sensitive biometric data being misused or compromised [14], [15].

Combining Blockchain with biometrics offers an intriguing solution to the dual problems of secure identity management and privacy protection [16]. This paper presents a novel approach that uses iris-based biometric data as a seed for generating key-pairs within a Blockchain platform. By doing so, it ensures not only that the keys are unique and securely tied to the individual, but also that the sensitive biometric data itself is not exposed or stored in a vulnerable manner. Instead, iris data is transformed into a non-reversible hash value that serves as the seed for key generation, preserving both the security of the Blockchain system and the privacy of the user.

The potential applications of such a system are vast. In contexts such as e-voting, where identity verification and anonymity must coexist [17], or in financial systems, where security is paramount, the combination of Blockchain and biometric authentication offers a powerful tool for ensuring both privacy and integrity [18]. Unlike traditional systems, where biometrics might be stored in centralized databases, this approach distributes biometric data across multiple nodes in a Blockchain, further enhancing security through decentralization [19], [20].

This work aims to address key challenges in using biometrics for Blockchain-based key generation and provides a robust solution that can be seamlessly integrated into existing Blockchain infrastructures. Specifically, the proposed system uses iris scanning as a biometric input to generate a key-pair, which can be used for authenticating transactions in a Blockchain platform without exposing the original biometric data.

Our approach uniquely integrates iris biometrics with Blockchain, leveraging the decentralization and immutability of Blockchain to enhance the security and privacy of biometric data. Unlike traditional methods that store sensitive data in centralized repositories, our system uses a distributed architecture, significantly reducing vulnerability to breaches. Additionally, by using iris-based cryptographic seeds, we ensure higher uniqueness and reliability in key-pair generation, surpassing conventional methods in security and

Manuscript received November 6, 2024; revised November 26, 2024. Date of publication May 12, 2025. Date of current version May 12, 2025.

Authors are with the Department of Electrical and Information Engineering, Polytechnic University of Bari, Bari, Italy (e-mail: name.surname@poliba.it).

Digital Object Identifier (DOI): 10.24138/jcomss-2024-0100

1845-6421/06/2024-0100 © 2025 CCIS

scalability.

The paper is structured as follows: Section II describes some related work, Section III introduces the used technologies, Section IV analyzes the proposed architecture with details of its implementation in Section V and validation aspects in Section VI. Section VII concludes the paper with some insights on future research directions.

II. Related Work

Authors of paper [21] underline that biometric authentication is not ready to be available for a widespread use, even if it could be used to create an online community based on security and safety: we can consider biometric authentication and privacy preserving techniques as a state-of-the-art subject. Various works have been presented in this topic, mixing biometrics and a Blockchain-based system [22]–[27]. The usage of distributed networks ensures high availability of data, while Blockchain guarantees immutability and trust characteristics. The absence of a third party actor ensures privacy in the system [22]: a secure users authentication is enabled, but sensitive data are not exposed to anyone. User templates are stored in the InterPlanetary File System (IPFS) and used for enrolling the user and sign transactions. Authors of paper [23] propose a Blockchain-based user re-enrollment authentication schemes based on biometric data and using a secure multi-party sum protocol. In this paper, a private Blockchain is preferred and there is no storing of user data in the back-end. Authors of paper [24] use face recognition to develop a cross-domain authentication protocol, divided in certificate generation stage, face collection stage, and contract authentication stage. To ensure privacy for users, an encryption algorithm is applied to user's face characteristics. The security of biometrics using a Blockchain platform is also analyzed in [28], where a model for a secure transmission of 3D face and 3D ear biometrics is proposed. Biometrics also play a crucial role in Cognitive Internet of Things (C-IoT) security [29]: in the proposed paper, authors use Blockchain to store the decision on the similarity of the submitted biometrics information with an existing one. Practical implementations have also been proposed in different fields, from smart healthcare [25] to payment systems [26].

Our work is different to the ones proposed above because its main aim is to let users generate a restricted number of key-pairs using biometrics data. Also, biometrics will not be just stored in the Blockchain, but they will be used to log into the user account and to avoid value loss and theft. To reach this goal, a feature extraction and encryption process is applied to acquired data, then the obtained hash is used as a seed to generate the key-pair. The starting point is explained in [27]. Application fields that can take advantage of this method regard systems where a user should be anonymous but should not have the opportunity to create more than a defined number of wallets (i.e., a voting system).

An overview of the described works is shown in Table I.

III. Background

In this section, we introduce the foundational technologies utilized in this paper, including Blockchain, biometrics, key-pair generation, and feature extraction algorithms.

A. Blockchain Technology

Blockchain technology is a specific implementation of Distributed Ledger Technologies (DLTs), enabling secure, transparent, and decentralized recording of transactions . Each block in the blockchain contains a list of transactions, which are verified by a distributed network of nodes [30]. Once verified, the block is appended to the chain, making it immutable and resistant to tampering. This decentralized nature ensures that no central authority has control over the data, thus enhancing trust and security [31].

A key feature of Blockchain systems is the cryptographic hashing used to validate transactions. Consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), ensure that transactions are authenticated and agreed upon by the network [32], [33]. Privacy in Blockchain systems is managed through the use of cryptographic techniques, which enable users to interact anonymously using cryptographically generated public and private keys [34]. This security model aligns well with biometric authentication, where users need to protect their identity while engaging in secure digital transactions. To enhance security in distributed systems, such as Blockchain-based architectures, various strategies have been explored to mitigate cyber-attacks. Nocera et al. propose an ensemble machine learning model, which effectively identifies and mitigates attacks within Cloud and Fog environments, highlighting the importance of data analysis and responsiveness in distributed contexts [35]. Security in Blockchain systems can be further enhanced by applying User Behavior Analytics (UBA) and LSTM neural networks for DDoS attack prevention in Cloud and Fog environments. This approach can be also relevant for monitoring biometric access and usage in decentralized Blockchain settings, reducing attack risks and ensuring system security [36].

B. Biometrics

Biometrics refers to the measurement and statistical analysis of people's physical and behavioral characteristics. Biometric authentication is commonly used in various security systems to identify individuals based on unique physical attributes such as fingerprints, facial structure, or iris patterns [37]–[40]. Among these, iris scanning stands out as one of the most secure and accurate forms of biometric authentication due to the highly unique patterns found in the human iris, which remain stable over time [41].

Iris scans are considered highly reliable because they have a lower False Acceptance Rate (FAR) and False Rejection Rate (FRR) compared to other biometric methods [42], [43]. The iris's complex texture provides a vast amount of distinctive data points that can be captured and converted into a digital template, making it particularly suited for environments where high security is required, such as government systems [44], financial institutions [45], and blockchain-based platforms.

TABLE I
RELATED WORK

Ref	Title	Keywords	Main contribution	Biometrics
[22]	A distributed biometric authentication scheme based on blockchain	biometric, authentication, blockchain, homomorphic encryption, privacy	Users authentication and storage of biometrics template in IPFS	General
[23]	Blockchain-based user re-enrollment for biometric authentication systems	Authentication, Biometric, Blockchain, Re-enrollment, Secure Multi-Party Computation	Protection of users privacy using a secure multi-party computation	General
[24]	Cross-Domain Identity Authentication Protocol of Consortium Blockchain Based on Face Recognition	cross-domain authentication, consortium blockchain, ArcFace, biometric	Cross-domain authentication using an encryption system in a consortium Blockchain	Face
[25]	Privacy Preserving Biometric Authentication on the blockchain for smart healthcare	Privacy Preserving Biometric Authentication (PPBA), Smart healthcare, Blockchain, Monero, Hill climbing attacks, Low-entropy, Identity privacy, Public Key Cryptography (PKC), Zero Knowledge Proofs (ZKP), GDPR, IPFS	Blockchain-based biometric authentication	General
[26]	Biometric Creation of Digital Signatures and Their Application in Blockchain	Blockchain, Biometrics, Fuzzy Signature, PKI, Payment card system	Analysis of digital signatures using biometrics in a Blockchain	General
[28]	Blockchain-based Secure Storage Model for Multimodal Biometrics Using 3D Face and Ear	Blockchain, Biometric, Security, Ethereum	Storage of multimodal biometrics in a Blockchain	Face and ear
[29]	An efficient security system based on cancelable face recognition with blockchain over cognitive IoT	Blockchain, Cancelable biometrics, Image authentication, Machine learning, Face recognition	Securing IoT applications using Blockchain to check the truthfulness of biometric data	Face
Our contribution		Blockchain, Key-pair generation, Iris scan, Biometrics	Using extracted features of a biometric to obtain an hash used as a seed for generating a key-pair	Iris

In the context of this paper, the biometric data from iris scans is used to generate a cryptographic seed, ensuring that the derived key pairs are unique to the individual and securely tied to their identity. This biometric method surpasses traditional password-based systems in security, as it is extremely difficult to replicate or forge a user's iris data.

C. Key-Pair Generation

Key-pair generation is a fundamental process in Blockchain systems, where each user is assigned a public key and a private key. This cryptographic mechanism, known as asymmetric cryptography, ensures that the private key, which is kept secret, can be used to sign transactions, while the public key can be used by others to verify the signature. The use of key-pairs guarantees that transactions can be securely authenticated without revealing the identity of the user [46].

The processes of hashing and key-pair generation employed in this work follow standard Blockchain-based systems. The SHA-256 algorithm is utilized to hash the feature vector extracted from the iris scan. SHA-256 ensures non-reversibility and a high level of cryptographic security. For key-pair generation, we use the Edwards-curve Digital Signature Algorithm (EdDSA), which provides secure and efficient asymmetric cryptography. These methods are widely adopted in Blockchain platforms to maintain robustness and reliability. The generated keys have the same level of entropy and security as traditional Blockchain systems, ensuring full compatibility and robustness.

The process of generating key-pairs is enhanced by incorporating biometric data as the seed for the cryptographic algorithm. Seeds are values from which cryptographic key-pairs can be deterministically generated. Using iris-based biometric data as a seed increases security because the biometric data is unique and bound to a specific individual. The key-pair derived from this seed allows the user to sign and verify transactions within the Blockchain, without compromising the privacy of their biometric data.

Entropy analysis reveals that the keys generated using iris-based seeds achieve equivalent or superior security compared to traditional methods. With 256-bit hash-based seeds, the keys exhibit high randomness and resilience against brute-force attacks [47].

D. Feature Extraction Algorithm

Feature extraction is a critical step in biometric systems, as it involves processing biometric inputs to extract distinctive features that can uniquely identify an individual [48]. In this work, a Convolutional Neural Network (CNN) is employed to extract features from iris scan data. CNNs are a class of deep learning models particularly effective in image analysis tasks due to their ability to automatically detect relevant features

in a hierarchical fashion through multiple convolutional layers [49], [50].

The iris scan is processed by the CNN, which transforms the image into a numerical feature vector that encapsulates the unique attributes of the individual's iris. This feature vector is then hashed using a cryptographic hash function, such as SHA-256, to ensure the resulting seed is non-reversible. The hash function provides an added layer of security by ensuring that the original biometric data cannot be reconstructed from the hash. This hashed seed is used in the key-pair generation process, ensuring that the keys are both unique and secure.

The use of CNNs for feature extraction offers a high level of accuracy and robustness in distinguishing between individual users, which is essential in biometric-based authentication systems [51], [52]. By leveraging the power of deep learning, this approach ensures that the biometric data is processed efficiently, resulting in high-quality cryptographic keys for use in Blockchain-based platforms.

IV. Architecture

The architecture of the proposed system is designed to securely handle biometric data, particularly iris scans, for the purpose of generating a seed used in key-pair generation within a Blockchain platform. The architecture consists of several interconnected modules responsible for different stages of enrollment, authentication, and key generation. Each module is designed to ensure data integrity, security, and privacy while maintaining a decentralized approach through the use of Blockchain.

A. System Overview

The system architecture is divided into three primary modules, as depicted in Fig. 1: (i) the Template Generation module, which extracts features from the submitted iris scan, (ii) the Enrollment Request (Sign-Up) module, which handles user registration and ensures that each user is uniquely enrolled, and (iii) the Authentication Request (Sign-In) module, which verifies that the user's biometric data matches the enrolled profile. Each of these modules communicates with the Blockchain network for secure storage and retrieval of the relevant biometric data.

The primary objective of the architecture is to securely generate and manage key-pairs by using iris scans while distributing the biometric data across multiple nodes in the Blockchain. This decentralized approach increases security by ensuring that no single node has access to the complete biometric template, thus minimizing the risk of data theft or compromise.

B. Data Flow and Process

The data flow in the system begins with the user submitting their iris scan through the client-side application. This data is passed through the Template Generation module, where a Convolutional Neural Network (CNN) extracts the unique features of the iris. The resulting feature vector is then hashed using a cryptographic hash function, such as SHA-256, to generate a non-reversible and secure representation of the biometric data.

Once the feature vector is processed, the Enrollment Request module handles the registration of the user in the Blockchain. If the user is enrolling for the first time, the system checks the uniqueness of the submitted biometric data by comparing the feature vector to the stored fragments in the Blockchain. The system ensures that no two users share the same biometric signature, thus preventing duplicate enrollments. Once the uniqueness is confirmed, the system generates a key-pair based on the hashed feature vector.

During the authentication process, the user submits their iris scan again, which is processed similarly to the enrollment phase. The Authentication Request module compares the newly submitted feature vector with the stored fragments in the Blockchain. If the comparison yields a match, the user is authenticated, and access is granted.

C. Distributed Storage of Biometric Data

A critical aspect of the system's architecture is the distributed storage of biometric data. To enhance security and fault tolerance, the extracted feature vector from the iris scan is divided into multiple fragments, which are stored across different nodes in the Blockchain network. Each fragment is stored in random nodes, ensuring that no single node holds the complete biometric template.

This fragmentation and distribution of biometric data significantly reduce the risk of data breaches, as an attacker would need to compromise multiple nodes to reconstruct the full feature vector. Furthermore, each fragment is stored with replication to ensure redundancy and fault tolerance. The system uses a consensus mechanism to guarantee that data fragments are securely and consistently stored across the network.

The decision to adopt a distributed architecture ensures that the system remains highly available and scalable. Even in the event of node failures, the redundant storage of fragments across multiple nodes allows the system to continue operating without data loss or disruption.

For the management of the enrollment and authentication phases, the adopted distributed architecture guarantees the requirements of (a) reliability of the entire system without relying on a central point, (b) availability of the network at any given moment, (c) robustness and fault tolerance: no single point failures and (d) scalability. The solution adopts a logical subdivision of the network into organizations characterized by two types of nodes called superpeers and peers, as shown in Fig. 2.

D. Fault Tolerance and Redundancy

The architecture incorporates several fault tolerance mechanisms to ensure the system's reliability. Each fragment of the biometric data is replicated across multiple nodes, ensuring that if one node fails, the data can still be retrieved from other nodes. This redundancy is crucial for maintaining the system's availability, especially in a decentralized network where individual nodes may go offline.

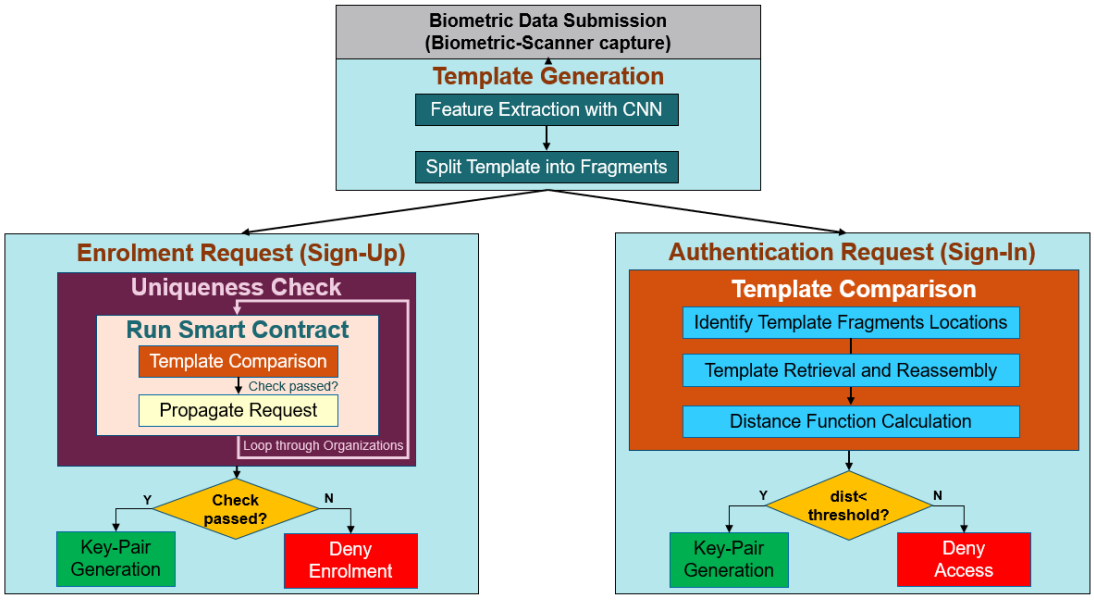

Fig. 1. Architecture of the proposed approach

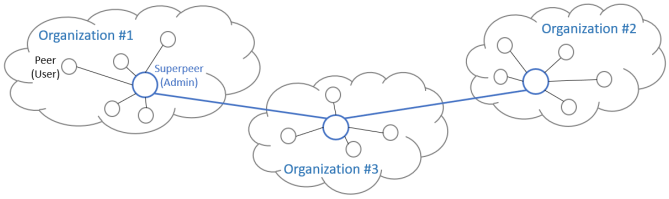

Fig. 2. Distributed architecture organization

In addition, the architecture uses a Byzantine Fault Tolerance (BFT) consensus mechanism to ensure that even if some nodes behave maliciously or unpredictably, the system as a whole remains secure. This consensus model is particularly suited for permissioned Blockchain networks like Hyperledger Fabric, where trust between participants is necessary but cannot always be guaranteed.

The redundancy and fault tolerance features allow the system to handle node failures, network partitioning, and other potential disruptions without compromising the security or availability of the biometric data or the key-pair generation process.

E. Security Considerations

Security is a critical concern in the proposed architecture, particularly given the sensitive nature of biometric data. Several layers of security are incorporated into the design to mitigate potential risks:

- **Data Encryption:** All biometric data, including the feature vector fragments, are encrypted before being stored in the Blockchain. This ensures that even if an attacker gains access to a node, they cannot reconstruct the original biometric data.
- **Decentralization:** By distributing biometric data across multiple nodes, the architecture reduces the risk of data breaches. No single point of failure exists, and attackers would need to compromise a significant portion of the network to access complete biometric information.
- **Sybil Attack Prevention:** To prevent Sybil attacks (where malicious actors control multiple nodes in the network), the system requires nodes to authenticate themselves using cryptographic keys and membership certificates issued by a trusted Certificate Authority (CA) in the Hyperledger Fabric network.
- **Smart Contract Security:** All enrollment, authentication, and storage operations are handled by smart contracts deployed on the Blockchain. These smart contracts ensure that biometric data is handled securely and that no unauthorized modifications are made to the stored data.

These security measures are designed to protect the integrity of the system while ensuring the privacy of the users.

1) Potential Risks and Mitigation Strategies: Despite its strengths, the system faces certain risks, such as data compromise during distributed storage and potential Sybil attacks on the network. To mitigate these, all biometric data fragments can be encrypted with advanced cryptographic techniques. Moreover, Blockchain systems employ a robust Byzantine Fault Tolerance mechanism to handle malicious nodes. Regular audits and updates to the smart contracts further ensure data integrity.

F. Smart Contract Integration

Smart contracts play a vital role in managing the enrollment and authentication processes. During enrollment, the smart contract verifies the uniqueness of the submitted biometric data and stores the template fragments across different nodes. It also logs the user's key-pair in the Blockchain ledger, ensuring transparency and immutability.

For authentication, the smart contract retrieves the relevant template fragments and compares the newly submitted bio-

metric data to the stored templates. If the match is successful, the contract grants access to the user and updates the ledger with the authentication transaction.

Smart contracts are written in Go and deployed on the Hyperledger Fabric network. These contracts are essential to the system's operation, providing the business logic necessary to manage user data, process transactions, and ensure the secure handling of biometric information.

G. System Workflow

The complete system workflow, from enrollment to authentication, can be summarized in the following steps, as shown in Fig. 3:

1) User submits an iris scan via the client-side application.
2) The scan is processed by the Template Generation module, which extracts a feature vector using a CNN.
3) The feature vector is hashed and divided into multiple fragments, which are stored across the Blockchain network.
4) During enrollment, the system verifies that the biometric data is unique and generates a key-pair for the user.
5) During authentication, the user submits another iris scan, which is processed and compared to the stored fragments.
6) If the biometric data matches, the user is authenticated, and access is granted.

This workflow ensures that biometric data is handled securely at every stage, from initial submission to key-pair generation and user authentication.

V. Implementation

A Web Application named Iris-Chain has been developed to handle the user's biometric data, the connection to the permissioned Blockchain to perform the enrollment or authentication tasks, and the generation of the user's key-pair starting from the submitted biometric material and the subsequent registration of the performed transaction in the Distributed Ledger. The languages and technologies adopted to implement the proposed architecture are: a) biometric materials: iris; b) client-side application: ReactJS framework; c) server-side application: NodeJS; d) template generation: PyTorch; e) feature extraction: ResNet18 CNN; f) distance function: cosine distance; g) hash function: SHA256; h) Blockchain: Hyperledger Fabric; i) signature algorithm: EdDSA; j) smart contracts: GO.

A. Client-side and server-side application

The client-side of the web application has been developed using JavaScript and the React framework.
The user first has to authenticate to access the Iris-Chain platform, which means signing in if the enrollment step has already been completed or signing up in the case of first access. In both cases, the platform will require the user to provide his username and submit the biometric material. Then, the username and the iris image are fetched from a peer in the network through an HTTP POST request. After the server-side calculation is complete, the user will be forwarded to a page that displays the result of the enrollment/authentication request.

The server-side of the web application has been developed using JavaScript and the Node.js framework. Its main function is to receive the biometric material from the client and compute the feature vector by performing a feature extraction using the last convolutional layer of "ResNet18" Convolutional Neural Network (CNN) from the PyTorch framework. The resulting feature vector, which consists of 262144 float64 values, is then divided into 3 fragments. Regardless of the request type, the network node needs to check first whether the submitted username is already present in the ledger. Then, if the request type is a sign up, the submitted username must be new to the ledger; if the request is a sign in, the username must already be present in the ledger. The smart contract "searchUser" has been developed to perform this query. The next operations that are carried out differ based on the request type. If a user wants to enroll, the peer checks the uniqueness of the submitted biometric material by comparing the feature vector extracted from the submitted image with the feature vectors of all the users currently enrolled in the platform. The information regarding which node of the network stores a Template Fragment for a certain user is included in the ledger. To retrieve these locations, the smart contract "searchTemplate" has been developed. For a given user, the output of this task is an extract of the ledger, providing the assets related to the storing locations of their template fragments (i.e., the address of the storing peer, its port number, and the identification number of the fragment it stores), as shown in Fig. 4.

The feature vector of an enrolling user is compared to the templates of every user already enrolled in the network. If the cosine distance of the submitted feature vector is equal to or above the defined threshold, access to Iris-Chain is granted to the enrolling user. The submitted biometric material is stored on randomly selected peers of the network, with each Template Fragment having n replicas to ensure fault tolerance. In the event that the user successfully enrolls/authenticates, a key-pair for asymmetric cryptography is provided. An elliptic-curve cryptography method has been used to generate key pairs with the Edwards-curve Digital Signature Algorithm (EdDSA). The complexity of the implemented method, used to detect whether a submitted iris image belongs to a certain individual or not, is kept to a simple level with the usage of cosine distance. In any case, being extremely unrealistic to have two perfectly identical acquisitions of the iris of one individual, and with it therefore two perfectly identical feature vectors, our approach is capable to provide to the same person a novel key-pair at every access.

The pseudocode for identifying template fragments locations is shown in Algorithm 1, the pseudocode for the authentication request is shown in Algorithm 2, while the pseudocode for the enrollment request is proposed in Algorithm 3.

The Hyperledger Fabric platform of the Linux Foundation was chosen for the creation of the Blockchain. Furthermore, unlike other Blockchain systems, Hyperledger Fabric is private and authorized. Rather than an open, permissionless system

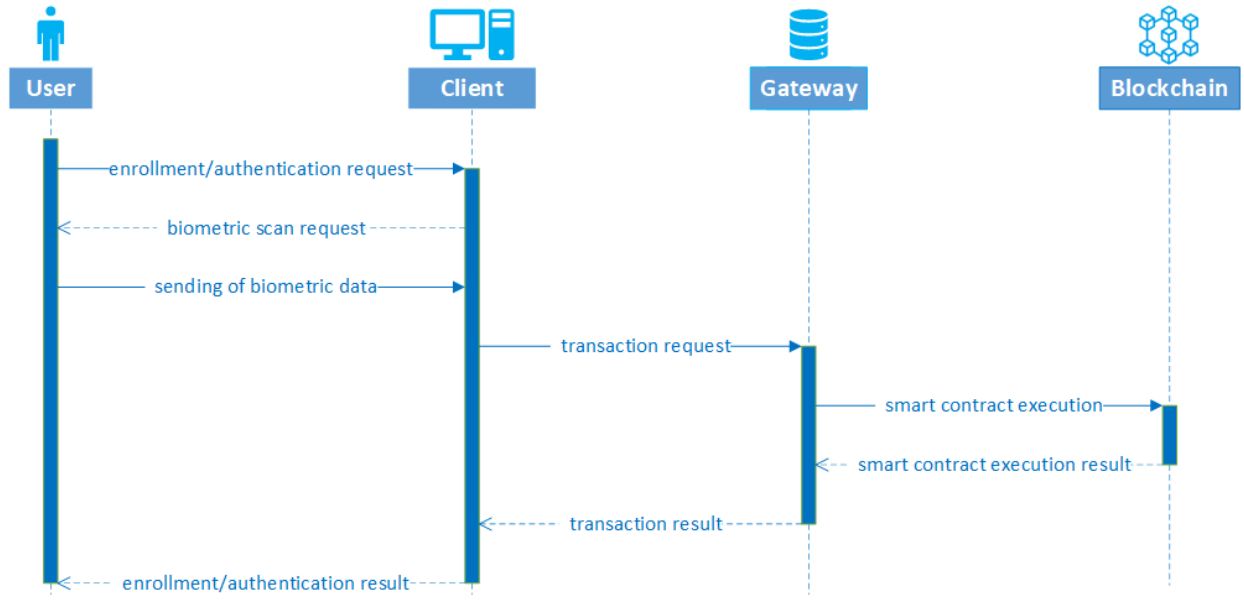

Fig. 3. UML Sequence diagram

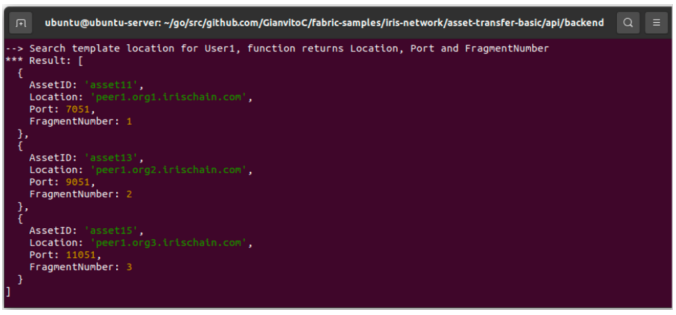

Fig. 4. "Search template" smart contract output

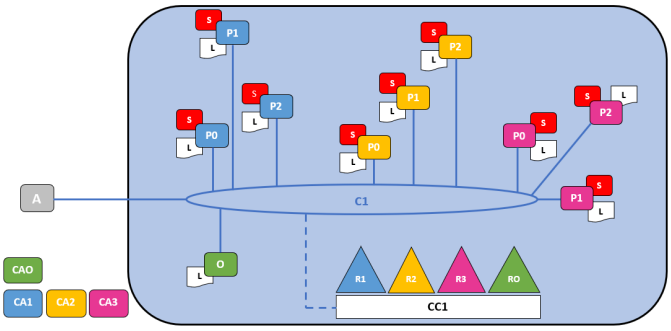

Fig. 5. HyperLedger Fabric network topology

Algorithm 1 Identify Template Fragments Locations: $searchTemplate(ledger, user)$

$ledger \leftarrow$ `connection instance to HyperLedger`
$user \leftarrow$ `provided Username`
$userInfo \leftarrow []$
for $asset$ `in` $ledger$ **do**
  if $user == asset.userID$ **then**
    $info = [asset.Location, asset.FragmentNumber]$
    $userInfo.append(info)$
  end if
end for
return $userInfo$

that allows unknown identities to join the network, members of a Hyperledger Fabric network sign up through a service provider membership (MSP). This feature is essential for certifying biometric information. The topology implemented for our purposes is shown in Fig. 5.

The infrastructure of the blockchain network consists of the R1, R2, R3, and RO organizations that interact through the C1 channel. Channel C1 features the CC1 configuration, agreed upon by all organizations, which includes definitions for all organizations and policies that define each organization's roles. In particular, in this implementation, the organizations R1, R2, and R3 will take care of joining the peers to the network, while RO owns O, the ordering service for the channel. The decision to implement a network with 3 peers per organization is in line with the decision to segment the features of the scanned iris into 3 segments so as to have a multiple of 3 peers. Peers P* and ordering node O will contain a copy of the channel ledger (L), which is the structure where transactions are recorded. P* peers represent the physical point with which organizations connect to the channel and through which they interact with the channel by carrying out transactions. The business logic that governs the transactions is implemented in the smart contract (S), which, according to the Hyperledger Fabric life cycle, has undergone the following phases: (i) packaged in a chaincode, (ii) installed on every peer in every organization, (iii) approved by every organization, and (iv) committed to the channel. The ordering service (O) collects approved transactions and sorts them into transaction blocks, which are then sent to peers to record the transaction and update their local copy of the ledger. Organizations interact

Algorithm 2 Authentication Request: $authenticate(ledger, user, biometric)$

Import: $searchTemplate$
$ledger \leftarrow$ `connection instance to HyperLedger`
$user \leftarrow$ `provided Username`
$biometric \leftarrow$ `feature vector extracted from submitted biometric material`
$template \leftarrow$ `empty`
$userInfo \leftarrow searchTemplate(ledger, user)$
if $userInfo.length > 0$ **then**
  for $fragmentNum.unique$ `in` $userInfo$ **do**
    $fragment = GET(userInfo.Location[fragmentNum])$
    $template.concatenate(fragment)$
  end for
  if $cosineDistance(biometric, template) <$ `threshold` **then**
    $keyPair \leftarrow generateKeyPair(SHA256(biometric))$
    $ledger.storeTransaction$
    return $keyPair$
  else
    // Authentication denied
    $ledger.storeTransaction$
  end if
else
  `// User not enrolled, authentication denied`
  alert("User not enrolled")
end if

Algorithm 3 Enrollment Request: $enroll(ledger, user, biometric)$

Import: searchTemplate
$ledger \leftarrow$ `connection instance to HyperLedger`
$user \leftarrow$ `provided Username`
$biometric \leftarrow$ `feature vector extracted from submitted biometric material`
$template \leftarrow$ `empty`
$index \leftarrow 0$
$flag \leftarrow False$
$userInfo \leftarrow searchTemplate(ledger, user)$
if $userInfo.length > 0$ **then**
  alert("Username already registered in the Blockchain")
else
  while $flag == False$ **do**
    $userInfo \leftarrow searchTemplate(ledger, index)$
    for $fragmentNum.unique$ `in` $userInfo$ **do**
      $fragment = GET(userInfo.Location[fragNum])$
      $template.concatenate(fragment)$
    end for
    $flag \leftarrow cosineDistance(biometric, template) <$ `threshold`
    $index \leftarrow index + 1$
  end while
  if $flag == False$ **then**
    $keyPair \leftarrow generateKeyPair(SHA256(biometric))$
    $POST(biometric)$
    $ledger.storeTransaction$
    return $keyPair$
  else
    alert("User not enrolled")
  end if
end if

with the channel through the client application (A), which interacts with the network through the Fabric Gateway. All organizations have a Certificate Authority (CA) that generates the necessary certificates for their organization's nodes, administrators, organization definitions, and applications.

VI. Validation

To validate the proposed architecture, several testing scenarios were designed to evaluate the system's performance, security, and scalability, as shown in Table II. The validation process includes a series of functional tests, performance evaluations, and security analyses to ensure that the system operates reliably and efficiently under various conditions. Additionally, comparisons with existing biometric-based authentication systems highlight the advantages of the proposed solution in terms of security and performance.

A. Validation Scenarios

Six primary testing scenarios were defined to validate the correctness and robustness of the system:

- **Scenario 1 (Enrollment of a New User):** A user whose biometric data is not present in the system submits a valid username and iris scan for the first time. The system successfully generates a key-pair, stores the biometric data fragments across the network, and provides the private key to the user.
- **Scenario 2 (Duplicate Enrollment Attempt):** A user who has already enrolled attempts to enroll again using a different username. The system correctly identifies the biometric data as already registered and denies the new enrollment request, preventing duplicate accounts.
- **Scenario 3 (Username Conflict):** A new user attempts to enroll using a username that has already been taken by another individual. The system detects the conflict and prompts the user to choose a different username, ensuring that username collisions do not occur.
- **Scenario 4 (Correct Authentication):** A previously enrolled user submits their biometric data for authentication. The system successfully matches the submitted iris scan with the stored template fragments, generates a new key-pair, and grants access to the user.
- **Scenario 5 (Authentication Attempt with Another User's Credentials):** A user attempts to authenticate using another individual's username and submits their own biometric data. The system correctly denies access, as the biometric data does not match the stored template for the given username.
- **Scenario 6 (Unregistered User Authentication):** An individual who has not enrolled in the system attempts to

TABLE II
VALIDATION SCENARIOS, CONDITIONS AND EFFECTS

Scn	Required process	Already enrolled	Chosen username	Effect	Description
a	Enrollment	No	Available	User successfully enrolled	Private Key provided to user
b	Enrollment	Yes	Available	Enrollment denied	Enrollment denied
c	Enrollment	No	Not available	Enrollment denied	Choose another username (new users) or sign-in (enrolled user mistakenly signing-up again)
d	Authentication	Yes	His own	User successfully authenticated	Private Key provided to user
e	Authentication	Yes	Another user's	Authentication denied	Authentication denied
f	Authentication	Yes	Not present in the ledger	Authentication denied	Check the submitted username (username mistakenly typed) or sign-up (new user)

authenticate using a username that is not present in the ledger. The system denies access and prompts the user to enroll first, ensuring that unregistered users cannot access the system.

These scenarios demonstrate the system's ability to handle various edge cases, ensuring that it behaves securely and reliably under normal and exceptional conditions.

Performance tests were conducted to evaluate the efficiency of the system, particularly focusing on the speed of key-pair generation and the latency of biometric data processing

1) Key-Pair Generation Time: The system was tested for the time required to generate a key-pair using the EdDSA cryptographic algorithm with a biometric seed derived from the iris scan. Comparisons were made between key-pair generation using a random seed (32-byte) and the proposed method using the 2-MB iris-based seed. Results showed that while the use of a biometric seed increased the time for key-pair generation slightly (from 31 ms to 47 ms), the increase in time was not significant enough to impact system usability. Even under stress tests involving the simultaneous generation of 1000 key-pairs, the system exhibited a moderate increase in processing time from 8.5 seconds to 14.1 seconds. This performance is deemed acceptable for practical applications where user key-pair generation happens infrequently. Graphical results are shown in Fig. 6.

2) Latency in Distributed Storage and Retrieval: The latency involved in storing and retrieving biometric template fragments was measured across a network of nodes. Tests showed that the time to store the fragments across three randomly selected nodes averaged 250 ms, while retrieval of the fragments for authentication averaged 300 ms. The system demonstrated efficient handling of biometric data, even under load, with minimal delays during the authentication process. This performance ensures a smooth user experience during both enrollment and authentication phases.

B. Comparative Analysis

The proposed system was compared to existing biometric-based authentication systems in terms of security, performance, and scalability. In contrast to traditional systems where biometric data is stored centrally, the proposed architecture's use of distributed storage significantly enhances security by mitigating the risk of data breaches. Additionally, the performance metrics for key-pair generation and biometric processing were comparable to state-of-the-art systems, with the added benefit of using biometric data as a cryptographic seed for key-pair generation.

While performance benchmarks are valuable for evaluation, a direct comparison with other systems is challenging due to the lack of detailed metrics, such as processing time and error rates, in existing literature on Blockchain-based biometric systems. For instance, paper [27] analyzes biometrics in Blokchain obtaining an authentication time of 680 ms, but it does not cover error rates. Most studies focus on architectural or security features without providing quantitative measures of system performance. This highlights the need for future research to standardize performance reporting in this domain.

C. Scalability Tests

To evaluate the system's scalability, stress tests were performed involving multiple concurrent users. The system was able to handle up to 1000 simultaneous authentication requests with an average latency increase of only 200 ms. In larger networks with more nodes, the system demonstrated linear scalability, as the distributed nature of the architecture allows for the parallel handling of authentication and enrollment requests. This ensures that the system can be scaled to accommodate a large user base without significant performance degradation.

D. Summary of Results

The validation tests conducted on the proposed system confirm that it operates securely and efficiently under various conditions. The system was able to successfully handle edge cases, mitigate security threats, and perform well under stress tests. In summary, the system provides a robust and scalable solution for integrating biometric data into Blockchain-based key-pair generation, with clear advantages in terms of security, performance, and scalability.

VII. CONCLUSION

In this paper, we presented a novel approach to key-pair generation in Blockchain systems that utilizes iris-based

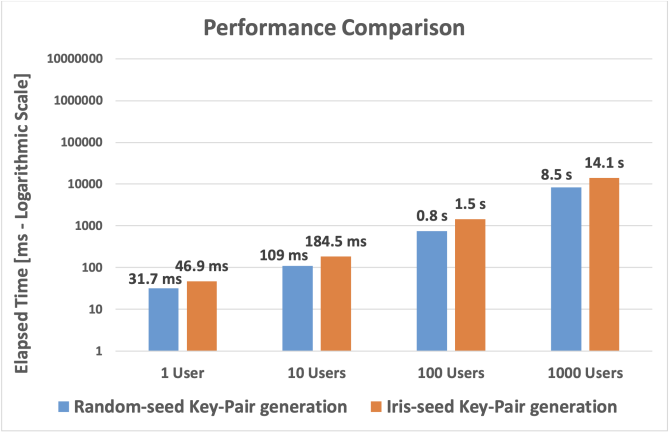

Fig. 6. Required time comparison to generate 1, 10, 100 and 1000 simultaneous key-pairs

biometric data. Our proposed architecture successfully addresses the challenges of identity management and privacy by securely integrating biometric authentication with Blockchain technology. By using a non-reversible hash of the biometric data as a seed for key-pair generation, we ensure that sensitive user information remains protected while enabling secure and efficient access to digital resources.

The findings of this study highlight several key contributions to the field. First, the proposed system significantly enhances the security of identity verification processes by leveraging the unique characteristics of iris scans, which are difficult to replicate or forge [53], [54]. This advancement is particularly relevant in an era where traditional authentication methods, such as passwords, are increasingly vulnerable to cyber threats. Additionally, the distributed storage of biometric fragments across multiple nodes in the Blockchain provides a robust defense against data breaches, ensuring that no single point of failure exists.

The implications of this research extend beyond academic interest; the proposed system has the potential to revolutionize various sectors that require secure identity management [11], [55], [56]. In the financial industry, for example, our architecture can enhance transaction security by ensuring that only authorized users can access their accounts. In healthcare, where patient data privacy is paramount, the integration of biometric authentication can facilitate secure access to sensitive medical records [57]. Furthermore, the application of this technology in e-voting systems can ensure both voter anonymity and integrity, fostering greater trust in democratic processes [58].

While this work lays the groundwork for integrating biometrics with Blockchain technology, several avenues for future research remain. Enhancing the feature extraction process through advanced deep learning techniques could improve accuracy and reliability, enabling the system to handle a wider range of biometric modalities. Exploring the integration of other biometric traits, such as fingerprints or facial recognition, could further broaden the applicability of the proposed system. Additionally, future studies could focus on optimizing the scalability of the architecture to accommodate a growing user base and increasing transaction volumes.

The integration of biometrics and Blockchain technology presents a promising solution to the pressing challenges of digital identity management. By addressing security, privacy, and usability concerns, our proposed system represents a significant step forward in the quest for secure authentication methods in a rapidly evolving digital landscape.

Future work includes exploring scalability for national-scale implementations by segmenting the Blockchain into regional sub-networks. Additionally, integrating advanced deep learning models like Vision Transformers could improve feature extraction accuracy. Expanding compatibility to support multimodal biometrics, such as fingerprints and voice recognition, would enhance system versatility. To address accessibility challenges, the architecture can be adapted to accept various biometric inputs, such as fingerprints or voice recognition. This would involve modifying the feature extraction pipeline to accommodate diverse data formats while maintaining the security principles of distributed storage and cryptographic hashing. Future research will also include more extensive comparisons with existing systems and larger-scale tests to evaluate performance under broader use cases. The development of a benchmarking tool regarding biometric authentication in Blockchain systems is also being considered.

As we move towards a future where digital interactions are increasingly prevalent, the adoption of robust solutions that combine the strengths of biometrics and Blockchain will be essential for ensuring trust and security in digital transactions.

REFERENCES

[1] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets internet of things: Characteristics, challenges, and business opportunities," *Journal of industrial information integration*, vol. 15, pp. 21–28, 2019.

[2] K. K. Vaigandla, R. Karne, M. Siluveru, and M. Kesoju, "Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications," *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 73–84, 2023.

[3] V. Ali, A. A. Norman, and S. R. B. Azzuhri, "Characteristics of blockchain and its relationship with trust," *Ieee Access*, vol. 11, pp. 15364–15374, 2023.

[4] G. Spadavecchia, M. Fiore, M. Mongiello, and D. De Venuto, "A Novel Approach for Fast and Secure Data Transmission using Blockchain and IoT," in *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–4, June 2024.

[5] M. Mongiello, F. Nocera, A. Parchitelli, L. Patrono, P. Rametta, L. Riccardi, and I. Sergi, "A smart iot-aware system for crisis scenario management," *Journal of Communications software and Systems*, vol. 14, no. 1, pp. 91–98, 2018.

[6] M. Mongiello, F. Nocera, A. Parchitelli, L. Riccardi, L. Avena, L. Patrono, I. Sergi, and P. Rametta, "A microservices-based iot monitoring system to improve the safety in public building," in *2018 3rd International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, IEEE, 2018.

[7] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *Journal of network and computer applications*, vol. 166, p. 102731, 2020.

[8] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," *ICT express*, vol. 7, no. 1, pp. 76–80, 2021.

[9] Z. A. Khattak, S. Sulaiman, and J.-L. Ab Manan, "A study on threat model for federated identities in federated identity management system," in *2010 International Symposium on Information Technology*, vol. 2, pp. 618–623, IEEE, 2010.

[10] C. K. Dominicini, M. Simplício, R. R. Sakuragui, T. Carvalho, M. Näslund, and M. Pourzandi, "Threat modeling an identity management system for mobile internet," in *Proc. of the 9th International Information and Telecommunication Tech. Symposium (I2TS)*, 2010.

[11] R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion," *Computers and Electrical Engineering*, vol. 119, p. 109485, 2024.

[12] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, "A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection," *IEEE Access*, 2024.

[13] S. Pahuja and N. Goel, "Multimodal biometric authentication: A review," *AI Communications*, no. Preprint, pp. 1–23, 2024.

[14] S. M. Arman, T. Yang, S. Shahed, A. Al Mazroa, A. Attiah, and L. Mohaisen, "A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions," *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 78, no. 2, pp. 2087–2110, 2024.

[15] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, and C. Busch, "An overview of privacy-enhancing technologies in biometric recognition," *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–28, 2024.

[16] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-based biometric identity management," *Cluster Computing*, vol. 27, no. 3, pp. 3741–3752, 2024.

[17] J. K. Adeniyi, S. A. Ajagbe, E. A. Adeniyi, P. Mudali, M. O. Adigun, T. T. Adeniyi, and O. Ajibola, "A biometrics-generated private/public key cryptography for a blockchain-based e-voting system," *Egyptian Informatics Journal*, vol. 25, p. 100447, 2024.

[18] H. Cai, H. Li, J. Xu, L. Li, and Y. Zhang, "Bpkem: A biometric-based private key encryption and management framework for blockchain," *Plos one*, vol. 19, no. 3, p. e0286087, 2024.

[19] J. Lai, T. Wang, S. Zhang, Q. Yang, and S. C. Liew, "Biozero: An efficient and privacy-preserving decentralized biometric authentication protocol on open blockchain," *arXiv preprint arXiv:2409.17509*, 2024.

[20] N. A. Alzahab, G. Rafaiani, M. Battaglioni, F. Chiaraluce, and M. Baldi, "Decentralized biometric authentication based on fuzzy commitments and blockchain," *arXiv preprint arXiv:2409.11303*, 2024.

[21] Y. Kaga, Y. Matsuda, K. Takahashi, and A. Nagasaka, "Biometric authentication platform for a safe, secure, and convenient society," *Hitachi Review*, vol. 64, no. 8, p. 473, 2015.

[22] F. Toutara and G. Spathoulas, "A distributed biometric authentication scheme based on blockchain," in *2020 IEEE International Conference on Blockchain (Blockchain)*, pp. 470–475, IEEE, 2020.

[23] N. Hamian, M. Bayat, M. R. Alaghband, Z. Hatefi, and S. M. Pournaghi, "Blockchain-based user re-enrollment for biometric authentication systems," *IJ of Electronics and Information Engineering*, vol. 14, no. 1, pp. 18–38, 2022.

[24] X. Chen, S. Xu, K. Ma, and P. Chen, "Cross-domain identity authentication protocol of consortium blockchain based on face recognition," *Information*, vol. 13, no. 11, p. 535, 2022.

[25] N. D. Sarier, "Privacy preserving biometric authentication on the blockchain for smart healthcare," *Pervasive and Mobile Computing*, vol. 86, p. 101683, 2022.

[26] N. Badovinac and D. Simić, "Biometric creation of digital signatures and their application in blockchain," in *Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the Post-COVID Era*, pp. 3–13, Springer, 2022.

[27] Y. K. Lee and J. Jeong, "Securing biometric authentication system using blockchain," *ICT Express, Volume 7, Issue 3*, pp. 322–326, 2021.

[28] V. Kaur, D. P. Bhatt, S. Tharewal, and P. K. Tiwari, "Blockchain-based secure storage model for multimodal biometrics using 3d face and ear," in *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, pp. 860–865, IEEE, 2023.

[29] R. Kamal, E. E.-D. Hemdan, and N. El-Fishway, "An efficient security system based on cancelable face recognition with blockchain over cognitive iot," *Multimedia Tools and Applications*, pp. 1–21, 2023.

[30] W. Liang, Y. Liu, C. Yang, S. Xie, K. Li, and W. Susilo, "On identity, transaction, and smart contract privacy on permissioned and permissionless blockchain: A comprehensive survey," *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–35, 2024.

[31] M. Fiore, M. Frem, M. Mongiello, F. Bozzo, C. Montemurro, G. Tricarico, and A. Petrontino, "Blockchain-based food traceability in Apulian marketplace: Improving sustainable agri-food consumers perception and trust," *Internet Technology Letters*, p. e503, 2024.

[32] I. Abellán Álvarez, V. Gramlich, and J. Sedlmeir, "Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake," in *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*, pp. 278–287, 2024.

[33] P. R. Nair and D. R. Dorai, "Evaluation of performance and security of proof of work and proof of stake using blockchain," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pp. 279–283, IEEE, 2021.

[34] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the application of cryptography on the blockchain," in *Journal of Physics: Conference Series*, vol. 1168, p. 032077, IOP Publishing, 2019.

[35] F. Nocera, S. Abascià, M. Fiore, A. A. Shah, M. Mongiello, E. Di Sciascio, and G. Acciani, "Cyber-Attack Mitigation in Cloud-Fog Environment Using an Ensemble Machine Learning Model," in *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, IEEE, 2022.

[36] F. Nocera, S. Demilito, P. Ladisa, M. Mongiello, A. A. Shah, J. Ahmad, and E. Di Sciascio, "A user behavior analytics (uba)-based solution using lstm neural network to mitigate ddos attack in fog and cloud environment," in *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH 2022)*, pp. 74–79, IEEE, 2022.

[37] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "Ai-powered biometrics for internet of things security: A review and future vision," *Journal of Information Security and Applications*, vol. 82, p. 103748, 2024.

[38] D. Sharma and A. Selwal, "Biometrics: Introduction and applications," in *Leveraging Computer Vision to Biometric Applications*, pp. 1–18, Chapman and Hall/CRC, 2025.

[39] W. Yang, S. Wang, J. Hu, X. Tao, and Y. Li, "Feature extraction and learning approaches for cancellable biometrics: A survey," *CAAI Transactions on Intelligence Technology*, vol. 9, no. 1, pp. 4–25, 2024.

[40] A. Hassanpour, Y. Kowsari, H. O. Shahreza, B. Yang, and S. Marcel, "Chatgpt and biometrics: an assessment of face recognition, gender detection, and age estimation capabilities," *arXiv preprint arXiv:2403.02965*, 2024.

[41] A. Alqahtani, "Evaluation of the reliability of iris recognition biometric authentication systems," in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 781–785, IEEE, 2016.

[42] N. Kochher and S. Kochher, "Improving far and frr of an iris recognition system,"

[43] A. Bansal, R. Agarwal, and R. Sharma, "Far and frr based analysis of iris recognition system," in *2012 IEEE International Conference on Signal Processing, Computing and Control*, pp. 1–6, IEEE, 2012.

[44] S. Tambe-Jagtap, "The use of biometrics in digital identity: Legal implications for governments," *Biometric Technology Today*, pp. 10–17, 2024.

[45] R. C. Agidi, "Biometrics: the future of banking and financial service industry in nigeria," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 91–105, 2018.

[46] S. Y. Bonde and U. Bhadade, "Analysis of encryption algorithms (rsa, srnn and 2 key pair) for information security," in *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, pp. 1–5, IEEE, 2017.

[47] Y. Soulaimani and K. Nehéz, "Blockchain and hashing algorithms: A review," *Production Systems and Information Engineering*, vol. 11, no. 3, pp. 140–157, 2023.

[48] Y. Xu, D. Zhang, and J.-Y. Yang, "A feature extraction method for use with bimodal biometrics," *Pattern recognition*, vol. 43, no. 3, pp. 1106–1115, 2010.

[49] J. Gupta, S. Pathak, and G. Kumar, "Deep learning (cnn) and transfer learning: a review," in *Journal of Physics: Conference Series*, vol. 2273, p. 012029, IOP Publishing, 2022.

[50] L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma, J. Santamaría, M. A. Fadhel, M. Al-Amidie, and L. Farhan, "Review of deep learning: concepts, cnn architectures, challenges, applications, future directions," *Journal of big Data*, vol. 8, pp. 1–74, 2021.

[51] J.-h. Roh, S. Cho, and S.-H. Jin, "Learning based biometric key generation method using cnn and rnn," in *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pp. 136–139, IEEE, 2018.

[52] R. J. Tazim, M. M. M. Miah, S. S. Surma, M. T. Islam, C. Shahnaz, and S. A. Fattah, "Biometric authentication using cnn features of dorsal vein pattern extracted from nir image," in *TENCON 2018-2018 IEEE Region 10 Conference*, pp. 1923–1927, IEEE, 2018.

[53] A. A. AbdulRaheem and S. A. Hasso, "Key generation and testing based on biometrics," *AL-Rafidain Journal of Computer Sciences and Mathematics*, vol. 18, no. 1, 2024.

[54] D. Aparna, M. Malarkodi, S. Lakshmanaprakash, R. Priya, and A. Nair, "Data anonymization on biometric security using iris recognition technology," *Automated Secure Computing for Next-Generation Systems*, pp. 191–204, 2024.

[55] T. Arpitha, D. Chouhan, and J. Shreyas, "Anonymous and robust biometric authentication scheme for secure social iot healthcare applications," *Journal of Engineering and Applied Science*, vol. 71, no. 1, p. 8, 2024.
[56] S. Ayeswarya and K. J. Singh, "A comprehensive review on secure biometric-based continuous authentication and user profiling," *IEEE Access*, 2024.
[57] M. Z. Nezhad, A. J. J. Bojnordi, M. Mehraeen, R. Bagheri, and J. Rezazadeh, "Securing the future of iot-healthcare systems: A meta-synthesis of mandatory security requirements," *International Journal of Medical Informatics*, vol. 185, p. 105379, 2024.
[58] G. Sathwik, P. D. T. Reddy, M. Gupta, M. Rahul, and M. Dholvan, "Secured voting system based on multilayered biometric authentication," in *2024 Second International Conference on Inventive Computing and Informatics (ICICI)*, pp. 502–509, IEEE, 2024.

Marco Fiore was born in Puglia, Italy in 1997. He received the M.S. degree in Computer Science Engineering from the Polytechnic University of Bari, Italy, in October 2020, with full marks with honors. His master thesis was focused on Blockchain technology applied to agri-food traceability. He is a Ph.D. student and his main research interests regard Distributed Contexts, Blockchain and Software Engineering.

Federico Carrozzino was born in Puglia, Italy, in 1998. He received the master degree in computer engineering from the Polytechnic University of Bari, Italy, in November 2024. His master's thesis was focused on post-quantum cryptography applied to Flutter technology. His main research interests include cybersecurity, blockchain, and software engineering.

Gianvito Coppola was born in Puglia, Italy, in 1984. He received the M.S. degree (Hons.) in mechanical engineering from the Polytechnic University of Bari, Italy, in April 2011. He is currently pursuing the M.S. degree in computer science engineering. His professional career is focused on the design of control logics for embedded systems in automotive sector.

Gianni Guariglia was born in Puglia, Italy, in 1983. He received the Bachelor's degree in computer science engineering from the Polytechnic University of Bari, Italy, in July 2019. He is currently pursuing the M.S. degree in computer science engineering. His professional career is focused on the design of data architecture in financial sector.

Marina Mongiello is an Associate Professor at Politecnico di Bari. Her recent research interests include: Software Engineering and Software Architecture, Formal methods, and model checking, Mobile and distributed reasoning and applications, software architecture for self-adaptive and context-aware software. She has served in both organizing and in the Program Committee of several International conferences and workshops.