SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

MBZKPS: Multimodal Biometric-Enabled Secure Data Storage And Access Scheme For Heterogeneous Network Data

Ms. Gunjan H. Deshmukh[1*] and Dr. Mahesh R. Sanghavi[2*]

[1*]Department of Computer Engineering, MET's BKC Institute of Engineering,Nashik, Affiliated to Savitribai Phule Pune University,Pune. ORCID:0009-0008-8121-1454,
Maharashtra, India.
[2*]Department of Computer Engineering, SNJB's KBJ College of Engineering,Chandwad, Affiliated to Savitribai Phule Pune University,Pune.ORCID:0000-0001-7482-7455,
Maharashtra, India.
*Corresponding author(s). E-mail(s): gunjandeshmukh1011@gmail.com; sanghavi.mahesh@gmail.com;

Abstract
Advancements in networking applications increase the requirement for secure data storage and an efficient data access mechanism with robust networking characteristics. Consequently, the huge volume of data generated from the het-erogeneous networks, such as smart cities, healthcare, and smart energy trading systems, suffers from scalability issues and generates insights for secure data storage and effective data management. Therefore, the research proposes a secure data storage and access scheme named Multimodal Biometric-enabled Zero-Knowledge Proof of Stake(MBZKPS). The Multimodal Biometric Data Access(MBDA) ensures secure and robust access to the heterogeneous data with reduced computational overhead. The Distributed Storage System and the Zero Knowledge Protocol with Proof of Stake alleviate the storage pressure on the blockchain and regulate the heterogeneous data storage and access in the blockchain. The Message Digest 5(MD5) with Homomorphic Encryption enables computations on the encrypted data with better data confidentiality preserva-tion. The introduction of the blockchain eliminates the scalability issues with improved privacy preservation and data integrity. Simulation results validate the superiority of the MD5 with Homomorphic Encryption (HE) used in research by achieving 0.95ms decryption time, and 0.97 encryption time with 0.73 Genuine User Rate occupying 363.76KiloBytes of memory for 250 nodes. In addition, the proposed research performs secure data storage with a 1025.85 ms response time and 1.01ms transaction time using blockchain.

Keywords: Data storage, Blockchain, Heterogeneous network, Homomorphic Encryption, security.

1 Introduction

In today's digital era, information and communication technology play a crucial role in shaping a secure revolutionary future due to the significant advancements in het-erogeneous networks, including smart cities, healthcare, and smart energy trading systems [1]. Through the interconnection of multiple devices, protocols, operating systems (OS), and nodes, heterogeneous networks are capable of delivering multiple services to users in a wireless medium [2]. Accordingly, heterogeneous networks facili-tate better transactions and Quality of Service (QoS) for big data through the usage of emerging technologies [3]. The users in heterogeneous networks access data from numerous access points across the network, and they utilize cloud storage to store het-erogeneous data [4]. However, the centralized nature of cloud data storage mechanisms results in data security issues, single-point failures, and malicious data tampering [5]. Hence, heterogeneous data are highly vulnerable due to their sensitive nature [6].

Cybersecurity acts as a lifesaver in securing heterogeneous data through the effec-tive utilization

of techniques, software, and processes to protect sensitive information from unauthorized access or damage [7]. The emergence of blockchain technol-ogy exemplifies its ability to foster user-centric, streamlined, and secure digital frameworks [8]. The inherent decentralization, immutable storage, and anonymous data-sharing characteristics of blockchain have expanded its application in secure data storage processes [9]. Thereby, users can keep track of the services that take place in the heterogeneous paradigm. Owing to its unique characteristics, blockchain has been deployed in diverse applications, including healthcare, insurance, industry, finance, social media, smart homes, and voting [10]. Conversely, higher computational and communication overhead introduces significant security challenges in heteroge-neous networks [11]. In addition, authentication, data confidentiality, user privacy preservation, scalability, interoperability, and compatibility remain major concerns in heterogeneous environments [12, 13].

Although numerous conventional security approaches have been proposed, their resource-intensive nature increases implementation costs, thereby affecting QoS, latency, and data integrity in heterogeneous networks [14]. Furthermore, the inclu-sion of complex cryptographic algorithms in previous authentication methods requires third-party authentication approval, which is time-consuming and expensive [15, 16]. Traditional security frameworks are also susceptible to eavesdropping attacks during runtime, thereby reducing the reliability of heterogeneous data-sharing networks [17]. Moreover, the use of centralized storage systems slows data retrieval while increas-ing computational requirements and the possibility of data manipulation [18]. The sophisticated nature of traditional Public Key Infrastructure (PKI) protocols intro-duces additional security and privacy vulnerabilities [19]. Furthermore, the adoption of Proof-of-Work (PoW)-based consensus mechanisms affects the feasibility of traditional security frameworks in resource-constrained environments and fails to adequately preserve data privacy [20].

To address the challenges associated with conventional approaches, this research introduces a flexible Multimodal Biometric-enabled Zero-Knowledge Proof of Stake (MBZKPS) scheme for secure data storage in heterogeneous networks. To main-tain data confidentiality and secure storage, the proposed framework integrates a Proof of Stake (PoS) consensus mechanism with blockchain technology. Moreover, the incorporation of Zero-Knowledge Proof (ZKP) enhances data privacy without reveal-ing sensitive information acquired from heterogeneous networks. The combination of MD5 with Homomorphic Encryption (HE) improves data confidentiality while reduc-ing computational overhead. Furthermore, the Data Storage System (DSS) provides streamlined data flow within the network, thereby enhancing resilience. The major contributions of the proposed MBZKPS scheme are summarized as follows:

- **Multimodal Biometric Data Encryption (MBDE):** The MBDE framework effectively addresses security challenges by minimizing unauthorized data accessi-bility. Consequently, it enhances secure data utilization from diverse heterogeneous sources.
- **Brakerski–Gentry–Vaikuntanathan (BGV)-based Homomorphic Encryption:** The BGV-based homomorphic encryption scheme outsources com-putational requirements while preserving data privacy. Its capability to perform computations directly on encrypted data enables secure data transmission and storage.
- **Multimodal Biometric-enabled Zero-Knowledge Proof of Stake (MBZKPS):** The proposed MBZKPS scheme employs the DID-ZKPS consensus protocol to ensure authenticated data transactions in heterogeneous networks. The integration of blockchain technology improves network scalability by establishing a secure and distributed storage system. Furthermore, the proposed MBDA scheme mitigates critical security concerns while ensuring secure data transmission.

The remainder of this paper is organized as follows. Section 2 reviews the exist-ing literature and related frameworks. Section 3 presents the proposed methodology for secure access and storage of heterogeneous network data. Section 4 describes the proposed MBZKPS scheme for secure heterogeneous data storage. Section 5 presents the experimental results and discussion. Finally, Section 6 concludes the paper and outlines future research directions.

2 Literature Review

The conventional methods developed by numerous researchers for secure data storage and access are analyzed in this section, along with their downsides.

Shahnawaz Ahmad and Shabana Mehfuz [21] introduced a Time-based Latency Approximation Data Encryption (TLADE) method to secure data in the cloud. Pri-marily, the available routes for the source to reach the destination were identified. Preprocessing of the traced data, estimating the Quality of Service support Value (QoSV) using the latency, throughput, and traffic features, followed by the selection of the best route with better QoSV values, were performed. Thereby, the encrypted data were transmitted via the selected route in less time with reduced computational over-head. However, the presented approach concentrated mainly on the selection of the least latency data encryption scheme, while data security was not considered, which affected the robustness of the approach.

Shahnawaz Ahmad et al. [22] established Secure Policies of the Cloud Security Framework (SPCSF) to prevent malicious users from accessing the data. The per-mission detection engine and registration authorization engine were the two distinct strategies followed to determine legitimacy and ensure secure registration. Thus, the two different strategies that encompass the security mechanisms guarantee authorized access to the crucial resources and ensure data security. Despite better reliability and security, the presented approach was susceptible to scalability issues.

Asad Abbas et al. [23] presented a Blockchain-assisted Secure Data Management Framework (BSDMF) to secure healthcare data. The data were stored in an encrypted format, thereby preserving data confidentiality. In addition, a smart contract mecha-nism was introduced to facilitate numerous functions on the distributed blockchain. The inclusion of blockchain in the healthcare management framework eliminated the issues related to single-point failure while providing better transparency. On the con-trary, the requirement for huge computational resources, along with security concerns, affected efficient data interpretation.

Yusuf Perwej et al. [24] developed an Intelligent Quantum-Health Data Manage-ment (IQ-HDM) framework to secure healthcare data. Here, the Quantum One-Time Padding Encryption (QOTPE) was used as a storage medium for healthcare data. Then, the quality of the healthcare data was analyzed using Quantum Protected Healthcare Data Communication (QPHDC). Thus, the security issues related to data breaches were accurately predicted using the presented quantum-based security approach. Conversely, the fragility to decoherence and external noise affected the qubit states and increased erroneous states.

Anichur Rahman et al. [25] designed a Distributed Blockchain-based Vehicular Adhoc Network (DisB-VNet) to classify malicious traffic in smart cities. The inte-gration of the Software Defined Network (SDN) equally divided the load between the controllers and the devices. In addition, the network resources required for effective traffic management were allocated using Network Function Virtualization (NFV). Thus, the distributed nature of blockchain in the DisB-VNet ensured secure vehicular communication with better traffic management. However, the scalability of the DisB-VNet was adversely affected due to increased computational resource requirements.

Abdullah Ayub Khan et al. [26] deployed machine learning-based data manage-ment techniques to handle remote sensing data. Here, the data sensed from multiple devices were effectively handled using Particle Swarm Optimization (PSO). The Arti-ficial Neural Network (ANN) was used to optimize problems related to data delivery. In addition, the data with distinct characteristics were encrypted using the NuCypher Re-Encryption mechanism, thereby diminishing cipher conversion. Yet, the highly sen-sitive nature of PSO resulted in inefficient resource allocation issues and failed to address complex threats.

Wenchao Li et al. [27] propounded Public Verification Public Key Encryption with Equality Test (PVPKEET) to secure encrypted data on the cloud. Here, dif-ferent public keys were used by the cloud server to examine the encrypted copies, thereby enabling better public verification with increased reliability. The introduc-tion of rigorous security proof provided better security against the Chosen Plaintext Attack (CPA) and guaranteed verifiability with reduced computational burden. How-ever, the efficiency of the PVPKEET was limited compared with traditional encryption frameworks, which restricted its flexibility.

Abdulrahman Mohammed Ahmed Alamer [28] proposed Secure and Privacy Blockchain-based Data Sharing (SPB-DS) in the Mobile Edge Caching (MEC) system. Blockchain-based Data Sharing (B-DS) and Encryption Attribute-based Searchable Key (E-SK) were deployed in the SPB-DS scheme to enhance data security. Proof of Existence (PoE) was used as the consensus mechanism for block validation. Thus, the data were stored in encrypted form within the blockchain, thereby preserving bet-ter data integrity and confidentiality. However, the inclusion of two smart contract mechanisms resulted in scalability issues and increased computational complexity.

2.1 Challenges

Although numerous secure data sharing schemes have been developed, there exist cer-tain significant downsides in offering optimal performance for heterogeneous networks, which are listed below.

- The conventional TLADE concentrated mainly on QoS improvement but failed to concentrate on data security, which affected the robustness of the approach [21].
- Meanwhile, data integrity was the major issue faced when using SPCSF for secure and reliable data transmission [22].
- Despite offering better security, the lower efficiency of PVPKEET in preserving data privacy limited its flexibility in practical applications [27].
- The inclusion of two smart contract mechanisms in the conventional SPB-DS resulted in scalability issues and increased computational complexity [28].

2.2 Problem Formulation

With a massive amount of heterogeneous data being generated from heterogeneous networks, including healthcare, smart cities, and smart energy trading systems, secu-rity and privacy concerns have become increasingly significant. Accordingly, numerous technologies have evolved to mitigate these concerns. Earlier, heterogeneous data were stored in centralized cloud storage systems. However, the reduced transparency of cloud storage increased the security issues related to data confidentiality [21]. Tra-ditional encryption techniques used for effective key management suffer from data confidentiality issues and higher computational complexity [1].

Moreover, the ever-changing nature of cloud environments introduced challenges related to inefficient key management and security vulnerabilities. Hence, such intrica-cies increase the requirement for secure data storage while potentially compromising availability, confidentiality, and integrity [2]. Furthermore, there is a possibility of data tampering by attackers in the cloud, thereby affecting data authenticity and integrity. Other issues such as poor scalability [22], compatibility, reliability, and high maintenance costs with increased computational overhead also affect the accessibility of heterogeneous data [3].

Hence, this research proposes a robust Multimodal Biometric-enabled Zero-Knowledge Proof of Stake (MBZKPS) scheme to provide secure sharing and access of heterogeneous data. The Homomorphic Biometric-based Data Encryption (HBDE) and Multimodal Biometric Data Access (MBDA) schemes ensure secure data stor-age in the blockchain, thereby eliminating unauthorized data access attempts and scalability issues through the integration of Decentralized Identity (DID)-based Zero Knowledge Proof (ZKP) and the Proof of Stake (PoS) consensus mechanism.

3 System Model for Secured Data Storage in Heterogeneous Data Network

Secure data sharing and access is the phenomenon of exchanging heterogeneous data from multiple systems or users in a controlled manner, thereby ensuring the security requirements. Here, the security requirements highlight the need for data integrity, con-fidentiality, and access control. The systematic representation for secure data sharing in the heterogeneous network is shown in Figure 1.

As depicted in Figure 1, the data from the heterogeneous network devices are shared via the blockchain through the incorporation of a trusted privacy computing mechanism between the heterogeneous devices across the communication channel. The data aggregator merges or aggregates the data from heterogeneous networks, such as smart cities, healthcare, and smart energy trading.

All the heterogeneous devices in the network are managed or controlled via the Authority Center (AC). In addition, for the Heterogeneous Devices (HNDs) to join the heterogeneous system, authentication is required from the AC. The HNDs are the devices that are actively involved in gathering crucial information from different types of networks, such as real-time traffic details, environmental conditions, and health information.

A decentralized Distributed Storage System (DSS) is used to eliminate the storage capacity issues encountered while storing data from heterogeneous networks, thereby enhancing data privacy and reliability. Each file shared through the heterogeneous network possesses a unique hash value depending on its contents. The hash value serves as an identifier for the heterogeneous network data, thereby enabling precise storage, identification, and retrieval of the file stored in the DSS.

Moreover, the blockchain network plays a crucial role in providing secure data sharing and data access in the heterogeneous network. All the data transactions that take place in the heterogeneous network are recorded in the blockchain to identify the data across multiple locations.

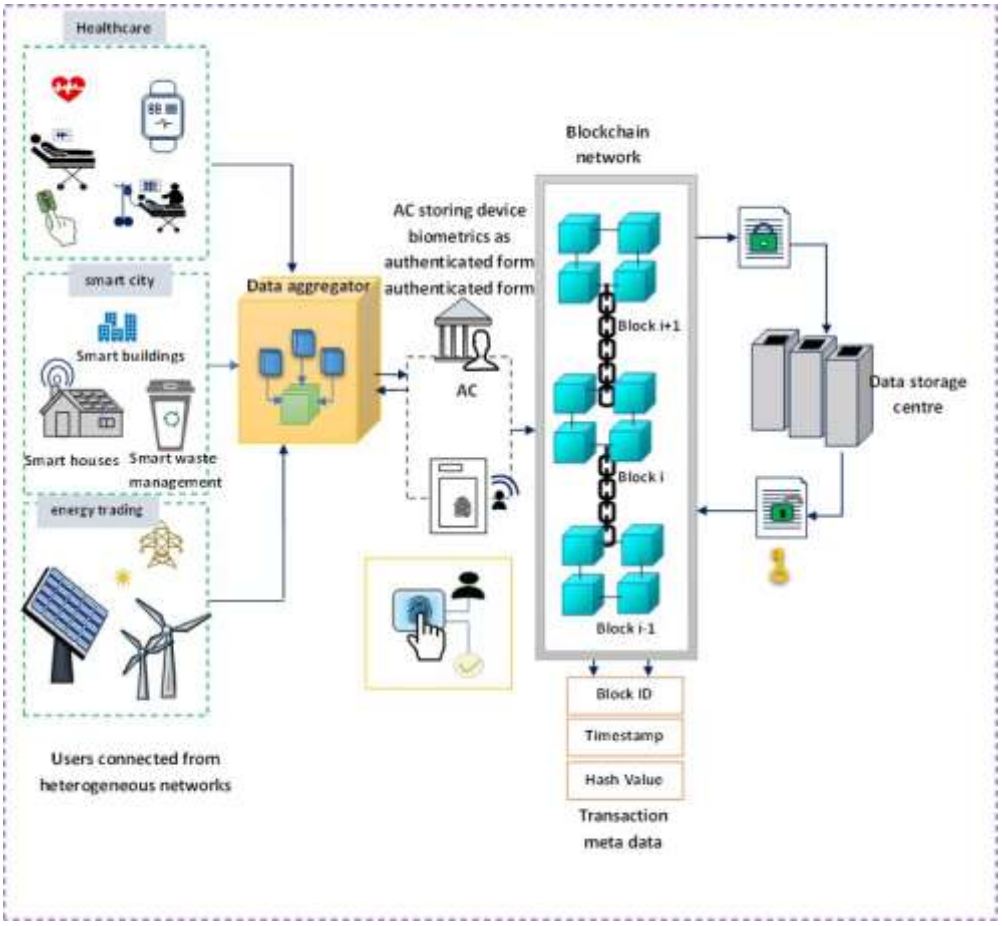


Fig. 1 Systematic representation for secure data sharing in the heterogeneous network.

4 Proposed Multimodal Biometric-Enabled Zero Knowledge Proof of Stake Scheme for Secure Data Storage and Access in Heterogeneous Networks

The research proposes a robust Multimodal Biometric-enabled Zero Knowledge Proof of Stake (MBZKPS)-based secure data sharing and access scheme for heterogeneous networks using blockchain technology. Initially, the proposed MBZKPS-based robust data access mechanism acquires data from heterogeneous networks such as health-care, smart cities, and smart energy trading systems. The acquired heterogeneous data are then secured using the Homomorphic Biometric-based Data Encryption (HBDE) scheme and stored in the Distributed Storage System (DSS) in encrypted form through the blockchain for future use. The blockchain employs the DID-based Zero Knowledge Proof of Stake (DZKPS) strategy to validate heterogeneous data transactions within the heterogeneous network. For users to access the heterogeneous data, the proposed framework utilizes the Multimodal Biometric Data Access (MBDA) scheme. The dia-grammatic representation of the proposed MBZKPS-based secure data sharing and access scheme for heterogeneous networks is illustrated in Figure 2.

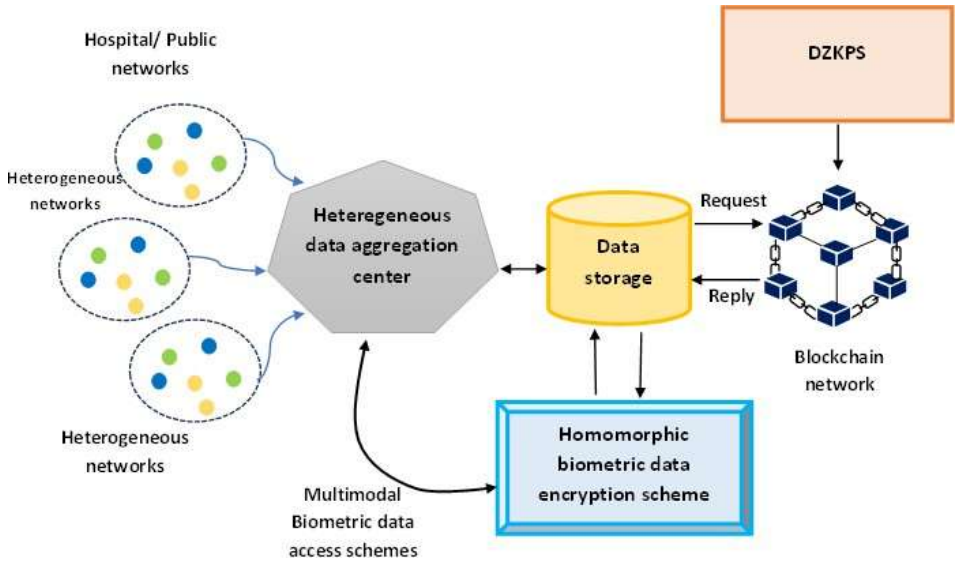


Fig. 2 Diagrammatic representation of the MBZKPS-based secure data sharing and access scheme

4.1 Heterogeneous Network Parameter Setup Phase

Primarily, all the parameters of the heterogeneous networks are initialized to render secure data sharing and data access in the heterogeneous networks. Accordingly, all the devices in the heterogeneous networks are initialized. Here, the devices correspond to the Devices Accessed by the Users (DAUs), denoted by H_{dau}, in the heterogeneous net-works. Consider a heterogeneous network (H) with N heterogeneous DAUs (H_{dauN}). The mathematical representation for the N heterogeneous DAUs in the heterogeneous network (H) is given in Equation (1).

$$H_{dau} = \{H_{dau1}, H_{dau2}, H_{dau3}, \ldots, H_{daui}, \ldots, H_{dauN}\} \quad (1)$$

In Equation (1), H_{daui} indicates the i^{th} heterogeneous DAU used for secure data storage and access using the MBZKPS scheme. Each device has its unique confidential parameters, such as the device's unique name (H_{name}), location (H_{lctn}), contact infor-mation (H_{cnct}), generation timestamp (H_{gtm}), along with the biometric details (H_{bio}). The mathematical formulation for the above-mentioned confidential parameters is depicted as follows.

$$H_{name} = \{H_{name1}, H_{name2}, H_{name3}, \ldots, H_{nameN}\} \quad (2)$$

$$H_{lctn} = \{H_{lctn1}, H_{lctn2}, H_{lctn3}, \ldots, H_{lctnN}\} \quad (3)$$

$$H_{cnct} = \{H_{cnct1}, H_{cnct2}, H_{cnct3}, \ldots, H_{cnctN}\} \quad (4)$$

$$H_{gtm} = \{H_{gtm1}, H_{gtm2}, H_{gtm3}, \ldots, H_{gtmN}\} \quad (5)$$

$$H_{bio} = \{H_{bio1}, H_{bio2}, H_{bio3}, \ldots, H_{bioN}\} \quad (6)$$

Here, H_{nameN} , H_{lctnN} , H_{cnctN} , H_{gtmN} , and H_{bioN} symbolize the name, location, contact information, generation timestamp, and biometric details of the N^{th} het-
erogeneous DAU, respectively. The sequence diagram for the heterogeneous network parameter setup phase is shown in Figure 3.

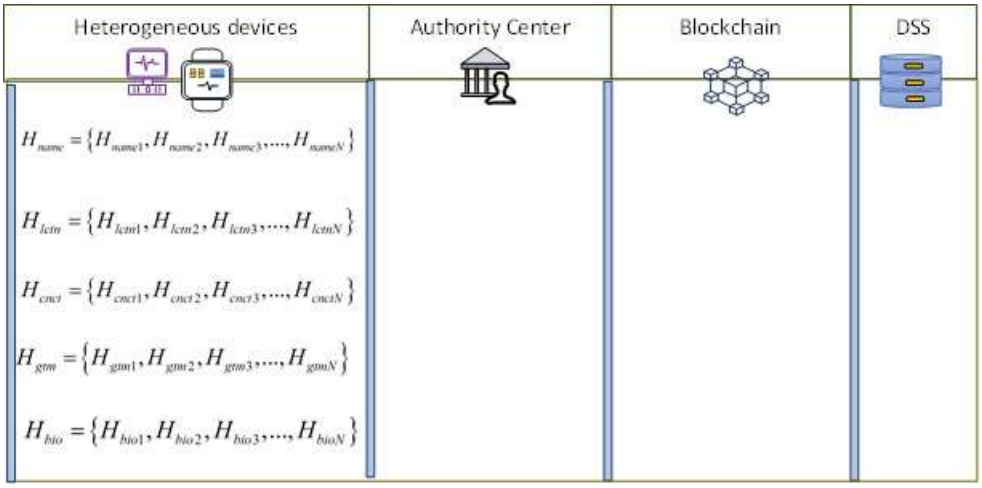


Fig. 3 Sequence diagram for the heterogeneous network parameter setup phase

4.2 Heterogeneous Device Registration Phase

After initializing the heterogeneous network parameters, the MBZKPS-based secure data storage process begins by initiating the registration phase. Conceptually, the i^{th} heterogeneous Device Accessed by the User (DAU) sends a registration request R_{req} to the Authority Center (AC) as an initiator for the data storage process, as modeled in Equation (7).

$$R_{req} = f(H_{name}, H_{lctn}, H_{cnct}, H_{gtm}) \quad (7)$$

where H_{name}, H_{lctn}, H_{cnct}, and H_{gtm} signify the name, address, contact informa-tion, and generation timestamp details of the i^{th} heterogeneous DAU. Upon receiving the registration request R_{req}, the AC returns a random nonce along with a mutual hash generation condition M_h to the heterogeneous DAU, as depicted in Equation (8).

$$R_{nonce}, M_h \leftarrow AC \quad (8)$$

Here, the random nonce R_{nonce} is generated using a cryptographically secure Pseudo-Random Number Generator (PRNG) [12] through its deterministic random number generation characteristics. Subsequently, the AC evaluates the hash fac-tor H_f generated using the Message Digest-5 (MD-5) algorithm, as represented in Equations (9) and (10).

$$H_f = MD5(R_{req} \mid R_{nonce}) \quad (9)$$

$$H^{std} = MD5(R_{req} \mid R_{nonce}) \quad (10)$$

If the generated hash factor matches the standard hash factor H^{std}_f Generated

If the heterogeneous DAU is identified as a new device, the AC generates a Decen-tralized Identity (DID) for the heterogeneous DAU. The DID provides a unique identity representation for heterogeneous devices. Therefore, the AC acts as a decen-tralized identity issuer rather than a centralized controller. The generated DID ensures the privacy and security of heterogeneous data transmitted through the heteroge-neous network. For generating the DID, the proposed MBZKPS framework integrates the MD-5 algorithm with Brakerski–Gentry–Vaikuntanathan Homomorphic Encryp-tion (BGV-HE), and the generated DID is forwarded to the heterogeneous DAU upon successful registration.

For an already registered heterogeneous DAU, the DID is retrieved from the AC database. The decentralized identity generation process for an existing heterogeneous DAU is represented in Equation (11).

$$DID = f(H_f, H_{bio}) \quad (11)$$

After successful authentication of either a new or an existing heterogeneous DAU, a registration acknowledgement is transmitted to the heterogeneous DAU, as shown in Equation (12), containing the success notification S_{ack} together with the decentralized identity DID.

$$Ack = \{S_{ack}, DID\} \quad (12)$$

The heterogeneous DAU then shares the biometric information, including iris and fingerprint details, with the AC. The biometric information undergoes further processing using the Multimodal Biometric Data Access (MBDA) scheme to ensure enhanced security and privacy. Simultaneously, the AC forwards the registration acknowledgement to the blockchain, as represented in Equation (13).

$$Ack \rightarrow Blockchain \quad (13)$$

Consequently, the blockchain generates the corresponding blockchain address together with the blockchain private key and forwards them to the AC. The sequence diagram for the heterogeneous device registration phase is illustrated in Figure 4.

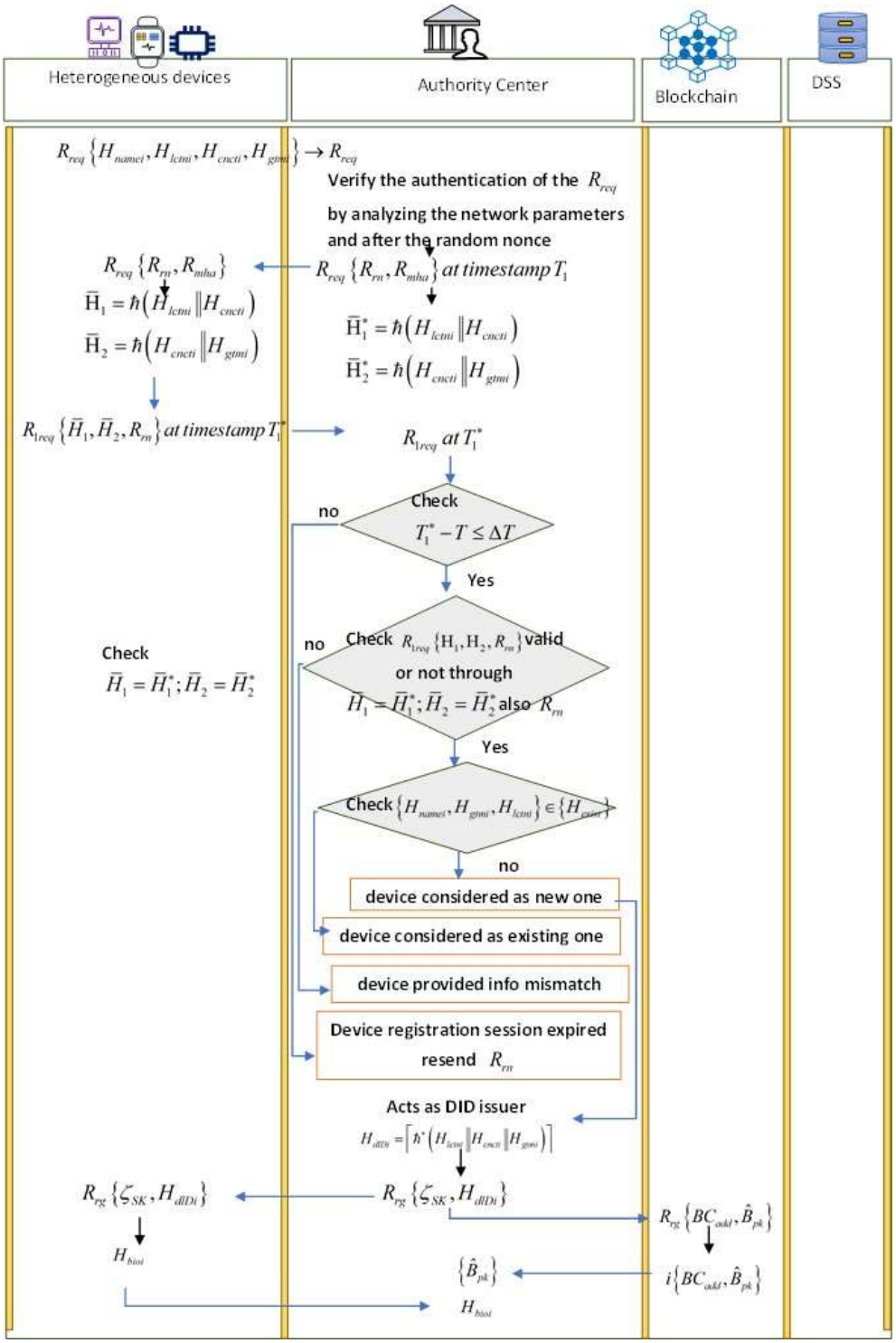


Fig. 4 Sequence diagram for the heterogeneous [1]d[2]evice registration phase.

4.3 Heterogeneous Device Authentication Phase

Upon successful registration of the i^{th} heterogeneous DAU (H_{dau_i}), the Authority Center (AC) employs the Multimodal Biometric-based Feature Transformation mech-anism. Conceptually, the biometric details (H_{bio_i}), including the fingerprint and iris images, are collected from the i^{th} heterogeneous DAU (H_{dau_i}). These biometric details undergo further processing in the AC to ensure secure data sharing and data access in heterogeneous networks. The processing of fingerprint and iris images for the i^{th} heterogeneous DAU is described as follows.

4.3.1 Heterogeneous DAU's Fingerprint Image Processing

The fingerprint details collected from the i^{th} heterogeneous DAU (H_{dau_i}) are in the form of a grayscale image with an intensity range of [0, 255]. Since the fingerprint remains unchanged throughout the lifespan of the DAUs in heterogeneous networks, its distinctiveness, reliability, and permanence make it a suitable biometric trait for ensuring security and privacy.

Conceptually, the fingerprint collected from the i^{th} heterogeneous DAU (H_{dau_i}) undergoes the following processing steps [30] to extract discriminative features for secure data storage and access.

To enhance the quality of ridge and valley structures in the grayscale fingerprint image, preprocessing is first performed. The proposed MBZKPS scheme employs a binarization technique to generate a binary image from the grayscale fingerprint image. The ridge structures represent the pixel values. If the pixel intensity is below the threshold value, it is assigned a value of 0; otherwise, it is assigned a value of 1.

After binarization, the fingerprint ridges are thinned to extract minutiae points effectively without altering the orientation or location of the ridge structures. For fingerprint ridge thinning [30], the proposed MBZKPS framework utilizes a block filter. The block filter reduces the thickness of every ridge in the binarized fingerprint image to a single-pixel width, thereby improving the accuracy of minutiae extraction.

Subsequently, the principal curve technique is employed for minutiae extraction. This process involves determining the principal curves, identifying the starting and ending points of each principal curve, and filtering ridge endings and ridge bifurcations. The resultant fingerprint feature vector is represented as M_1, as given in Equation (14).

$$M_1 = \{F_1, F_2, F_3, \ldots, F_q\} \quad (14)$$

where F_q represents the total number of features extracted from the fingerprint image.

4.3.2 Heterogeneous DAUs' Iris Image Processing

The iris image of the i^{th} heterogeneous DAU (H_{dau_i}) undergoes effective processing in this subsection to ensure data security and provide reliable data access using its multiscale features. The iris image processing procedure [31] is described as follows.

The obstacles caused by non-uniform illumination effects on the iris images are initially eliminated through image preprocessing. A single-scale retinal approach is employed to suppress unwanted abnormalities in the iris image. Subsequently, only the iris region is segmented using the random-walker-based segmentation algorithm. The segmented iris image is then normalized to eliminate the effects of dilation or contraction.

From the normalized iris image, both local and global features are extracted using the Histogram of Oriented Gradients (HoG) descriptor. The HoG descriptor [32] per-forms gradient computation, orientation binning, block descriptor generation, block normalization, and feature concatenation to extract discriminative local and global features. The mathematical representation of the extracted iris feature vector M_2 is given in Equation (15).

$$M_2 = \{f_1, f_2, f_3, \ldots, f_p\} \quad (15)$$

where f_p represents the total number of features extracted from the iris image.

The resultant feature vectors (M_1, M_2) obtained after fingerprint and iris feature extraction are subsequently encrypted using the Brakerski–Gentry–Vaikuntanathan Homomorphic Encryption (BGV-HE) scheme to enhance data confidentiality, privacy, and transaction authenticity.

4.3.3 Brakerski–Gentry–Vaikuntanathan (BGV)-Based Homomorphic Encryption

To encrypt the incoming feature vectors (M_1, M_2) and generate the ciphertext C, the initial setup is defined as

$$m \in R^2, \qquad a \xleftarrow{\$} R^{n+1}(1, 0, 0, \ldots, 0), \qquad g \xleftarrow{\$} R^2,$$

followed by the encryption process.
Here, R^{n+1} denotes the prime modulus a defined over the ring R, while B represents the logarithmic modulus and is expressed as
$B = \lfloor \log_3 a \rfloor$.

The ciphertexts generated for the incoming feature vectors (M_1, M_2) are mathe-matically represented as follows.

$$C_1 \leftarrow aM^T g + \kappa \in R^2 \quad (16)$$

$$C_2 \leftarrow M^T g + \kappa \quad (17)$$

where κ denotes the public key and g represents an integer vector. If the incoming feature vector $M = (M_1, M_2)$ fails to satisfy the condition $m \in R^2$, internal coefficient embedding is performed before encryption.

Therefore, the encryption stage serves as a crucial component of the proposed MBDA scheme by ensuring data confidentiality, transaction authenticity, and privacy.

The encrypted feature vectors are securely stored in the Authority Center (AC). The sequence diagram for the BGV-based homomorphic encryption process is illustrated in Figure 5.

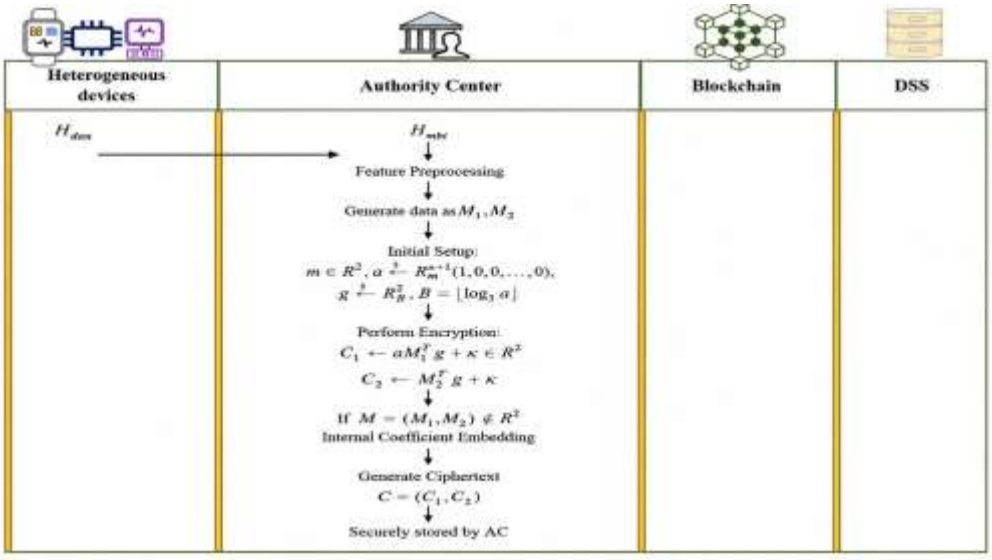


Fig. 5 The sequence diagram for the BGVH-based encryption

4.4 Heterogeneous Device Data Transmission Phase

Once the Authority Center (AC) completes the authentication verification by ana-lyzing the biometric details, the i^{th} heterogeneous DAU (H_{dau}) initiates the data transmission process using the data collected through the i^{th} heterogeneous device (H_i) in the heterogeneous network.

Conceptually, only an authenticated DAU possessing a data transfer request ($D_{T\ req}$) and a decentralized identity (H^{id}) is allowed to participate in the data transmission phase at timestamp t^*. The data transmission process is represented in Equation (18).

$$\{D_{Treq}, H^{id}_{ID}\} : H_{dau_i} \Rightarrow AC \quad (18)$$

Once the Authority Center (AC) verifies the decentralized identity (H^{id}) of the authenticated user, it returns the data access status (D_{stat}) to the requested i^{th} heterogeneous DAU (H_{dau_i}). When $D_{stat} = 1$,

the Authority Center enters the active state, allowing the heterogeneous device to upload the collected device data (D_{data}). The encrypted biometric feature vectors (C_1

and C_2) are securely maintained by the AC before being forwarded to the blockchain and the Distributed Storage System (DSS).

The sequence diagram for the heterogeneous device authentication and secure data transmission phase is illustrated in Figure 6.

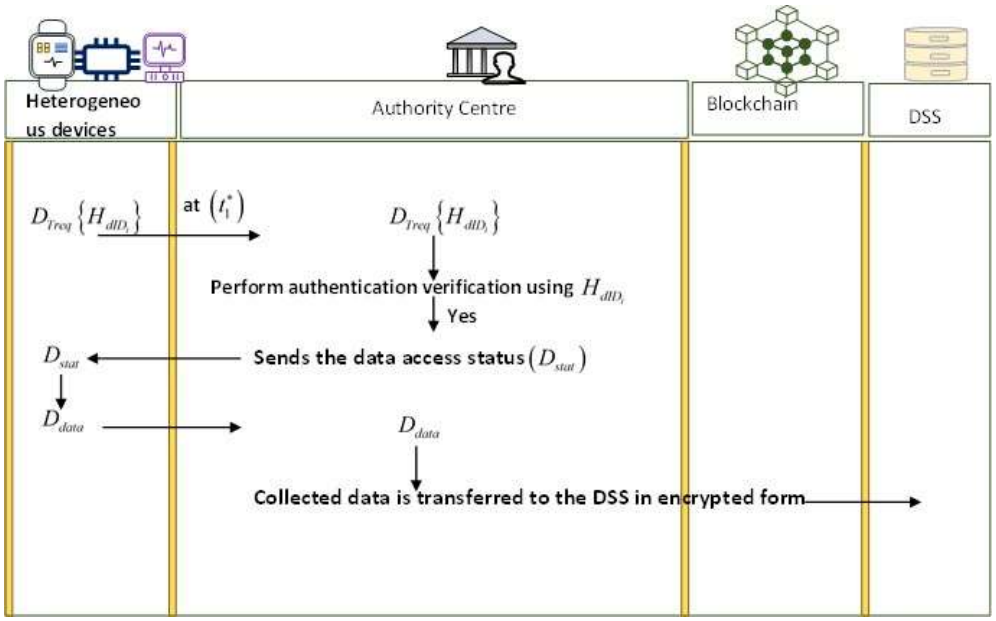


Fig. 6 Sequence diagram for the heterogeneous device authentication phase

4.5 Heterogeneous Data Sharing and Upload Phase

After collecting the data from the heterogeneous devices (H) of the i^{th} heterogeneous DAU (H_{dau_i}) in the heterogeneous network, the Authority Center (AC) ensures that the heterogeneous data are encrypted before transmission to the Distributed Storage System (DSS). To accomplish this, the proposed MBZKPS scheme employs the Feature Matching-enabled Biometric Link Data (FMEBD)-based encryption mechanism.

In the FMEBD-based encryption mechanism, the SHA-256 algorithm is used to generate a hash of the feature vectors extracted from the fingerprint and iris images, namely (M_1, M_2). The generated hash value (H) using the SHA-256 hashing process is expressed as

$$H = \hbar(M_1 \,||\, M_2) \quad (19)$$

where $\hbar(\cdot)$ denotes the SHA-256 hashing function and || represents the concatena-tion operation. The generated hash value is then integrated with the heterogeneous device data (D_{data}) and is utilized during the decryption process.

4.5.1 Heterogeneous Data Encryption

To encrypt the data collected from the i^{th} heterogeneous DAU (H_{dau_i}), the initializa-tion parameters are defined as the message

$m_{data} = \langle H, sep, D_{data} \rangle$,

public key κ, and modulus a, where sep denotes the separator used to distinguish the hash feature (H) from the device data (D_{data}).

The generated ciphertext (C_{data}) is expressed as

$$C_{data} \leftarrow a\, m^T \qquad g + \kappa \in R^2 \quad (20)$$

The generated ciphertext C_{data} represents the encrypted data collected from the i^{th} heterogeneous DAU.

After encryption, the Authority Center sends the data storage request (D_{sreq}) to the Distributed Storage System (DSS) through the blockchain using the blockchain private key ($\hat{p}k_B$), the generated ciphertext (C_{data}), and the decentralized identity (Id_{pi}), as represented in Equation (21).

$$D_{sreq}, \hat{pk}_B, C_{data}, H^{i}_{ID} \rightarrow DSS \quad (21)$$

After successful verification, the DSS returns the data storage address (D_{saddr}) to the Authority Center, as shown in Equation (22).

$$DSS: D_{saddr} \rightarrow AC \quad (22)$$

When the i^{th} heterogeneous DAU (H_{dau}) requires heterogeneous data, it sends a data access request (D_{Treq}) to the Authority Center (AC) using its decentralized identity (H^{id}_i), biometric details (H_{bio}), and the current timestamp (t^*). The heterogeneous data access request (D_{Treq}) using the identity credentials ensures an authenticated transaction and is mathematically represented as follows.

$$\{D_{Treq}, H^{id}_i, H_{bio}, t^*\} : H_{dau} \Rightarrow AC \quad (23)$$

Depending on the requested data, the Authority Center retrieves the corresponding biometric details from its database using the decentralized identity (H^{id}_i). Authentication verification is then performed by decrypting the biometric feature vectors using the private key (κ_{pvt}), modulus (a), and the ciphertexts (C_1 and C_2) generated during the MBDA scheme.

$$M \leftarrow C_1 \cdot \kappa_{pvt} \quad (24)$$

$$M \leftarrow C_2 \cdot \kappa_{pvt} \quad (25)$$

where $C_1 \cdot \kappa_{pvt}$ and $C_2 \cdot \kappa_{pvt}$ denote the dot product of the ciphertext and the private key, while the division by modulus a performs the corresponding modular reduction. Upon successful authentication of the data access request (D_{Treq}), the request is forwarded to the Distributed Storage System (DSS) through the blockchain using the blockchain private key ($\hat{pk}_B$) and the data storage address (D_{saddr}). The blockchain validates the transaction using the DID-ZKPS consensus protocol.

The hash value of the decrypted biometric features is generated using the MD-5 hashing algorithm and is expressed as

$$H_1 = \hbar(M_1 \,||\, M_2) \quad (26)$$

where $\hbar(\cdot)$ denotes the MD-5 hashing function.

After successful transaction validation, the encrypted heterogeneous data (C_{data}) are retrieved from the DSS and forwarded to the Authority Center. The original data are recovered through the decryption process as follows.

$$m_{data} \leftarrow C_{data} \cdot \kappa_{pvt} \quad (27)$$

The feature matching mechanism is defined as

$$H_{match}(m_{data}) = H1 \quad (28)$$

If the hash value of the stored data (H) matches the hash value of the decrypted data (H_1), the original heterogeneous data (D_{data}) are transferred to the requested heterogeneous DAU. Otherwise, the data access request is rejected.

4.6 Blockchain Network: Decentralized Identity (DID)-Based Zero Knowledge Proof (ZKP) and Proof of Stake (PoS) Consensus Mechanism

The emergence of blockchain technology has significantly increased the adoption of decentralized storage systems as blockchain-friendly off-chain mechanisms. Blockchain provides a highly secure, transparent, and immutable storage platform for digital information. It functions as a distributed ledger that records data transactions in chronological order. Similar to a shared database, blockchain maintains the transac-tion details of numerous participants involved in the data transmission process. Each transaction occurring in the network is encapsulated into a block and linked to the previous block, thereby forming a blockchain. Consequently, the

proposed MBZKPS scheme ensures transaction authenticity through the integration of the Decentralized Identity (DID)-based Zero Knowledge Proof of Stake (DID-ZKPS) consensus proto-col. To facilitate blockchain formation, the proposed framework adopts the Proof of Stake (PoS) consensus mechanism. The PoS protocol validates newly generated trans-actions before appending them as new blocks to the blockchain. In this mechanism, validators lock a specific amount of their cryptocurrency holdings as stake within the network. Based on the amount of stake, the blockchain selects a validator for block generation. Generally, validators with higher stakes possess a greater probability of being selected to validate the subsequent block of transactions. Zero Knowledge Proof (ZKP) is an efficient cryptographic mechanism that enables one entity to prove knowl-edge of specific information without revealing the actual information itself. In the proposed MBZKPS framework, the Decentralized Identity (DID) is incorporated into the blockchain network, allowing the verifier to authenticate the data requester without learning the requester's confidential information. Instead, the ZKP protocol convinces the verifier that the requester possesses valid credentials while preserving complete pri-vacy. Accordingly, the proposed DID-ZKPS consensus protocol authenticates the data requester by selecting an eligible validator based on stake availability and verifying the requester's decentralized identity together with private authentication credentials. This mechanism effectively prevents malicious validators from participating in the blockchain network while enhancing data security and transaction reliability. There-fore, the integration of the DID-ZKPS consensus protocol into the proposed MBZKPS framework provides scalable and trustless data access with enhanced privacy preserva-tion, reduced computational overhead, improved resistance against malicious attacks, and effective protection against Sybil attacks. Consequently, the proposed framework prevents data leakage while ensuring secure and efficient block creation within the heterogeneous network.

5 Results and Discussion

The performance of the proposed Multimodal Biometric-enabled Zero Knowledge Proof of Stake (MBZKPS) scheme for secure data access and storage in heteroge-neous networks is evaluated in this section by varying the number of network nodes. The experimental setup, performance metrics, dataset description, and experimental analysis are discussed as follows.

5.1 Experimental Setup

The proposed MBZKPS scheme is implemented using the PyCharm Integrated Development Environment (IDE) on the Windows 11 Operating System (OS). The implementation utilizes 16 GB of Random Access Memory (RAM) to perform secure data storage and access in heterogeneous networks. Furthermore, the system is equipped with a Central Processing Unit (CPU) operating at a clock frequency of
1.7 GHz for executing the proposed MBZKPS-based heterogeneous data storage and access framework.

5.2 Performance Metrics

The performance of the proposed MBZKPS-based heterogeneous data storage and access mechanism is evaluated using the following performance metrics: encryption time, encryption rate, decryption time, decryption rate, memory usage, Genuine User Rate (GUR), gas consumption, transaction time, and response time.

Encryption time represents the total time required to convert heterogeneous net-work data into ciphertext. Accordingly, the encryption rate indicates the speed at which the encryption process is completed. Similarly, the decryption rate represents the speed at which encrypted data are converted back into their original readable for-mat, whereas decryption time denotes the total duration required for the decryption process.

Memory usage refers to the amount of memory consumed during secure data stor-age and retrieval using the proposed MBZKPS scheme. Transaction time denotes the time required to store the encrypted data into the blockchain-based storage system. Response time measures the overall system performance by representing the time required to respond to a user request. Gas consumption represents the computational resources required to execute blockchain transactions. Genuine User Rate (GUR) mea-sures the proportion of legitimate users successfully authenticated by the proposed framework.

Collectively, these performance metrics demonstrate the effectiveness of the proposed MBZKPS framework for secure heterogeneous data storage and access.

5.3 Dataset Description

The performance of the proposed MBZKPS framework is evaluated using the Multimodal Iris Fingerprint Biometric dataset [38] and the Healthcare dataset [39].

The Multimodal Iris Fingerprint Biometric dataset [38] contains biometric informa-tion collected from multiple individuals, including fingerprint images and iris images, which are utilized for authentication and secure user verification.

The Healthcare dataset [39] contains real-world healthcare information, including patient details, admission records, and healthcare service information, and is employed to evaluate the secure storage and access capabilities of the proposed framework.

5.4 Experimental Analysis

Figure 7 illustrates the simulation results obtained using the proposed MBZKPS-based secure data storage and access mechanism in heterogeneous networks. In the simulation environment, the yellow circles represent the heterogeneous network nodes, while the inverted blue triangles denote the base stations. The red dotted lines illus-trate the communication links established between the heterogeneous nodes and the corresponding base stations during secure data transmission.

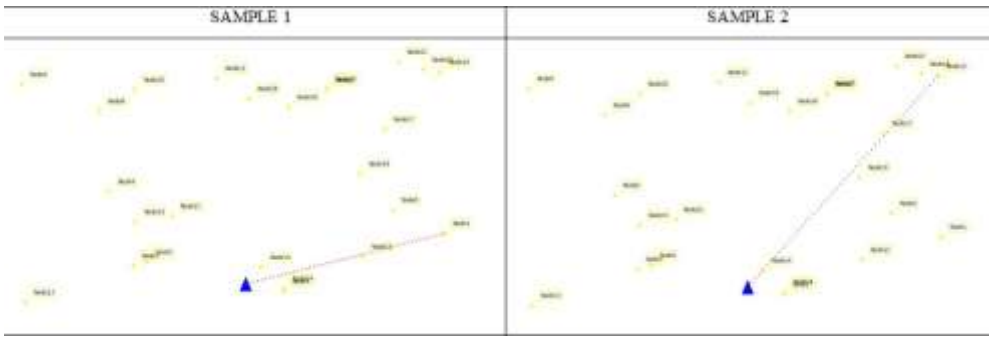


Fig. 7 Experimental analysis for the MBZKPS scheme

5.5 Comparative Methods

The proposed MBZKPS scheme for secure heterogeneous data access and storage is compared with existing approaches, namely DDPOS [29], Proof of Author-ity [30], Green-POW model [31], Proof of Zero [32], Proof of Stake [33], MD5 with HE authentication-based DIDZKP and DPOS, MD5 with DES authentication-based DIDZKP and DPOS [29], MD5 with AM authentication-based DIDZKP and DPOS [30], MD5 with RSA authentication-based DIDZKP and DPOS [20], and MD5 with AES authentication-based DIDZKP and DPOS [34]. The comparative evaluation is discussed in the following subsections.

5.5.1 Comparative Evaluation for the Encryption Algorithm

Figure 8 presents the comparative analysis of the MD5 with Homomorphic Encryption (HE) algorithm employed in the proposed MBZKPS-based secure heterogeneous data storage and access framework.

The experimental results demonstrate that, for 150 heterogeneous network nodes, the proposed MBZKPS scheme achieves a decryption rate of 1.11, which is 0.18 higher than the conventional MD5 with DES algorithm. Likewise, the decryption time of the proposed scheme is only 0.95 ms, showing an improvement of 0.10 ms compared with the traditional MD5 with AM algorithm.

Similarly, for 250 heterogeneous network nodes, the proposed MD5 with HE algo-rithm achieves an encryption rate of 1.03, which is 0.33 higher than the conventional MD5 with AM algorithm. The corresponding encryption time is 0.97 ms, whereas the conventional MD5 with AM algorithm requires 1.42 ms, resulting in a reduction of
0.45 ms.

Furthermore, the proposed MD5 with HE algorithm achieves a Genuine User Rate (GUR) of 0.73, which is 0.09 higher than that obtained using the conventional MD5 with AM algorithm for secure heterogeneous data storage and access in healthcare, smart city, and smart energy trading applications.

The memory consumption of the proposed MD5 with HE algorithm is 363.76 KB. In contrast, the existing MD5 with AES algorithm consumes 32.97 KB more memory than the proposed approach.

Similarly, the proposed MBZKPS framework completes the encryption process with a response time of 459.73 ms, representing an improvement of 94.53 ms compared with the conventional MD5 with AM encryption algorithm.

From the comparative analysis, it is evident that the integration of MD5 with Homomorphic Encryption effectively enhances data security and integrity. Further-more, the incorporation of the Feature Matching-enabled Biometric Link Data (FMEBD) mechanism improves data confidentiality and anonymity while reducing computational overhead in heterogeneous network environments.

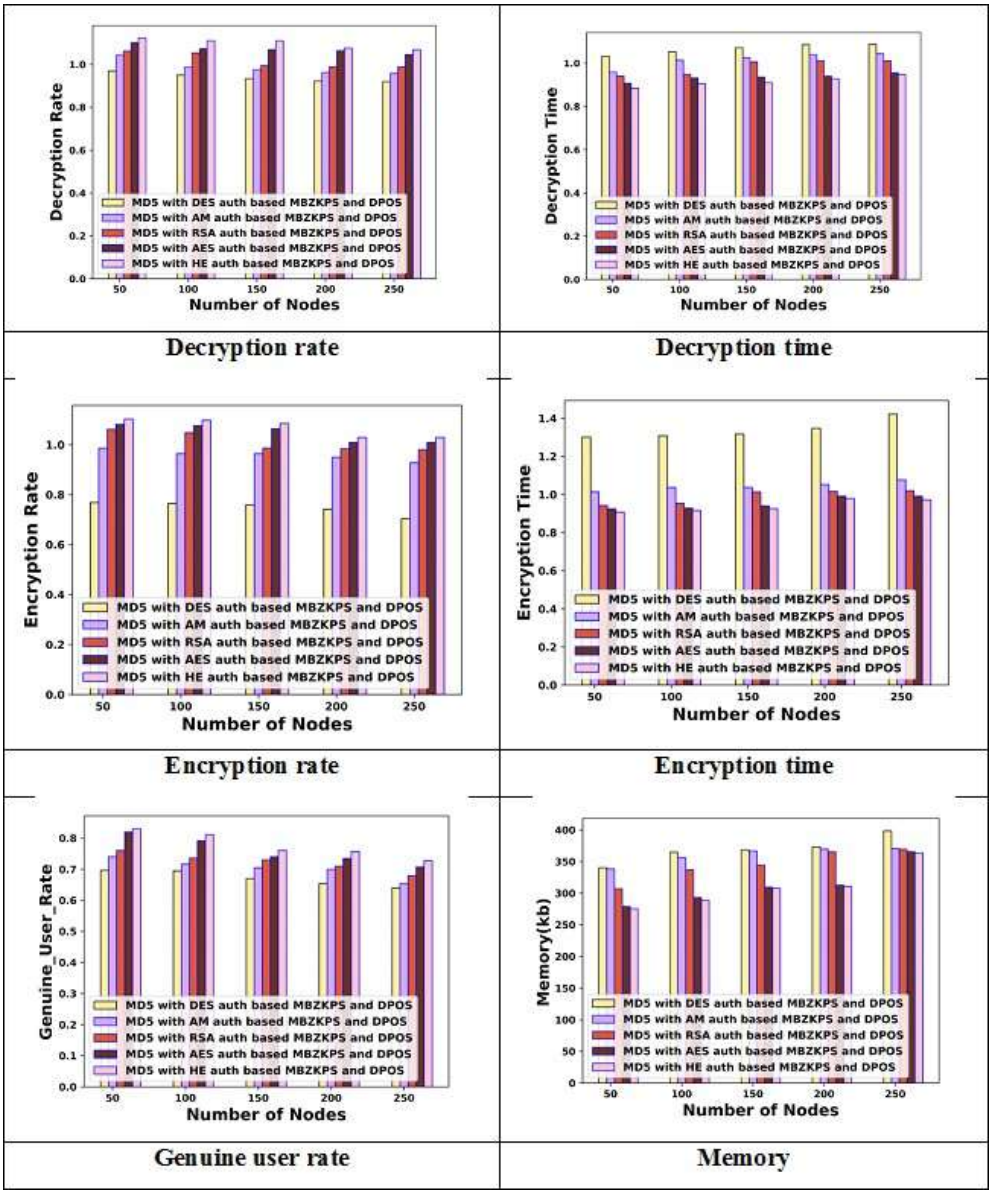


Fig. 8 Comparative evaluation of encryption algorithms used in the proposed MBZKPS framework.

5.5.2 Comparative Evaluation with Blockchain Analysis

Figure 9 illustrates the comparative performance of the proposed MBZKPS frame-work with existing blockchain-based approaches. The proposed MBZKPS scheme consumes only 280.85 Kbps of gas for securing heterogeneous data transactions on the blockchain, demonstrating improvements of 35.33 Kbps and 9.65 Kbps compared with the conventional Proof of Authority and Proof of Zero mechanisms, respectively.

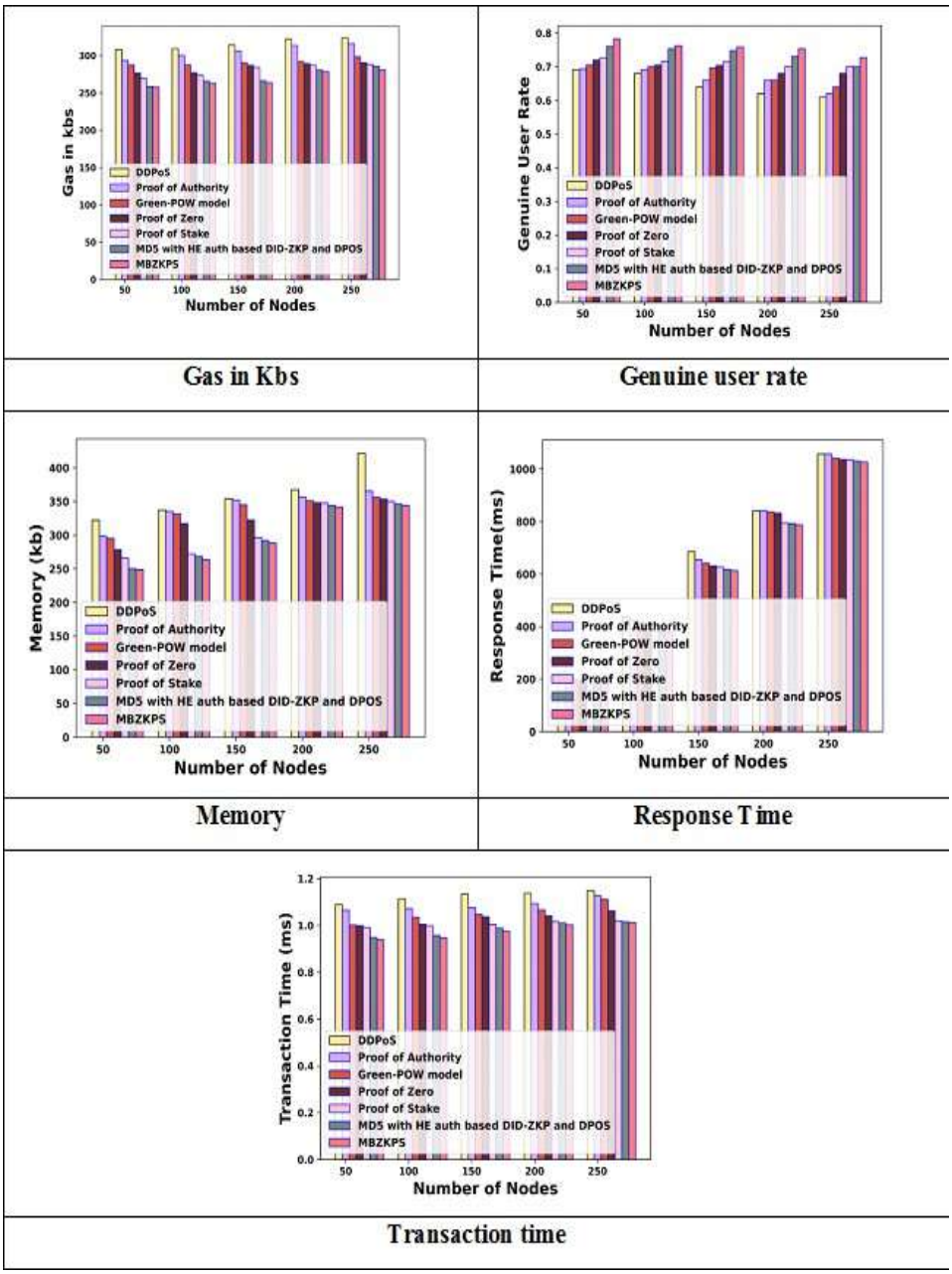
Furthermore, the proposed MBZKPS framework achieves a Genuine User Rate (GUR) of 0.73 during

heterogeneous data storage, which is 0.12 and 0.03 higher than the existing DDPoS and MD5 with HE authentication-based DID-ZKP and DPoS approaches, respectively.
In terms of memory utilization, the proposed MBZKPS framework requires only
343.86 KB, which is 6.26 KB and 12.20 KB lower than the conventional Proof of Stake and Green-POW models, respectively.

Moreover, the proposed MBZKPS scheme responds to user data requests within 1025.85 ms. In comparison, the response times of the existing Proof of Authority and Proof of Stake mechanisms are 31.45 ms and 9.93 ms higher, respectively.

Similarly, the proposed MBZKPS framework completes blockchain transactions in only 1.01 ms, outperforming the conventional DDPoS and Proof of Authority approaches by 0.14 ms and 0.11 ms, respectively.

The superior performance of the proposed MBZKPS framework is primarily attributed to the integration of the Proof of Stake (PoS) consensus mechanism, which ensures fair validator selection, preserves user privacy, and enables secure data distribution among authorized entities. Furthermore, the incorporation of the Zero Knowledge Proof (ZKP) mechanism enhances data integrity while reducing memory consumption and computational complexity.



Gas in Kbs | Genuine user rate

Memory | Response Time

Transaction time

Fig. 9 Comparative blockchain performance analysis of the proposed MBZKPS framework with existing approaches.

5.6 Statistical Analysis

Tables 1 and 2 demonstrate the accuracy and consistency of the proposed MBZKPS framework for secure heterogeneous data storage and access through statistical analysis. The analysis is performed using the best, mean, and variance values of the performance metrics employed for evaluating the proposed framework. The obtained statistical measures provide valuable insights for performance comparison and facilitate meaningful decision-making in heterogeneous network environments.

Table 1 Statistical analysis of the encryption algorithm used in the proposed MBZKPS scheme.

Metrics	Statistics	MD5+DES	MD5+AM	MD5+RSA	MD5+AES	MD5+HE
Decryption	Best	1.087299	1.044002	1.011810	0.955657	0.946763
	Mean	1.065546	1.016127	0.983806	0.934083	0.914713
	Variance	0.000434	0.000949	0.001019	0.000241	0.000448
Encryption	Best	1.422089	1.077599	1.020017	0.991168	0.979755
	Mean	1.339372	1.043771	0.989064	0.955216	0.940412
	Variance	0.001961	0.000441	0.001148	0.000878	0.000876
GUR	Best	0.696	0.740	0.760	0.820	0.830
	Mean	0.670867	0.702867	0.723200	0.758733	0.777287
	Variance	0.000495	0.000804	0.000721	0.001697	0.001436
Memory Usage (KB)	Best	398.30	370.30	369.19	365.34	363.76
	Mean	368.90	360.14	344.39	311.84	309.26
	Variance	345.74	146.68	501.22	861.85	907.69
Response Time (ms)	Best	554.27	548.02	501.35	462.84	459.73
	Mean	322.18	316.16	300.89	267.27	263.32
	Variance	23690.64	24089.36	20756.93	17347.35	17363.16

Table 2 Statistical analysis of the blockchain used in the proposed MBZKPS scheme.

Metrics	Statistics	DDPoS	PoAS	Green-POW	PoZ	PoS	MD5+HE	MBZKPS
Gas (Kbps)	Best	323.91	316.19	298.33	290.50	288.26	285.75	280.85
	Mean	315.58	305.95	291.14	284.14	280.48	271.57	268.81
	Variance	42.44	70.82	16.04	36.07	57.50	100.35	83.84
Transaction Time (ms)	Best	1.148816	1.126032	1.111689	1.062200	1.018795	1.01513	1.012876
	Mean	1.124447	1.086505	1.052336	1.028933	1.005966	0.98374	0.975200
	Variance	0.000452	0.000478	0.001315	0.000552	0.000104	0.00072	0.000852

GUR	Best	0.692	0.693 333	0.705000	0.720 000	0.726 667	0.760000	0.782988
	Mean	0.648 400	0.665 067	0.680200	0.697 800	0.711 533	0.738267	0.757032
	Variance	0.001 050	0.000 721	0.000656	0.000 243	0.000 105	0.000465	0.000316
Memory Usage (KB)	Best	421.89	365.42	356.06	353.49	350.12	346.51	343.86
	Mean	360.68	341.50	335.80	323.98	306.48	300.23	297.26
	Variance	1169.89	560.33	476.75	714.77	1309.94	1531.24	1545.81
Response Time (ms)	Best	1057.57	1057.30	1042.17	1036.91	1035.78	1030.60	1025.85
	Mean	649.35	635.90	627.32	620.40	609.53	601.71	597.35
	Variance	85750.43	90742.55	88866.94	89116.91	86975.63	88300.38	87828.79

5.7 Comparative Discussion

The superiority of the proposed MBZKPS over traditional heterogeneous data storage systems is analyzed based on encryption algorithms and blockchain mechanisms, as presented in Tables 3 and 4. The comparative evaluation demonstrates the effective-ness of the proposed framework in achieving secure, efficient, and privacy-preserving heterogeneous data storage.

For the MD5 with HE-based MBZKPS scheme, secure data storage is achieved with a decryption time of 0.95 ms, decryption rate of 1.07, encryption rate of 1.03, and encryption time of 0.97 ms. The proposed scheme achieves a GUR value of 0.73 with only 363.76 KB memory utilization and a response time of 459.73 ms for 250 nodes. Furthermore, the blockchain-based evaluation of MBZKPS demonstrates improved performance with a response time of 1025.85 ms, transaction time of 1.01 ms, gas consumption of 280.85 Kbps, GUR value of 0.70, and memory utilization of 343.86 KB.

The improved performance of MBZKPS is mainly attributed to the integration of blockchain technology, which provides transparency, decentralization, immutability, and enhanced scalability. The limitations of traditional Secure Privacy-Centric Stor-age Frameworks (SPCSF) in maintaining data integrity are addressed through the incorporation of the Decentralized Security Scheme (DSS) in MBZKPS [22]. More-over, the integration of Zero-Knowledge Proof (ZKP) with the Proof-of-Stake (PoS) consensus mechanism enhances secure authentication and improves flexibility in het-erogeneous data storage [27]. The proposed Flexible Multimodal Encryption-Based Data (FMEBD) approach further mitigates privacy concerns and prevents data leak-age during data exchange [28]. Specifically, the combination of MD5 authentication with Homomorphic Encryption (HE) ensures data integrity and prevents unauthorized data modification or malicious attacks [21].

Table 3 Comparative discussion of the MBZKPS scheme with encryption algorithms

Methods/Metrics	Decryption Rate	Decryption Time (ms)	Encryption Rate	Encryption Time (ms)	GUR	Memory Usage (KB)	Response Time (ms)	250 Nodes
MD5 with DES auth based MBZKPS and DPoS [19]	0.92	1.09	0.70	1.42	0.64	398.30	554.27	
MD5 with AM auth based MBZKPS and DPoS	0.96	1.04	0.93	1.08	0.65	370.30	548.02	
MD5 with RSA auth based MBZKPS and DPoS [20]	0.99	1.01	0.98	1.02	0.68	369.19	501.35	
MD5 with AES auth based MBZKPS and DPoS [34]	1.05	0.96	1.01	0.99	0.71	365.34	462.84	
MD5 with HE auth based MBZKPS and DPoS	**1.07**	**0.95**	**1.03**	**0.97**	**0.73**	**363.76**	**459.73**	

Table 4 Comparative discussion of the MBZKPS scheme with blockchain mechanisms

Methods/Metrics	Gas (Kbps)	GUR	Transaction Time (ms)	Memory (KB)	Response Time (ms)
		250 Nodes			
DDPoS [29]	323.91	0.60	1.15	421.89	1057.57
Proof of Authority [30]	316.19	0.61	1.13	365.42	1057.30
Green-POW Model [31]	298.33	0.62	1.11	356.06	1042.17
Proof of Zero [32]	290.50	0.64	1.06	353.49	1036.91
Proof of Stake [33]	288.26	0.68	1.02	350.12	1035.78
MD5 with HE auth based DID-ZKP and DPoS	285.75	0.70	1.02	346.51	1030.60
MBZKPS	**280.85**	**0.70**	**1.01**	**343.86**	**1025.85**

6 Conclusion

This research proposed a holistic Blockchain-based Multimodal Biometric Zero-Knowledge Proof of Stake (MBZKPS) scheme for secure storage and access of heterogeneous healthcare data. The proposed Decentralized Security Scheme (DSS), integrated with blockchain technology, addresses the limitations of centralized stor-age systems by enabling secure data storage and retrieval with reduced computational overhead.

The proposed Flexible Multimodal Encryption-Based Data (FMEBD) approach efficiently handles computationally intensive encryption operations through the inte-gration of Multimodal Biometric Data Access (MBDA) and BGV-based Homomorphic Encryption (HE), thereby enhancing privacy preservation. Furthermore, blockchain technology improves resource utilization and provides a secure data-sharing environ-ment through MD5-based hash generation, ensuring data integrity and resistance against unauthorized modifications.

The integration of Decentralized Identity (DID) generation ensures secure identity management for users and heterogeneous data sources. Additionally, the combina-tion of Zero-Knowledge Proof (ZKP) and Proof-of-Stake (PoS) consensus enhances anonymity, reduces computational complexity, and improves blockchain scalability. Experimental results validate the effectiveness of the proposed MBZKPS scheme, achieving a decryption time of 0.95 ms, encryption time of 0.97 ms, GUR value of 0.73, and memory consumption of 363.76 KB for 250 nodes.

Furthermore, blockchain performance evaluation demonstrates that MBZKPS achieves a response time of 1025.85 ms, transaction time of 1.01 ms, gas consumption of 280.85 Kbps, and memory utilization of 343.86 KB. These results confirm the supe-riority of the proposed framework over existing blockchain-based storage mechanisms. However, future enhancements can focus on integrating advanced encryption tech-niques and deep learning-based intrusion detection models to further improve security, adaptability, and threat detection capabilities.

7 Declaration

Funding: The authors received no financial support for the research, authorship, and publication of this article.

References

[1] Shree, S., Zhou, C., Barati, M.: Data protection in the internet of medical things using blockchain and secret sharing method. The Journal of Supercomputing **80**(4), 5108–5135 (2024)

[2] Siyal, R., Long, J., Asim, M., Ahmad, N., Fathi, H., Alshinwan, M.: Blockchain-enabled secure data sharing with honey encryption and dsnn-based key genera-tion. Mathematics **12**(13), 1956 (2024)

[3] Xu, G., Qi, C., Dong, W., Gong, L., Liu, S., Chen, S., Liu, J., Zheng, X.: A privacy-preserving medical data sharing scheme based on blockchain. IEEE Journal of Biomedical and Health Informatics **27**(2), 698–709 (2022)

[4] Álvarez, R., Mart´ınez, F., Zamora, A.: Improving the statistical qualities of pseudo-random number generators. Symmetry **14**(2), 269 (2022)
[5] Han, S., Han, K., Zhang, S.: A data sharing protocol to minimize security and privacy risks of cloud storage in the big data era. IEEE Access **7**, 60290–60298 (2019)
[6] Khashan, O.A., Khafajah, N.M.: Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous iot systems. Journal of King Saud University–Computer and Information Sciences **35**(2), 726–739 (2023)
[7] Xu, G., Qi, C., Dong, W., Gong, L., Liu, S., Chen, S., Liu, J., Zheng, X.: A privacy-preserving medical data sharing scheme based on blockchain. IEEE Journal of Biomedical and Health Informatics **27**(2), 698–709 (2022)
[8] Zhang, D., Wang, S., Zhang, Y., Zhang, Q., Zhang, Y.: A secure and privacy-preserving medical data sharing via consortium blockchain. Security and Com-munication
[9] Networks **2022**, 2759787 (2022)
[10] Feng, T., Yang, P., Liu, C., Fang, J., Ma, R.: Blockchain data privacy protection and sharing scheme based on zero-knowledge proof. Wireless Communications and Mobile Computing **2022**, 1040662 (2022)
[11] Zheng, B.K., Zhu, L.H., Shen, M., Gao, F., Zhang, C., Li, Y.D., Yang, J.: Scalable and privacy-preserving data sharing based on blockchain. Journal of Computer Science and Technology **33**(3), 557–567 (2018)
[12] Pan, J., Cui, J., Wei, L., Xu, Y., Zhong, H.: Secure data sharing scheme for vanets based on edge computing. EURASIP Journal on Wireless Communications and Networking **2019**(1), 169 (2019)
[13] Lu, X., Pan, Z., Xian, H.: An efficient and secure data sharing scheme for mobile devices in cloud computing. Journal of Cloud Computing **9**(1), 60 (2020)
[14] Huang, H., Zhu, P., Xiao, F., Sun, X., Huang, Q.: A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Computers & Security **99**, 102010 (2020)
[15] Liu, J., Fan, Y., Sun, R., Liu, L., Wu, C., Mumtaz, S.: Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system. IEEE Internet of Things Journal **10**(24), 21377–21388 (2023)
[16] Zhuang, Y., Sheets, L.R., Chen, Y.W., Shae, Z.Y., Tsai, J.J., Shyu, C.R.: A patient-centric health information exchange framework using blockchain tech-nology. IEEE Journal of Biomedical and Health Informatics **24**(8), 2169–2176 (2020)
[17] Zhang, H., Babar, M., Tariq, M.U., Jan, M.A., Menon, V.G., Li, X.: Safecity: Toward safe and secure data management design for iot-enabled smart city planning. IEEE Access **8**, 145256–145267 (2020)
Badii, C., Bellini, P., Difino, A., Nesi, P.: Smart city iot platform respecting gdpr privacy and security aspects. IEEE Access **8**, 23601–23623 (2020)
[18] Qi, L., Hu, C., Zhang, X., Khosravi, M.R., Sharma, S., Pang, S., Wang, T.: Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment. IEEE Transactions on Industrial Informatics **17**(6), 4159–4167 (2020)
[19] Sreehari, K.N., Bhakthavatchalu, R.: Implementation of a hybrid cryptosystem using des and md5. In: 2018 3rd International Conference on Communication and Electronics Systems (ICCES), pp. 52–55 (2018). IEEE
[20] Lenka, S.R., Nayak, B.: Enhancing Data Security in Cloud Computing Using RSA Encryption and the MD5 Algorithm. Vol. 2, pp. 60–64 (2014)
[21] Ahmad, S., Mehfuz, S.: Efficient time-oriented latency-based secure data encryp-tion for cloud storage. Cyber Security and Applications **2**, 100027 (2024)
[22] Ahmad, S., Mehfuz, S., Urooj, S., Alsubaie, N.: Machine learning-based intelligent security framework for secure cloud key management. Cluster Computing **27**(5), 5953–5979 (2024)
[23] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., Almansour, F.M.: Blockchain-assisted secured data management framework for health information analysis based on internet of medical things. Personal and Ubiquitous Computing **28**(1), 59–72 (2024)
[24] Gupta, K., Saxena, D., Rani, P., Kumar, J., Makkar, A., Singh, A.K., Lee, C.N.: An intelligent quantum cyber-security framework for healthcare data management. IEEE Transactions on Automation Science and Engineering (2024)
[25] Rahman, A., Eidmum, M.Z.A., Kundu, D., Hossain, M., Tashrif, M.T.A., Karim, M.A., Islam, M.J.: Distb-vnet: Distributed cluster-based blockchain vehicular ad-hoc networks through sdn-nfv for smart city. In: 2024 27th International Con-ference on Computer and Information Technology (ICCIT),

pp. 3372–3377 (2024). IEEE
[26] Khan, A.A., Laghari, A.A., Alroobaea, R., Baqasah, A.M., Alsafyani, M., Bacarra, R., Alsayaydeh, J.A.J.: Secure remote sensing data with blockchain distributed ledger technology: A solution for smart cities. IEEE Access **12**, 69383–69396 (2024)
[27] Li, W., Susilo, W., Xia, C., Huang, L., Guo, F., Wang, T.: Secure data integrity check based on verified public key encryption with an equality test for multi-cloud storage. IEEE Transactions on Dependable and Secure Computing **21**(6), 5359–5373 (2024)
Alamer, A.M.A.: A secure and private blockchain-based data sharing scheme in a mobile edge caching system. Expert Systems with Applications **237**, 121572 (2024)
[28] Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N.N., Zhou, M.: Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with a downgrade mechanism. IEEE Access **7**, 118541–118555 (2019)
[29] Manolache, M.A., Manolache, S., Tapus, N.: Decision-making using the blockchain proof of authority consensus. Procedia Computer Science **199**, 580–588 (2022)
[30] Lasla, N., Al-Sahan, L., Abdallah, M., Younis, M.: Green-pow: An energy-efficient blockchain proof-of-work consensus algorithm. Computer Networks **214**, 109118 (2022)
[31] Yang, X., Li, W.: A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security **99**, 102050 (2020)
[32] Zhao, W., Yang, S., Luo, X., Zhou, J.: On peercoin proof of stake for blockchain consensus. In: Proceedings of the 2021 3rd International Conference on Blockchain Technology, pp. 129–134 (2021)
[33] Indrayani, R., Nugroho, H.A., Hidayat, R., Pratama, I.: Increasing the security of mp3 steganography using aes encryption and md5 hash function. In: 2016 2nd International Conference on Science and Technology-Computer (ICST), pp. 129–132 (2016). IEEE
[34] Raja, K.B.: Fingerprint recognition using minutia score matching. arXiv preprint arXiv:1001.4186 (2010)
[35] Kareem, K.A., Ghany, A., Moneim, M.A., Ghali, N.I., Hassanien, A.E., Hefny, H.A.: A symmetric bio-hash function based on fingerprint minutiae and prin-cipal curves approach. In: Proceedings of the 3rd International Conference on Mechanical and Electrical Technology (ICMET), Dalian, China, pp. 405–410 (2011)
[36] Kitayama, M., Kiya, H.: Hog feature extraction from encrypted images for privacy-preserving machine learning. In: 2019 IEEE International Conference on Consumer Electronics–Asia (ICCE-Asia), pp. 80–82 (2019). IEEE
[37] Kaggle: Multimodal Iris Fingerprint Biometric Dataset. Avail-able at https://www.kaggle.com/datasets/ninadmehendale/ multimodal-iris-fingerprint-biometric-data. Accessed August 2025 (2025)
[38] Kaggle: Healthcare Dataset. Available at: https://www.kaggle.com/datasets/ prasad22/healthcare-dataset. Accessed August 2025 (2025)