Multimedia Tools and Applications (2024) 83:52451–52480
https://doi.org/10.1007/s11042-023-17643-5

A blockchain-based security system with light cryptography for user authentication security

Imen Hagui[1] · Amina Msolli[1] · Noura ben Henda[1] · Abdelhamid Helali[1] · Abdelaziz Gassoumi[2] · Thanh Phuong Nguyen[3] · Fredj Hassen[1]

Received: 8 March 2023 / Revised: 9 October 2023 / Accepted: 30 October 2023 /
Published online: 13 November 2023

Abstract
Nowadays, the Internet of Things (IoT) enables the creation of a wide range of new services, including smart cities, agriculture, energy, technology, healthcare, and other security concerns. Safety concerns currently limit the development of this advanced technology. On the other hand, traditional security protocols and existing solutions cannot be used for IoT because most of them cannot guarantee good performance. Furthermore, they are often severely limited in terms of storage, computing power, and performance. The aim of the proposed research is to introduce a secure verification framework for user authentication, with a special focus on the communication between access points and node databases. The main goal is to increase the level of security within the proposed approach, ensuring the confidentiality, integrity, and availability of the image verification system during the authentication process. To achieve this goal, three phases were implemented. First, a new hybrid biometric pattern is proposed that merges image and password features to enhance the security of user authentication. Second, lightweight Encryption and Blockchain technologies are also utilized to ensure secure communication of patterns between the access point and the node database. Finally, in order to verify authenticity, a new proposed matching process involves comparing image and password features with the database records. The experimental analysis has been carried out in terms of accuracy, False Rejection Rate (FRR), False Acceptance Rate (FAR), and error rate. The proposed approach attained an accuracy of 98%, FAR of 0.1, FRR of 0.992, and an error rate of 0.017.

Keywords Blockchain · Cryptography · Shift-advanced encryption Standard (Shift-AES) · Internet of things (IoT) · Secure hash algorithm 256 (SHA-256) · Lightweight cryptography

✉ Abdelhamid Helali
abdelhamid.helali@gmail.com

[1] Laboratory of Micro-Optoelectronics and Nanostructures, University of Monastir, Avenue of the Environment, Monastir 5019, Tunisia

[2] Department of Physics, Faculty of Sciences, King Khaled University, P.O. Box 9004, Abha 61413, Saudi Arabia

[3] Laboratory of Computer Science and Systems, University of Toulon, Toulon, Toulon Cedex 9 83041 , France

1 Introduction

Progress in the electronics industry and scientific advancements have enabled the mass production of affordable smart products. Consequently, there has been a significant rise in the number of internet-connected devices, leading to the utilization and improvement of existing services across various fields. The Internet of Things (IoT) has gained prominence as a research area, where smart devices can be interconnected globally via wired or wireless networks. IoT finds application in diverse domains such as connected cars, smart cities, government agencies, and wireless sensor networks. These IoT structures are characterized by heterogeneity, employing different technologies, operating on distinct systems and architectures, and relying on unique devices [1].

IoT represents the concept of connecting the entire internet, encompassing various communication objects and data exchange methods. It forms a powerful and efficient network of interconnected physical devices that operate within cyberspace, facilitating real-time data processing, peer-to-peer connectivity, and advanced analytics.

However, the security of IoT frameworks has emerged as the primary challenge for researchers and analysts, impeding the rapid development and widespread adoption of this transformative technology [2]. Many IoT devices lack sophistication and cannot support complex security measures due to limitations in capacity, power handling, and performance. Existing security protocols and conventional approaches are often inadequate for ensuring the security of IoT systems. To ensure the success of IoT, it is crucial for companies and devices to prioritize security aspects such as protection against attacks, data authenticity, controlled access, and consumer privacy. Data integrity and privacy are crucial factors influencing the adoption of IoT services and applications, particularly in the realm of social media. While several privacy and security initiatives are underway, effective IoT security mechanisms that meet the requirements of information integrity, privacy, and trust are still needed [3]. Therefore, the implementation of robust security measures is essential to prevent unauthorized or malicious entities from compromising the integrity and functioning of IoT systems. In this context fits the purpose of this paper.

Where the main objective of this paper is to introduce a secure verification framework for user authentication, specifically between an access point and a node database. To achieve this objective, three stages are implemented.

Firstly, a novel hybrid biometric pattern represented by a merge algorithm is proposed. This model combines image and password features to enhance randomization and bolster the security levels within the pattern structure.

Secondly, a combination of encryption and blockchain techniques suitable for the new hybrid pattern is developed. This ensures the secure transmission of patterns from the access point to the node database. By adhering to the information security standard requirements of confidentiality, integrity, and availability, the proposed approach guarantees the security of the image verification system during the authentication process.

Finally, a new matching process is proposed. The latter involves of comparing the image features and the password features with the corresponding records in the database at the destination level.

The main contributions of this paper are the following:

- A merging algorithm of image and password has been proposed to enhance the security of the authentication process.

- Hash Function SHA-256 has been utilized, to ensure data integrity and security of the hybrid model.
- Shift-AES algorithm has been implemented to offer an extra layer of safety to the hybrid pattern.
- Blockchain technology has been utilized to secure communication between access point and destination.
- Finally, a matching process has been implemented to compare the image and password features from the node database with those from the access point.

By encouraging the use of the proposed methods in this article, as it addresses the problem of pattern information leakage and enhance the level of security. The protection of both image and password data is guaranteed by the proposed hybrid verification model, and it applies not only to the user enrollment device and node database but also to the transmission of data from the identification phase to the development phase. This new model also addresses other challenges, such as pattern randomization and the authentication of the user's location. As a result of the framework's adaptability to decentralized systems, it can be used for a variety of applications.

The proposed approach's efficiency and resistance to attacks have been proven through experimental results. These results demonstrate that the proposed approach outperforms the benchmark in terms of execution time, making it faster and more efficient. Moreover, the proposed framework exhibits a higher level of security.

In terms of accuracy, the proposed framework achieves an impressive rate of 98.3%. It also shows a False Rejection Rate (FRR) of 0.992. Conversely, the False Acceptance Rate (FAR) is 0.1, and the error rate is 0.017 when securing the hybrid pattern during data transmission between the access point and the node database. The robustness of the proposed approach against attacks makes it highly suitable for Internet of Things networks. However, the main goal of future research is to improve the performance of the algorithm by focusing on minimizing the false acceptance rate (FAR).

The rest of the paper is organized as follows. Section 2 presents the recent related work papers. Section 3 describes the proposed methodology. Section 4 focuses on results and discussion. Section 5 provides the validation and evaluation of the proposed approach. Finally, Section 6 concludes the paper.

2 Related work

Data reliability and privacy are key factors affecting how distributed IoT products and software packages spread through social means. Although a lot of privacy and security software has emerged in recent years. Several IoT security solutions have been proposed in the literature, including encryption and blockchain technology.

Wan et al. [4] presented a distributed blockchain-based industrial automation platform that is more secure and private than traditional centralized architecture.

The above articles suggested application scenarios and feasible solutions to implement blockchain on the Internet of Things. However, the current implementation of blockchain still has problems with the balance of efficiency and security. The following documentation described the solution and provided ideas.

To develop a decentralized architecture for storing IoT data produced by smart homes and cities, Uddin et al. [5] suggested adopting blockchain. IoT device privacy and

security are ensured by the architecture, which includes a secure communication protocol for power-constrained IoT devices and a gateway that employs sign encryption, a type of lightweight cryptography for IoT devices. To bridge the gap between IoT devices with limited power and memory and blockchain, the writers improved Gateway's capability as a miner selector. A software agent operating on the gateway was suggested to choose a miner node based on the criteria governing the performance of the miner.

In the recognition framework proposed by Mohsin et al. [6], blockchain and other techniques (RFID, steganography…) were used to verify access control by finger vein recognition. This proposition is ingenious in so far as the results could be just unique and strong as a proof of security. But an angle was missed. It concerns the emergency cases where the finger vein recognition does not permit to give access to unconscious patient data. The aforementioned point of view seems to be a start for more research.

To verify user identity, In [7], the authors propose a new authentication security framework to confirm user identification. To improve the randomness and security of the system, this framework uses a new composite algorithm-based control protection framework that combines RFID and Finger Vein (FV) biometric functions. In addition, it combines blockchain and steganography technology to ensure the confidentiality, integrity, and availability of user data. In [7], the authors conceived a flexible iris authentication system. The information about the iris feature is encrypted by the system using homogenous encryption technology before being saved on the blockchain for authentication, certification, and high accuracy.

In [8], the authors examined privacy concerns in IoT systems and explored five privacy preservation strategies based on blockchain technology. These strategies encompass private contracts, anonymization, encryption, differential privacy, and privacy mixing. The authors also discussed future directions and challenges related to privacy preservation in IoT systems based on blockchain. Their research provides a foundation for the development of privacy preservation strategies in the near future.

A blockchain-assisted authentication method that facilitates the authentication of devices in various Internet of Things domains was proposed in the article [9]. The protocol devises an identity management system to keep the authenticated nodes anonymous and introduces a consortium blockchain to foster trust between various domains.

In paper [10] ,the authors introduces and explores the elliptic Galois cryptography protocol, which involves utilizing a cryptographic technique to encrypt sensitive data from various medical sources. Subsequently, a Matrix XOR encoding steganography technique is employed to conceal the encrypted data within a low complexity image. Additionally, the proposed approach incorporates an optimization algorithm known as Adaptive Firefly to enhance the selection of cover blocks within the image.

To address the privacy and security challenges associated with centralized IoT, the authors in [11] proposed a solution by integrating blockchain technology with IoT. They introduced a decentralized security mechanism based on blockchain, aiming to mitigate these issues. Additionally, the widespread adoption of this approach ensures enhanced transparency, which proves advantageous for handling data streaming from various devices and equipment. However, to address the widespread issue of user privacy in the Industrial Internet of Things, A new blockchain-based intelligent industry identification management system was suggested in the paper [12]. Through biometric and fuzzy extractors, the system offers participants anonymous credentials. It also permits selective sharing, suspension/unfreezing, and revocation of credentials. Targeting the issues with the biometric authentication system's opaque biometric information management, ineffective authentication module, and risk of biometric information leakage, A blockchain-based biometric

authentication system was suggested in the article [13]. By dispersing biometric templates and maintaining them with the decentralized and tamper-proof blockchain method, the system enhances the security and dependability of current biometric authentication systems. The blockchain-based infrastructure suggested in the paper [14] enables for safe, transparent, and privacy-protected biometric authentication. The system uses distributed DID to handle biometric data and gives users authority over their own electronic identities, enabling them to fully manage their biometric identification data and guarantee user data security. Given the difficulties that blockchain technology has in storing and allowing access to private files, A biometric-based blockchain file storage and access permission mechanism are suggested in the paper [15]. This system is suitable for usage on devices with limited resources because all file storage and access requests and responses are handled on the blockchain and the file owner is not needed to store any data locally. In conclusion, while there are certain cross-domain authentication solutions based on blockchain, there are significantly fewer of them that can combine security, privacy, adaptability, and robustness, making it challenging to apply to challenging real-world scenarios. Therefore, the need for an effective and all-encompassing cross-domain authentication technique is important.

In [16], the author presented a centralized cloud cross-domain data-sharing platform based on blockchain with several security gateways to address the problem of cross-domain data access in product manufacturing. The technology uses blockchain to store data in a centralized cloud that can be audited, and smart contracts may be used to punish apps or data providers who are found to be acting improperly.

In [17], the author proposes the utilization of smart contracts in the insurance industry to streamline the processing of insurance claims. This approach offers the potential to reduce costs and errors associated with manual claim processing, while also significantly improving processing speed. The study also explores the feasibility of implementing conditional triggers within smart contracts. By leveraging smart contracts, customers can place their trust in the software rather than solely relying on the insurance company, thereby enhancing transparency between clients and the insurance provider. To address the security and privacy concerns between drones, In the paper [18], the authors suggest a blockchain-based intelligent 5G interconnection cross-domain certification scheme for drones. This approach combines smart contracts with multiple signatures based on threshold sharing to create a collaborative domain and validate trustworthy communication across cross-domain devices. The certification link between IoT intelligent devices is abstracted in the paper. [19], and the certification problem is then transformed into a signature transitivity problem using the blockchain. Here, the strain of digital signature authentication can be significantly reduced because the signature only needs to calculate the signatures and witnesses of the pertinent edges. The genuine identity of the present key user cannot be ascertained during authentication in any of the aforementioned studies that use key pairs as the unique identifier of user identity authentication, increasing the danger of account attacks.

The paper [20], examined the effectiveness of blockchain in vehicular ad-hoc networks (VANETS). As the number of transactions increases and the endorsement policy evolves, there is a corresponding increase in the volume of reads and writes occurring within a single transaction. Consequently, the overall block size of the blockchain-based VANET expands. This expansion leads to improvements in throughput and network utilization, while simultaneously reducing latency.

According to the authors in the paper [21], blockchain technology has the potential to empower patients by allowing them to maintain sovereignty and control over their personal data. This enables the availability of accurate data for precision medicine. Additionally, the high level of transparency offered by blockchain can enhance trust in

various aspects of healthcare, such as drug delivery, conditions, documentation, and end-to-end visibility. This transparency is particularly beneficial for cold chain management in ensuring the integrity of temperature-sensitive products.

In paper [22], the authors propose advanced versions of blockchain technology with the aim of accelerating various demanding real-time applications. Through simulation analysis, the proposed architecture is shown to meet all essential requirements, empowering network entities to fully leverage the benefits of 5G network sharing. The results of the simulation kernel demonstrate the effectiveness of the suggested approach.

In the paper [23] ,the authors introduced solutions for ensuring efficient blockchain hashing and validation, including approaches that address deadline, latency, and energy considerations. They also presented a BEFC scheme (Blockchain-Enabled Fog Computing) with the objective of enhancing scalability in edge computing and expanding the computational capacity for processing IoT data. These technologies hold promise in improving the overall efficiency and performance of edge computing systems when it comes to blockchain operations and IoT data processing.

Anitha et al [24],introduced a novel approach for secure authentication and improved performance in a multi-Wireless Sensor Network (WSN) model using a Light-Weight Authentication Algorithm (LWAA). Their method is based on a public blockchain and aims to enhance the verification process in Internet of Things (IoT) applications. The proposed method divides the WSN nodes into access points, group head nodes, and regular nodes based on their power variations, creating a hierarchical model. Through the utilization of blockchain, the authentication of nodes in various communication scenarios is established, ensuring a secure and reliable network. By implementing cryptography techniques, the proposed method not only enhances the lifespan of the network but also effectively reduces computation time. This combination of blockchain-based authentication and efficient cryptography contributes to the overall security and performance improvement of the multi-WSN environment, specifically in IoT applications.

Author in paper [25],created a decentralized e-healthcare framework that grants exclusive access to the user for their stored data on the server. This framework incorporates various security components that ensure data integrity and protection.

In the context of the Internet of Medical Things (IoMT), the author of [26], put forth a novel system that combines deep reinforcement learning (DRL) with blockchain technology. This system incorporates DRL-based offloading and blockchain-based task scheduling mechanisms, creating a distinctive approach for healthcare applications in the IoMT.

This paper [27] examines the implementation of a patient healthcare data blockchain that utilizes off-chain storage to enhance scalability. The blockchain includes the hash value of the medical data, while the original data is stored in multiple off-chain servers. Through a multi-server authentication system, a patient can conveniently access these servers through a single enrollment process and share their health data with authorized care providers.

In paper [28], the authors propose a method that combines blockchain with wireless-based public administration process (WBPAP) technique and auto-metric graph neural network (AGNN) approaches. The main goal of this method is to address payload balancing and node authentication in order to mitigate money mishandling and provide benefits to farmers through the implementation of a secure connection. By utilizing this approach, the diffusion, tamper-resistance, and traceability of blockchain movements are improved. This helps to reduce the integrity issues related to routing information through routing nodes. The integration of WBPAP and AGNN techniques in the blockchain system enhances the

overall security and efficiency of the process, ensuring a more secure and transparent environment for public administration and benefiting the farmers involved.

In paper [29], The authors introduce a hybrid intelligent Intrusion Detection System (HIIDS) for Internet of Things (IoT) applications, particularly in the healthcare domain. The proposed system combines machine learning and metaheuristic algorithms to enhance the detection capabilities. In IoT-based smart healthcare, biomedical sensors play a crucial role in capturing vital health parameters. These parameters are then transmitted to a cloud server for storage and analysis. However, the security and privacy of the Electronic Health Record (EHR) data stored in the cloud server are of utmost importance. The focus of this research is on identifying security attacks on cloud servers by employing an anomaly-based intrusion detection approach. By leveraging machine learning and metaheuristic algorithms, the HIIDS system aims to detect and mitigate potential security breaches, ensuring the integrity and confidentiality of sensitive health data stored in the cloud server.

Overall, these studies and proposals demonstrate the wide-ranging applications and potential benefits of blockchain technology in ensuring data reliability, privacy, and security across various IoT domains.

3 Methodology

This section describes the data security mechanism of the authentication system. It integrates blockchain technology and a hybrid cryptographic image model. As suggested by this study, providing a secure way to authenticate the system requires two phases.

In the identification phase, a hybrid pattern is represented by combining image and password features using a merging algorithm. To ensure data integrity and security, a SHA-256 hashing function is applied to the hybrid pattern. Additionally, the Shift-AES algorithm has been implemented to add an extra layer of safety to the hybrid pattern. Finally, blockchain technology is utilized to secure the communication between the access point and the destination.

In the development phase, the processes implemented in the identification phase is applied in the reverse order to separate the image features from the password features. The final step involves comparing these extracted features with the corresponding records in the database.

Figure 1 illustrates the framework of our technique and its processing at base stations and nodes for the use of the proposed technique. The diagram above suggests the proposed study architecture.

The decentralized nature of blockchain allows the distributed transmission of the hybrid pattern, obtained by merging image and password features using a merge algorithm, in a distributed manner at the blockchain level. This approach ensures that participating nodes are distributed and operate in a relaxed manner in terms of memory, computing power, and execution time. The even distribution of resources contributes to enhanced efficiency and mitigates potential bottlenecks within the system.

3.1 The merge algorithm

The purpose of the proposed new merge method is to ensure the security and integrity of each recording method and avoid duplicate references in the database. This proposed

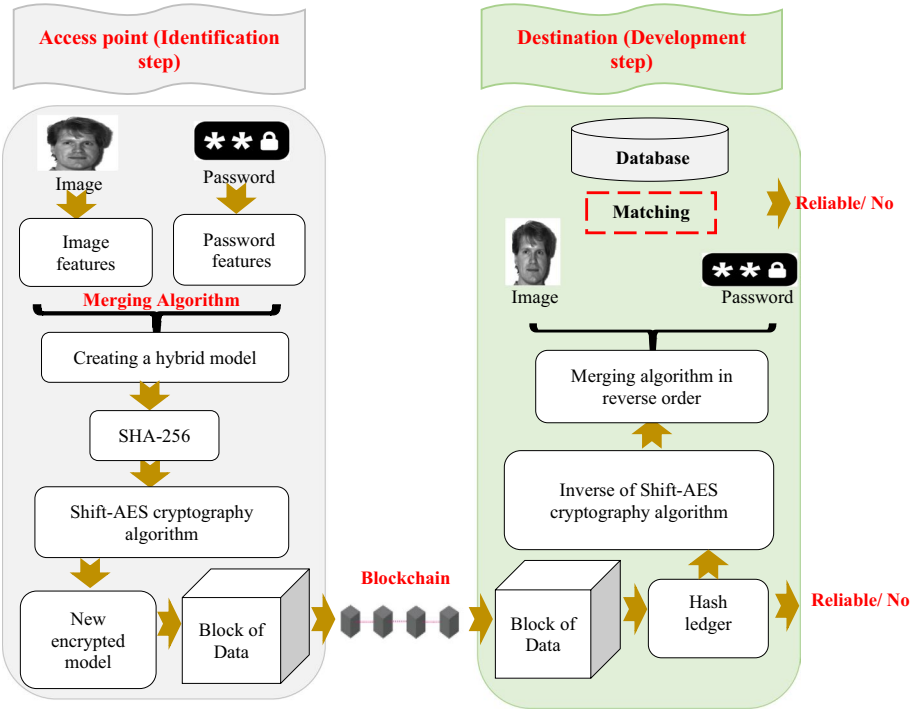

Fig. 1 Verification secure framework

method involves combining a password string and a randomly selected string from an image. The image features and password features are merged using a three-step process.

In the first step, the image and password features are extracted and converted into a binary string using a simple protocol.

The second step involves concatenating the binary-converted strings. During the rotation phase, repeated data is replaced with bit-word data.

The third step applies a chaotic function to the data using the equation provided in (1) and (2). This chaotic function is known as the standard Chirikov map, commonly referred to as the Chirikov-Taylor.

$$p_{n+1} = p_n + k \sin(\theta_n) \tag{1}$$

$$\theta_{n+1} = \theta_n + p_{n+1} \tag{2}$$

Where p and θ are angles calculated mod 2π and K is a positive constant.

3.2 Secure hash algorithm

The Secure Hash Algorithm (SHA) is a cryptographic hash function developed jointly by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). It was published as the Secure Hash Standard in May 1993, the main objective of ensuring data integrity and security, especially during transmission.

```
FUNCTION merge_algo (Hybrid_Pattern, chaotic_Hybrid_Pattern)
Hybrid_Pattern: Input
chaotic_Hybrid_Pattern: Output
Start
For n=0 to length (Hybrid_Pattern)
p(n+1) =p(n) +K*sin((n)
θ(n+1) =θ(n)+p(n+1)
end for
chaotic_Ind = int0
chaotic_Ind= chaotic_Ind%length (Hybrid_Pattern)
chaotic_Hybrid_Pattern=Hybrid_Pattern
for n=0 to length (Hybrid_Pattern)
id1=n
id2=chaotic_Ind(n)
swap (chaotic_Hybrid_Pattern (id1), chaotic_Hybrid_Pattern (id2))
end for
End
```

Algorithm 1 Illustrates the pseudo-code of merge algorithm

In the context of SHA, hashing involves taking an input, such as a message or data file, and generating a fixed-length string of characters called a hash value or message digest. The length of the hash value depends on the specific hash algorithm used.

The SHA family of algorithms includes four additional hashing algorithms known as SHA-224, SHA-256, SHA-384, and SHA-512. The suffix in their names indicates the bit size of the message digests they produce [30]. Among them, Secure Hash Algorithm 2 (SHA-2) is widely recognized and utilized, with SHA-256 being a well-known subset of SHA-2.

SHA-2 remains widely supported and used in various cryptographic applications due to its strong security properties and widespread adoption.

The Secure Hash Algorithm plays a critical role in cryptography and data security. Its main functions include verifying the integrity of data, authenticating messages, and securely storing passwords. By generating unique hash values for input data, SHA ensures that even a small modification in the input will produce a significantly different output. This property makes it challenging for attackers to tamper with or forge data without detection.

Overall, SHA is an essential component in ensuring the security and reliability of digital communications and data storage. It provides a robust cryptographic foundation for a wide range of applications, safeguarding sensitive information, and mitigating the risks associated with unauthorized access or data manipulation. And for these reasons the hybrid architecture contains SHA-256.

3.3 Encryption using shift-AES algorithm

Encryption techniques have emerged as the most critical approach to protecting recordings from strangers. Encryption structures required records to be encrypted using mathematical

algorithms and become incomprehensible during transmission, these would need to be decrypted in order to be used. Although many encryption algorithms have emerged in recent years to provide privacy and security. Several security solutions have been proposed in the literature as shown in Table 1.

According to the table, AES outperforms RSA and DES algorithms [31]. Accordingly, the first-class encryption method for information protection is the AES symmetric key encryption standard [32, 33].

The US government employs AES as a symmetric data encryption technique [34]. It can be used to encrypt data in both hardware and software. The AES algorithm can work with any combination of data (128 bits) and key lengths of 128, 192, and 256 bits. Before delivering the final cipher text or retrieving the original plain text, the AES system performs 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys, respectively.

Due to the restrictions, physical constraints and hostile conditions imposed by the IoT; power consumption which is a crucial concern in IoT network to increase network lifetime. Traditional encryption techniques are not suitable for this industry. It was necessary to adjust the traditional encryption algorithms, to increase storage memory, reduce computational complexity and strengthen security. This introduces a new type of encryption called lightweight cryptography. Shift-AES [35] is a new lightweight algorithm that can be used with IoT applications. It is an improvement of the AES algorithm and takes all these specifications. The idea of the Shift-AES algorithm is to replace the Mix-Column transformation of the AES algorithm with another Shift-Column transformation, since the multiplication process consumes more execution time and storage memory. While the other adjustments are very similar to those of the AES algorithm. As a result, the idea of replacing one process with another that requires less execution time while adhering to Shannon's concepts of dissipation and confusion emerged. Shift-AES [35] is based on four processes in the following sequence:

- AddRoundKey: is a simple xor function between the data entity and the encryption key.
- ShiftCols: is a column shift function. The ShiftCols transformation process is based on several cyclic movements of columns with different offsets, allowing a good state swapping, as shown in Eq. 3.

$$S'_{r,c} = S_{(r+offset\_shift(c))\ mod\ N_b,c} \tag{3}$$

$$\text{With} \begin{cases} offset\_shift(0) = 1\ for\ \ shift = 3 \\ offset\_shift(1) = 2\ for\ \ shift = 2 \\ offset\_shift(2) = 3\ for\ \ shift = 1 \\ offset\_shift(3) = 0\ for\ \ shift = 0 \end{cases}, N_b = 4\ and\ 0 \le r,\ c < N_b$$

Table 1 Comparison of encryption algorithms, DES, RSA, AES, and Shift-AES

	Key length	Round	Block size	Security	Speed	Flexibility
DES	64	16	64	Adequate	Very Slow	No
RSA	Variable	1	1024	Least Secure	Slowest	No
DSA	Variable			Good	Fast	Yes
AES	128, 192, 256	10,12,14	128	Excellent	Faster	Yes
Shift-AES	128, 192, 256	10, 12, 14	128	Excellent	Very Faster	Yes

Where S is the state before the change. S' is the state after the change. r is the state line. and N_b is the variety of rows similar to the state size.

- SubBytes: is a process of changing entity bits by other bits of the S-Box.
- ShiftRows: is a row shift function by its offset.

Figures 2 and 3 shows the design flow of the Shift-AES encryption algorithm that demonstrates all the processes.

Shift-AES has become a step forward due to this modification to solve the problem of massive computations, and considered as a lightweight cryptography algorithm used for IoT networks. In addition, it is for this reason the hybrid architecture of this paper finds the Shift-AES algorithm splendid and realistic to improve it.

3.4 Blockchain technology

Blockchain technology is a decentralized digital ledger that enables secure and transparent transactions to occur without the need for intermediaries like financial institutions or governments [36].

In a blockchain, each block comprises information, metadata relating to the hash of the information, and a pointer to the hash of the past block. The primary components of blockchain include cryptography, transitive hash lists, digital signatures, and hash functions [37].

Cryptography ensures secure communication, even if a malicious entity gains access to confidential data on a device.

A hash function can be used to map data of any size to translated data of a fixed size. (i) One of the main features of the hash function that makes it interesting to implement is collision avoidance. The same action cannot be created by two different inputs, and (ii) even if they seem entirely random, deterministic concealment of random transcribed data will match the relevant information. These features make blockchain packets resistant to manipulation.

The transitive hash function connects the sites where data alterations may occur. Transitivity is depicted in Fig. 3. Any modification to the data will influence the data's hash function, which will subsequently affect the final hash because the hash function combines blocks. The hash references help ensure the accuracy of the census.

The digital signature serves as the final block in the blockchain. The owner of the digital hand encrypts the data using the private key, which can only be decrypted with the corresponding public key. The verified person is liable for using the private key to subscribe to the data.

Due to its decentralized nature, the blockchain can continue to function even if specific nodes are targeted or compromised. This resilience is one of the key advantages of blockchain technology [38]. Therefore, the proposed hybrid architecture uses Blockchain technology for secure communication between access point and destination to improve authentication.

By creating an unreadable string whose length is controlled by the hashing algorithm in use, hashing is a technique for preventing data from being altered while being transmitted. Blockchain uses a hash function to encapsulate data in blocks of data. The average string is produced by the hash algorithms SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256 regardless of the length of the input string. The genesis block, the very first block of data, is hashed using the SHA 256 hash function. This sample is then retained

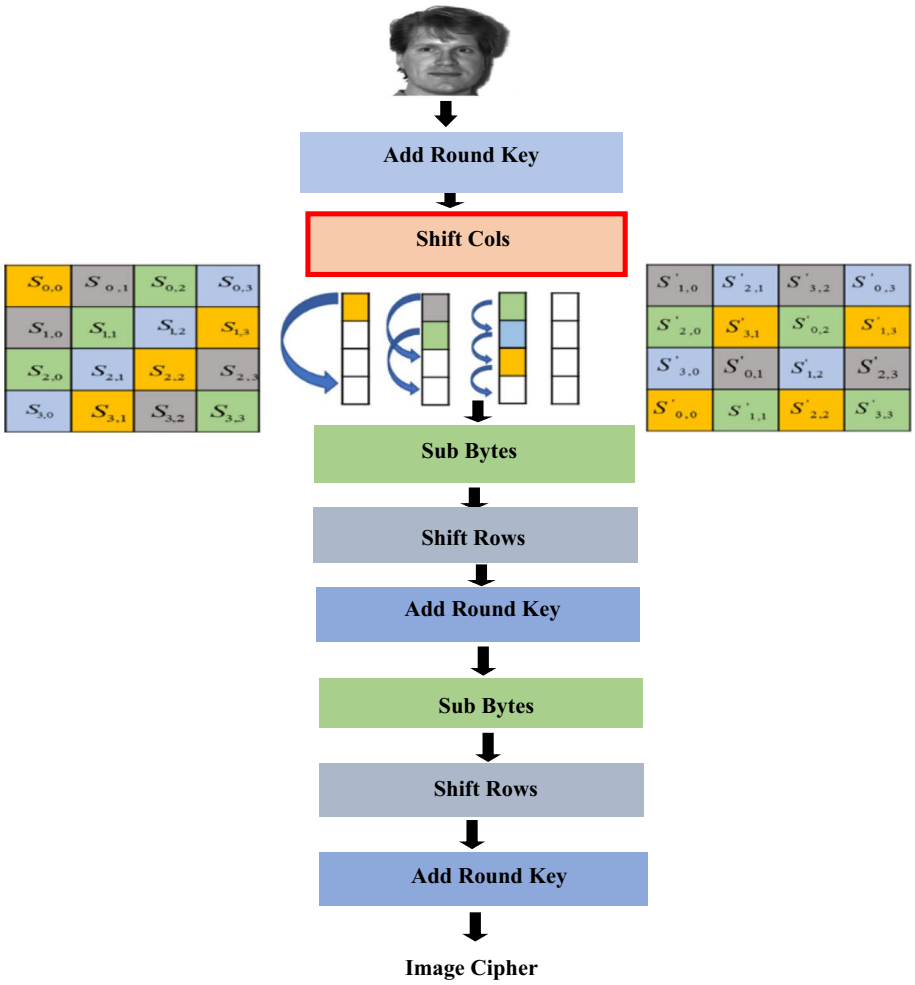

Fig. 2 Flow chart of the Shift-AES algorithm

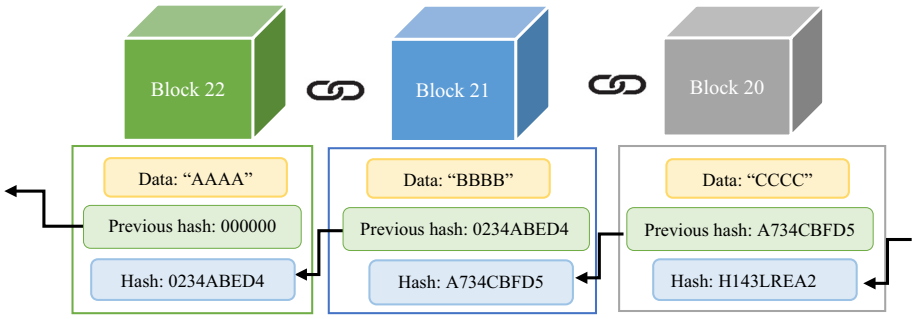

Fig. 3 Blockchain technology

in the notebook and forwarded to the node. Following that, the process is repeated for the next user.

Comparing the hashes of the present user and the prior user is the first phase in figuring out whether a second user's data block can be verified.

3.5 Matching

Verifying the authenticity of a user by comparing their provided image and password with the stored records in a database is a crucial step in the matching process. This task combines computer vision techniques and password verification methods to ensure accurate authentication. After applying the merging algorithm in reverse, which separates the image features from the password features, the next step involves comparing these features with the corresponding records in the database. The image features are compared using similarity measures to find the closest matches, while the encrypted password is compared using password verification techniques like salting to check for a match with the stored password.

When both the image characteristics and password are successfully validated against the database records, the user is granted authentication. However, if there is a mismatch, the user may be denied access or asked to re-enter their credentials. This approach of associating an image and a password with a database is commonly employed in biometric authentication systems that incorporate both visual and textual identification factors. By combining the uniqueness of the user's image with the confidentiality of their password, this new proposed approach adds an extra layer of security, thereby enhancing the accuracy and reliability of the authentication process. Figure 4 shows the comparison of the two images.

The methodology employed in this research draws on the statistical methods chosen above for the present specific motivations. First, these methods are crucial for integrating and analyzing complex data structures, particularly in merging image and password features, necessitating specialized techniques for effective handling. Second, they play a pivotal role in enhancing system security, ensuring generated patterns exhibit the required randomness and uniqueness. Third, efficiency and resource management are paramount, justifying the inclusion of lightweight cryptography like Shift-AES for resource-constrained IoT networks.

Additionally, statistical methods facilitate the integration of blockchain technology, which aligns with security objectives. They are also integral to user data validation and

Fig. 4 Comparison of the two images

```
FUNCTION compare_password (password, database)
IF password IN database THEN
    RETURN True  // Match found
  ELSE
    RETURN False  // No match found
  END IF
END FUNCTION
// Example usage
password= "my_password"
database= [" password1", " password2", " password3"]
IF compare_password (password, database) THEN
  OUTPUT "Valid password"
ELSE
  OUTPUT "Invalid password"
END IF
```

Algorithm 2 Illustrates the pseudo-code of the password comparison algorithm with the database

accurate pattern matching, ensuring reliability. Lastly, these methods emphasize the importance of transparency and reproducibility in research. Ultimately, method selection aligns closely with the research objective of improving authentication security and efficiency.

4 Results and discussion

The data security approach presented comprises two distinct phases, each aligned with a specific objective based on the research goals. The initial phase, referred to as the identification phase, focuses on determining the essential conditions required for data operation. This phase is elaborated in the dedicated subsection titled "Identification step." the second phase, known as the Development phase, it involves the creation of a secure framework for the verification system. This framework is based on a binary model recently discovered and detailed in the first phase, as described in the subsection titled "Development step".

4.1 Identification step

The method starts with the identification stage. This article explains record extraction for a new binary instance in data operations. In the second step, called development phase, a new security control architecture is built using the binary paradigm discussed above. The initial layer includes a new hybrid model based on password and image prediction to increase predictability. Password and image features are creatively combined to provide hybrid and random functionality. Figure 5 shows the access point process.

4.2 Access point

This section presents the outcomes of the enrolment process for the first user and provides information about the data types involved at each stage of processing. The enrolment process begins from the user side, followed by data transmission, and concludes with processing on the node side. Enrolment on the access point side involves utilizing the user's image and passwords. The research utilizes the Yale Face database and incorporates password functionality.

The features are enhanced by incorporating one of the earliest fossil images. Subsequently, a double string is created based on these features. To achieve this, a hybrid pattern is formed by combining the user's password features with image features (Fig. 6).

4.2.1 Datasets

Yale Face database The Yale Face Database is one of the most commonly used face datasets in face recognition. It was constructed in the early 1990s by Yale University researchers [39].

This dataset was chosen because it has the most relevant data. This series carries 165 GIF pictures of him in 15 special themes (Subject01, Subject02, etc.). Each character has eleven images of her for every facial emotion or composition indexed below: normal, medium light, the right light, wink, with glasses, without glasses, left light, sad, sleeping, happy, and Shock (Fig. 7).

Password dataset A password dataset was created for five users, containing their passwords and emails. There is a set of password information in Table 2.

4.2.2 Creation of a hybrid pattern

Given the properties of the image structure and the first user's password, use the fusion system to arbitrarily combine the two properties. The hybrid mode pattern can also be used

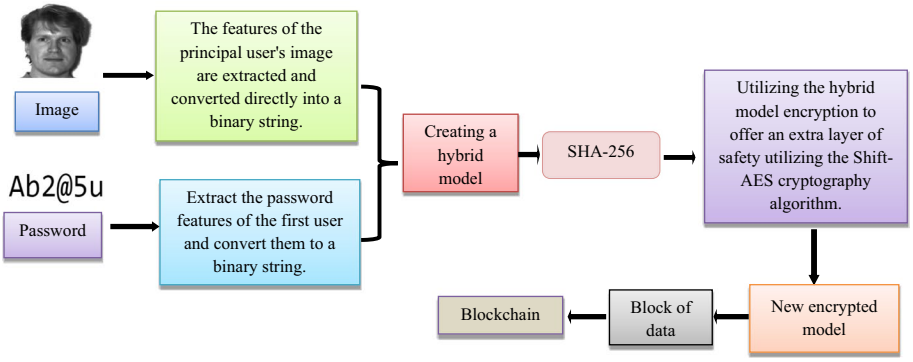

Fig. 5 Identification stage

Fig. 6 Image test

Fig. 7 Yale Face dataset

Table 2 Password dataset

	First name	Last name	Email	Gender	Password
0	Abagail	Francescone	afrancescone1@hud.gov	Female	GEdlBi
1	Sharity	Bunnell	sbunnell 1@dion.ne.jp	Female	gaAS409OR
2	Gayelord	Lepper	gLepper 0@ elpais.com	Male	XRSyUJO
3	Andrea	MacKniely	aMacKniely 2@ ftc.gov	Female	VUZw6X
4	Silvio	Synan	ssynan4@theglobeandmail.com	Male	xgRBLXTkC

to construct a double string. The 34 bits of the pixel word make up this design, along with the characteristics of the animated image corresponding to the pixel size. The model consists of images and password features and contains the first protective sublayer. To ensure

that the samples satisfy the randomness criterion, the two feature classes are also randomly combined (Fig. 8).

4.2.3 Production of hash from the random pattern

The SHA-256 algorithm is used in the proposed approach to generate a hybrid model hash. The SHA-256 algorithm should be used to create a 32-bit hash. This is because less data, regardless of the amount of input data, is created. Data integrity is ensured by utilizing hash functions, which is a benefit. Any modification or manipulation of the utility bill will modify the hash value and produce a different hash. The integrity of the secret data is thus achieved when the hash is matched in the node's ledger, revealing this modification.

4.2.4 Encryption of the hybrid pattern using Shift-AES algorithm

A security layer is added to the hybrid model using shift-AES encryption technology. Figure 9 describes the process of the new hybrid model as well as the location of the encryption algorithm. Subsequently, a validation of this process is presented.

Validation of Shift-AES algorithm Evaluation studies will be conducted to verify the new approach with the image database. The security analysis performance of the new Shift-AES method is explained at several levels: visibility scene, histogram, entropy image, near-pixel correlation, and execution time comparison with other works. These different parameters constitute the statistical attack analysis.

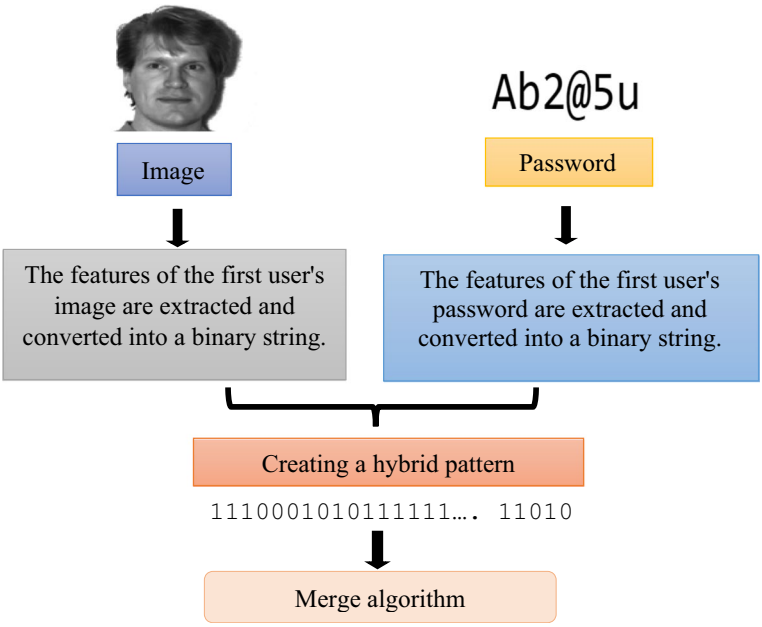

Fig. 8 Creating a hybrid model

Visibility scene

During the experiment, the standard images of the database with a size of 32 KB and a dimension (320×243) at the gray level will be used, along with a key size equal to 128 bits.

The visual observation of the standard image in Code Block Chaining (CBC) mode in given by Fig. 10, which explains well that the proposed version of the Shift-AES algorithm used in the proposed hybrid architecture satisfies the visual scene requirement and make blurry images.

Histogram images

Image histograms are crucial for statistical confidence assessment, and their purpose is to train you on image information, including distinguishing between darker and brighter images, or the degree of gradient from the most attractive elements in an image. For image security and anti-attack, the encrypted image map must be flat. Figure 11 shows the histograms of the encoded and real images. So, the result proves the efficiency of the algorithm.

The entropy analysis

The second analytical concept is entropy. It is the amount of calculation of random data, or the average uncertainty produced by each level of the input signal, as stated in Eq. 4.

$$E = \sum_{i=1}^{N} X_i\left(log2\left(X_i\right)\right) = \sum_{i=1}^{N} X_i\left(log2\left(1/X_i\right)\right) \tag{4}$$

If E is the entropy of the image in bits, X is the probability that intensity level i appears in the image, and N represents the total number of intensity levels of the image.

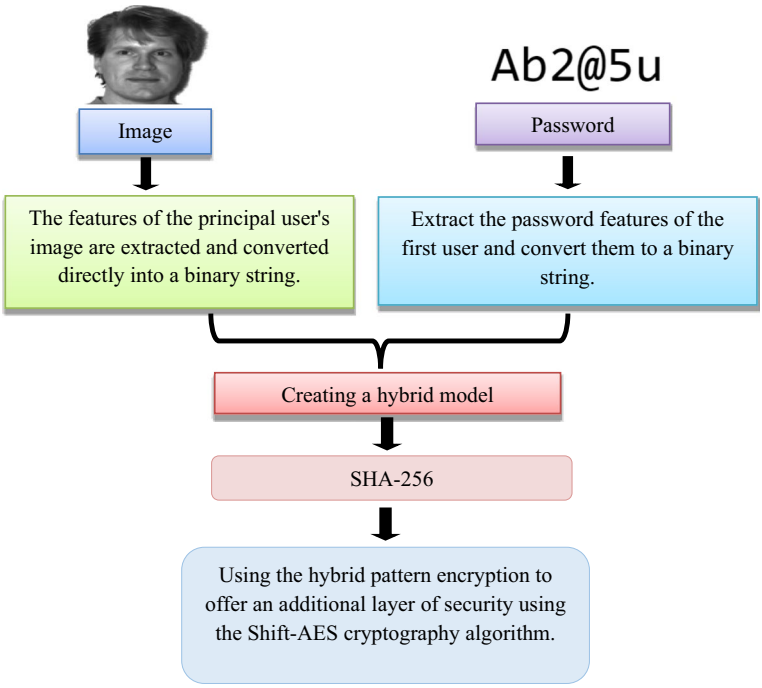

Fig. 9 Encrypt the hybrid model

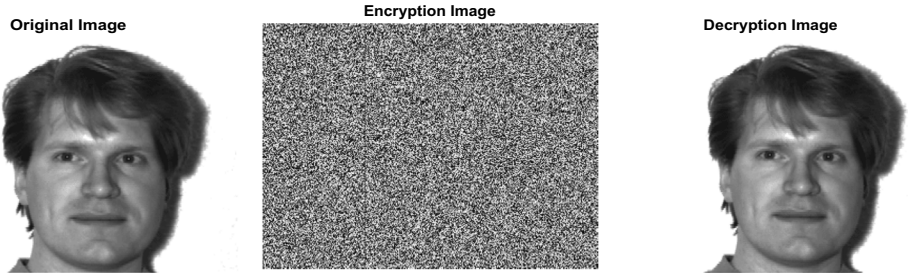

Fig. 10 Example of encryption of Image

According to the Eq. 4; to generate a single random distribution, the entropy of the gray code image should be 8.

These results show how this method works and how useful it is for statistical attacks. Feedback is more accurate when Shift-AES is enabled for a period, and graphical results are more consistent (Table 3).

Correlation coefficient

To locate shared data in the image, correlation coefficients of nearby pixels are computed. The standard image's correlation coefficients must be closely related for this to work. The combined photos, though, are incompatible. Utilizing formulas, as data analysis on correlations. (5)–(7).

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{6}$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{7}$$

Two adjacent image pixels x and y have the same grayscale. The total number of pixels taken from the image is N. The average values are E(x) and E(y). The variance is denoted

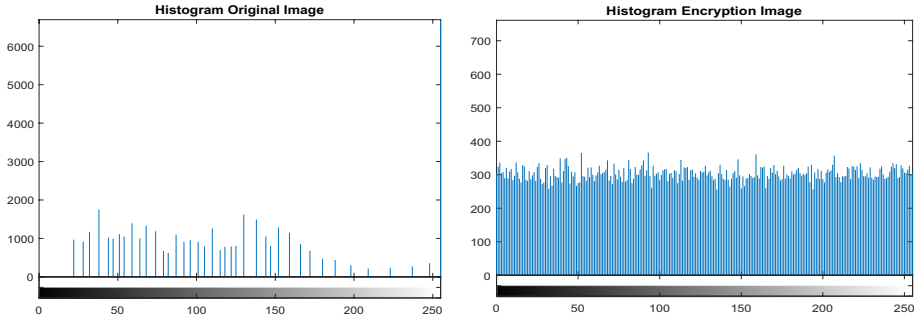

Fig. 11 Histogram analysis of image. **a** Histogram original image, **b** Histogram encrypted image

Table 3 Entropy information in CBC cipher mode

	Standard image	
	Amina [35]	Proposed system
Clear Image	7.3583	3.33
Encrypted Image	7.9993	7.9968

by D(x) and the covariance by cov (x, y). These algorithms evaluate the horizontal, vertical, and diagonal distribution of 2000 adjacent pixels in a transparent encrypted standard image. Figure 12 shows the correlation coefficient between the original image and the encrypted image. The results show a total difference between the clear image and the encrypted image. The original image pixel distribution in combined either into a single point or two points, while the pixel distribution is completely random in the encrypted image. These results express the algorithm efficiency in the proposed hybrid architecture.

Analysis of performance run time

All tweaks made for newer versions of AES are aimed at reducing execution time by changing complex math in MixColumn transformations with simple column shifts. This increases the lifetime of the sensor nodes and the entire network. Compare newer and HD image instances with different AES flavors with different encryption settings.

The results of execution in seconds of HD images in Table 4, show that the Shift-AES algorithm is faster than the standard AES algorithm and the paper [40]. Moreover, the standard database images used in the proposed architecture execute in a few milliseconds in CBC mode; where the execution time of the test image in Fig. 11 is equal to 1.451ms for encryption, while it is equal to 1.482 ms for decryption.

In conclusion, loading and processing are complete at this point. A new stage of communication uses the Blockchain technology started to transmit the encrypted data from the access point to the node.

4.2.5 Transmission to the node side

Firstly, the employment of blockchain technology is utilized to divide the data into blocks, and subsequently, the nodes are encrypted. The user pattern, starting from the access point device and extending to the node side, comprises an encrypted pattern alongside the hashes of both the current and previous users. In this chain, every subsequent user, except the first one, carries the information of the preceding user. Consequently, a sequential chain of data blocks is established, connecting the source to the destination (Fig. 13).

4.3 Development step

The development phase involves the creation of a new security control framework based on the recently identified binary model defined in the first phase. The first step is usually to create a new hybrid modeling template to add randomness based on image and password attributes. A combination algorithm is proposed that combines passwords and image functions in a mixed and random order. Because securing data from leakage is a common issue with authentication systems, a full framework for verifying user identity is proposed at this stage. A new verification model is created. This new verification model is

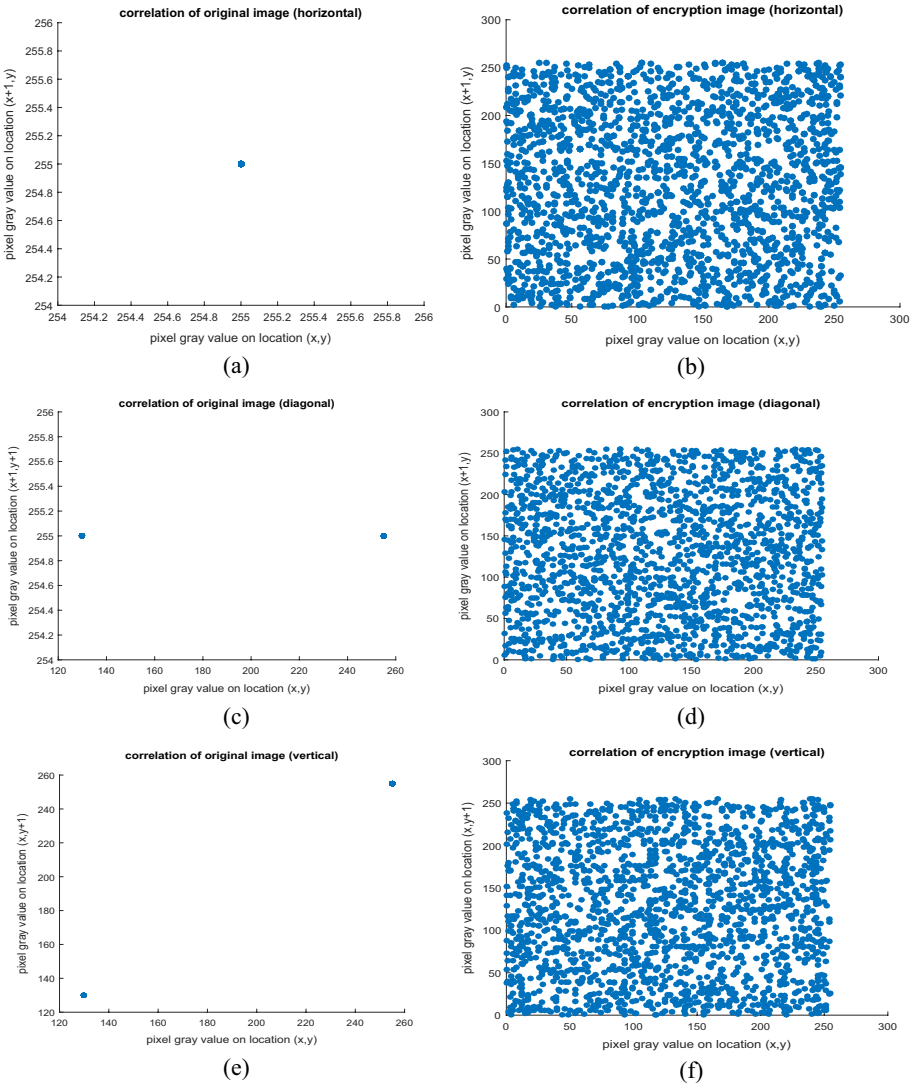

Fig. 12 Correlation coefficient between images. **a** The encrypted image's vertical, **b** The original image's horizontal correlation, **c** The encrypted image's horizontal correlation, **d** The encrypted image's horizontal correlation, **e** The encrypted image's diagonal correlation, **f** The diagonal correlation

based on biometric recognition. In the new hybrid pattern, the user-defined the first level. Fig. 14 depicts the processing on the node side.

In the user verification process, the data blocks containing encrypted patterns and hash values play a crucial role. These blocks are transmitted from the enrollment device to the node side, where the verification occurs. The first step is to compare the hash value of user N + 1 with the stored hash of user N in the node's database. This comparison ensures the consistency of subsequent user hashes with previous ones, enhancing the integrity of the verification process.

Table 4 Comparison of execution time in seconds of different types of images (HD and standard) and different algorithms in CBC encryption mode

Cipher mode	Run time (in a second)						
	Standard AES		Wadi and Zainal [40]	Shift-AES [35]			
	Image test		Image test	Image HD		Image test	
	Encryption time	Decryption time	Encryption time	Encryption time	Decryption time	Encryption time	Decryption time
CBC	1211	1217	704	199	20	1451×10^{-3}	1482×10^{-3}

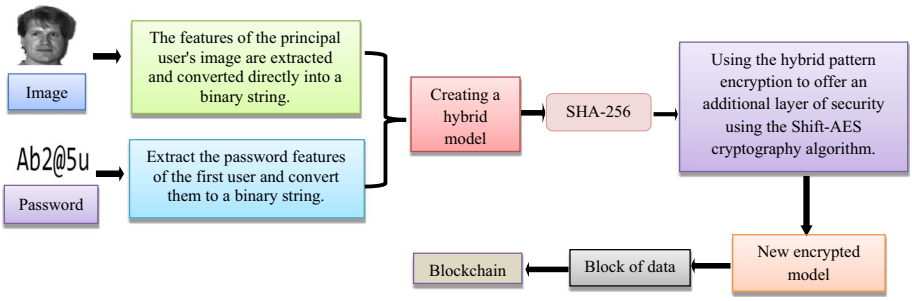

Fig. 13 Access point results

To maintain transparency and tamper-resistance, each hash that reaches the node is recorded in the ledger. The ledger acts as an initial filter, validating the integrity of the received data and authenticating the user's location. It serves as a secure repository for storing various user data, leveraging the robust protection mechanisms provided by blockchain technology. Any attempt to compromise the ledger would require gaining control over the majority (51%) of the network's nodes, which is a highly challenging task.

If the hash matching process yields positive results, indicating a match between the hashes, the verification process proceeds to the next stage. However, if the hash matching fails, indicating a discrepancy, the process is halted, and the user's request is rejected. This ensures that only users with valid and consistent data are granted access or further processing, reinforcing the security and accuracy of the system.

Afterwards, the hybrid pattern is decrypted using Shift-AES algorithm in reverse, resulting in the decrypted hybrid pattern. Subsequently, the reverse merge algorithm is applied to generate image and password features from the decrypted pattern. Finally, a matching process is executed to compare the image features extracted from the node database with

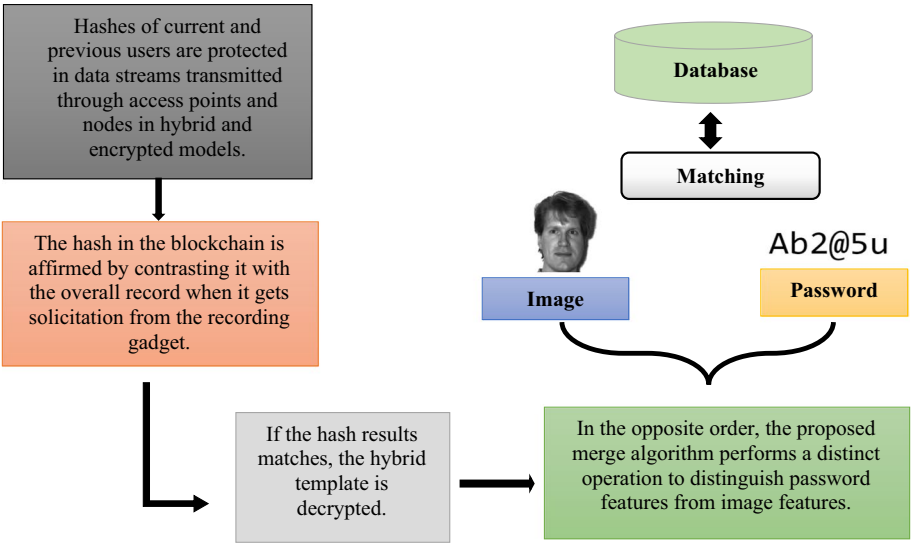

Fig. 14 Development phase

those from the access point side, as well as the password features extracted from the node database with those from the access point side. This comparison determines whether the user is genuine or an imposter.

5 Validation and evaluation

Data security is an important influencing factor that researchers grapple with. The method evaluates the proposed architecture to determine whether the research goals have been met. The motivation behind the testing is to determine whether the proposed method is suitable for the industry and whether obstacles can be avoided for its planned use. The proposed hybrid model may be suitable for applications such as.

1. Enterprise Systems and Network Security: Large organizations and businesses may implement the hybrid model for employee authentication and access control to sensitive systems and networks. Combining image and password authentication can strengthen security measures, especially for high-level access privileges.
2. Confidential Document Management Systems: Applications that handle confidential documents, such as legal or medical record management systems, may benefit from the hybrid model. It can help ensure that only authorized individuals with the correct credentials can access and modify sensitive information.

Where the verification system uses sensor nodes equipped with camera to capture images outside. In addition, there are keyboard on the door to enter the password if someone wants to enter.

In this section, the performance evaluation of the proposed approach is conducted using software implementation in Python Version 3.8.7. The experiments are executed on a machine equipped with an Intel(R) Core (TM) i7-4790 CPU running at a speed of 3.60 GHz, and 8.00 GB of RAM (Table 5).

5.1 Performance assessment of the proposed framework

The evaluation of the proposed cancelable biometric schemes involves estimating the main and imposter distributions using the chosen evaluation metric. The performance of these schemes is assessed by calculating four key metrics: the false positive rate (FAR), the false negative rate (FRR), the error rate, and accuracy.

The false positive rate (FAR) measures the probability of the biometric security system incorrectly accepting an access attempt by an unauthorized user. It indicates the system's vulnerability to falsely recognizing unauthorized users as legitimate.

$$FAR = \frac{\text{Number of successful authentications by impostors}}{\text{Number of attempts at authentication by unauthorized users}} \tag{8}$$

The false negative rate (FRR) quantifies the likelihood of the biometric security system incorrectly rejecting an access attempt by an authorized user. It represents the system's tendency to mistakenly identify authorized users as imposters.

Table 5 Comparison between proposed system and literature

	Mode of blockchain	Addressed blockchain technology	Solution type	Proposed solution	Supported IoT application
Uddin et al. [5]	Private	Consensus protocol	Architecture	Manage and monitor patient data	Smart health
Singh et al. [16]	Private	Consensus protocol	Architecture	Secure and scale of IoT resources	General IoT
Wang et al. [19]	Public	Consensus protocol	Model	Validate test-beds and impact on public blockchain	IoT devices
Mohsin [6]	private	Distributed ledger	Model	Secure patient data sharing based on blockchain	Healthcare applications
Proposed method	private	Distributed ledger	Model	Secure user information sharing of IoT based blockchain	IoT devices

$$FRR = \frac{\text{Number of failed attempts at authentication by authorized}}{\text{Number of attempts at authentication by genuine users}} \tag{9}$$

The error rate is a metric that quantifies the proportion of misclassifications or incorrect predictions made by a classification or prediction model. It provides a measure of the model's overall accuracy by considering both false positives and false negatives.

$$Error\ rate = 1 - Accruacy \tag{10}$$

In addition to these metrics, accuracy is also evaluated to assess the overall correctness of the biometric system's classifications defined as follow:

$$Accruacy = \frac{TP + TN}{TP + FN + TN + FP} \tag{11}$$

In this paper, the False Rejection Rate (FRR) is 0.992, which indicates the proportion of legitimate attempts that are incorrectly rejected by the system. On the other hand, the False Acceptance Rate (FAR) is 0.1, representing the rate at which the system incorrectly accepts unauthorized attempts. These rates are important measures of the system's accuracy and reliability.

With an impressive accuracy rate of 98.3%, the system's performance is considered outstanding. This means that it correctly identifies and verifies users with a high degree of precision.

The test level in this context refers to the process of applying the framework in a decentralized structure. It outlines how the system can be effectively utilized in a distributed network, where multiple nodes or entities are involved in the authentication process.

The mentioned research is compared to a recommended approach that involves a suitable biometric image framework. This comparison highlights that the suggested approach incorporates several significant modifications. These modifications could encompass improvements in algorithms, data preprocessing techniques, feature extraction methods, or other aspects to enhance the accuracy, efficiency, or security of the biometric system using image-based data (Table 6).

5.2 Benchmark checklist

The preceding parts describe the evaluation process. Each stage identifies and emphasizes issues that must be addressed with more attention when validating the security of a biometric image. These issues are highlighted and related to the stages of assessment and their relationships. These issues are established as a reference point for control comparisons that show the relationship between the sub-steps of the assessment and the related problems. Three essential components to recall while growing a biometric

Table 6 Comparison between proposed system and Mohsin method

	FAR	FRR	Accuracy	Error Rate
Proposed system	0.1	0.992	98.3%	0.017
Mohsin [6]	0.0377	0.1698	97.9%	0.021

Table 7 Comparison between the proposed system and other state-of-the-art approaches in the literature

Checklist issues	Mohsin [6]	Benchmark method	Proposed system
Hybrid and randomization pattern	They combined two different types of functions to create hybrid and random sampling. This increases security, and copies of the samples are stored in the node's database.	Bio-Key is combined with random numbers.	The Fusion method combines two properties to create a mixed random sample.
Secure transmission channel	Data in a chain is sent from each point of the block to the previous block, using blockchain technology to ensure a pattern in the transfer of data.	No consideration	During data transfer, the patterns were secured using blockchain technology.
Pattern cancellable	Used RFID features	Utilized random number	The password features are used algorithmic encryption technology (Shift-AES)
Pattern unreadable	AES algorithm is utilized for encryption.	Utilized hash technique	
Pattern concealing	Using steganography, the FV pattern was hidden and rendered invisible.	Not supported	
Applicable in decentralized architecture	Perfect for decentralized network architecture based on blockchain technology's unique properties.	No consideration	Decentralized network architecture makes advantage of it.
Confidentiality	Both steganography and the AES encryption scheme are fully supported.	Limited supported	Shift-AES encryption algorithm
Integrity	Integrity has been achieved through the usage of blockchain technology.	No consideration	blockchain technology
Availability	Blockchain technology opened up access to private data, which was particularly beneficial for decentralized designs.	No consideration	Of blockchain technology

image authentication gadget are accessibility, privacy, and integrity. In the primary and the second steps, you may locate associated objects inside the checklist. According to the literature studies, that is the maximum essential studies associated with the image biometric protection era, so this study is taken into consideration as a reference model. Instead, this comparative painting is applied to examine the cautioned steady biometric framework era for snapshots primarily based totally on sure essential components. A contrast between the questionnaires for this painting and Table 7 indicates the Comparison between the proposed system and other state-of-the-art approaches in the literature.

Table 7 provides a comprehensive comparison of benchmarking points between the proposed approach and the benchmark method in detail. As shown in the table, the proposed and benchmark approaches effectively solve four frequent issues: hybrid and randomisation pattern, pattern cancellability, pattern unreadability, and secrecy. However, as shown in the preceding table, the benchmark approach has limited support for hybrid and randomisation, as well as confidentiality problems.

Although the proposed method demonstrates superior performance compared to other approaches, it is essential to acknowledge its limitations, specifically in relation to the False Acceptance Rate (FAR). The FAR measures the probability of incorrectly accepting an unauthorized user, highlighting the system's vulnerability to impostors. Despite the method's high accuracy, there is still a possibility of false acceptances, underscoring the need for further improvements to enhance the system's security and reliability.

6 Conclusion

This paper has introduced a robust user authentication framework designed to secure the transmission of user data from access points to nodes. The method comprises two phases; the identification phase, wherein a hybrid pattern is generated by combining image and password features and applies SHA-256 hashing and Shift-AES for data integrity and security. Blockchain technology is used for secure communication.

The subsequent development phase reverses this process to facilitate the comparison of extracted features with those stored in the database. The proposed approach effectively addresses concerns related to the potential leakage of pattern information, enhancing overall security. It ensures the safeguarding of image and password data not only within the user enrollment device and node database but also during data transmission. Additionally, this method resolves issues like pattern randomization and user location authentication, making it adaptable across diverse fields. Experimental results validate the efficiency and security of the approach, outperforming benchmarks in execution time while achieving an impressive accuracy rate of 98.3%. With a False Rejection Rate (FRR) of 0.992 and a low False Acceptance Rate (FAR) of 0.1, the method demonstrates its resilience during data transmission between access points and node databases, rendering it highly suitable for Internet of Things networks.

Looking ahead, future work will concentrate on further optimizing the algorithm, with a specific focus on minimizing the FAR and bolstering security. The incorporation of three user information sources - face image, password, and Iris Print - is planned to enhance the method's integrity. Additionally, the intention is to validate the approach on hardware through an FPGA platform, ensuring its practical applicability.

Acknowledgements The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Research Groups Program under grant number (RGP.1/24/44).

Data availability The data that has been used is confidential.

Declarations

Conflict of interest The authors declare that they have no known personal relationships that could have appeared to influence the work reported in this paper.

References

1. Atlam HF, Walters RJ, Wills GB (2018) Internet of things: state-of-the-art, challenges, applications, and open issues. Int J Intell Comput Res 9(3):928–938. https://doi.org/10.20533/ijicr.2042.4655.2018.0112
2. Atlam HF, Wills GB (2020) IoT Security, privacy, Safety and Ethics. In: Internet of Things. https://doi.org/10.1007/978-3-030-18732-3_8
3. Zheng X, Martin P, Brohman K, Xu LD (2014) Cloudqual: a quality model for cloud services. IEEE Trans Ind Inform 10(2):1527–1536. https://doi.org/10.1109/TII.2014.2306329
4. Wan J, Li J, Imran M, Li D (2019) A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans Ind Inform 15(6):3652–3660. https://doi.org/10.1109/TII.2019.2894573
5. Uddin MA, Stranieri A, Gondal I, Balasubramanian V (2019) An efficient selective miner consensus protocol in blockchain oriented iot smart monitoring. Proc IEEE Int Conf Ind Technol 2019(Febru):1135–1142. https://doi.org/10.1109/ICIT.2019.8754936
6. Mohsin AH et al (2019) Based blockchain-PSO-AES techniques in finger vein biometrics: a novel verification secure framework for patient authentication. Comput Stand Interfaces 66:103343. https://doi.org/10.1016/j.csi.2019.04.002
7. Kumar MM, Prasad MVNK, Raju USN (2020) Blockchain-based multi-instance Iris authentication using additive ElGamal homomorphic encryption. IET Biom 9(4):165–177. https://doi.org/10.1049/iet-bmt.2019.0169
8. Hassan MU, Rehmani MH, Chen J (2019) Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions. Futur Gener Comput Syst 97:512–529. https://doi.org/10.1016/j.future.2019.02.060
9. Shen M et al (2020) Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J Sel Areas Commun 38(5):942–954. https://doi.org/10.1109/JSAC.2020.2980916
10. Khari M, Garg AK, Gandomi AH, Gupta R, Patan R, Balusamy B (2020) Securing data in internet of things (IoT) using cryptography and steganography techniques. IEEE Trans Syst Man Cybern Syst 50(1):73–80. https://doi.org/10.1109/TSMC.2019.2903785
11. Ge C, Liu Z, Fang L (2020) A blockchain based decentralized data security mechanism for the internet of things. J Parallel Distrib Comput 141:1–9. https://doi.org/10.1016/j.jpdc.2020.03.005
12. Sarier ND (2021) Efficient biometric-based identity management on the blockchain for smart industrial applications. Pervasive Mob Comput 71:101322. https://doi.org/10.1016/j.pmcj.2020.101322
13. Lee YK, Jeong J (2021) Securing biometric authentication system using blockchain. ICT Express 7(3):322–326. https://doi.org/10.1016/j.icte.2021.08.003
14. Mishra P, Modanwal V, Kaur H, Varshney G (2021) Pseudo-biometric identity framework: achieving self-sovereignity for biometrics on blockchain. Conf Proc- IEEE Int Conf Syst Man Cybern 945–951. https://doi.org/10.1109/SMC52423.2021.9659136
15. Ma J, Qi B, Lv K (2021) BSA: Enabling Biometric-Based Storage and Authorization on Blockchain. Proc– 2021 IEEE 20th Int Conf Trust Secur Priv Comput Commun Trust pp. 1077–1084. https://doi.org/10.1109/TrustCom53373.2021.00147
16. Singh P, Masud M, Hossain MS, Kaur A (2021) Cross-domain secure data sharing using blockchain for industrial IoT. J Parallel Distrib Comput 156:176–184. https://doi.org/10.1016/j.jpdc.2021.05.007
17. Panda SK, Mohammad GB, Nandan Mohanty S, Sahoo S (2021) Smart contract-based land registry system to reduce frauds and time delay. Secur Priv 4(5). https://doi.org/10.1002/spy2.172
18. Liu B, Yu K, Feng C, Choo KKR (2021) Cross-domain authentication for 5G-enabled UAVs: A blockchain approach. DroneCom 2021 - Proc. 4th ACM MobiCom Work. Drone Assist. Wirel. Commun. 5G Beyond 9(8):25–30. https://doi.org/10.1145/3477090.3481053

19. Wang L, Tian Y, Zhang D (2022) Toward cross-domain dynamic accumulator authentication based on blockchain in internet of things. IEEE Trans Ind Inform 18(4):2858–2867. https://doi.org/10.1109/TII.2021.3116049
20. Gaba P, Raw RS, Mohammed MA, Nedoma J, Martinek R (2022) Impact of block data components on the performance of blockchain-based VANET implemented on hyperledger fabric. IEEE Access 10(July):71003–71018. https://doi.org/10.1109/ACCESS.2022.3188296
21. Panwar A, Bhatnagar V, Khari M, Salehi AW, Gupta G (2022) A blockchain framework to secure personal health record (PHR) in IBM cloud-based data lake. Comput Intell Neurosci 2022:1. https://doi.org/10.1155/2022/3045107
22. Poongodi M et al (2022) 5G based blockchain network for authentic and ethical keyword search engine. IET Commun 16(5):442–448. https://doi.org/10.1049/cmu2.12251
23. Lakhan A, Mohammed MA, Kadry S, AlQahtani SA, Maashi MS, Abdulkareem KH (2022) Federated learning-aware multi-objective modeling and blockchain-enable system for IIoT applications. Comput Electr Eng 100(April 2021):107839. https://doi.org/10.1016/j.compeleceng.2022.107839
24. Anitha R, Tapas Bapu BR (2022) Blockchain-based light-weight authentication approach for a multiple wireless sensor network. IETE J Res. https://doi.org/10.1080/03772063.2022.2154710
25. Nanda SK, Panda SK, Dash M (2023) Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. Multimed Tools Appl. https://doi.org/10.1007/s11042-023-14846-8
26. Lakhan A et al (2023) Federated-learning based privacy preservation and Fraud-enabled blockchain IoMT system for healthcare. IEEE J Biomed Heal Inform 27(2):664–672. https://doi.org/10.1109/JBHI.2022.3165945
27. Barman S (2023) A light weight authentication protocol for a blockchain-based off-chain medical data access in multi-server environment, preprint. https://doi.org/10.21203/rs.3.rs-2727465/v1
28. Anitha Rajakumari P, Parwekar P (2023) Secure public administration using wireless blockchain technology with efficient routing policy. Int J Commun Syst 36(6):1–18. https://doi.org/10.1002/dac.5441
29. Saif S, Das P, Biswas S, Khari M, Shanmuganathan V (2022) Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare. Microprocess Microsyst 104622. https://doi.org/10.1016/j.micpro.2022.104622
30. Penard W, van Werkhoven T (2008) On the secure hash algorithm family. Cryptogr. Context, pp 1–18, [Online]. Available: https://blog.infocruncher.com/resources/ethereum-whitepaper-annotated/On%20the%20Secure%20Hash%20Algorithm%20family%20(2008).pdf
31. Rajan SP (2015) Review and investigations on future research directions of mobile based telecare system for cardiac surveillance. J Appl Res Technol 13(4):454–460. https://doi.org/10.1016/j.jart.2015.09.002
32. Singh G, Supriya S (2013) A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. Int J Comput Appl 67:33–38. https://doi.org/10.5120/11507-7224
33. Patil P, Narayankar P, Narayan DG, Meena SM (2016) A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES RSA and Blowfish. Procedia Comput Sci 78(December 2015):617–624. https://doi.org/10.1016/j.procs.2016.02.108
34. Zaidan AA, Majeed A, Zaidan BB (2009) High securing cover-file of hidden data using statistical technique and AES, encryption, algorithm. World Acad Sci Eng Technol 54:463–474
35. Msolli A, Helali A, Maaref H (2018) New security approach in real-time wireless multimedia sensor networks. Comput Electr Eng 72:910–925. https://doi.org/10.1016/j.compeleceng.2018.01.016
36. Dayal M, Chawla A, Khari M (2021) Coalescence of Neural Networks and Blockchain. In: Handbook of Green Computing and Blockchain Technologies, pp. 31–44. https://doi.org/10.1201/9781003107507
37. Sáenz-royo C, Fleta-asín J (2023) Evaluating blockchain as a participatory organisational system: looking for transaction efficiency. 0:1–31. https://doi.org/10.1111/itor.13329
38. Fernández-Caramés TM, Fraga-Lamas P (2018) A review on the use of blockchain for the internet of things. IEEE Access 6:32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685
39. Yale Face Database. https://www.kaggle.com/datasets/olgabelitskaya/yale-face-database
40. Wadi SM, Zainal N (2014) High definition image encryption algorithm based on AES modification. Wirel Pers Commun 79(2):811–829. https://doi.org/10.1007/s11277-014-1888-7