Cluster Computing (2024) 27:3741–3752
https://doi.org/10.1007/s10586-023-04180-x

Blockchain-based biometric identity management

Sherif Hamdy Gomaa Salem[1] · Ashraf Yehia Hassan[1] · Marwa S. Moustafa[2] · Mohamed Nabil Hassan[3]

Received: 1 April 2023 / Revised: 9 October 2023 / Accepted: 14 October 2023 / Published online: 7 November 2023

Abstract

In recent years, face biometrics recognition systems are a wide space of a computer usage which is mostly employed for security purpose. The main purpose of the face biometrics recognition system is to authenticate a user from a given database. Due to the widespread expansion of the surveillance cameras and facial recognition technology, a robust face recognition system required. The recognition system needs to store a large number of training samples in any storage unit, that time hackers can access and control that data. So, Protecting and managing sensitive data is essential object. This requires a technique that preserve the privacy of individuals, maintain data integrity, and prevent information leakage. The storage of biometric templates on centralized servers has been associated with potential privacy risks. To address this issue, we have developed and implemented a proof-of-concept facial biometric identification system that uses a private Blockchain platform and smart contract technology. So, the proposed approach is presented a secure and tamper-proof from data breaches as well as hacks with data availability, by using the Blockchain platform to store face images. This paper aims to utilize Blockchain technology to identify individuals based on their biometric traits, specifically facial recognition system makes it tamper-proof (immutable) ensuring security. The system consists of enrolment and authentication phases. Blockchain technology uses peer-to-peer communication, cryptography, consensus processes, and smart contracts to ensure the security. The proposed approach was tested on two popular datasets: CelebFaces Attributes (CelebA) and large-scale face UTKFace datasets. The experimental results indicate that the system yields highly performance outcomes, as evidenced by the Equal Error Rate (EER) values of 0.05% and 0.07% obtained for the CelebA and UTKFace datasets, respectively. The system was compared to three baseline methods and scored the lowest Equal Error Rate.

Keywords Deep learning (DL) · Biometric · Blockchain · Smart contract

1 Introduction

Digital Identity [24, 29] is digital representation of information about a person, group, or organization which include photos, bank account information, and physical identifiers [28]. Many organizations and governments have raised the alarm about identity theft and fraud. Biometric Authentication Systems (BASs) are using unique biometric features such as fingerprints, facial recognition, hand geometry, palm print, iris, signature, gait, and voice patterns to identify individuals. It has become popular due to their simplified enrolment. An administration module manages user biometric data (templates), and the authentication module analyses freshly individual trait against enrolled templates. The unique and complex nature of biometric data may result in several security concerns [9, 27]. In classical BASs, biometric data is maintained by

✉ Sherif Hamdy Gomaa Salem
Sherif22006@yahoo.com

Ashraf Yehia Hassan
Ashraf.fahmy@bhit.bu.edu.eg

Marwa S. Moustafa
marwa@narss.sci.eg

Mohamed Nabil Hassan
M_nabil1974@yahoo.com

[1] Electrical Engineering Department, Faculty of Engineering, Benha University, Banha, Egypt

[2] National Authority for Remote Sensing and Space Sciences, Cairo, Egypt

[3] Armed Forces Research and Development Center, Cairo, Egypt

central administration module, which questions the security. A centralized server should be “honest yet inquisitive”. But the centralized server may be hacked, which leads to an incorrect result.

Deep Learning (DL) has become a successful recipe for biometric authentication because it can extract features and learn from complex data, such as images and videos. So allows deep learning models to be used to identify individuals based on their unique biometric features such as fingerprints, facial recognition, hand geometry, palm print, iris, signature, gait, and voice patterns [1]. Deep learning is more accurate, scalable, and robust than traditional biometric authentication methods due to its ability to recognize even subtle differences in biometric features, robustness to noise and variations in biometric data, and scalability to handle larger biometric datasets. Due to its popularity, it is used in mobile devices, access control systems, and online banking [3]. On other hand, deep learning models can be vulnerable to attack, thrift and alteration which means that they can be tricked into misidentifying individuals [31]. Cyberattacks on a variety of services have become increasingly common, including Facebook, LinkedIn, Yahoo, and Zoom [30]. Recent research focused on enhancing the safety of biometric templates and reduce attacks [17, 22].

Blockchain technology is a distributed ledger, allows untrustworthy nodes to provide trustworthy and irreversible services [4, 13]. Since there is no central authority, distributed ledgers were employed to retain an immutable chronological record of all transactions. Blockchain technology was popularized by Bitcoin [18]. Blockchain might provide safe, efficient, and transparent information transmission to secure authentication, anonymity, and permanence [6] in digital identity, banking, healthcare, voting, real estate, social media and Internet of Things (IoT). A Blockchain network can be classified as: (1) public, (2) consortium, and (3) private. Public Blockchain are permissionless, economic incentives for anonymous and universal access. In contrast, consortium Blockchain are permissioned, semi-decentralized. Lastly, private Blockchain for small, trustworthy organizations. Biometrics integration is simpler with private Blockchain applications. To unlock the full potential of Blockchain-biometric synergy in public, consortium, and private Blockchain, we need to conduct further research and develop innovative security architectures [15, 26]. Smart contracts were originally coined by Nick Szabo [6] in 1996, long before the advent of Bitcoin and Blockchain. A smart contract is a piece of code that run in a safe setting to regulate digital assets [15]. Although smart contract execution is possible on a variety of public Blockchain. Ethereum smart contracts turn Blockchain into a reliable computing platform. The Blockchain network employs gas as a monetary unit to enable the execution of smart contracts. The expenditure of resources by a smart contract result in a gas expense that necessitates user responsibility. Therefore, programmers construct decentralized applications (DApps) using Solidity language.

The implementation of Blockchain technology has the potential to mitigate certain limitations associated with conventional biometric authentication methods. The technology of Blockchain has the potential to store biometric data securely and immutably. Furthermore, Blockchain technology has the potential to facilitate the development of DApps that operate without the need for a central governing entity. This implies that DApps have the potential to facilitate the creation of biometric authentication mechanisms that are impervious to security breaches. Blockchain can enhance biometric authentication in a number of ways, including security, transparency, scalability and decentralization [23, 25].

Therefore, the objective of this study is to present a decentralized biometric authentication system that employs Blockchain technology. The system employs various data types, including Ethereum address, username, and data derived from a facial biometric for the purpose of user registration and authentication. Blockchain technology incorporates several key features, including peer-to-peer communication, cryptography, consensus mechanism, and the utilization of smart contracts. These characteristics enable the technology to effectively address authentication concerns through the use of a decentralized database and communication between nodes. The system under consideration attains enrolment and authentication phases in the absence of a centralized governing body. The main contributions can be summarized as follows:

- The present study suggests the implementation of a decentralized and secure user authentication system that leverages Blockchain technology, smart contract, and secure ledger.
- The system is capable of processing authentication requests through the utilization of the Ethereum address, and biometric facial data obtained from a sensor, specifically a camera.
- It is imperative for the system to ensure that user’s data obtained from a biometric reader is non-transferable.
- The scalability of the system enables it to expand and accommodate numerous Internet of Things (IoT) devices.
- The proposed system might incorporate diverse authentication techniques and data formats for user enrolment and authentication, thereby presenting an advancement in contrast to current methods.

This paper is organized as follows: The second section briefly outlines the related work. The proposed face biometric authentication in the Blockchain setting is presented in Sect. 3. Section 4 introduced experimental data evaluation for the proposed approach. Section 5 presents the conclusions.

2 Related work

The limitations and vulnerabilities of biometric user identification open the door to benefits from recent technologies such as Blockchain and deep learning. Recently, several efforts had introduced deep learning and Blockchain to identity authentication problems. In this section, we discuss the current research in deep learning architecture for biometric authentication and then present the recent work related to Blockchain.

2.1 Biometric authentication

User authentication is a major digital challenge. Tokens, passwords, and personal identifications (PINs) are becoming outdated as they may be lost, stolen, forgotten, guessed, or compromised. In 2020, 80% of security breaches were due to weak and stolen passwords, according to the World Economic Forum [1, 22]. In recent years, biometric authentication has been a focus of research. It identifies and authenticates individuals using unique behavioural and biological traits such as face, fingerprints, hand geometry, iris, voice, palm, DNA, etc. Biometrics are unique to individuals and nearly impossible to copy or fake [25], which gives higher accuracy and prevents unauthorized access [3, 24]. A BAS [24] is composed of three main modules as illustrated in Fig. 1 (1). The biometric trait is collected by the sensor, (2) the trait is processed by the feature extractor to create biometric template, (3) the matcher module is used to identify the similarities between the input biometric trait, and the enrolled templates. Despite the boost in performance in recent years, the BASs may be vulnerable to a variety of security risks, such as the thrift or manipulation of registered templates [15, 25] due to immutability and management of biometric templates within a centralized database or module. The revelation of biometric data may give rise to diverse security risks, including the potential for stolen biometric data to be reused. Encryption, transformation, and dissemination of biometric templates have been the primary focus of previous research.

Deep neural network (DNN) helps facial authentication systems achieve tremendous progress. Transfer learning was used to train different deep convolutional neural network models for facial recognition. DeepFace [29], a pioneering work in face recognition, was based on the AlexNet convolutional neural network architecture. VGGFace [19] and FaceNet [7] use the Visual Geometry Group network (VGGNet) and GoogleNet convolutional neural networks as backbones, respectively. The utilization of triple loss function enables both models to outperform DeepFace. Later in 2017, SphereFace [16] used Residual Networks (ResNet) as backbone to future boost the performance. The large backbone networks are well known for their high computational needs, but embedded devices had trouble fitting these networks. MobileNet and SqueezeNet are compact convolutional neural network designs that are well-suited for devices with limited capabilities [8, 34]. In recent years, significant advancements have been made in BAS through the utilization of deep learning models. Despite these advancements, there remain several challenges that must be addressed in the coming years. Although some of the current biometric recognition system achieve accuracy rates of over 99%, some fundamental challenges such as matching faces/biometrics across ages, different poses, partial-data, different sensor types remain challenging. In real scenarios, datasets tend to be larger in size. Therefore, biometrics dataset which contains a much larger number of classes (10–100 M), as well as a lot more intra-class variations, would be another big step towards supporting all conditions. In real situations, the collected dataset is small size and the goal is to train powerful discriminative mode using very few samples for each

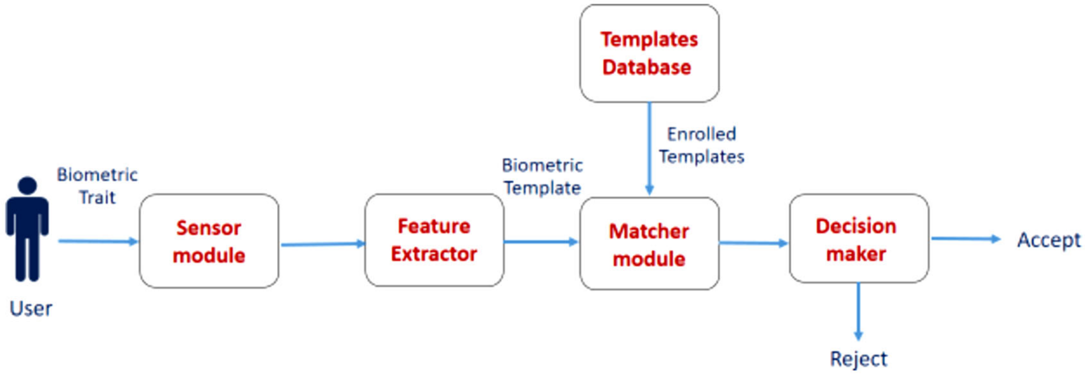


Fig. 1 Biometric system modules

individual or identity (zero/one shot in extreme case) [14]. In many applications, accuracy is most important, but a near real-time biometric identification model is also important. This could help on-device solutions like smartphone and tablet authentication. Some deep biometrics identification models are slow, therefore building near-real-time, accurate models would be useful. Knowledge distillation and model quantization may be considered. Many approaches were introduced to protect biometric templates. In [5], the authors proposed a novel approach to protect biometric templates from attack, even by quantum computers. The proposed scheme uses Learning Parity with Noise (LPN), which are a type of cryptographic that is resistant to quantum attacks. The proposed scheme works by first converting the biometric template into a binary string and then splitting the string into smaller blocks. Each block is then committed to using an LPN commitment scheme. The LPN commitments are then stored in a database. To authenticate a user, the system compares the user's biometric template to the LPN commitments stored in the database. If the template matches any of the commitments, the user is authenticated. Otherwise, the user is not authenticated. The proposed scheme has several advantages over traditional biometric template protection schemes. It is resistant to quantum attacks, it is efficient and can be implemented using existing cryptography libraries, and it is secure and can protect biometric templates from a variety of attacks. Overall, the proposed scheme is a promising approach to post-quantum biometric template protection. In [2], a new post-quantum fuzzy commitment scheme for biometric template protection was proposed. This scheme is resistant to attack by quantum computers, even when the biometric templates are noisy and imprecise. The scheme works by first converting the biometric template into a binary string and then splitting the string into smaller blocks. Each block is then committed to using an LPN fuzzy commitment scheme. The LPN fuzzy commitments are then stored in a database. To authenticate a user, the system compares the user's biometric template to the LPN fuzzy commitments stored in the database. If the template matches any of the commitments within a certain error threshold, the user is authenticated. Otherwise, the user is not authenticated. The proposed scheme was evaluated using a variety of biometric templates, including fingerprints, faceprints, and iris scans. The results showed that the proposed scheme was able to accurately authenticate users, even when the biometric templates were noisy and imprecise. Overall, the proposed scheme is a promising approach to post-quantum biometric template protection.

2.2 Blockchain using biometric authentication

Blockchain is a revolutionary and promising technology that records information in a way that makes it difficult or impossible to change, hack, or cheat. The exceptional security features of Blockchain have transformed various financial services and digital payments. Additionally, its distinct attributes, including decentralization, immutability, auditability, fault tolerance, and availability, have been instrumental in garnering increased public attention [11]. The decentralized and readily accessible nature of Blockchain technology makes it a viable solution for addressing security concerns that arise from the storage of biometric data. This is particularly relevant in cases where biometric data of the same individual is stored across multiple independent applications. Specifically, with regards to biometric authentication. On the other hand, Blockchain-based identity management (IDM) is essential for data protection. Blockchain-based identity management overcomes conventional IDM's defects such as security and scalability. Blockchain includes three crucial concepts: nodes, miners, and Blocks [21]. Blockchain simplifies life by altering the manner of personal data is kept are made available. As long as the governments and the other third parties are dealing with the problem, the users continue to be exposed. Personal IDM takes rising productivity and security. Blockchain gets rid of the third party by exchanging data between two nodes. Blockchain technology [10] can improve biometric systems by incorporating immutability, accountability, and availability.

- A Blockchain provides the immutability of its registers, which a biometric system might employ to save templates securely.
- A Blockchain enhances the auditability and accountability for data stored, which can prove to a third party that biometric patterns have not been altered.

In [21], the authors addressed a biometrics-based secure authentication system. User authentications rely on a modified approach based on discrete cosine transform (DCT) feature transformation and Lagrange's interpolation. The proposed method supplies secure authentication with high degree of accuracy, a constant-size database, and multi-biometric protection. The proposed system achieved an average of 95.42% and 4.57% for Genuine Acceptance Rate (GAR) and False Rejection Rate metric (FRR), respectively. In [12], Blockchain-based hybrid image encryption technique was proposed for IoT setting. The proposed technique creates a private Blockchain with smart contracts for seamless data exchange, automation, data monetization, which enhanced privacy and identity security, for IoT medical networks to increase data offloading safety. The Blockchain system uses a bi-scroller chaotic encryption algorithm to encode medical imagery. The proposed technique achieved an average of 34%. 99.65% in terms of Unified Averaged Changed Intensity (UACI) and Number of Pixel Change Rate (NPCR), respectively.

3 Proposed method

The proposed system for biometric-based face recognition employs a private Blockchain platform that incorporates smart contracts. The system is designed to verify user identity using face recognition, with the aim of ensuring data security and protecting user privacy, as depicted in Fig. 2 The components of the proposed system consist of a client device (CD) in the form of a smart phone, a trusted Agency (TA), a cloud server (CS), and a Blockchain (BC) platform that is equipped with a smart contract. The proposed system comprises of two distinct stages: (1) The enrolment (training) phase, and (2) The authentication (testing) phase. During the training phase, the employed face recognition system generates a database by capturing individual face images. During the testing phase, the system identifies individuals by comparing the similarity scores of facial features obtained from facial images submitted as test queries. The face recognition approach that has been adopted consists of the following steps.

3.1 Acquisition of biometrics data

The initial step of the proposed recognition system involves the acquisition of data. The database system necessitates the inclusion of a unique identifier (UID) for each user. During the process of data acquisition, a Client Device (CD) utilizes sensors such as a camera to capture face images of individual users. The process of image capturing is followed by face detection, wherein Viola-Jones algorithms face detection algorithm is employed to identify and isolate the facial region.

3.2 Face pre-processing and normalization

The pre-processing and normalization are essential step in the context of feature extraction and matching of facial images. We employed Contrast Limited Adaptive Histogram Equalization (CLAHE) technique to reduce noise to within the acquired facial images in order identifying distinctive features. The facial image is subjected to cropping and resizing, resulting in a final representation of the facial region with dimensions of 244 × 244 pixels × 3 channels.

3.3 Biometric feature extraction

Next, Client Device (CD) proceeds to transmit facial images to the Trusted Agency (TA). Trusted Agency is tasked with the generation of embedding for face images using the FaceNet [7] network due to its ability to overcome problems, like age, handling variations in pose, expression, illumination, and heterogeneous face matching. To overcome the influence of poses, illuminations, occlusions, different augmentation techniques had been. The overall structure of the FaceNet network, depicted in Fig. 3, is designed to optimize the squared L2 distances between the two embedding vectors.

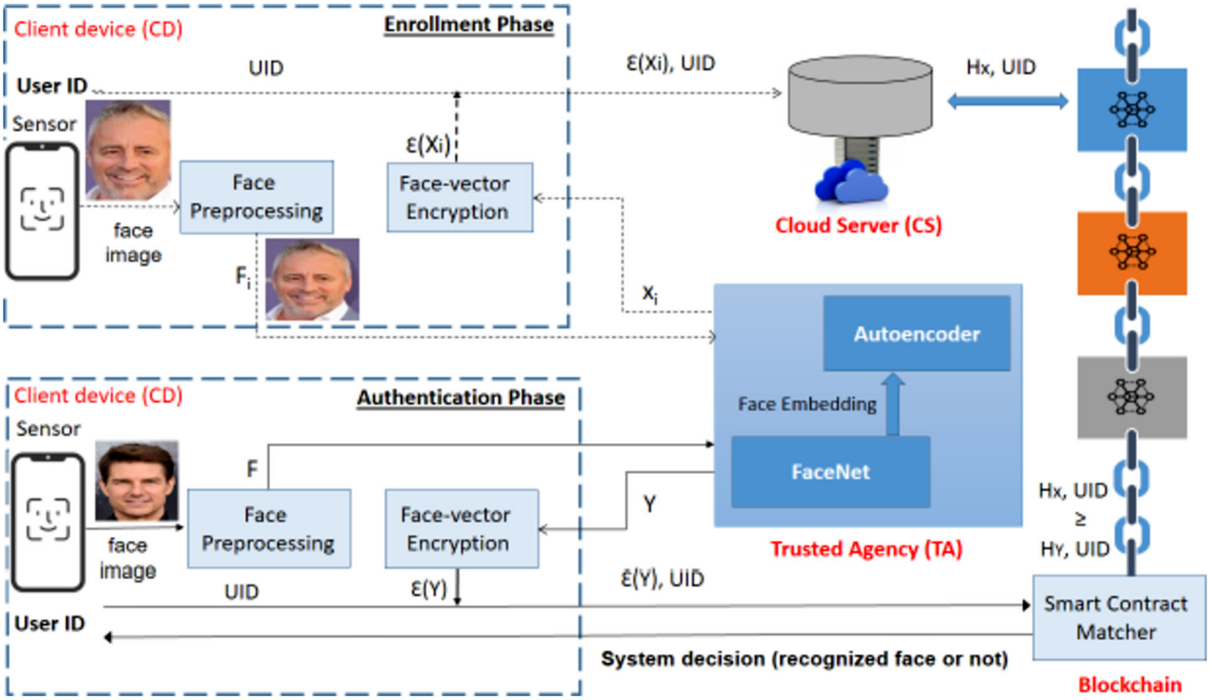


Fig. 2 The proposed biometric identity recognition system via blockchain platform

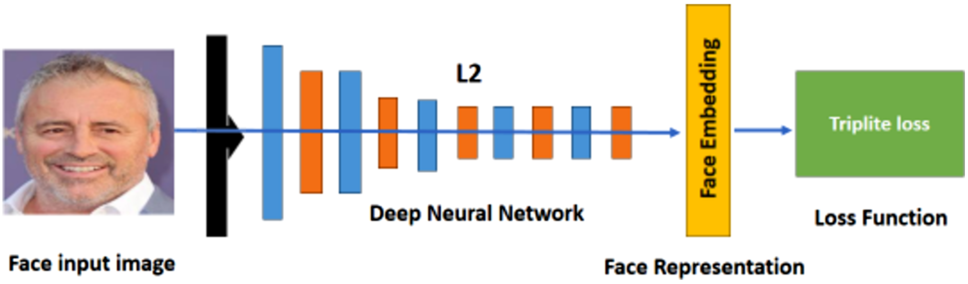


Fig. 3 FaceNet architecture: an input layer, deep convolutional neural network, L2 feature normalization give the face embedding, and training phase using triplet loss function

This optimization is achieved through the utilization of the triplet loss function defined in Eq. (1)

$$L = \sum_{i=1}^{N} \left[\left\| f(x_i^a) - f(x_i^p) \right\|_2^2 - \left\| f(x_i^a) - f(x_i^n) \right\|_2^2 + \alpha \right] \quad (1)$$

where $f(x_i^a)$ indicates the anchor input image, $f(x_i^p)$ indicates the positive input image, which corresponds to the same person as the anchor image. The $f(x_i^n)$ corresponds to the negative input image, i represents to the i'th input. The subscript a denotes an anchor image, p is a positive image, n is a negative image as depicted in Fig. 4, and α refers to the bias. The goal is to minimize Eq. (1) by minimizing the first term and maximizing the second term, and α bias acts as a threshold. The triplet loss function allows for embedding vectors with the same identity to have a lower distance, indicating similarity, while vectors representing different identities have a larger distance, indicating dissimilarity. During the testing phase, the FaceNet network utilizes these optimized embedding vectors to extract facial features. The network adopted in this study is designed to extract a face embedding of size 2048-D face embedding from a given face image. FaceNet is derived on the Inception model, which is itself based on the GoogleNet architecture.

3.4 Face vector and UID fusion

Additionally, the Trusted Agency uses a single layer autoencoder to combine the face embedding and UID to create the final template X_i, which is sent back to the client device. Then, the Rivest-Shamir-Adleman (RSA) algorithm, is used by the client device encrypts the final fused template X_i to produce the encrypted template $\varepsilon(X_i)$ then sent to the cloud server to be stored in the Blockchain.

3.5 The blockchain computation and matching process

Finally, the identification of individual users is achieved through the utilization of similarity matching techniques. The query face template fused by user identifier (UID) is compared to face templets saved on the Blockchain server using smart contracts to facilitate efficient processing. Within the realm of Blockchain technology, the procedure entails the calculation of the hash value for the encrypted facial template, symbolized as $\varepsilon(X_y)$, which yields the outcome marked as $H(\varepsilon(X_y))$. The smart contract Matcher illustrated in Fig. 5 is employed by the Blockchain to obtain $\varepsilon(X_i)$ from the cloud server that bears the same identity label.

The Blockchain computes the hash value H_x for the retrieved $\varepsilon(\mathrm{Xi})$ and then compares H_y with H_x. The Blockchain algorithm computes the distance $\varepsilon(\mathrm{d})$ to determine if the hash value matches, indicating successful recognition of the individual. Subsequently, the system transmits $\varepsilon(\mathrm{d})$ to the trusted Agency. In the event of such an occurrence, a message indicating an integrity failure will be transmitted to the user. The enrolment and authentication phases are illustrated in Algorithm 1 and Algorithm 2, respectively.

Algorithm 1: Enrolment Phase

```
Input: Identity Label, Reference face images, user identification
       UID of the user U.

1: The client device (CD) collects face images via sensor and apply face
   pre-processing techniques.
2: The CD send face Fi to Trusted Agency (TA).
3: The TA operates FaceNet to and generate the secret key Sk and the
   public key Pk.
4: The TA generates face embedding template of Fi then reduces dimensions
   and send the compressed template, Xi to the CD.
5: The client device (CD) encrypts Xi and sends ($\varepsilon$(Xi), UID) to the cloud
   server (CS) and the Blockchain (BC).
   6: The Blockchain (BC) calculates the hash value of $\varepsilon$(Xi)as $H_X$, and
   stores. ($H_X$, UID).
```

Algorithm 2. Authentication Phase

```
Input: Identity label, Probe images of face, UID.
Output: Accept or Reject.

1: The CD collects user face image via sensor and apply face pre-processing
   techniques.
2: The CD sends face F to the TA.
3: The TA operate FaceNet to generate face embedding then reduces the
   dimensions via single layer autoencoder and send the compressed template
   (Y) to the client device (CD.
4: The client device encrypts Y then sends (Ɛ(Y), UID) to the Blockchain.
5: The Blockchain runs smart contract Matcher to retrieve Ɛ(Xi) with the
   same identity label from the client device.
6: The hash value of retrieved Ɛ(Xi)is $H_y$ is computed by the Blockchain and
   compares $H_y$ and $H_X$.
7: The Blockchain computes the distance Ɛ(d) if the hash values are same and
   send Ɛ(d) to the trusted Agency. Otherwise, it will send an Integrity
   Failed message to the trusted authenticator.
8: The TA decrypts Ɛ(d) by secret key (Sk) and obtains R.
9: The trusted Agency (TA) compares a threshold with R, $\tau$ and decides
       whether the user is genuine or not.
```

Fig. 4 Training FaceNet with triplet loss function for face recognition

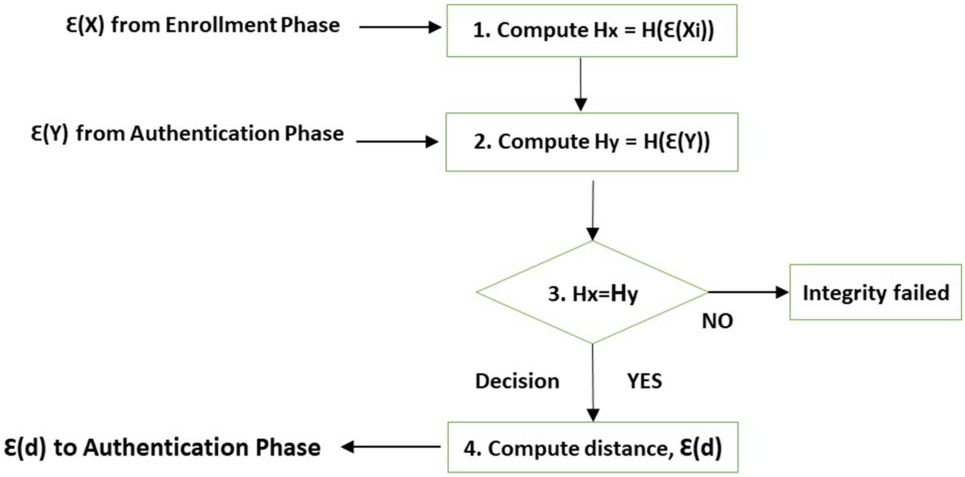

Ɛ(X) from Enrollment Phase
1. Compute Hx = H(Ɛ(Xi))
Ɛ(Y) from Authentication Phase
2. Compute Hy = H(Ɛ(Y))
3. Hx=Hy
NO
Integrity failed
Decision
YES
Ɛ(d) to Authentication Phase
4. Compute distance, Ɛ(d)

Fig. 5 The blockchain computation and matching flowchart

4 Experimental results and discussion

This section describes the test setup, database, parameters validation, and results for the proposed approach. The proposed system was tested on two widely popular datasets: CelebFaces Attributes (CelebA) and large-scale face UTKFace. A selected samples from CelebA and UTKFace as shown in Fig. 6. The test environment runs on Windows 10 Pro with Python 3.5.2. In a private Ethereum Blockchain, the smart contract is written in Solidity Language, as shown in Fig. 7. We utilized Remix IDE to create and communicate with smart contract. The experiments were run on a machine with Intel Core i7 CPU with 2.60GHz and 16 GB RAM. Truffle is used to access the Ethereum virtual network and is linked to a private Blockchain known as ganache. The connection between the host computer's local IP address (//127.0.0.1) and TCP port 8545 has been established. The contracts may be used immediately upon compilation using the 'truffle compile' command. The truffle's setup was verified, and the contracts were deployed using the 'truffle migrate' command. The instance may be put through its paces by using the 'truffle test' command, which shows the smart contract's events and operations as they unfold during testing. For all datasets, we chose 20 identities at random and 50 photos for each one, with a total of 1000 images. We consider 40 images per person in order to be used to generate the templates. Then, the rest 10 of images were used for identity authentication, with the total of 200 images for test set.

First, Tests were conducted of 20 users show that on average, 98% of users have been correctly identified. 65% identification is successful for at the first attempt, 22% at the second, 8% at the third, and 3% at the fourth as shown in Table 1.

As shown in Table 2, independent assessments pertain to the identity check conducted on 10 biometric samples for each individual. The many tries test examines the distribution of users who have successfully completed the identity check by providing one or more biometric instances. This analysis takes into account the Equal Error Rate (EER) % for two datasets, each consisting of 20 users. The majority of users may be accurately recognized within the initial two attempts, with a success rate of up to 87%. The quantity of tries required to ascertain the identity of the user is significantly impacted by the template photographs provided by the user. The presence of heterogeneity in the dataset photos results in noticeable variations among multiple shots of individuals. Given that hats and sunglasses are among the primary factors contributing to the three attempts requirement, it can be asserted with a reasonable degree of certainty that, in practical scenarios, their inclusion will yield results comparable to those achieved through experimental trials.

Next, Fig. 8 illustrates the EER (Equal Error Rate) results corresponding to various sizes of fused templates, which consist of both facial images and UID (Unique

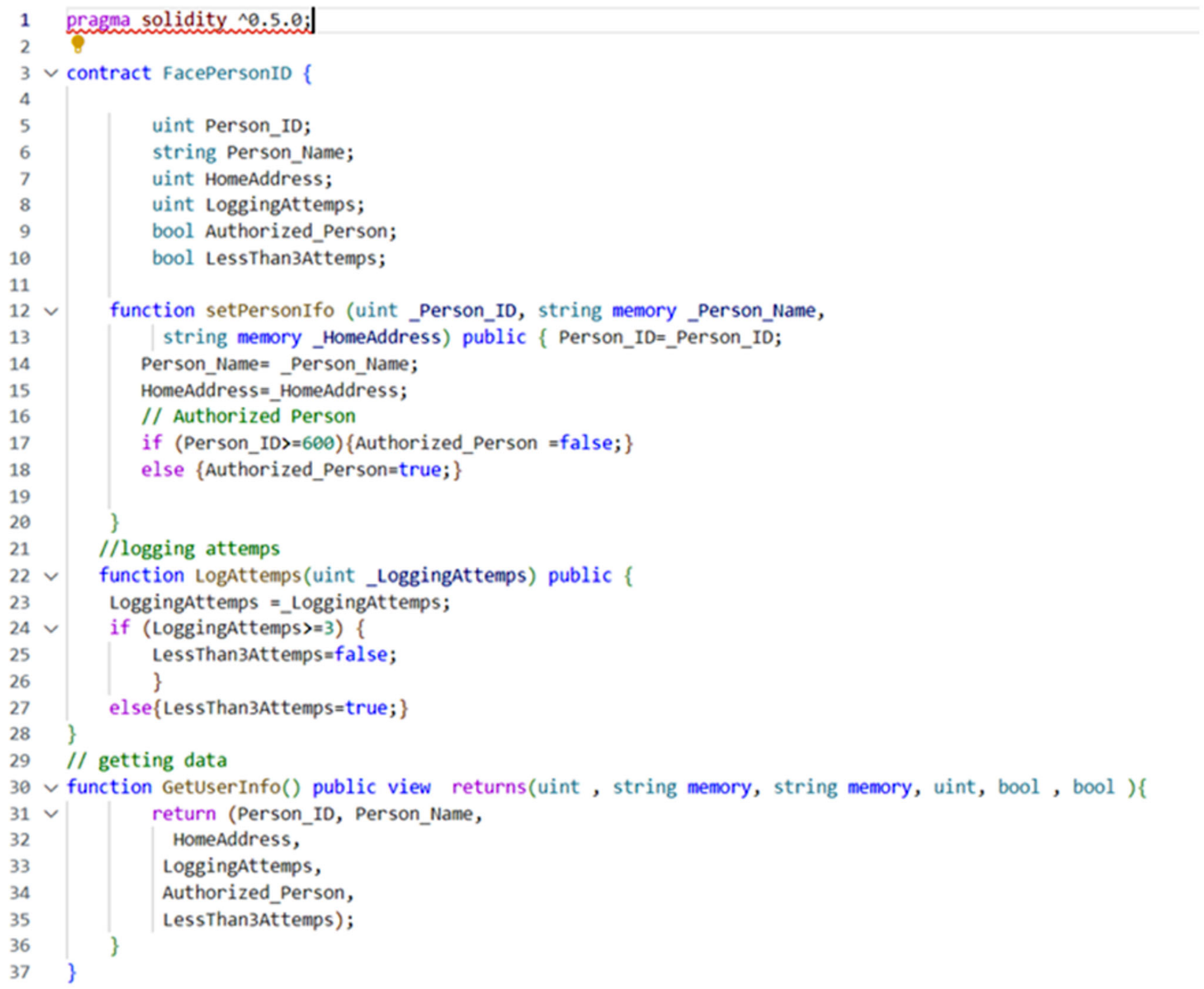
Fig. 6 Selected samples of **a** CelebFaces attributes (CelebA) and **b** large-scale faces UTKFace dataset

Identifier) data. The X-axis is representing the databases, while the Y-axis is employed to show the EER percent. In our experiment, it was determined that to achieve optimal accuracy, the fused code vector must be partitioned into blocks of size 16 bits, and 4-bits for the CelebA and UTKFace databases, respectively. The results show that the EER decreases as the block size increases. This is because a larger block size allows the face recognition system to learn more about the individual faces, which makes it more difficult to misidentify them. On the CelebA dataset, the EER decreases from 0.321 to 0.13% as the block size increases from 1 to 16. On the UTKFace dataset, the EER decreases from 0.13 to 0.0015% as the block size increases from 1 to 16 bit.

Next, experiments regarding the running time of the authentication. Table 3, show that the user authentication phases, i.e., the stage in which the biometric template is constructed, computation of hash, computing the distance between different user biometric traits. The distance computing is considered to be the most time-consuming step in the proposed approach as it done on Blockchain. Overall, the Table 3 shows that the operation time for the face recognition process varies depending on the dataset. The larger the dataset, the longer the operation time will be. On the CelebA dataset, the smart contract deployment time is 673.389 ms, the computation of hash and store it time is 877,741 ms, the verification of hash time is 797,410 ms, and the distance computation time is 2,751,053 ms. On the UTKFace dataset, the smart contract deployment time is 673.593 ms, the computation of hash and store it time is 1,753.485 ms, the verification of hash time is 1,673,154 ms, and the distance computation time is 5,885,037 ms.

Finally, Table 4 shows a comparison of the Equal Error Rate (EER) for the proposed method and different face recognition methods as Visual Geometry Group network VGGface, CosFace loss function, and adaptive and hyper-parameter P2SGrad Deep Face Model on our two datasets: CelebA and UTKFace. The proposed method achieves the lowest EER on both datasets, followed by VGGface [20], Cos Face [32], and P2SGrad [33]. This suggests that the proposed method is the most effective face recognition method on these two datasets. On the CelebA dataset, the proposed method achieves an EER of 0.341, which is significantly lower than the other methods. The second-best method is P2SGrad, with an EER of 0.482. On the UTK-Face dataset, the proposed method achieves an EER of 0.31, which is again significantly lower than the other methods. The second-best method is P2SGrad, with an EER of 0.4193. Overall, the results of the table suggest that the proposed method is a very effective face recognition method. It achieves the lowest EER on both the CelebA and UTKFace datasets, which indicates that it is able to correctly recognize faces with a high degree of accuracy.

These findings validate that the proposed approach as a trustworthy, time-saving, and biometric based identity management. Gaining access to a person's facial biometrics is a fool proof way to ensure their anonymity and speedy identification. All nodes in a Blockchain must be uniquely identifiable, and there must be a way to effectively monitor identify thrifting. Even on low-powered devices, the suggested framework may be used to execute the authentication procedure quickly.



```
pragma solidity ^0.5.0;

contract FacePersonID {

        uint Person_ID;
        string Person_Name;
        uint HomeAddress;
        uint LoggingAttemps;
        bool Authorized_Person;
        bool LessThan3Attemps;

    function setPersonIfo (uint _Person_ID, string memory _Person_Name,
         string memory _HomeAddress) public { Person_ID=_Person_ID;
       Person_Name= _Person_Name;
       HomeAddress=_HomeAddress;
       // Authorized Person
       if (Person_ID>=600){Authorized_Person =false;}
       else {Authorized_Person=true;}

    }
   //logging attemps
   function LogAttemps(uint _LoggingAttemps) public {
    LoggingAttemps =_LoggingAttemps;
    if (LoggingAttemps>=3) {
        LessThan3Attemps=false;
        }
    else{LessThan3Attemps=true;}
}
// getting data
function GetUserInfo() public view  returns(uint , string memory, string memory, uint, bool , bool ){
        return (Person_ID, Person_Name,
          HomeAddress,
         LoggingAttemps,
         Authorized_Person,
         LessThan3Attemps);
    }
}
```

Fig. 7 Implementation of matcher smart contract in blockchain platform using solidity programming language

Table 1 Percentage of 20 users identity check using the proposed method

1st att.	2nd att.	3rd att.	4th att.	Total identified check user
65%	22%	8%	3%	98%

Table 2 EER (%) regarding CelebA and UTFace dataset

Datasets		Test 1	Test 2	Test 3
CelebA	Standalone tests	0.33	0.36	0.34
UTKFace		0.35	0.33	0.31
CelebA	Multiple attempts test	0.34	0.12	0.05
UTKFace		0.38	0.16	0.07

5 Conclusions

In the past few years, the employment of facial biometrics has witnessed a surge in various corporate applications due to the constraints associated with conventional identification techniques. The widespread adoption of Blockchain technology enables companies to transition from inefficient and time-consuming processes to more reliable, secure, and cost-effective alternatives. The objective of this study is to explore the potential of Blockchain technology in the context of biometric identification, with a specific focus on facial recognition. The storage of biometric templates on remote servers has been associated with security apprehensions. In order to tackle this issue, we have developed and implemented a proof-of-concept mechanism that leverages smart contract technology integrated into a private Blockchain infrastructure to facilitate a facial

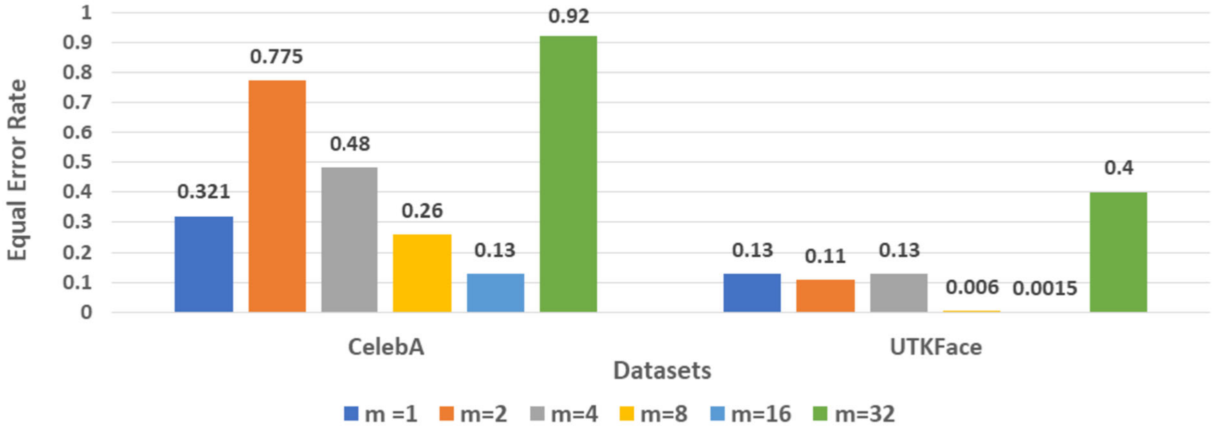


Fig. 8 The obtained equal error rate (EER) values across different sizes of face template code

Table 3 Smart contract computation time in terms of mile-second

Dataset	Operation time (ms) Smart contract deployment	Computation of hash and store it	Verification of hash	Distance computation
CelebA	673.389	877,741	797,410	2,751,053
UTKFace	673.593	1753.485	1,673,154	5,885,037

Table 4 Comparison of the proposed method with state-of-the-art approaches (EER in terms of %)

Datasets	Face recognition method	EER %
CelebA	VGGface [20]	0.7905
	Cos Face [32]	0.671
	P2SGrad [33]	0.482
	The proposed method	0.341
UTKFace	VGGface [20]	0.6522
	Cos Face [32]	0.5444
	P2SGrad [33]	0.4193
	The proposed method	0.31

biometric authentication system. During the enrolment process, the verification of a user's identity is facilitated through the utilization of both Ethereum address and facial biometric data. Blockchain technology comprises several elements, including smart contracts, distributed ledgers, decentralized consensus mechanisms, and cryptographic exchanges. We tested the proposed approaches on two publicly available face databases to ensure its efficacy. Experimental results show that our method achieves excellent performance (EER = 0.05 and 0.07% on Multiple attempts test for CelebA, and UTKFace datasets, respectively). The proposed method was compared to three other face recognition methods, VGGface, CosFace, and P2SGrad. The proposed method achieved the lowest EER on both datasets. In the future, the proposed approach can be extended in IoT setting to enable a solution for double spending problems.

Author contributions All authors conttributes equally to the manuscript.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). The authors have not disclosed any funding.

Data availability Data available on request from the authors.

Declarations

Conflict of interest All authors declare no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Ahmed, M.R., Islam, A.M., Shatabda, S., Islam, S.: Blockchain-based identity management system and self-sovereign identity ecosystem: a comprehensive survey. IEEE Access **10**, 113436–113481 (2022)
2. Al-Saggaf, A.A.: A post-quantum fuzzy commitment scheme for biometric template protection: an experimental study. IEEE Access **9**, 110952–110961 (2021)
3. Al-Waisy, A.S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., Nagem, T.A.: A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal. Appl. **21**, 783–802 (2018)
4. Aste, T., Tasca, P., Di Matteo, T.: Blockchain technologies: the foreseeable impact on society and industry. Computer **50**, 18–28 (2017)
5. Arjona, R., Baturone Castillo, M.I.: A post-quantum biometric template protection scheme based on learning parity with noise (LPN) commitments. IEEE Access **8**, 182355 (2020)
6. Cachin, C., Vukolic, M.: Blockchains consensus protocols in the wild (2017). arXiv preprint, arXiv:1707.01873
7. Cao, Q., Shen, L., Xie, W., Parkhi, O.M., Zisserman, A.: Vggface2: a dataset for recognising faces across pose and age, 13th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2018), IEEE, pp. 67–74 (2018)
8. Chen, J.-C., Ranjan, R., Kumar, A., Chen, C.-H., Patel, V.M., Chellappa, R.: An end-to-end system for unconstrained face verification with deep convolutional neural networks, Proceedings of the IEEE International Conference on Computer Vision Workshops, pp. 118–126. (2015)
9. CHOUDHARI, S., DAS, S.K., PARASHER, S.: Interoperable blockchain solution for digital identity management, 6th International Conference for Convergence in Technology (I2CT), IEEE, pp. 1–6. (2021).
10. Delgado-mohatar, O., Fierrez, J., Tolosana, R., Vera-rodriguez, R.: Blockchain and biometrics: a first look into opportunities and challenges, International Congress on Blockchain and Applications. Springer, Berlin (2019)
11. Delgado-Mohatar, O., Fierrez, J., Tolosana, R., Vera-Rodriguez, R.: Blockchain and biometrics: a first look into opportunities and challenges. In: Blockchain and Applications: International Congress, pp. 169–177. Springer (2020)
12. Durga, R., Poovammal, E., Ramana, K., Jhaveri, R.H., Singh, S., Yoon, B.: CES blocks—a novel chaotic encryption schemes-based blockchain system for an IoT environment. IEEE Access **10**, 11354–11371 (2022)
13. Gorkhali, A., Li, L., Shrestha, A.: Blockchain: a literature review. J. Manage Anal. **7**, 321–343 (2020)
14. Jing, L., Tian, Y.: Self-supervised visual feature learning with deep neural networks: a survey. IEEE Trans. Pattern Anal. Mach. Intell. **43**, 4037–4058 (2020)
15. Litke, A., Anagnostopoulos, D., Varvarigou, T.: Blockchains for supply chain management: architectural elements and challenges towards a global scale deployment. Logistics **3**, 5 (2019)
16. LIU, W., WEN, Y., YU, Z., LI, M., RAJ, B., SONG, L.: Sphereface: deep hypersphere embedding for face recognition, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 212–220. (2017)
17. Montessoro, P.L.: Biometric-based human recognition systems: an overview. In: Sarfraz, M. (ed.) Recent advances in biometrics. Intechopen, London (2022)
18. Nakamoto, S.: Bitcoin: A Peer to Peer Electronic Cash System (2008). https://bitcoin.org/bitcoin.pdf. Accessed 20 Mar 2018
19. Parkhi, O.M., Vedaldi, A., Zisserman, A.: Deep face recognition. University of Oxford, Oxford (2015)
20. PARKHI, O., VEDALDI, A., ZISSERMAN, A.: Deep face recognition, BMVC 2015-Proceedings of the British Machine Vision Conference 2015, British Machine Vision Association, (2015)
21. Patil, S.D., Raut, R., Jhaveri, R.H., Ahanger, T.A., Dhade, P.V., Kathole, A.B., Vhatkar, K.N.: Robust authentication system with privacy preservation of biometrics. Secur. Commun. Netw. (2022). https://doi.org/10.1155/2022/7857975
22. Mandalapu, H., Aravinda Reddy, P.N., Ramachandra, R., RAO, K.S., Mitra, P., Prasanna, S.M., Busch, C.: Audio-visual biometric recognition and presentation attack detection: a comprehensive survey. IEEE Access **9**, 37431–37455 (2021)
23. Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Yang, C.: The blockchain as a decentralized security framework [future directions]. IEEE Consum. Electron. Mag. **7**, 18–21 (2018)
24. Rivera, R., Robledo, J.G., Larios, V.M., Avalos, J.M.: How digital identity on blockchain can contribute in a smart city environment, international smart cities conference (ISC2). IEEE **2017**, 1–4 (2017)
25. Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: review and open research challenges. IEEE Access **7**, 10127–10149 (2019)
26. Kouhizadeh, M., Sarkis, J.: Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability **10**, 3652 (2018)
27. Sin, E.S., Naing, T.T.: Digital identity management system using blockchain technology, International Conference on Innovative Computing and Communications: Proceedings of ICICC, 2021 Vol. 2, pp. 895–906. Springer (2020)
28. Sullivan, C., Burger, E.: Blockchain, digital identity, e-government. Bus. Transform. Blockchain **2**, 233–258 (2019)
29. Taigman, Y., Yang, M., Ranzato, M.A., Wolf, L.: Deepface: closing the gap to human-level performance in face verification, In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1701–1708. (2014)
30. Umoren, O., Singh, R., Pervez, Z., Dahal, K.: Securing fog computing with a decentralised user authentication approach based on blockchain. Sensors **22**, 3956 (2022)
31. Volkova, S.: Attacks on facial biometrics systems: an overview. Comput. Appl. Manag. Sustain. Dev. Prod. Ind. (CMSD2021) **12251**, 20–25 (2022)
32. WANG, H., WANG, Y., ZHOU, Z., JI, X., GONG, D., J. ZHOU, Z., LI: and W. LIU, Cosface: large margin cosine loss for deep face recognition, In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 5265–5274. (2018)
33. ZHANG, X., ZHAO, R., YAN, J., GAO, M., QIAO, Y., WANG, X., LI, H.: P2sgrad: Refined gradients for optimizing deep face

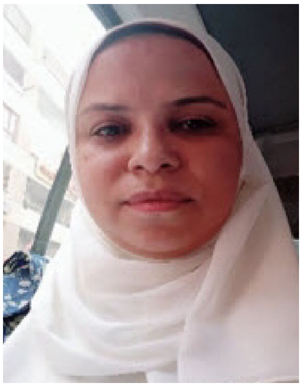
models, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 9906–9914. (2019)

34. Zhong, Y., Huang, B.: Toward end-to-end face recognition through alignment learning. IEEE Signal Process. Lett. **24**, 1213–1217 (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Sherif Hamdy Gomaa Salem was born in Egypt in 1973. He received the B.Sc. degree in Electronics and communications from Air defense college, Alexandria University, Egypt, in 1995. He received the M.Sc. degree in Electronics and Electrical Communications Engineering from faculty of engineering Aswan University, Egypt, in 2017. He is currently a demonstrator at Faculty of Engineering, Benha University, Egypt. His current research interests include data security, and cryptography.

Ashraf Yehia Hassan received the B.Sc. degree (with honors) and the M.S. degree in electrical engineering from, Benha University, Benha, Egypt, in 2000 and 2004, respectively, and the Ph.D. degree in Electronics and Electrical Communications Engineering from Cairo University, Cairo, in 2010. From 2000 to 2010, he served as a research and teaching assistant at the electrical technology department in Benha Faculty of Engineering. He works nine years as a researcher in the research and development center in Egyptian Telephone Company from 2000 to 2009. From 2012 until 2015, he works as a visiting assistant professor at Northern Border University – Faculty of Engineering, Saudi Arabia. In 2017, he has promoted to associate professor degree. Now he was the head of the electrical engineering department from 2017 to 2019 in Benha faculty of engineering – Benha University, Egypt. Now he is the head of a research group working in physical layer researches for new communication standards such as 5G, DVB-S2, and ISDB-S3 standards.



Marwa S. Moustafa received the B.Sc. and M.Sc. degrees in computer science from the Faculty of Science, Helwan University, and the Ph.D. degree in computer and information sciences from Ain Shams University, Egypt, in 2016. She is currently head of the Department of Digital Image Processing and Its Applications, Data Reception, Analysis and Receiving Station Affairs Division, National Authority for Remote Sensing and Space Sciences, Cairo. Her research interests include image processing, machine learning, and computational intelligence.

Mohamed Nabil Hassan was graduated from military technical college from communication department with grade excellent in 1996. He got his master degree from faculty of engineering - Cairo University in the field of hardware cryptography in 2005. He continued his research work in this area and pursed his Ph.D. from Department of electronic and electric engineering - The University of Sheffield in 2010. He is experienced Senior Researcher with a demonstrated history of working in the Cyber security field. Current research is in the area of the design space of cryptographic systems (Software, Hardware-software, and Hardware). Specific focus includes the implementations and the analysis of the block ciphers, hash functions, Elliptic curve cryptography, Key management protocols, and recently in Blockchain.