Computer Standards & Interfaces 92 (2025) 103929

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

DBAC-DSR-BT: A secure and reliable deep speech recognition based-distributed biometric access control scheme over blockchain technology

Oussama Mounnan [a,b], Larbi Boubchir [a,*], Otman Manad [a], Abdelkrim El Mouatasim [b], Boubaker Daachi [a]

[a] LIASD Laboratory, University of Paris 8, France
[b] LabSi Laboratory, AMCS Team, Ibn Zohr University, Morocco

ARTICLE INFO

Keywords:
Blockchain
Biometrics
Cybersecurity
Speech recognition
Deep learning
Access control

ABSTRACT

Speech recognition systems have been widely employed in several fields including biometric access control. In such systems, handling sensitive data represents a real threat and risk to security and privacy, namely in the central environment. This paper proposes an innovative solution that integrates speech recognition power as a biometric modality with the decentralized and tamper-resistant nature of blockchain technology aims at designing, implementing, and evaluating an access control system that not only leverages the unique characteristics of speech recognition through the AutoEncoding Generative Adversarial Network (AE-GAN) model for user authentication but also ensures the enforcement of access policies and voice templates storage through two distinct Smart Contracts. The first smart contract aims at storing the ID of encrypted templates matched to the hash of the public address and encrypted attributes. While the second smart contract incorporates the security policy and takes charge of generating an access token if the conditions have been satisfied. Which makes it easier to upgrade specific components without affecting the entire system. Moreover, this architecture delegates the extraction features, conversion into template, encryption, and similarity calculation functions of encrypted templates using homomorphic encryption to an API to provide more security, privacy, scalability and interoperability and reduce the overhead within the blockchain. This API interacts with the smart contract using Oracle services that ensure the interaction between on-chain and off-chain, which provide a reliable, fine-grained, and robust scheme. The simulation of this proposed scheme proves its robustness, efficiency, and performance in terms of security, reliability, and resistance to several attacks.

1. Introduction

Biometric access control solutions have revolutionized how organizations and enterprises secure and protect their physical spaces, digital assets and resources, and sensitive data. Traditional methods based on passwords, access cards, or PINs are prone to security breaches and identity theft. Hence, the need for robust and reliable biometric authentication systems has emerged. Their main purpose is to put in place measures and mechanisms that govern and manage access to resources or systems securely, preventing unauthorized access and providing security properties, including integrity, availability, and confidentiality. These systems offer several benefits, which include enhanced security, Non-transferable of individual traits unlike passwords and PINs, User-friendly, i.e., eliminating the need to remember passwords or carry access cards, velocity and efficiency of managing credentials, and enhanced accountability and traceability through the audit trail of access events. These systems [1,2] can use various biometric modalities, namely unique physiological or behavioral characteristics, to verify the individual's identity. Physiological biometrics consist of an individual's physical characteristics such as fingerprint, facial, iris, retina recognition, etc. The other focuses on an individual's behavior, including voice, gait, signature recognition, etc [3].

Speech recognition-based biometric access control systems are promising solutions used in various domains and aim at facilitating daily life through a panoply of applications that enhance security and access control. These systems offer significant advantages over other modalities such as fingerprint, faceprint, etc., namely Non-Intrusiveness (do not require physical contact) [4], efficiency and speed, convenience

* Corresponding author.
E-mail address: larbi.boubchir@univ-paris8.fr (L. Boubchir).

https://doi.org/10.1016/j.csi.2024.103929
Received 1 July 2024; Received in revised form 7 August 2024; Accepted 21 September 2024
Available online 24 September 2024

(does not require users to touch or look at a sensor), no need for additional hardware, and user identification over distance, etc. The advent of deep learning technology has revolutionized speech recognition-based biometric access control, enhancing its accuracy, adaptability, robustness, and versatility. Furthermore, this technology has opened up opportunities that were not available before, for deploying secure, reliable, and user-friendly access control systems in various industries and applications. However, its benefits include improved accuracy, which makes the system more reliable for access control, and end-to-end models, which can take raw audio data as input and directly produce the desired output, such as in user authentication cases, robustness to variability: handle variability such as changes in accent, pronunciation, and background noise, making speech recognition systems more robust and suitable for real-world environments, and accelerating hardware through GPU utilization.

However, although deep learning and its potential have contributed to the development of biometric access control mechanisms and provided a robust and reliable infrastructure, it still faces several significant security and privacy challenges [5]. Among these are security vulnerabilities such as spoofing and voice data theft. The confidentiality of stored voice templates can be at risk if not adequately securely stocked. Data tampering can affect the integrity of the system. Privacy limitations include concerns about user privacy and the necessity for consent and transparency in data collection. Maintaining user privacy may be difficult with cross-device authentication. Also, data breaches can lead to severe privacy implications. Furthermore, outsourcing voice recognition to third-party providers can introduce privacy risks.

Blockchain is a decentralized, distributed digital ledger technology that stores transactions on multiple computers, guaranteeing data security, transparency and immutability [6]. This technology has proved its efficiency in many projects in various fields including healthcare [7–10], education [11,12], food [13,14], security [15,16], etc., leveraging its potential, including transparency, security and data integrity, immutability, data encryption and decentralization, interoperability, resilience to centralized attacks, and user trust, etc. Several works have been proposed integrating this paradigm to overcome security and privacy concerns [17–19]. Each research has tackled an aspect of security properties and produced a new scheme that preserves and maintains system functionality securely. To address the aforementioned limitations and drawbacks of existing techniques, we proposed a novel speech recognition-based biometric access control scheme using blockchain. This latter allows application systems to create robust security measures without the need for a central authority. Our approach proposes: (i) a decentralized and distributed scheme for handling biometric access control, (ii) an auditable mechanism for managing biometric data, and (iii) an automated check of security policy to allow access to the resources. Our scheme offers safe biometric information management by running the first smart contract that checks the existence of an encrypted ID that is related to the encrypted data in the API. If exists, it demands the similarity value from an external API that takes charge of calculating the similarity between the encrypted templates through the oracle service that ensures the communication between blockchain, i.e., On-Chain and off-chain (outside). If the similarity value is greater than a threshold defined by the manager, another smart contract will be executed to check the policy deployed and will generate an access token to authenticate and allow access to the resource. This threshold is defined according to the security policy and critical actions level.

Generally, the main aspects that make our approach different from the previous studies are: It relies on a hybrid generative deep-learning model namely the AutoEncoding Generative Adversarial Network (AE-GAN) model [20] for features extraction and blockchain technology for the users' credentials storage and the deployment of security policy. Moreover, it resolves the transparency issues that leak personal information, despite using encryption mechanisms for all critical information. This feature is not tackled by all the presented previous studies. Furthermore, it separates the execution of the smart contract into two distinct parts, the first part is dedicated to the user's credentials storage and the second is for deploying policy security. This separation simplifies the development and maintenance processes without affecting any component.

The main contributions of this paper are summarized as follows:

- We suggested a novel scheme based on blockchain for biometric access control using speech recognition, that preserves the security and privacy of all system processes.
- We proposed a modular, scalable and granular access control scheme that makes use of maintenance and upgrades more straightforward, by dividing the processes into two parts, two different smart contracts.
- We presented a novel biometric access control based on speech recognition using deep learning, namely the AE-GAN model, that enables getting the relevant and robust speech features for authentication operation.
- We designed a novel granular biometric access control that tackles existing system issues such as biometric template protection, and unreliable access control and authentication procedure, by using homomorphic encryption.
- We established the implementation of our prototype to prove its operationality, functionality, performance in terms of robustness and accuracy and resistance to several attacks.

The rest of this paper is organized as follows: Section 2 presents a background of concepts related to the proposed contributions; including blockchain technology, blockchain Oracle, AE-GAN model, and homomorphic encryption; and related work overview. The proposed solution is presented in Section 3. The outcomes analysis and discussion are given in Section 4 including simulations and results, security analysis, performance analysis, approach limitations, and some innovative mechanisms that are beneficial in such system. Finally, the conclusion and future work are presented in Section 5.

2. Background and related work overview

This section provides an overview of the technologies and backgrounds relevant to our solution, along with recent advances in research conducted in this field of study.

2.1. Blockchain technology

Blockchain is a data storage and transmission technology in a decentralized and secure manner. This paradigm was designed by Satoshi Nakamoto [21]. The principle it operates on is based on the decentralization aspect, without requiring third party, and distribution, tackling the challenges of centralization that commonly affect centralized approaches and data management. This approach consists of nodes forming a network called miners, which collaborate between them to establish consensus and produce novel blocks. These are interconnected in a chronological and immutable manner. Each block contains a header for block identification in the network including three sets of block metadata, the previous block hash, a timestamp, a nonce, and a Merkle Root [22], which represents the data structure used to check if a transaction exists or no. The primary objective of this technology is to ensure transparency, security, and availability of transactions to collaborators during the consensus operation.

Blockchain technology is characterized by many properties among them: security and integrity, decentralization, incorporation of many consensus mechanisms [23] such as proof of work, proof of stack, proof of authority, and smart contracts, etc. With these features, this paradigm has become increasingly reliable and robust. Also, the use of this technology has expanded from digital currencies to various areas and different industries.

2.1.1. Smart contract

This concept refers to a set of code lines representing an agreement that runs automatically when predefined conditions are met without the need of a third party or central entities for validation. The smart contract [24] is the main component of blockchain and is primarily associated with decentralized applications (DApps) and platforms such as Ethereum [25]. The main features of smart contracts include self-execution of the engagement by eliminating the need for intermediaries, trust and transparency (all transactions and their execution are stored in the blockchain) building trust among participants through code visibility and tamper-proof measures, security by cryptography mechanism, autonomy reducing the risk of human error and the potential of disputes, and decentralization making it resilient to central points of failure and censorship. Smart contracts have a wide range of applications, including financial services, supply chain management, real estate transactions, and more. This mechanism has the potential to revolutionize industries by automating and streamlining complex processes while enhancing security and trust in transactions.

2.1.2. Consensus protocol

Consensus protocols [23] refers to mechanisms enabling the validation of transactions and agreements by the nodes forming the decentralized network in the blockchain. These protocols play a crucial role in maintaining the security and integrity of the blockchain. Several consensus protocols exist, and each one is defined with its own advantages and use cases. In our case, we use the Proof of Authorities (POA) consensus protocol. POA is designed for permissioned blockchains and focuses on reaching a consensus among a group of nodes. However, it is used in some private and consortium blockchains where participants are known and trusted. POA also is characterized by its high security, quick consensus achievement compared to some other consensus algorithms, efficiency in terms of energy consumption, velocity of transaction validation, fast verification and access decisions in the case of access control, and finally, privacy and compliance that are important when dealing with sensitive biometric data.

2.2. Blockchain oracles

Oracle is a mechanism that ensures the interaction between blockchain (on-chain) and the external world off-chain [26]. This mechanism represents a data agent that retrieves information from outside to a smart contract which can use this information to make a decision. Fig. 1 depicts the main function of the oracle, which represents an intermediary between the on-chain through smart contract and the off-chain. Generally, the process of oracle involves three entities. Each entity has a specific role, the first one facilitates the utilization of various Web APIs and communication interfaces to retrieve and transmit data to Oracle nodes from a wide array of online sources, including sensors, stocks, and crypto exchanges. The second one implements notarization and certification procedures, ensuring the delivery of highly accurate, pertinent, and dependable data to the blockchain. Finally, enables ecosystems by executing smart contracts on networks in a secure and safe manner.

Implementing Oracle services to ensure the communication between on-chain and off-chain, and to mitigate security issues, requires the implementation and integration of various approaches, including cryptographic techniques, consensus mechanisms, reputation systems, and decentralization strategies in Oracle designs. Additionally, ongoing research and development in the field aim to enhance the security and reliability of Oracle solutions. Chainlink [27] is an example of Oracle blockchain that has gained widespread adoption in the blockchain space and is used in various applications, including decentralized finance, insurance, supply chain management, and more. Its decentralized nature and focus on providing secure and reliable data make it a key component in expanding the capabilities of smart contracts.

2.3. AE-GAN model

AE-GAN model is a combination of deep learning models, namely AutoEncoders (AE) and Generative Adversarial Networks (GAN) that are both based on neural network architecture [20]. This hybrid model aims to leverage the strengths of both AEs and GANs to generate realistic and diverse data. Fig. 2 depicts the autoencoder model architecture that consists of three components, namely the encoder that takes the voice as inputs, extracts the main relevant features and important representations, and then converts them into latent space, this latter represents the main features that make up the voice. Whereas the decoder tries to reconstruct the input data from the latent space, getting, therefore, the same data. Autoencoders [28] can be used to enhance the quality of speech signals by training to learn the relationship between noisy and clean speech data, they can be used to enhance the quality of speech signals by removing distortions, noise or artefacts. This model is often used in conjunction with other deep learning techniques, such as Recurrent Neural Networks (RNNs) and convolutional Neural Networks (CNNs), to build more complex speech recognition systems.

The GANs [29] are part of the broader category of generative models, and they are characterized by their ability to generate realistic and high-quality synthetic data. The key idea behind GANs is to train two neural networks, a generator and a discriminator, in a competitive or adversarial manner as shown in Fig. 3. The generator takes charge of generating more data that resemble the reel data, and the discriminator distinguishes between the generated samples and the reel data. The generator and discriminator are trained simultaneously through adversarial training. The main objective is to drive the GAN towards generating high-quality and diverse synthetic data.

In our case, we use the AE in conjunction with the GAN, known as the AE-GAN model, to generate more data that are crucial for training, aiming to get an accurate and robust model. The main idea is to use the AE model to extract the relevant representations of the voice namely the latent space and reconstruct the data from this latter. The latent space data is input into the generator of the GAN model to produce additional data resembling the latent space data. After training the model, the outputs are used in the discriminator of GAN to extract the main features from the generated samples, and these samples are used again by the discriminator to distinguish them from the features that come from the decoder of the AE model. Fig. 4 depicts the AE-GAN model architecture.

2.4. Homomorphic encryption

Homomorphic encryption [30] is an exciting field of cryptography with the potential to address privacy and security concerns in data processing and cloud computing. It is a cryptography technique that enables computations to be performed on encrypted data without the need to decrypt it. In other words, it allows to perform operations on data in its encrypted form, and output encrypted results, which maintains the confidentiality and privacy of sensitive data. Homomorphic encryption has been applied in various applications, especially in scenarios where privacy and security are crucial. We distinguish two homomorphic encryption types; Partially Homomorphic Encryption (PHE) which allows only one type of operation (addition or multiplication) to be performed on the encrypted data, and Fully Homomorphic Encryption (FHE) which allows both addition and multiplication operations on the encrypted data, making it more versatile.

2.5. Related work

In the literature, several studies have been carried out and proposed new paradigms that integrate blockchain technology. However, this technology has demonstrated its effectiveness across various domains, particularly in the biometric access control context, including speaker authentication and verification.

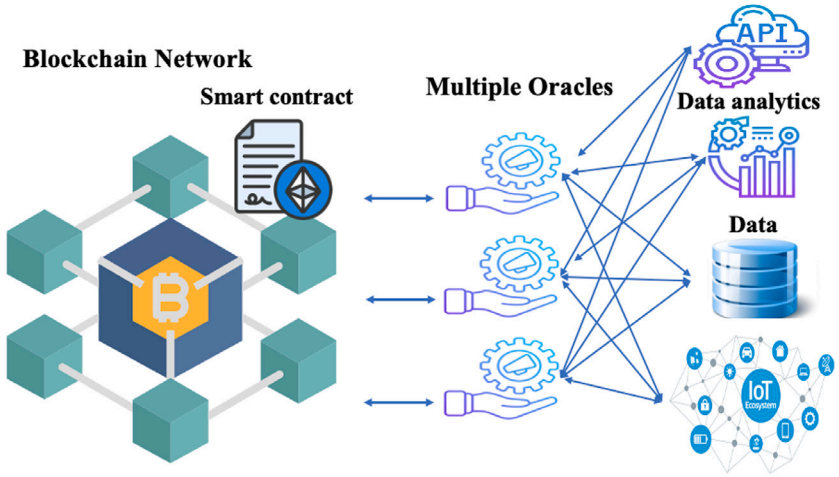

Fig. 1. The main function of Oracle in blockchain system.

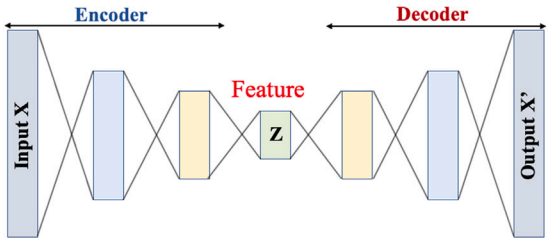

Fig. 2. The AutoEncoder architecture.

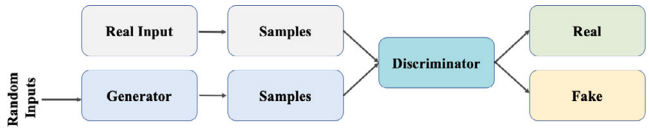

Fig. 3. The generative adversarial network architecture.

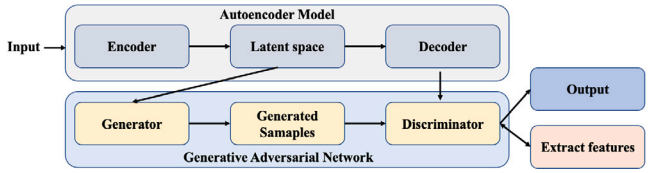

Fig. 4. The AE-GAN model architecture.

R. Kamal et al. [17] have proposed a new approach based on blockchain to guarantee system security for health data. The suggested proposition utilizes the distributed networks to share the data and monitor it at home. The gathered data namely, facial images, heart rate, and blood pressure, are encrypted and sent to the doctor for analysis. There are three consortium blockchains applied in this approach, each one has its specific tasks. The first one is used to store the facial transformed images, and credentials of each entity, which the second one is reserved to store the prescription and recommendation after the validation by the administrator. The third one is dedicated to the pharmacists who provide patients with medications, which will be stored in the chain3. The findings proved that the system has achieved successful outcomes in terms of energy and time consumption compared with other studies carried out in the same context. However, this approach faces several limitations, including scalability concerns, since the system has adopted three different blockchains, it is difficult to handle a large number of patients and healthcare providers in the real world in a larger geographic area. Also, the use of devices such as mobile to transmit health data can be a weak point, which represents a real security threat. Furthermore, the use of cancellable biometrics adds an extra layer of complexity to the system, which increases the processing time and computational requirements and the transformation process might result in the loss of some biometric information, which impacted negatively the authentication process. In addition, the performance of the entire system depends on the robustness of the transformation algorithm.

In [18], the authors proposed a novel approach based on blockchain for authentication in IoT networks to handle privacy and trust challenges, that have been witnessed in the IoT environment. The aim is to use the blockchain to stock and check the identity of devices for secured and decentralized authentication. Also, the encryption mechanism is used, namely homomorphic encryption, before uploading data to the cloud. The experiments have proved the efficiency of their approach providing an infrastructure that increases privacy and trust. Nevertheless, this scheme has presented some challenges among them, the architecture of the system involves several points of failure, which make up a vulnerability. Also, homomorphic encryption requires important computational resources, which limits its use in resource-constrained IoT environments. In addition, the use of multiple security layers and data processing may increase the latency issues that are not suitable for real-time industrial applications. Furthermore, the biometric and video data are not discussed in how they can the privacy protected.

A.A. Addobea et al. in [19] provides an access control mechanism for authenticating individuals using blockchain that integrates numerous criteria of knowledge, competence, and possession. The combination of various criteria produces a temporary access code for users, intended for generating private keys. This suggested method is examined using a Py-Eth-pairing module, estimating the calculation cost and transmission overhead. Experiments confirm that the proposed framework achieves the lowest operating cost, scalability on the blockchain, and practicability. Although this approach has achieved good results, it suffers from many challenges, namely, the complexity due to the combination of multi-factor authentication and blockchain and certificateless cryptography, which affects user experience and system implementation. Furthermore, this combination could increase the processing time and resource usage, especially for large-scale deployments. On the other hand, the scheme aims to eliminate centralized issues, but the use of elected authority in the PoA could potentially introduce some level of centralization.

In [31], Lee et al. have presented a new paradigm called BDAS, based on blockchain to authenticate system users with their biometric

credentials presented as a template. The main principle of this approach is to divide each user template into pieces and save it using blockchain to safeguard user credentials. However, this approach faces some shortcomings. The dependency on the number of activated nodes is one of the major concerns, i.e., the security and reliability of the system is related to the sufficient number of participating nodes in the network, especially in smaller deployments, which impacts negatively the performance. Furthermore, in larger deployments, the system's performance may degrade due to potential increases in authentication time. Additionally, this approach introduces some performance overhead, especially in recording authentication activities.

The authors in [32] suggested a new paradigm, as an access control system that uses the Attribute-Based Encryption technique and blockchain. The Blockchain is used to decrypt the sensitive data using the ABE mechanism. Furthermore, they incorporate the user credibility incentive mechanism that evaluates the credibility of users relying on access behavior and then assigns a score to the user. The suggested technique is trustworthy and efficient, according to security analysis and experimental findings. Despite this paradigm offering benefits in terms of security, it may face several challenges. Firstly, since access records can be stored in the blockchain, all the participating nodes can view the ledger, which raises privacy issues. In addition, the integration of blockchain technology with the ABE and IoT systems adds complexity to the system architecture, which makes the implementation and maintenance more difficult. Moreover, although shifting the processing to the blockchain eases the strain on IoT devices, running a blockchain network increases additional overheads related to the computation, storage, and network resources.

A. Zahoor et al. [33] have proposed a new approach based on Blockchain for IoT-Smart Grid to address security and privacy concerns. They propose an access control mechanism based on blockchain which makes use of Physically Unclonable Functions (PUF), allowing safe communication between the service providers and Smart meters. The blockchain nodes are formed by the service providers, and each peer node is responsible for securely constructing the blocks from the acquired data. However, to validate and add the newly formed block on the blockchain network the approach uses a voting-based consensus method. The evaluation of this paradigm is done using the Random or Real (RoR) concept. The findings and the security feature analysis reveal that this scheme is more efficient and robust than competitors, providing, therefore, considerable security qualities. However, it has some shortcomings. Blockchain provides transparency, but this could potentially conflict with privacy requirements in some cases, necessitating careful design of privacy-preserving mechanisms. Furthermore, the adoption of the voting-based consensus algorithm is resource-intensive, particularly in large deployments and necessitates also significant communication between nodes, which can lead to increased network traffic and potential congestion. In addition, the need for multiple rounds of communication to reach a consensus could cause latency issues, leading to slower confirmation time. Moreover, PUFs are sensitive to environmental factors such as temperature, humidity, and voltage fluctuations, which affect their reliability and consistency in generating challenge-response pairs.

In [34], A.H. Mohsin et al. designed a new scheme based on blockchain that aims to authenticate patients between two extremities: the access point and the node database. They combine radio frequency identification and the finger vein biometric characteristics to boost pattern structure randomization and security levels. Furthermore, they integrate the encryption, Blockchain, and steganography approaches for the hybrid pattern model. This combination guarantees that the Finger Vein biometric verification system stays safe during authentication by satisfying the information security standard criteria of confidentiality, integrity, and availability while transmitting the pattern from an enrollment device (access point) to the node database. Blockchain technology is used to ensure data integrity and availability. For secrecy in a transmission channel, particle swarm optimization steganography and sophisticated encryption standard techniques are applied. Experiments have proved the efficiency of the model in terms of protection against the attacks, namely spoofing and brute-force attacks, and the safeguard of biometric templates during data transfer.

Although this approach achieves good results and offers several security features, it comes with several challenges. The dependency on multiple technologies, namely RFID and Steganography increases the potential points of failure. Moreover, the use of multiple authentication factors might increase also the chances of legitimate entities being denied access due to the small variations in biometric data. Furthermore, the storage and transmission of details biometric data raise potential privacy issues. Additionally, the system implementation requires specialized hardware and software, which could be expensive in terms of costs.

The authors of [35] designed a method using three 3D templates captured from the user's fingerprint, aiming at generating a secure template by calculating the minutiae triplets. This technique has proved its efficiency on various fingerprint databases, providing a robust, revocable, secure, and performant biometric authentication system, guaranteeing, therefore, a user template. Despite these benefits, there are some shortcomings, including the complexity since it encompasses multiple transformations and key sets, which could make the implementation and maintenance more challenging. Furthermore, the dependency on singular points in the matching step could be challenging, i.e., these points may not always be present or easily detectable in partial fingerprints. In addition, key management could be also challenging at scale, because the system requires secure storage and management of multiple user-specific keys. 3D transformed templates also require more space for storage than traditional 2D templates. As well as these transformations and matching processes may introduce significant processing overhead, which could impact the performance of the system.

Another research conducted by the authors in [36] aims at providing a unique encryption system designed exclusively for authorizing and signing transactions in digital or smart contracts. FaceNet, a CNN, encodes the face as a biometric key. The hybrid information fusion technique is then used to fuse this encoding with an RSA key. The findings indicate a composite key that verifies the identification of the individual doing the transaction while maintaining privacy. Experiments show that even under very varied acquisition settings for the biometric characteristic, the user's identification is assured and the contract is appropriately signed in less than 1.86 s. The suggested system is also highly quick in the production of user templates and requires just four trails for recognizing the user.

However, this approach faces several challenges. Since this paradigm aims at enhancing overall security, it does not adequately address the security of the stored biometric data itself. Furthermore, the linkability of biometric data to blockchain transactions could raise potential privacy concerns. Moreover, the system's reliance on storing and processing biometric data could compromise user anonymity and create vulnerability if the data is breached. The complex computational requirements also of face detection, encoding, RSA key generation, and BNIF algorithm for each transaction could significantly increase processing times, network load, and storage requirements, this additional overhead may impact transaction speeds, scalability, and overall system efficiency, particularly in high-volume scenarios.

Another novel approach has been suggested by the authors in [37], which consists in implementing a system based on blockchain using biometrics and aims to preserve security, Privacy, and access control for Healthcare records. This solution eliminates the reliance on the cryptographic pair keys strategy widely used in blockchain systems for patient identification, which is important in numerous cases, including the private key loss that prevents access to patients' records. Besides, they designed a prototype to assess the permanent risk loss of records access by utilizing fingerprints. The findings reveal the efficacy of this

approach, maintaining patients' access control to their records and guaranteeing their identification.

One of the main shortcomings of this approach is the system relies only on fingerprints, which may not be suitable for all patients or situations. Furthermore, the proposed scheme does not address the protection of biometric data. The performance analysis mentioned also is not detailed enough to fully validate the system's effectiveness. The paper also does not adequately discuss how the system would perform with large-scale entities and transactions.

N.D. Sarier [38] has proposed a new model based on blockchain to manage the user's identity, ensuring non-transferability by generating a newly computed concealed biometric property for each authentication. This technique, in conjunction with external storage, ensures the General Data Protection Regulation (GDPR), which is necessary for personal data protection. The blindfolded aspect is defined to offer unlinkability, which is a characteristic absent in most systems. Furthermore, to boost scalability, the authors redesigned the system for bigger organizations by substituting the Merkle Tree with an accumulator. Experiments have proved that this new approach is more suited to the Industrial IoT environment and enables auditing. However, there are some potential limitations. Indeed, the system requires tamper-proof devices for storing credential data and performing biometric verification. This could be a point of vulnerability if tamper-proofing is compromised. Moreover, the system combines multiple advanced cryptographic techniques, which may be challenging to implement and maintain. Additionally, for large systems using accumulators, keeping witnesses updated effectively for resource-constrained IoT devices could be problematic. Advances in cryptanalysis or quantum computing could also threaten the security assumptions in this architecture since the system's security relies on the underlying cryptographic primitives and blockchain integrity.

In deed, our approach differs from previous research in several ways:

- It presents a secure and reliable scheme relying on a hybrid deep learning model, namely the AutoEncoding Generative Adversarial Network (AE-GAN) model [20] for optimizing the extraction of the relevant and significant speech features that are crucial for the model performance.
- It handles template security by using homomorphic encryption for similarity calculation to preserve and ensure privacy and confidentiality.
- It resolves the transparency issues by using the encryption mechanism to encrypt all critical information related to the user in interaction over the network.
- It adopt two distinct smart contracts to get a more modulable and scalable system in which we can update or replace one component without affecting the other, making maintenance and upgrades more straightforward.
- It delegates the similarity calculation and the voice preprocessing to an external API, which offers efficiency, cost and overload savings, flexibility, and enhanced privacy. Furthermore, it uses Oracle blockchain technology to facilitate interactions between off-chain and on-chain environments.

3. Proposed approach

This section presents our proposed scheme, a novel approach based on blockchain technology for biometric access control using deep speech recognition (DBAC-DSR-BT), including a biometric authentication system, speaker identification and access control system. DBAC-DSR-BT is a decentralized and distributed infrastructure for biometric access control that eliminates the need for any third party or central point, leveraging, therefore the potential of blockchain. The proposed solution incorporates several entities, each one of them has its main function. These entities are described as follows:

User The individual who wants to access the proposed system through his/her wallet. He/She provides credentials to the application interface for authentication that necessitates logging in to his/her Metamask wallet to retrieve their Addresses.

Application interface The user interacts with the application interface to provide credentials. This interface makes easy the communication between the user and the blockchain through the wallet. After receiving the user's public address from the wallet (i.e., Metamask), the communication is established with the first smart contract to check if the user exists, before sending the request to the API to preprocess the voice signal and get an encrypted speech template. If the requirements are met, an access token is generated by the smart contract 2 that grants access.

Wallet (Metamask) A cryptocurrency wallet that the user is connected to. The user obtains their public address from the wallet, which is then used in the subsequent steps. Indeed, it enables the user to interact with our private blockchain system. In addition, all the transactions will be validated by this wallet through the private key.

API An external service or module responsible for extracting features from voice using the AE-GAN model. It also takes charge of converting and encrypting these features into a template, then generating an ID related to this encrypted template, encrypting the ID, and finally, storing them before sending the encrypted ID to the application interface. Furthermore, it has another function that computes the similarity between the encrypted templates using homomorphic encryption.

Smart Contract 1 Its main role is storing the template IDs with their associated hashed address and encrypted attributes. When a requester authenticates from his wallet, he interacts with the smart contract deployed on the blockchain, which verifies the presence of the user's hashed public address. It communicates also with the API to obtain the value of similarity calculation through the Oracle blockchain.

Smart Contract 2 Another smart contract deployed on the blockchain. If the similarity between templates exceeds a threshold defined by the manager, Smart Contract 2 is invoked. It checks a policy, possibly predefined by the manager, and generates an access token if the conditions are satisfied.

Blockchain The decentralized and immutable ledger where the smart contracts are deployed. It provides a secure and transparent environment for executing and recording transactions related to identity verification. All transactions are stored on the blockchain network.

Oracle blockchain The entities set that ensure the interaction between the on-chain within Blockchain and off-chain (outside). In the proposed scheme, it plays an intermediary between the API and Smart contract. This mechanism takes charge of providing the smart contract with the similarity calculation value.

Manager The entity responsible for defining policies, thresholds, roles attribution, and overall access control system management. The manager sets criteria for similarity checks and policy enforcement.

Access token A token generated by Smart Contract 2 if the conditions are met. This token serves as proof of successful authentication and authorization, allowing the user to access their account or perform specific actions.

The proposed approach involves two distinguished processes. The first one focuses on the enrollment process, while the other focuses on the authentication and access control process.

3.1. Enrollment process

In the enrollment process, the user has to log in to his Metamask wallet. Once connected, the system retrieves automatically the public address and hashes it. Then the hashed address will be sent to the smart contract 1 to check its existence. If so, the user will be redirected to the login page, otherwise, the user provides his/her credentials (name, email, phone number, voice and password) by filling out a form in the application interface, and the latter sends the request with the raw voice to the API to process it. Algorithm 1 represents the first step of the enrollment process that checks the existence of the request's hashed address. The API takes charge of extracting features from the voice, converting them into templates, encrypting the template, generating an ID related to the encrypted template, storing them (both the encrypted template and the ID related to it), and finally encrypting ID with the public key and sends the encrypted ID back to the application interface as represented by the algorithm 2. When the application interface receives the encrypted ID, it sends a request again to smart contract 1, including the encrypted ID, the hashed public address and the encrypted attributes, to add the user into the blockchain, storing thus the hashed public addresses, the encrypted ID and the encrypted attributes. Once the smart contract 1 adds the user, the smart contract 2 will be triggered and receive the hashed address. Then, Smart Contract 2 sends a request to the manager to validate the account and attribute the roles according to the security policy. The manager requests smart contract 1 to get the encrypted attributes to add them to the security policy, then sends a request to add the roles in smart contract 2. The validation step is done by the algorithm 3. Once the roles are attributed and stored in the smart contract 2, the user will receive a notification indicating that the account is validated. Fig. 5 demonstrates the enrollment process.

Algorithm 1 Address verification

Input: Public Address (PA), User credentials (UC) (Optional)
Output: User Status (US)(Existing, Not Existing)

```
Initialization
Connect to the Metamask wallet
Function HashAddress(PA):
    return HashedAddress (HA)
Function CheckAddressExistence(HA):
    if HA exists then
        return Existing
    else
        return Not existing
    end
UserStatus ← CheckAddressExistence(HA))
if UserStatus is Existing then
    Redirect User to authentication page
else
    return Prompt user to provide credentials
    InitiateOnboarding(PA, UC)
end
return userStatus
```

3.2. Authentication and access control process

In the authentication and access control process, as shown in Fig. 6, the user provides the system with his/her voice. Then the system connects to the Metamask wallet and retrieves the user's public address which will be hashed by the application interface, and sent to the smart contract 1 to check its existence. If the user's address does not exist, a notification will be sent to the application and redirect the user to the enrollment page. Otherwise, It notifies the application interface by sending the encrypted ID related to the hashed address. This first phase is done by Algorithm 4. Then, the application interface sends the voice to the API that takes charge of extracting features from the voice, converting them into a template, encrypting it, and finally resending it back to the interface that redirects the request to the smart contract, including the hashed address and encrypted template. The algorithm 5 describes the process of the encrypted template creation. Smart contract 1 retrieves the encrypted ID matched to the hashed address and sends it with the encrypted template received from the interface to the API. Once the API receives both the encrypted template and the encrypted ID, it decrypts this latter and retrieves the encrypted template related to the ID and calculates the similarity between the encrypted templates

Algorithm 2 Template and ID generation

Input: Voice
Output: EncryptedID, EncryptedTemplate

```
Initialization
Function GetTemplate(voice):
    return Template
Function Encrypt(Template, EncryptionKey):
    return EncryptedTemplate
Function GenerateID(EncryptedTemplate):
    return TemplateID
Function HashTemplate(Template):
    return HashedTemplate
Function Store(EncryptedTemplate, TemplateID):
    return receipt
Template ← GetTemplate(voice)
EncryptedTemplate ← Encrypt(Template, SystemKey)
TemplateID ← GenerateID(EncryptedTemplate)
AddLine ← Store(EncryptedTemplate, TemplateID)
EncryptedID ← Encrypt(TemplateID, UserPublicKey)
Transaction ← CreateTransaction(EncryptedID)
receipt ← SubmitTransaction(Transaction)
```

Algorithm 3 Account validation

Input: Hashed Address (HA), EncryptedID (EncID)
Output: Account Validation Status

```
Initialization
SC1 = SmartContract1
SC2 = SmartContract2 EncAtt = Encrypted Attributes
DecAtt = Decrypted Attributes
PrivKey = PrivateKey
Function RetrieveEncryptedAttributes(HA, EncID):
    return SC1.GetAttributes(HA, EncID)
Function DecryptAttributes(EncAtt, PrivKey):
    return DecryptetAttributes
Function ValidateAccount(DecAtt):
    if not SC2. IsValidAccount(DecAtt) then
        Invalid
    else
        Valid
    end
Function AssignRoles(HA, DecAtt):
    roles ← SC.DetermineRoles(HA, DecAtt)
    SC2.AssignRoles(DecAtt, roles)
    return roles
EncAtt ← RetrieveEncryptedAttributes(HA, EncID)
DecAtt ← DecryptAttributes(EncAtt, PrivKey)
validationStatus ← ValidationAccount(HA, DecAtt)
if ValidationStatus is invalid then
    Invalid
else
    Valid
end
return Account validation Status
```

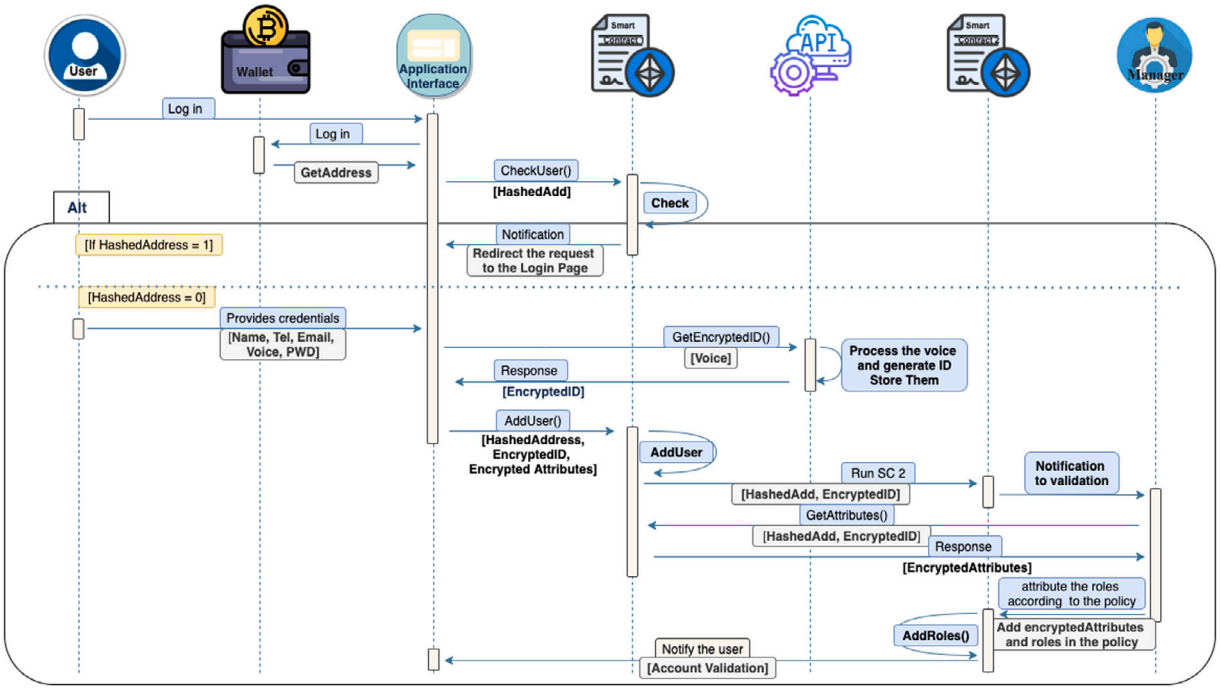

Fig. 5. Sequence diagram of enrollment process to DBAC-DSR-BT system.

using homomorphic encryption as summarized in the algorithm 6, then resends the similarity value to the SC 1 that takes charge of checking the value using the algorithm 7. If this value is lower than a predefined threshold by the manager, the request will be rejected and a notification will be sent back to the user informing him to log in differently in the application. Otherwise, a request will be sent to the second smart contract address to check the policy deployed on it and provide the user with a token including relevant information about their identity or access rights through the algorithm 8. The user can use this token to access the desired resources or perform specific actions in the system.

Algorithm 4 Check user existence

Input: Public address
Output: Encrypted ID or Enrollment Redirect

Initialization:
Connect to MetaMask wallet
Function `HashAddress(`*address*`):`
  return HashedAddress
Function `CheckAddressExistence(`*hashedAddress*`):`
  return SC1.Exists(hashedAddress)
Function `RetrieveEncryptedID(`*hashedAddress*`):`
  return SC1.GetEncryptedID(hashedAddress)
hashedAddress ← `HashAddress(`*Public address*`)`
if `CheckAddressExistence(`*hashedAddress*`)` **then**
  encryptedID ← `RetrieveEncryptedID(`*hashedAddress*`)`
  return encryptedID
else
  Redirect user to enrollment page
  return EnrollmentRedirect
end

4. Analysis and discussion

This section presents an analysis and discussion of the proposed approach. It encompasses an overview of simulations and results, then highlights security and privacy analysis; including resistance to several attacks; performance analysis, approach limitations, and finally, some innovative mechanisms that are beneficial and crucial in such systems.

Algorithm 5 Request encrypted template creation

Input: Voice input ($VoiceInput$)
Output: Encrypted template ($EncTemplate$)

Initialization
Function `ExtractVoiceFeatures(`*voiceInput*`):`
  return VoiceFeatures
Function `CreateVoiceTemplate(`*features*`):`
  return VoiceTemplate
Function `EncryptTemplate(`*Template, EncKey*`):`
  return EncTemplate
VoiceFeatures ← `ExtractVoiceFeatures` (voiceInput)
Template ← `CreateVoiceTemplate(`*VoiceFeatures*`)`
EncTemplate ← `EncryptTemplate(`*Template, EncKey*`)`
SendToInterface(EncTemplate)
return EncTemplate

4.1. Simulations and results

Evaluating the efficiency of the proposed scheme necessitates conducting some simulations. These latter involve private Ethereum blockchain through Ganache version 2.7.0, which represents an environment for testing and running smart contracts, enabling interaction with it as a real blockchain network, language programming Solidarity v0.5.0 for coding smart contracts, Python 3.9.6 for coding the interfaces through Flask, Visual Studio IDE for compiling and migrating the smart contracts through Truffle, Node JS for running JavaScript code outside of a web browser, and Web3.py which refers to a Python library that provides convenient access to the Ethereum blockchain, it allows developers to interact with Ethereum nodes using Python, enabling the creation of Ethereum applications (DApps) and the automation of various tasks related to the blockchain.

Flask is a lightweight and modular Web Development Platform used to build the required web interfaces for users, including enrollment, log-in, and admin interfaces. Additionally, it allows developers to integrate customized Python modules for specific functionalities like Ethereum integration, making it a versatile choice for web development

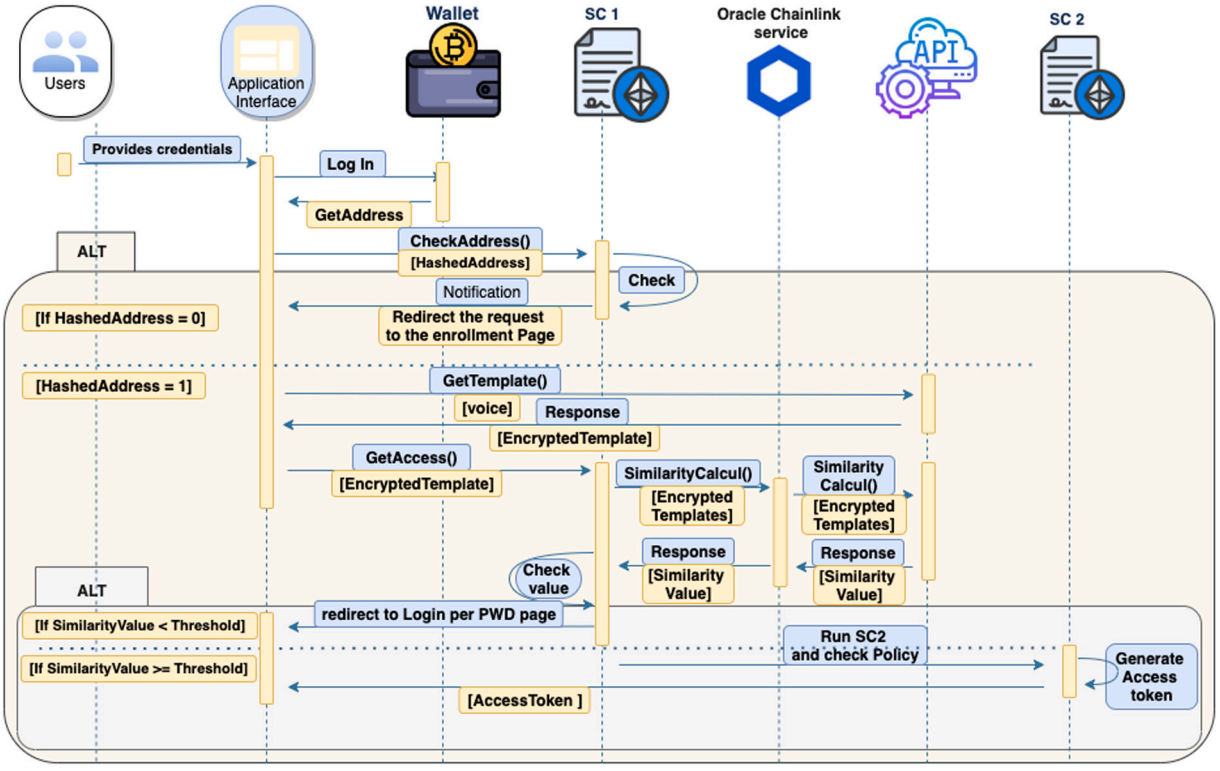

Fig. 6. Authentication and access control process.

Algorithm 6 Similarity Calculation

Input: Voice sample (VS), HashedAddress
Output: Encrypted Similarity Value Enc_{SV}

Initialization
$Pk = PublicKey$
$Sk = SecretKey$
$RT = RequestTemplate$
$EncT_{Req} = EncryptedTemplateRequest$
$EncT = EncryptedTemplateStored$
Function `GenerateHomomorphicKeys()`:
  return (pk, sk)
Function `ExtractVoiceFeatures(VS)`:
  return VoiceFeatures
Function `CreateRequestTemplate(VoiceFeatures)`:
  return RequestTemplate (RT)
Function `EncryptTemplate(RT, pk)`:
  return EncryptedRequestTemplate ($EncT_{Req}$)
Function `RetrieveEncryptedTemplate(HashedAddress)`:
  return EncryptedTemplate (EncT)
Function `CalculateSimilarity(`$EncT_{Req}$`, EncT, pk)`:
  return $Enc(SV)$
$(pk, sk) \leftarrow$ `GenerateHomomorphicKeys()`
VoiceFeatures $\leftarrow$ `ExtractVoiceFeatures(VS)`
RT $\leftarrow$ `CreateRequestTemplate(VoiceFeatures)`
$EncT_{Req} \leftarrow$ `EncryptTemplate(RT, pk)`
$EncT \leftarrow$ `RetrieveEncryptedTemplate(HashedAddress)`
$Enc(SV) \leftarrow$ `CalculateSimilarity(EncT,` $EncT_{Req}$`, pk)`
`TriggerSmartContract(`$Enc(SV)$`, HashedAddress)`
return $Enc(SV)$

Algorithm 7 Access request response

Input: Similarity value (SV) , Threshold (Th)
Output: Decision making (D)

Initialization
$D \leftarrow$ Null
Decision making
if $SV \geq Th$ **then**
  $D \leftarrow$ "Access granted"
  SendRequestToSmartContract2()
else
  $D \leftarrow$ "Access diened"
  PromptUserReconnection()
end
return D

and API creation.

Visual Studio IDE is used to create, run, and compile smart contracts, that are running in a personal machine equipped with a CPU intel quad core of 2.60 Hz and 16 GB RAM.

Truffle is an open-source framework that provides developers with a suite of tools to streamline the process of building, testing, and deploying smart contracts on the blockchain (ganache). Indeed, it is used to compile and migrate the solidity contracts within the specified contracts directory generate corresponding JSON artefacts for each contract and view them in the build directory. Then deploy the compiled smart contracts to the blockchain through the truffle migrate command as shown in Fig. 7, we have deployed the smart contracts within the blockchain.

The proposed scheme is tested and evaluated on 45 users. This evaluation involves calculating different rates through performance metrics, including True Positive Rate (TPR) or Sensitivity, False Positive Rate (FPR), True Negative Rate (TNR) or Specificity, False Negative Rate (FNR), False Acceptance Rate (FAR), False Rejection Rate (FRR),

Algorithm 8 Enhanced Access Token Generation

Input: Encrypted attributes ($EncAtt$), User ID (UID)
Output: Access token

```
Initialization
Function DecryptAttributes(EncAtt, UserKey):
    return Attributes
Function CheckPolicy(Attributes, UID):
    return PolicyResult
Function GenerateAccessToken(Attributes, PolicyResult, UID):
    return Token
Attributes ← DecryptAttributes(EncAtt, UserKey)
PolicyResult ← CheckPolicy(Attributes, UserID)
if policyResult.IsAuthorized() then
    TokenPayload ← GenerateAccessToken(Attributes, policyResult, UserID)
    Token ← JWT.Sign(TokenPayload, SecretKey)
    SendToUser(accessToken)
    return accessToken
else
    return AccessDenied
end
```

and finally the Accuracy. All these metrics provide insights towards the efficiency and effectiveness of this proposed approach.

The TPR aims at defining the number of correct identifications average and is calculated through this formula:

$$TPR = \frac{TP}{TP + FN} \tag{1}$$

where true positives (TP) indicate the number of correct identifications and false negatives (FN) represent the incorrect identifications. Whereas, the goal of the FPR is to calculate the average of identifications missed in the test using this formula:

$$FPR = \frac{FP}{FP + TN} \tag{2}$$

False positives (FP) indicate the incorrect identifications and True negatives (TN) represent the correct rejections.

The main purpose of calculating the TNR is to identify the average of the correct rejections by this formula:

$$TNR = \frac{TN}{TN + FP} \tag{3}$$

where TN represents the correct rejections and FP represents the incorrect identifications. While the FNR aims to indicate the average of the incorrect rejections using this formula:

$$FNR = \frac{FN}{FN + TP} \tag{4}$$

where FN is the number of incorrect rejections and TP represents the correct identifications.

The FAR shows the average of instances that should have been rejected that were erroneously accepted. It is a measure of the system's proclivity to accept erroneously rejected inputs, resulting in false positive mistakes. It is calculated by this equation:

$$FAR = \frac{FP}{Number\ of\ Authentication\ Attempts} \tag{5}$$

where FP represents false positives or the number of false Acceptances, in opposition, the FRR reflects the proportion of occurrences that should have been accepted, that were mistakenly refused. It measures the system's proclivity to reject inputs that should have been accepted, resulting in false negative errors. The FRR is calculated by dividing the number of false incorrect identification by the number of authentication attempts through this equation.

$$FRR = \frac{FN}{Number\ of\ Authentication\ Attempts} \tag{6}$$

Table 1
Confusion matrix results.

Test	Positive	Negative	Total
Positive	TP = 44	FP = 1	TP+ FP = 45
Negative	FN = 0	TN = 0	FN+ TN = 0
Total	TP+ FN = 44	FP+ TN = 1	N = 45

Table 2
Performance metrics results: Sensitivity, Specificity, FPR, FNR, FAR, FRR, and Accuracy.

Metric	Formula	Value
Sensitivity or True Positive Rate	$TPR = \frac{TP}{TP+FN}$	0.97
Specificity or True Negative Rate	$TNR = \frac{TN}{TN+FP}$	0
False Positive Rate	$FPR = \frac{FP}{FP+TN}$	1
False Negative rate	$FNR = \frac{FN}{FN+TP}$	0
False Acceptance Rate	$FAR = \frac{FP}{Number\ of\ Attempts}$	0.022
False Rejection Rate	$FRR = \frac{TN}{Number\ of\ Attempts}$	0
Accuracy	$\frac{TP+TN}{N}$	97.78%

Finally, the accuracy aims at calculating the ratio of correctly identified instances, both true positives and true negatives, to the total number of attempts. It is calculated through this formula:

$$FRR = \frac{TP + TN}{Total\ Number\ of\ Attempts} \tag{7}$$

The relationship between these metrics and accuracy is inversely proportional. A higher accuracy indicates a better-performing system in terms of correctly identifying both authorized and unauthorized users. Table 1 represents the results of the test on 45 users.

The FAR and FRR are two critical indicators for assessing the performance of a biometric system. They have an impact on the security of a biometric system. This implies that when changing these rates, the number of usable authentication attempts will drop or rise. A high FAR indicates that the system is more likely to accept an unauthorized user improperly, compromising system security. A high FRR indicates that the system is more likely to wrongly reject an authorized user, causing annoyance and a decrease in productivity. A low FAR combined with a low FRR suggests a high level of security. It is critical to strike a balance between the FAR and the FRR when determining threshold values for a specific system. The choice of threshold should represent the balance between security and usability. Table 2 summarizes the performance metrics results.

According to the results of the system assessment represented in Tables 1 and 2, the system provides perfect accuracy, due to the high TPR that is 0.97, i.e., it identifies all legitimate users, the FAR is relatively high, 0.022, due to the FPR which is not good for security. The FRR is also low, due to the low TNR and FNR, indicating that the system did not reject legitimate users.

4.2. Security analysis

Blockchain technology offers numerous advantages and benefits to its users thanks to its inherent properties, including decentralization, distribution, tamper-resistant, immutability, integrity, transparency and traceability, on so. By leveraging their potential, the proposed scheme ensures robust security and privacy for biometric data by utilizing advanced encryption techniques and the AE-GAN model for extracting features that convert them into templates. These biometric templates are stored within the blockchain securely, with only the encrypted IDs that match the encrypted templates stored off-chain. This approach safeguards sensitive information from unauthorized access, giving users control over their data, i.e., adds an extra layer of protection to the biometric data. The decentralized nature of blockchain contributes also to ensuring security, by making the system resistant

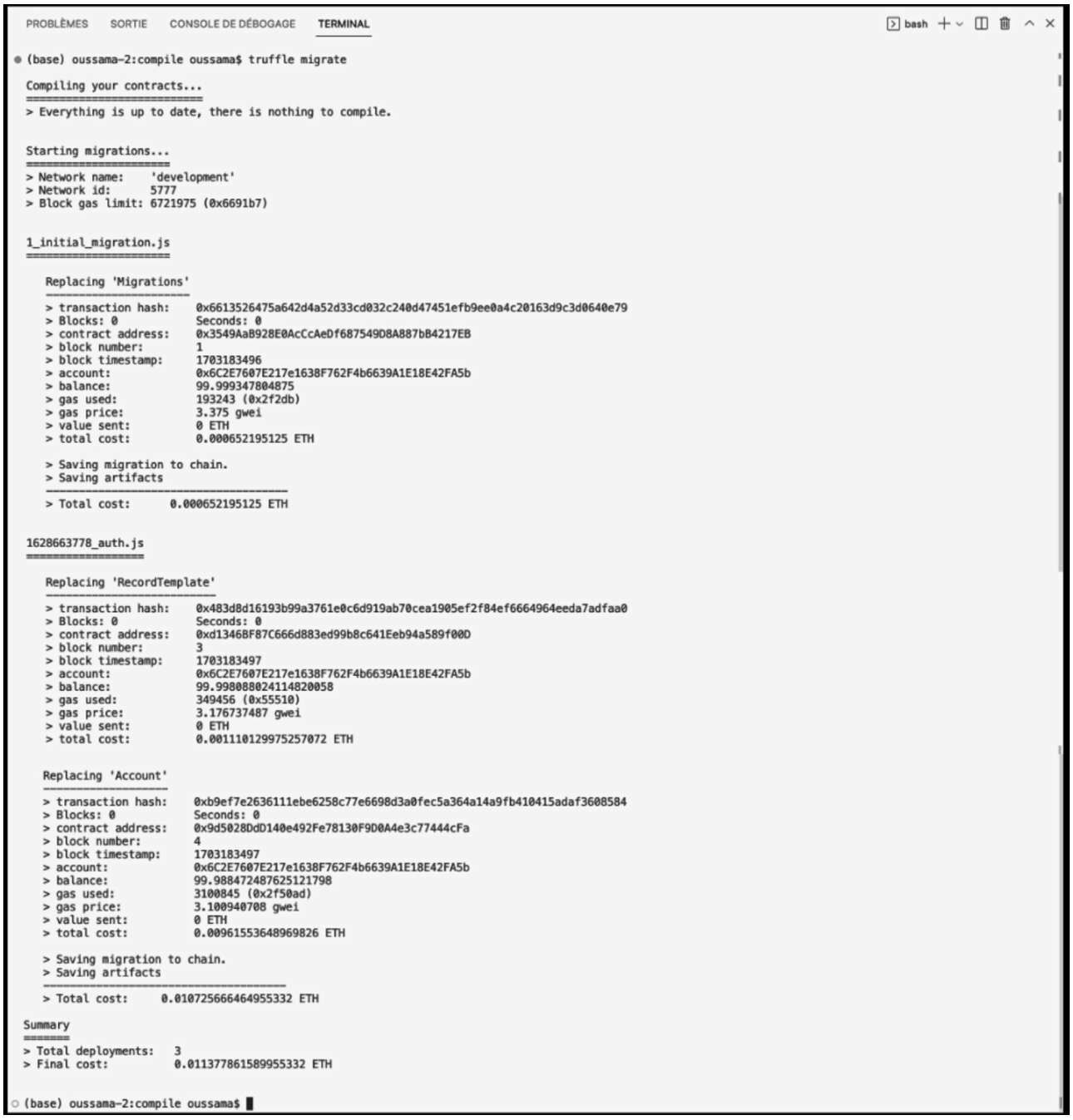

Fig. 7. Migrate the smart contracts to the blockchain.

to tampering and ensuring data integrity, since distribution makes the system difficult for a single entity to alter or manipulate the entire history of transactions, ensuring data integrity. The consensus protocols also contribute to providing a secure environment, once the block is added to the blocks, it is impossible to alter the previous blocks without the consensus of the majority, ensuring therefore, immutability.

The use of public address hash and the encrypted attributes stocked in the blockchain brings numerous advantages in terms of security and privacy. The address hash ensures that the actual public address is not publicly visible on the blockchain. This provides, on one hand, more privacy, as external parties can only see the hash, making it computationally infeasible to reverse-engineer the original address from the hash. This is particularly useful for privacy-focused applications. On the other hand, any attempt to tamper with the address would require changing the original data and recalculating the hash, which is computationally difficult. This enhances the integrity and security of the stored data, which provides tamper-resistant data storage. Applying a homomorphic encryption mechanism also enables secure similarity calculations without revealing the template contents which is crucial for privacy-preserving biometric systems. In addition, using an Oracle API service as a bridge between on-chain and off-chain components offers several benefits, particularly, in terms of security and privacy. It facilitates the secure transfer of data between on-chain and off-chain environments, which ensures that sensitive information is transmitted securely. It enhances interoperability by allowing the blockchain system to interact with various external services and APIs. This flexibility enables the integration of specialized or industry-specific services for enhanced functionality without compromising the security of the blockchain. The separation of on-chain and off-chain components makes it more challenging for malicious entities

or actors to compromise the entire system, as critical operations are not directly exposed on the blockchain. Which improves resilience against potential attacks.

Moreover, all the interactions between the system entities are ensured by the use of HTTPS and JSON Web Token (JWT) protocols aiming at encrypting all the sensitive information transmitted over the network. The combination of these protocols enhances the security, privacy and interoperability of the system, since HTTPS secures data in transit, while JWT reduces the resilience session storage and promotes scalability. Which contributes to providing a secure communication environment.

Furthermore, the proposed approach has proved its efficiency in terms of security and privacy, providing an infrastructure resistant to several attacks, including the 51% attacks, Man-in-the-Middle (MITM) attacks, identity spoofing attacks, Replay attacks, Sybil attacks, and Brute force attacks, for many factors and mechanisms that have been adopted:

4.2.1. Resistance to 51% attacks

The use of a private blockchain provides a private network that has restricted access and is usually operated by a known set of participants. It is not open to the public, so an attacker needs to gain control over a significant portion of the participating nodes. In addition, the Proof of Authority (PoA) consensus application makes it more challenging for an attacker to accumulate the majority of the network's computational power or stake. Additionally, participants in private blockchains are often known entities, and they are typically governed by some level of trust. This makes it harder for an attacker to infiltrate the network without detection, which proves its resistance to the 51% attacks.

4.2.2. Resistance to man-in-the-middle attacks

The use of secure communication protocols such as HTTPS to encrypt data transmitted between nodes ensures that data is protected during transit. The use of JWT protocol adds an extra layer of security, which protects access from unauthorized entities. Furthermore, encrypting sensitive data stored on the blockchain to protect it from unauthorized access adds also another layer of security. It protects the confidentiality of the information, making it challenging for unauthorized entities to access or decipher the data without the appropriate decryption keys. In addition, using peer verification mechanisms by using cryptographic keys as a means of identity verification ensures the connection to legitimate peers, which protects the system against MITM attacks. These measures collectively contribute to a robust security posture for the system.

4.2.3. Resistance to identity spoofing attacks

By leveraging blockchain properties, including the implementation of a robust PKI to manage and verify digital identities, as well as the use of cryptographic key pairs, with private keys securely stored to sign and verify transactions, deploying smart contracts that include identity verification mechanisms, ensuring that transactions or interactions with the blockchain are conditional upon proper identity validation, the use of tokens or digital signatures for authentication, i.e., all users should sign their transactions with their private keys, and the network should verify the authenticity of these signatures. Furthermore, adopting the encryption mechanism to the template adds another security layer to store and protect biometric templates, which prevents unauthorized access to raw biometric data even if blockchain data is compromised. All these factors contribute to the robustness of the proposed scheme making it more robust against impersonation attacks.

4.2.4. Resistance to replay attacks

Using a unique transaction nonce, which represents a sequential number associated with the Ethereum address, ensures that each transaction has a unique nonce, which prevents replay attacks since a repeated transaction with the same nonce would be denied. Furthermore, incorporating timestamps or time-based signatures into transactions guarantees that transactions are only valid for a set amount of time, mitigating therefore, the danger of replay attacks. Also, including a hash of the transaction payload in the transaction itself is important for verifying the transaction's integrity by smart contracts that can check the hash and guarantee that the payload has not been changed, which prevents this kind of attack. In addition, authenticating transactions with cryptographic signatures and adopting the tokenization technique guarantees that only authorized parties can initiate transactions, which proves that the proposed scheme is resistant to replay attacks.

4.2.5. Resistance to Sybil attacks

A Sybil attack is defined as the creation of many false identities to acquire control or influence over a network. In the context of a private blockchain, a Sybil attack might be especially dangerous since it may compromise the network's decentralized and trustless character. By establishing the identity verification step for network participants that requires their identification before being permitted network access. This can reduce the likelihood of such assaults. Furthermore, by incorporating proof of identity procedures within the consensus process, which will force participants to prove their identification with cryptographic proofs during the consensus, can also mitigate the danger of these attacks. Another component in combating Sybil attacks is establishing clear governance processes by defining the rules and procedures for admitting new users to the network, which prevents illegal access. Consequently, resists this sort of assault.

4.2.6. Resistance to brute force attacks

A brute force attack refers to a hacking method that aims at getting illegal access to individual accounts as well as systems and networks. The attackers frequently use a computer to try a variety of combinations until they locate the proper credentials that are looking for. In the context of a blockchain-based biometric access control system, brute force assaults can be aimed against the authentication process, attempting numerous combinations until the proper match is identified. By using the rate-limiting principle to the proposed scheme, i.e., implementing rate restriction to limit the amount of authentication attempts within a given period defined by the manager. If too many attempts are made, the system may temporarily lock out the user or cause delays between subsequent attempts. This approach mitigates and prevents this type of attack.

4.2.7. Resistance to poisoning attacks

Poisoning attacks [39] refer to a significant threat to deep learning models, including those used in biometric access control systems. The main objective of these attacks is to compromise the integrity of the model during the training phase by introducing carefully crafted malicious data into the training dataset, which leads potentially to severe security vulnerabilities. These manipulated samples could be designed to create backdoors or weaken the model's ability to distinguish between authorized and unauthorized users. In our approach, the use of AE-GAN is particularly interesting in these attacks' resistance. Autoencoders can help in feature extraction and dimensionality reduction, potentially making it harder for poisoned data to significantly influence the model. The GANs also are trained to distinguish between real and fake data. This adversarial training process can potentially help in identifying and filtering out anomalous inputs. Furthermore, the combination of these models can create a more robust feature space, which might be more resilient to subtle manipulations in the input data. Moreover, Applying the normalization and regularization techniques to the data before the training phase can help mitigate some

forms of poisoning attacks. Adopting also permissioned blockchain, that restricts access only to authorized participants and limits the number of entities that can interact with the system, reduces significantly the attack surface. However, It is crucial to note that while this approach provides some resistance, it is not foolproof. Several ways can be used to protect from these attacks that are tackled by many studies [40].

Indeed, The multifaced aspects of our approach provide some robustness against several security attacks, namely evasion attacks, model inversion attacks and transferability attacks. The combination of the AE-GAN architecture, the normalization methods, regularization techniques and blockchain makes the attacks more challenging, which potentially reduces their effectiveness. However, additional measures are needed to specifically enforce the protection against these threats. For instance, the adoption of ensemble methods with different architectures to increase the robustness, the implementation of the federated learning approach to make it difficult to invert any single user's data, and the implementation of techniques such as gradient obfuscation to mask the model's gradient information to make it harder to craft transferable adversarial examples.

The proposed scheme achieves a high security and privacy level throughout the entire process from feature extraction to similarity calculation by combining AE-GAN for feature extraction, encryption for template storage, and homomorphic encryption for secure computations. Generally, This approach lies in striking a balance between privacy, security, and transparency. While ensuring privacy and security, the blockchain still maintains its transparency.

4.3. Performance analysis

In biometric access control systems, extracting features from biometric data represents a pivotal phase, since it directly impacts the accuracy and robustness of the system. Generally, feature extraction aims to identify invariant and robust characteristics within the data. It involves often reducing the data dimensionality by retaining the important information. The robust and efficient feature extraction step ensures that the system remains effective in real-world scenarios and can reliably identify individuals based on their unique biometric features. These latter serve as discriminative markers that differentiate one individual from another. The better the system can extract relevant features, the higher its ability to distinguish between different users, contributing to more reliable and precise identification, which reduces the likelihood of false positives or negatives. Extracted features are typically used to create a template or a representation of an individual's biometric traits. This template serves as a condensed and standardized version of the raw data, facilitating comparison and matching during identification. The features' quality and informativeness directly impact the template creation's accuracy. The proposed scheme combines two deep learning models namely, AE and GAN in a complementary manner. AutoEncoders models are well-suited for unsupervised feature learning. They can capture the most relevant representations and patterns from raw data, providing then, a compact representation. While the Generative adversarial network models are characterized by their capability to generate synthetic data. The combination of both models can enhance the robustness of the extraction process. GANs can generate data from the learned features, making the model more resilient to variations and distortions in the input data. This can contribute to improved recognition performance in real-world scenarios. Furthermore, GAN is used to augment the training dataset by generating additional realistic samples. This artificial dataset expansion helps the model generalize better to unseen variations, reducing the risk of overfitting and improving system performance. The resort to the delegation of the voice processing, the encryption, and the similarity calculation to an external API outside of the blockchain brought several benefits, including :

(1) Scalability, which allows resources to be efficiently scaled based on demand, assuring peak performance.

(2) Because of the modularity and flexibility of the API, additions or improvements to the processing pipeline may be implemented without affecting the blockchain smart contracts.

(3) Reduced computational strain on the blockchain network. This can help to speed up transaction processing and reduce fees.

(4) Response velocity, customers trying biometric access can obtain faster replies, adding to a smoother and more user-friendly experience.

(5) The blockchain network's resources are minimized by outsourcing processing duties to a dedicated API. This is especially significant in decentralized systems where resource efficiency is critical for network performance.

(6) Using an API allows for easier compatibility with multiple systems and technologies. It enables easy integration with other services, apps, or platforms that could interact with the biometric access control system.

Another factor that provides more flexibility, modularity, scalability, maintainability, and interoperability, which improves the system performance, is the separation of the functions into two distinct smart contracts. The first one focuses on checking and storage of addresses and their corresponding templates' IDs, and the other on security policy to generate an access token. Each contract has a specific purpose, which makes the overall system more modular and easier to understand. In addition, updates to the storage logic can be made without affecting the security policy. This makes it easier to manage and maintain the system over time. Furthermore, the integration of the storage component with other systems or smart contracts becomes easier with other security policies or access control requirements.

Furthermore, according to the evaluation results of the proposed model. It has achieved a high accuracy rate of 97.78%. This proves the efficiency of the proposed approach in terms of performance, indicating its effectiveness in correctly identifying users. The FAR of 2.2% suggests a little high rate of false acceptances, indicating a high rate of FPR, which is generally undesirable for security and performance. In contrast, the FRR of 0% indicates that there are no false rejections, meaning the system does not mistakenly reject authorized users. Based on these metrics, the overall system performance appears strong but needs to properly adjust the FPR. It is important to note that there is often a trade-off between FAR and FRR. Adjusting the system's threshold for accepting or rejecting biometric data can impact these rates. Therefore, finding the right balance depends on the specific requirements of the system.

4.4. Approach limitations

DBAC-DSR-BT offers significant and notable benefits in terms of security, privacy, reliability and robustness; however, it faces certain challenges that warrant discussion. Generally, speech recognition systems are susceptible to environmental factors, including background noise or variations in the user's voice due to several things, namely health or emotional states, which could potentially lead to false negatives or false positives in the cases. Furthermore, the system architecture relies on multiple technologies blockchain, smart contract, external API, and Oracle services. This dependency could be a concern, i.e., a failure in any of these could impact the overall functionality of the access control system. This inter-dependency requires careful monitoring and failsafe mechanisms to maintain consistent operation in environments where access control is crucial. Additionally, the reliance on an external API for critical functions, namely the similarity calculation and voice template storage introduces several vulnerabilities and risks to the overall system. By centralizing these functions in an external service, the system depends totally on the availability and reliability of this API, which represents a single point of failure. If this API becomes unreachable due to several factors, it could, potentially, render the entire access control unfunctional. The external API also makes up a reel target for potential attackers. If compromised, it could lead to unauthorized access to critical biometric data or manipulation

of similarity computations. Moreover, the voice recognition process and the subsequent homomorphic encryption computations introduce additional computational requirements compared to the traditional access control systems. While these operations enhance security, they may result in latency issues, which could be a concern particularly, in time-sensitive scenarios. In addition, the advent of practical quantum computers [41] poses significant risks to many current cryptographic systems. Most blockchain systems rely on cryptographic hash functions and digital signatures that are vulnerable to quantum attacks. Particularly, Shor's algorithm [42] could potentially break the elliptic curve cryptography often used in blockchain, compromising the integrity of our stored IDs and security policy. Addressing these challenges will be crucial for the system's practical implementation and widespread adoption in different environments and domains. As we consider the evolving landscape of cryptography and potential threats, two recent notable studies highlight crucial areas for further consideration and improvement, namely, the study conducted by authors in [43] that brings to light the potential of integrating lightweight cryptography into complex systems, as our case, and the other research in [44] that raises critical points about the limitations of focusing only on algorithmic security which underscores the importance of considering implementation attacks, which could potentially compromise even theoretically secure post-quantum algorithms.

4.5. Innovative research

Generally, Biometric access control systems based on blockchain are progressively using sophisticated cryptographic methods to enhance security and privacy. Two significant advancements in this field are the lightweight cryptography and post-quantum computing. These may be used with blockchain technology to provide a strong and efficient system for managing access.

4.5.1. Lightweight cryptography

Lightweight Cryptography (LWC) [45] has become an important field of study, particularly in resource-limited contexts namely IoT sensors, RFID tags, and industrial control systems. It refers to cryptographic algorithms and protocols. This concept aims at balancing the security and the performance, especially in scenarios where traditional cryptographic methods are too resource-intensive. It has several characteristics, namely minimal computational and memory requirements, compact implementation in hardware and software, low power consumption, and adequate security. The latest studies offer useful insights that may be integrated into our system to enhance security and performance. The authors in [46] have introduced innovative fault detection strategies that may improve the security of encryption operations without imposing a substantial computing burden. This can be beneficial for our approach to maintaining stringent security measures, which will achieve optimal efficiency. Another notable research also [47] has proposed an innovative approach for detecting faults that can be modified to safeguard our paradigm against specific types of side-channel attacks, which we had previously identified as a security concern in our analysis. Integrating the LWC concept into our scheme has the potential to provide many advantages, among them : Decrease the amount of computing work required for cryptographic operations Utilizing less resource-intensive cryptographic processes might enable effective management the number of access requests and blockchain transactions, which enhances the scalability. Increase the suitability of our approach for deployment in industrial IoT scenarios with restricted device capabilities, thus, enhancing its utility in such contexts.

4.5.2. Post-quantum computing

Post-quantum computing [48] pertains to the advancement of computational systems that possess the ability to endure attacks from quantum computers, that can exponentially processing power to solve complex problems much faster than traditional computers. With the advancement of this paradigm, they pose a significant risk and threat to many current encryption methods, including those used in blockchain and biometric systems. Actually, it is essential to include post-quantum algorithms into these systems to guarantee long-term security. In our context, the integration of post-quantum cryptography could be beneficial to secure the storage and transmission of voice data. For instance, using post-quantum digital signatures for transactions and post-quantum encryption for sensitive data storage within blockchain. This could be protecting the system against potential future attacks by quantum computers that could otherwise compromise the integrity of the system. Which ensure the system's resilience against advanced computational assaults. However, implementing such systems would bring challenges, namely the computational overhead of post-quantum algorithms and the complexity to using within blockchain, etc. Ongoing research and development in these fields will be essential for fully harnessing the whole capabilities of this technological confluence.

5. Conclusion and perspectives

This paper introduced a novel deep speech recognition-based-biometric access control scheme using blockchain, called DBAC-DSR-BT. The latter offers a secure, fine-granular, reliable, scalable, modular, tamper-resistant and intrusion-tolerant solution that, on one hand, preserves the security and privacy of the sensitive data in all the system processes, by using the hash and encryption mechanisms whether within the system or outside. Additionally, the use of secure communication protocols, such as HTTPS and JWT, ensures that data transmitted between nodes is encrypted, safeguarding it from unauthorized access. On the other hand, DBAC-DSR-BT provides great reliability and accuracy in user authentication by utilizing modern speech recognition technology through the new deep learning model, AE-GAN, for feature extraction which is considered the key step of this solution. Furthermore, the proposed scheme delegates the speech processing, including features extraction, conversion into template, encryption, storage, and similarity calculation using homomorphic encryption, off-chain to reduce the calculation and overhead within blockchain which enhances the scalability, modularity, time-response and flexibility of the system. The system prioritizes user privacy by employing hashing and encryption methods for sensitive data, such as templates and public address and ID whether on-chain or off-chain. Additionally, using homomorphic encryption for similarity calculation adds another level of security.

Among the main features that make our approach distinct from previous work is, tackling the transparency issues in the blockchain to preserve privacy, as well as, the adoption of two different smart contracts instead of one smart contract to enhance flexibility, modularity, scalability, maintainability, and interoperability, which improve system performance in a general manner. The first contract focuses on storing the encrypted template ID and its related hashed address and encrypted attributes, while the second applies security policies to produce access tokens. Each contract serves a distinct purpose, making the system more modular and easier to understand. Additionally, adjustments to storage logic may be done without impacting security policies, which simplifies long-term system management and maintenance. Also, integrating storage components with other systems or other smart contracts becomes easy, according to the security needs.

Implementation and evaluation show that the proposed model is functional and operational, and achieves high performance in terms of accuracy of up to 97.78% and a high TPR which suggests great correctness in affirmative identification. In contrast, the high FPR shows a relatively high proportion of false positives, which might indicate a

weakness in the system's specificity. Further refining may be required to achieve optimal performance by balancing sensitivity and specificity. In addition, DBAC-DSR-BT proves its resistance to several attacks, including 51% attacks, Man-In-The-Middle attacks, identity spoofing attacks, Sybil attacks, and brute force attacks. The suggested system strikes a compromise between security and usability, establishing itself as a comprehensive solution for applications that require reliable and user-friendly access management.

In future work, we will emphasize on optimizing the proposed solution, by adopting heuristics methods for more reliability and accuracy, the IPFS storage system for storing securely sensitive data, and post-quantum cryptography for ensuring more security and privacy.

This research will be focused on:

- Developing adaptive feature selection techniques using distributed genetic algorithms and Particle Swarm Optimization to improve speaker verification accuracy.
- Developing efficient retrieval and verification mechanisms for biometric data stored on IPFS.
- Integrating post-quantum computing to enhance security and privacy, and to protect against post-quantum attacks.

These research directions demonstrate a commitment to innovation and addressing potential challenges in digital credential systems.

CRediT authorship contribution statement

Oussama Mounnan: Writing – review & editing, Writing – original draft, Validation, Software, Methodology, Investigation, Conceptualization. **Larbi Boubchir:** Writing – review & editing, Validation, Supervision, Methodology, Conceptualization. **Otman Manad:** Writing – review & editing, Validation, Supervision, Methodology. **Abdelkrim El Mouatasim:** Writing – review & editing, Validation, Supervision, Methodology. **Boubaker Daachi:** Writing – review & editing, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] A. Habeeb, Comparison between physiological and behavioral characteristics of biometric system, J. Southwest Jiaotong Univ. 54 (6) (2019) Number: 6.

[2] R. Alrawili, A.A.S. AlQahtani, M.K. Khan, Comprehensive survey: Biometric user authentication application, evaluation, and discussion, Comput. Electr. Eng. 119 (2024) 109485, http://dx.doi.org/10.1016/j.compeleceng.2024.109485.

[3] S.A. Abdulrahman, B. Alhayani, A comprehensive survey on the biometric systems based on physiological and behavioural characteristics, Mater. Today: Proc. 80 (2023) 2642–2646, http://dx.doi.org/10.1016/j.matpr.2021.07.005.

[4] P.A. Thomas, K. Preetha Mathew, A broad review on non-intrusive active user authentication in biometrics, J. Ambient Intell. Humaniz. Comput. 14 (1) (2023) 339–360, http://dx.doi.org/10.1007/s12652-021-03301-x.

[5] K. Shaheed, P. Szczuko, M. Kumar, I. Qureshi, Q. Abbas, I. Ullah, Deep learning techniques for biometric security: A systematic review of presentation attack detection systems, Eng. Appl. Artif. Intell. 129 (2024) 107569, http://dx.doi.org/10.1016/j.engappai.2023.107569.

[6] D. Bennet, L. Maria, Y. Putri Ayu Sanjaya, A. Rahmania Az Zahra, Blockchain technology: Revolutionizing transactions in the digital age, ADI J. Recent Innov. 5 (2) (2024) 192–199, http://dx.doi.org/10.34306/ajri.v5i2.1065, URL https://www.adi-journal.org/index.php/ajri/article/view/1065.

[7] A. Atadoga, O.A. Elufioye, T.T. Omaghomi, O. Akomolafe, I.P. Odilibe, O.R. Owolabi, et al., Blockchain in healthcare: A comprehensive review of applications and security concerns, Int. J. Sci. Res. Arch. 11 (1) (2024) 1605–1613.

[8] J.J. Hunhevicz, D.M. Hall, Do you need a blockchain in construction? Use case categories and decision framework for DLT design options, Adv. Eng. Inform. 45 (2020) 101094, http://dx.doi.org/10.1016/j.aei.2020.101094.

[9] M.T. de Oliveira, L.H.A. Reis, R.C. Carrano, F.L. Seixas, D.C.M. Saade, C.V. Albuquerque, N.C. Fernandes, S.D. Olabarriaga, D.S.V. Medeiros, D.M.F. Mattos, Towards a blockchain-based secure electronic medical record for healthcare applications, in: ICC 2019 - 2019 IEEE International Conference on Communications, ICC, 2019, pp. 1–6, http://dx.doi.org/10.1109/ICC.2019.8761307.

[10] A. Rghioui, Managing patient medical record using blockchain in developing countries: Challenges and security issues, in: 2020 IEEE International Conference of Moroccan Geomatics, Morgeo, 2020, pp. 1–6, http://dx.doi.org/10.1109/Morgeo49228.2020.9121901.

[11] A. El Koshiry, E. Eliwa, T. Abd El-Hafeez, M.Y. Shams, Unlocking the power of blockchain in education: An overview of innovations and outcomes, Blockchain: Res. Appl. 4 (4) (2023) 100165, http://dx.doi.org/10.1016/j.bcra.2023.100165.

[12] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, A. Kamišalić, EduCTX: A blockchain-based higher education credit platform, IEEE Access 6 (2018) 5112–5127, http://dx.doi.org/10.1109/ACCESS.2018.2789929.

[13] P. Giganti, M. Borrello, P.M. Falcone, L. Cembalo, The impact of blockchain technology on enhancing sustainability in the agri-food sector: A scoping review, J. Clean. Prod. 456 (2024) 142379, http://dx.doi.org/10.1016/j.jclepro.2024.142379.

[14] Y. Xu, X. Li, X. Zeng, J. Cao, W. Jiang, Application of blockchain technology in food safety control:current trends and future prospects, Crit. Rev. Food Sci. Nutr. 62 (10) (2022) 2800–2819, http://dx.doi.org/10.1080/10408398.2020.1858752, PMID: 33307729. arXiv:https://doi.org/10.1080/10408398.2020.1858752.

[15] K. Azbeg, O. Ouchetto, S. Jai Andaloussi, BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security, Egypt. Inform. J. 23 (2) (2022) 329–343, http://dx.doi.org/10.1016/j.eij.2022.02.004.

[16] B. Annane, A. Alti, A. Lakehal, Blockchain based context-aware CP-ABE schema for Internet of Medical Things security, Array 14 (2022) 100150, http://dx.doi.org/10.1016/j.array.2022.100150.

[17] R. Kamal, E.E.-D. Hemdan, N. El-Fishway, Care4U: Integrated healthcare systems based on blockchain, Blockchain: Res. Appl. (2023) 100151, http://dx.doi.org/10.1016/j.bcra.2023.100151.

[18] A.K. Al Hwaitat, M.A. Almaiah, A. Ali, S. Al-Otaibi, R. Shishakly, A. Lutfi, M. Alrawad, A new blockchain-based authentication framework for secure IoT networks, Electronics 12 (17) (2023) 3618, http://dx.doi.org/10.3390/electronics12173618, Number: 17 Publisher: Multidisciplinary Digital Publishing Institute.

[19] A.A. Addobea, Q. Li, I.A. Obiri, J. Hou, Secure multi-factor access control mechanism for pairing blockchains, J. Inf. Secur. Appl. 74 (2023) 103477, http://dx.doi.org/10.1016/j.jisa.2023.103477.

[20] O. Mounnan, O. Manad, A.E. Mouatasim, L. Boubchir, B. Daachi, Deep speech recognition system based on AutoEncoder-GAN for biometric access control, Int. J. Adv. Comput. Sci. Appl. (IJACSA) 14 (11) (2023) http://dx.doi.org/10.14569/IJACSA.2023.01411132, Number: 11 Publisher : The Science and Information (SAI) Organization Limited.

[21] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, http://dx.doi.org/10.2139/ssrn.3440802.

[22] H. Liu, X. Luo, H. Liu, X. Xia, Merkle tree: A fundamental component of blockchains, in: 2021 International Conference on Electronic Information Engineering and Computer Science, EIECS, 2021, pp. 556–561, http://dx.doi.org/10.1109/EIECS53707.2021.9588047.

[23] B. Lashkari, P. Musilek, A comprehensive review of blockchain consensus mechanisms, IEEE Access 9 (2021) 43620–43652, http://dx.doi.org/10.1109/ACCESS.2021.3065880, Conference Name: IEEE Access.

[24] H. Taherdoost, Smart contracts in blockchain technology: A critical review, Information 14 (2) (2023) 117, http://dx.doi.org/10.3390/info14020117, Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

[25] C. Dannen, Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners, Apress, Berkeley, CA, 2017, http://dx.doi.org/10.1007/978-1-4842-2535-6.

[26] H. Al-Breiki, M.H.U. Rehman, K. Salah, D. Svetinovic, Trustworthy blockchain oracles: Review, comparison, and open research challenges, IEEE Access 8 (2020) 85675–85685, http://dx.doi.org/10.1109/ACCESS.2020.2992698, Conference Name: IEEE Access.

[27] L. Breidenbach, C. Cachin, A. Coventry, S. Ellis, A. Juels, A. Miller, B. Magauran, S. Nazarov, A. Topliceanu, F. Zhang, B. Chan, F. Koushanfar, D. Moroz, F. Tramer, Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks, Vol. 1, Chainlink Labs, 2021.

[28] P. Li, Y. Pei, J. Li, A comprehensive survey on design and application of autoencoder in deep learning, Appl. Soft Comput. 138 (2023) 110176, http://dx.doi.org/10.1016/j.asoc.2023.110176.

[29] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, Generative adversarial networks, 2014, http://dx.doi.org/10.48550/arXiv.1406.2661, arXiv:1406.2661 [cs, stat].

[30] A. Acar, H. Aksu, A.S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: Theory and implementation, ACM Comput. Surv. 51 (4) (2018) 79:1–79:35, http://dx.doi.org/10.1145/3214303.

[31] Y.K. Lee, J. Jeong, Securing biometric authentication system using blockchain, ICT Express 7 (3) (2021) 322–326, http://dx.doi.org/10.1016/j.icte.2021.08.003.
[32] X. Qin, Y. Huang, Z. Yang, X. Li, LBAC: A lightweight blockchain-based access control scheme for the internet of things, Inform. Sci. 554 (2021) 222–235, http://dx.doi.org/10.1016/j.ins.2020.12.035.
[33] A. Zahoor, K. Mahmood, S. Shamshad, M.A. Saleem, M.F. Ayub, M. Conti, A.K. Das, An access control scheme in IoT-enabled Smart-Grid systems using blockchain and PUF, Internet Things 22 (2023) 100708, http://dx.doi.org/10.1016/j.iot.2023.100708.
[34] A.H. Mohsin, A.A. Zaidan, B.B. Zaidan, O.S. Albahri, A.S. Albahri, M.A. Alsalem, K.I. Mohammed, Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication, Comput. Stand. Interfaces 66 (2019) 103343, http://dx.doi.org/10.1016/j.csi.2019.04.002.
[35] S.S. Ali, V.S. Baghel, I.I. Ganapathi, S. Prakash, Robust biometric authentication system with a secure user template, Image Vis. Comput. 104 (2020) 104004, http://dx.doi.org/10.1016/j.imavis.2020.104004.
[36] C. Bisogni, G. Iovane, R.E. Landi, M. Nappi, ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions, J. Inf. Secur. Appl. 59 (2021) 102814, http://dx.doi.org/10.1016/j.jisa.2021.102814.
[37] E. Barka, M. Al Baqari, C.A. Kerrache, J. Herrera-Tapia, Implementation of a biometric-based blockchain system for preserving privacy, security, and access control in healthcare records, J. Sens. Actuator Netw. 11 (4) (2022) 85, http://dx.doi.org/10.3390/jsan11040085, Number: 4 Publisher: Multidisciplinary Digital Publishing Institute.
[38] N.D. Sarier, Efficient biometric-based identity management on the Blockchain for smart industrial applications, Pervasive Mob. Comput. 71 (2021) 101322, http://dx.doi.org/10.1016/j.pmcj.2020.101322.
[39] T.T. Nguyen, N. Quoc Viet Hung, T.T. Nguyen, T.T. Huynh, T.T. Nguyen, M. Weidlich, H. Yin, Manipulating recommender systems: A survey of poisoning attacks and countermeasures, ACM Comput. Surv. (2024).
[40] M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, N.K. Jha, Systematic poisoning attacks on and defenses for machine learning in healthcare, IEEE J. Biomed. Health Inf. 19 (6) (2015) 1893–1905, http://dx.doi.org/10.1109/JBHI.2014.2344095.
[41] A. Khang, Applications and Principles of Quantum Computing, IGI Global, 2024.
[42] N. Ahmed, Quantum computing algorithms for integer factorization: A comparative analysis, Mod. Dyn.: Math. Progress. 1 (1) (2024) 6–9.
[43] A. Cintas-Canto, J. Kaur, M. Mozaffari-Kermani, R. Azarderakhsh, ChatGPT vs. Lightweight security: First work implementing the NIST cryptographic standard ASCON, 2023, arXiv:2306.08178. URL https://arxiv.org/abs/2306.08178.
[44] A.C. Canto, J. Kaur, M.M. Kermani, R. Azarderakhsh, Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security, 2023, arXiv:2305.13544. URL https://arxiv.org/abs/2305.13544.
[45] Z. A.Mohammed, K.A. Hussein, Lightweight cryptography concepts and algorithms: A survey, in: 2023 Second International Conference on Advanced Computer Applications, ACA, 2023, pp. 1–7, http://dx.doi.org/10.1109/ACA57612.2023.10346914.
[46] M. Mozaffari-Kermani, A. Reyhani-Masoleh, Concurrent structure-independent fault detection schemes for the advanced encryption standard, IEEE Trans. Comput. 59 (5) (2010) 608–622, http://dx.doi.org/10.1109/TC.2010.33.
[47] M. Mozaffari-Kermani, A. Reyhani-Masoleh, A lightweight high-performance fault detection scheme for the advanced encryption standard using composite fields, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 19 (1) (2011) 85–91, http://dx.doi.org/10.1109/TVLSI.2009.2031651.
[48] D. Yang, Post-quantum cryptography: Effects of quantum computing on modern cryptography, Int. J. High Sch. Res. 6 (6) (2024).