IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5936~5948
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5936-5948

Hybrid AES RSA blockchain based mutual authentication for secure decentralized storage access

Abhijeet Cholke[1], Vaishali V. Mandhare[2], Pratap S. Vikhe[3]
[1]Department of Computer Engineering, Matoshri College of Engineering and Research Centre, Nashik, India
[2]Department of Computer Engineering, Pravara Rural Engineering College, Ahmednagar, India
[3]Department of Instrumentation and Control Engineering, Pravara Rural Engineering College, Ahmednagar, India

Article Info

Article history:

Received Dec 13, 2025
Revised Aug 31, 2026
Accepted Sep 19, 2026

Keywords:

Advanced encryption standard
Matching phase
Mutual authentication model
Rivest-Shamir-Adleman
Token generator

ABSTRACT

In decentralized storage systems, authentication ensures only authorized users can access data. Existing models face challenges with scalability, security, and privacy. To address these, a new hybrid advanced encryption standard (AES)-Rivest-Shamir-Adleman (RSA)-based mutual authentication (MA) model is proposed, using a two-way authentication mechanism. The model introduces two main innovations: a key setup algorithm combining RSA's robust security for secure key exchange with AES's efficiency for bulk data encryption, and a novel post-matching MA step where the data owner (DO) verifies the user–blockchain link. This strengthens access control by confirming user identity and privileges, preventing breaches and unauthorized access. The model's performance was tested against existing approaches with 250 users. Results showed substantial improvements in decryption time (0.025), encryption time (0.35), gas usage (120.56), information loss (0.12), memory usage (214.63), privacy ratio (1.44), and transaction time (0.51). These findings demonstrate the proposed hybrid model's superior efficiency, security, and privacy protection for decentralized storage systems.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Abhijeet Cholke
Department of Computer Engineering, Matoshri College of Engineering and Research Centre
Nashik, Maharashtra 422105, India
Email: abhijeet.cholke@gmail.com

1. INTRODUCTION

The increasing population growth and technological advancements in internet of things (IoT) systems have led to a rise in the demand for IoT-based smart grids. These smart grids are equipped with smart sensors, objects, and IoT devices, allowing for efficient energy transmission and automation. This not only improves economic benefits but also enhances the quality of services provided [1], [2]. While IoT-based smart grid systems offer many benefits, they also bring about challenges like centralized control, lack of transparency, interoperability issues, as well as privacy and security concerns, particularly in energy trading among untrusted networks. Furthermore, it is necessary to carry out audits and confirm the accuracy of transaction records within the system [3]–[5]. The IoT is an expansion of the internet's capabilities, enabling digital devices to interact with each other and exchange information [6], [7]. Essentially, IoT is a network of connected devices with unique identifiers that can communicate with one another, facilitating connections between individuals and businesses to make strategic decisions [8].

The advanced power grid enables energy to flow bidirectional between customers and utility providers, allowing for the optimization and control of power consumption based on real-time customer needs. This approach benefits both customers and power generation sectors [8], [9]. The smart grid plays a crucial role in

cyber physical systems, connecting sensors, smart objects, and physical devices through a network to enhance service delivery. It enables communication between grid components like service providers and smart meters [10], [11]. The smart grid architecture consists of four main components: energy generators, transmission, distribution, and end users, as well as three types of networks: wide area network (WAN), neighborhood area network (NAN), and home area network (HAN) [12], [13]. The smart grid maximizes supply chain management by combining energy production, IT infrastructure, and various stakeholders like service providers, consumers, and smart meters. The ultimate goal of the smart grid is to evolve into the next-generation power system that seamlessly integrates cyber physical systems, information and communication technologies (ICT), and power industry [14]. This complex system utilizes electronic devices, software applications, and advanced technology to enhance energy production and utilization [11], [15].

Block chain is a rising technology that facilitates efficient and clear communication among entities within a system. It operates as a decentralized and distributed database, with data blocks arranged in a linked list on a peer-to-peer network [16]. There are numerous advantages to utilizing blockchain-based smart grid infrastructure, such as decentralization, immutability, transparency, confidentiality, and trust. Transparency permits the visibility of all transactions conducted with public addresses, even if they involve secure real identities. Immutability guarantees that information added to the blockchain cannot be changed later on [17]. There are various forms of blockchain technology, including public, private, and consortium. In a public blockchain system, transactions are verified by miner nodes and added to blocks which are then linked in the blockchain network. The integration of blockchain into smart grid systems is an expanding technological field that addresses present centralized infrastructure challenges. The block chain of things (BCoT) has recently been applied in various new uses including smart grid systems [18]–[20], healthcare systems [21], [22], internet of vehicles (IoV), smart manufacturing, IoT applications [22]–[26], and industry 4.0 [27].

The remainder of the manuscript is organized as follows: section 2 covers the recent works on blockchain integrated IoT and access control models. Section 3 outlines the system model for access control along with the foundational preliminaries and proposed methodology. Section 4 presents the results of the hybrid AES-RSA-based mutual authentication schemes and discusses the technical findings, while section 5 concludes with a final summary.

2. RELATED WORK

Existing authentication models in decentralized storage systems face problems like restricted security, complexity of implementation, scalability issues, interoperability issues, risks to privacy, vulnerability to attacks, and complexity of management. To this end, a new approach towards authentication is proposed in this research. The Table 1 shows the various literature review of blockchain integrated IoT systems.

Table 1. Literature review of blockchain integrated IoT systems

No	Author	Methodology	Advantages	Disadvantages
1.	Bera *et al.* [1]	Novel access control protocol for smart grid systems enabled by IoT.	Protocol ensured secure data transmission from smart meters to service providers, offering enhanced functionality and improved security at lower message and computation costs compared to other similar schemes.	The model also faced challenges including centralized control, lack of transparency, and interoperability issues.
2.	Naseer *et al.* [3]	A decentralized trusted access control system utilizing block chain technology.	Security and performance assessment confirmed the scheme's ability to prevent attacks, decrease communication work load.	Facing issues with efficiency.
3.	Chattaraj *et al.* [14]	A new access control protocol based on block chain to safeguard the software defined networks platform.	New system provides improved security, extra capabilities, and requires less communication and computation costs in comparison to other similar systems currently in use.	It poses a significant challenge for an attacker attempting to alter, remove, or manipulate a block within the block chain.
4.	Bera *et al.* [28]	An access control framework using block chain technology.	This framework successfully decreased communication and computational burdens.	Facing issues with efficiency problems.
5.	Guan *et al*. [29]	A distributed block chain trading system.	The privacy protection and access control, aiming to enhance operational efficiency.	The system still facing challenges related to privacy breaches.
6.	Li *et al.* [30]	Dual-block chain system for protecting and sharing privacy in smart grid intelligent pricing systems.	Demonstrated the solution offers benefits such as quick response time, minimal latency, and low storage requirements, meeting the increasing need for secure communication	The model encountered issues regarding time complexity.
7.	Li *et al.* [31]	A secure structure for Edge computing in IoT-enabled healthcare platforms, integrating software-defined networking.	This framework aimed to improve efficiency, reduce latency and response time, and provide proximity services.	The model encountered challenges due to its high computation costs.
8.	Ye *et al.* [32]	A method to confirm identity by merging attribute-based access control, smart contracts, and edge computing.	This approach establishes a secure system for IoT devices in smart homes while keeping computational expenses low	There is a compromise between precision and confidentiality

2.1. Challenges

Security issues of power systems are more complex than stability and reliability of smart grids in IoT-based systems [1]. Security and privacy are still big issues in IoT because of the variety of IoT devices [8]. It is not easy to design a good access control model for large scale IoT devices [28]. The use of blockchain in smart homes is a difficult task because of its high resource requirements for consensus and lack of power in devices [29].

3. METHOD

3.1. System model

The system model follows a secular and decentralized approach to authenticate and maintain control on the cloud data using data user (DU) [6], data owner (DO), blockchain [1], and interplanetary file system (IPFS) technologies [8]. Figure 1 represents the system model for secure and decentralized authentication and control of users. It commences with registration where users are required to provide their details to the DO who will then record them on the blockchain, which includes the private keys and blockchain addresses that guarantees authenticity.

Once the blockchain confirmation is received, the DU transfers the encrypted data at the index number to the DO who later uploads the encrypted data on IPFS system for the decentralized storage. The IPFS automatically calculates a hash of the data to be stored, which is then stored in the blockchain block, thus providing for data integrity and immutability. Thereafter, the DU begins a matching process via the blockchain to verify the access rights, as the DO retrieves the hash from the blockchain and returns it to the user. When the DU sends a hash for the data they request, IPFS securely fetches and shares the encrypted data with the DU thus realizing the secure and verified data access process.

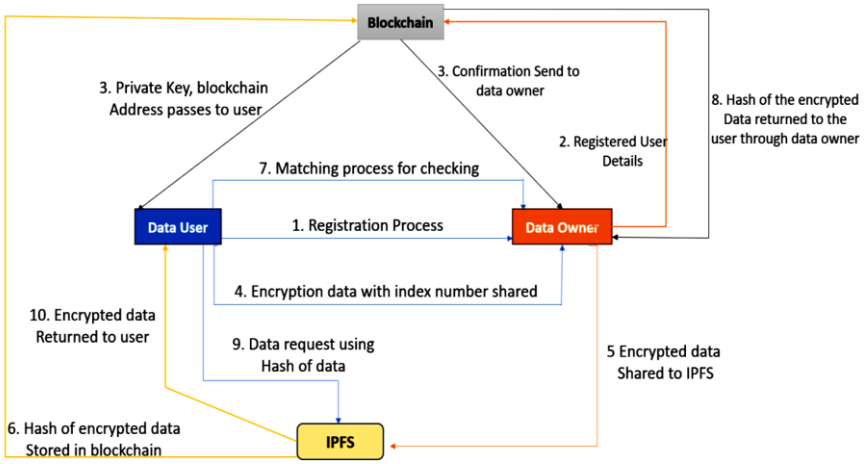

Figure 1. System model for secure and decentralized authentication and access control

3.2. Proposed methodology for the authentication model using the hybrid AES-RSA based MA model

The main aim of this research is to develop a system utilizing blockchain technology for authenticating and managing data access in cloud environments. This involves establishing a framework for confirming the identities of both the DO and the DU. The system comprises of two key entities: the DO who possesses the files intended for sharing, and the DU who is permitted to access certain files. The process of verification and control for accessing includes nine steps: establishment, registration, encryption, index formation, token production, comparison, testing, verification, and decoding. During the establishment stage, the DO establishes security settings, generates the main system key and public parameters, and incorporates the main key into an Ethereum transaction. The registration of users within this suggested data exchange system is managed by the DO, who uses the main system key to generate the secret key. During encryption, documents are encoded using a specific algorithm, with the shared document serving as input to produce cipher text, document encryption key, and keyword group. The token generation phase then creates the search token. The control establishment is an additional step in the process. The testing phase shows the relevant transaction ID and successful key match results, which are later confirmed in the validation phase. Ultimately, the decryption phase utilizes an algorithm to decode the encrypted file. The architecture for the proposed authentication model is shown in Figure 2.

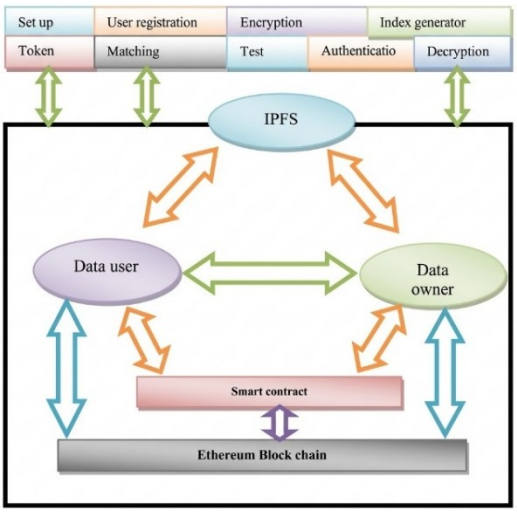

Figure 2. Architecture for the proposed authentication model

3.3. User registration phase

During this stage, the DU enrolls with the DO via the block chain technology. User registration is essential for linking the user within the block chain system in order to establish proper authentication and data access control. The (1) represents the count of DU names and (2) represents the password, while N represents the total count of users who possess both the data and a secret key that includes a randomly generated number r.

$$U = \{U_{ID}^{1}, \ldots \ldots \ldots U_{ID}^{N}\} \quad (1)$$

$$pw = \{pw_{1,\ldots\ldots} pw_{N}\} \quad (2)$$

The random number r signifies the specific mechanism for registering new users. Initially, users are required to register with a user name and password. The DO verifies if the user already exists in the system. If the user is already registered, the DO acknowledges them as an existing user. Otherwise, they are considered a new user, prompting the DO to register them and confirm the information in a block chain. After the block chain process is finished, the DO provides the user with the block chain address and private key, along with a confirmation message. Figure 3 represents the user registration phase with all conventions.

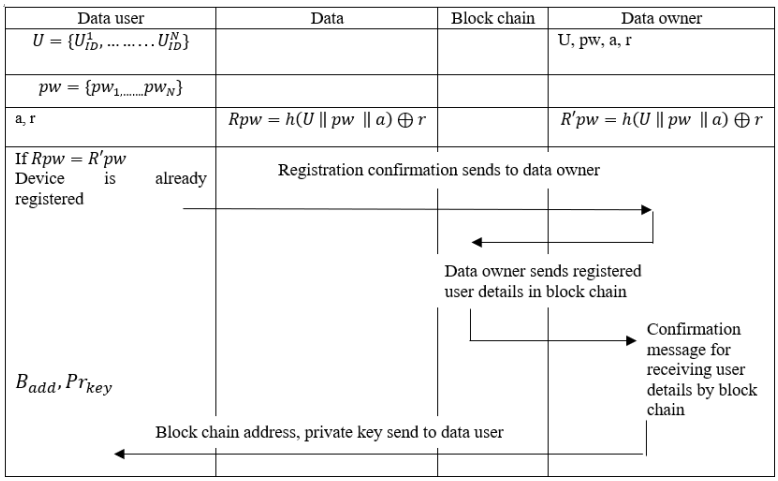

Figure 3. User registration phase

3.4. Data encryption phase

During the data encryption process following user registration, the user encrypts the data and sends it to the DO along with an index number R. The data number is saved by the DO and will be used in the

future when accessing data to confirm the user's authorization status. After the DO gives permission, the data is sent to IPFS through blockchain for storage, with the hash ID of the data being documented on blockchain.

The data encryption is as shown in Figure 4. In this research, the reason behind the utilization of the hybrid Rivest-Shamir-Adleman (RSA) and advanced encryption standard (AES) algorithm for encryption is based on the complementary nature of both encryption techniques. RSA has strong key management features, with the most notable ones being in the field of secure key exchange. Thus, it is perfectly suitable for encrypting small amounts of data in an efficient manner. On the contrary, AES performs very well at the task of quickly encrypting large amounts of data with a high level of cryptographic security. This is accomplished through the combination of RSA for key exchange that is done during secure key exchange and AES for bulk data encryption that provides efficiency in terms of encrypting large volumes of data.

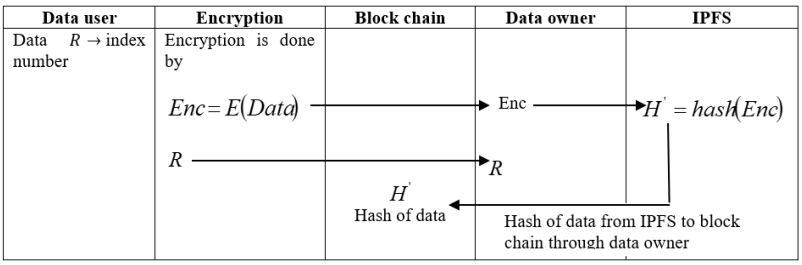

Figure 4. Data encryption phase

3.5. Proposed hybrid AES-RSA mutual authentication model

Figure 5 illustrates the proposed model with hybrid RSA–AES encryption mechanism for secure data protection and efficient key management. Using the RSA public key, the user data is encrypted, and masked data and an encrypted AES key are generated. The encrypted key is retrieved using the corresponding private key and passed through AES for decrypting to get the original key for encryption. The retrieved key is then applied to the masked data to retrieve the original user data. This is a hybrid of two types of encryptions, asymmetric RSA and symmetric AES, which combines the security benefits of the former with the computational advantages of the latter. Hybrid RSA-AES based mutual authentication (MA) architecture incorporates both fast encryption capabilities of AES and secure key management and reliability of RSA as represented in Figure 5. The proposed approach capitalizes on the merits of both algorithms, thus improving data encryption while also solving information confidentiality (IC) when it comes to data privacy.

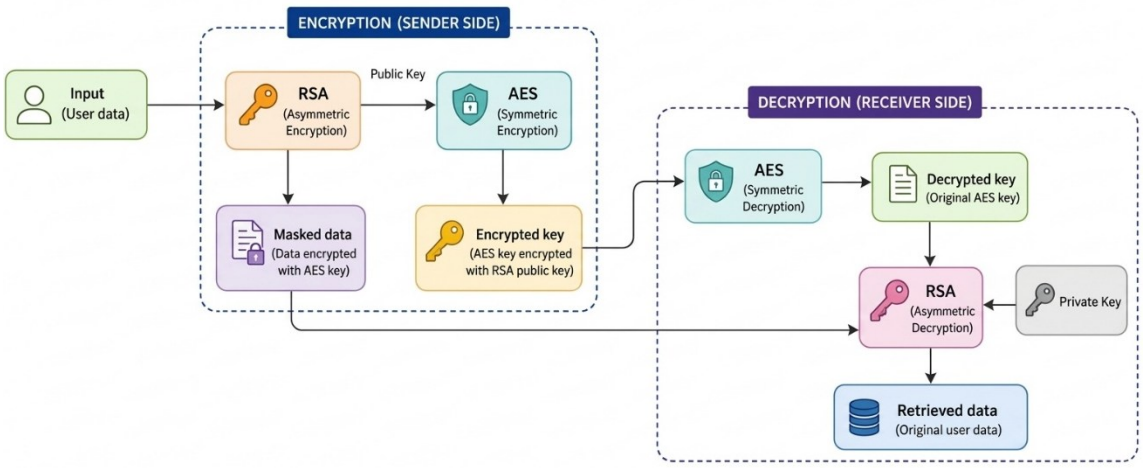

Figure 5. Hybrid RSA- AES architecture

3.6. Index generator

The index generator is a component that creates an index of each ciphered data file. This index is used as a pointer or a parameter for the encrypted data, enabling the system to retrieve and verify the information in an efficient manner. The index generator employs a mixture of encryption methods and

algorithms to generate a unique index for every encrypted file. This index is paramount for the sake of data integrity by giving access to the right information to the authorized users during the matching process. Furthermore, the index may contain metadata or keywords related to the encrypted data, making search and retrieval operations simpler and faster within the system.

3.7. Token generation

The token generator is a key element in the authentication and access control process of the proposed system. It produces the access tokens that allow authorized users to have certain permissions or privileges to access the encrypted data. These tokens are cryptographic signs of authorization that are usually created by the user's authentication and access. The token generator is based on cryptography to generate distinctive and non-editable tokens that cannot be replicated or tempered with. These tokens may represent the user's information like their identity, permission rights and expiration date. During the access control process, these tokens will be presented by the users so that the encrypted data can be decrypted only by the authorized users. Beyond this, the token generator may consider implementation of access revocation mechanisms to deactivate the privileges in the event of security breaches or attempted unauthorized access.

When T needs to request data from the server, it starts by creating a range query like $Q = (b_1 \leq y_1 \leq c_1) \wedge (b_2 \leq y_2 \leq c_2)\ldots\ldots\ldots\wedge (b_1 \leq y_1 \leq c_1)$ and then calculates a signature $\delta_T = Sig_{tl_t}(Q)$. During each interval of questioning T sends the query to DD as shown in (3)

$$T \rightarrow DD: \{Q, ID_T, \delta_T\} \tag{3}$$

The DD confirms the authenticity of T 's signature by utilizing T 's public key. If T is an authorized requester, the DD may provide query tokens to T by taking specific measures given by (3). The Q partitions $Q \geq= (y_1 \geq b_1) \wedge (y_2 \geq b_2)\ldots\ldots\ldots\wedge (y_1 \geq b_1) and Q \leq= (y_1 \leq b_1) \wedge (y_1 \leq b_2)\ldots\ldots\ldots\ldots\ldots\ldots\wedge (y_1 \leq b_m)$ into two sections: Q. Let $x \geq= (b_1, \ldots\ldots\ldots b_m)$ and $x \leq= (c_1, \ldots\ldots\ldots c_m)$. The DD creates two query vectors, $\sigma_{\geq}^{*}(x)$ and $\sigma_{\leq}^{*}(x)$, to symbolize $Q_{\geq}$ and $Q_{\leq}$. The wildcard $*$ in the vector $\sigma_{\geq}^{*}(x)$ indicates that T is indifferent towards attributes associated with $*$. Let $t\left(\sigma^{*}(x_h)\right)$ denote the collection of elements l that fulfill $\sigma_{\geq}^{*}(x_l) \neq *$. Let $t\left(\sigma_{\leq}^{*}(x)\right)$ represent the group of elements $l^{'}$ that meet the criteria of $\sigma_{\leq}^{*}(x_l) \neq *$. Subsequently, the DD calculates a token $U_{q\geq}$ by employing the query vector $\sigma_{\geq}^{*}(x)$ in the described manner.

- Choose a random value for $\alpha, \beta \in A_q$ and produce a $\lambda_l, \Psi_l, \gamma_l, \tau_l \in A_q$ so that $\lambda_l z_1 + \psi_l z_2 = \alpha, \gamma_l z_1 + \tau_l z_2 = \beta$ for every $l \in t\left(\sigma_{\geq}^{*}(x)\right)$.
- Compute a token $U_{q\geq}$ as (4) to (8)

$$L_{M1}^{t} = h1 \prod_{l \in t\left(\sigma_{\geq}^{*}(x)\right)} \left(i_l v_l^{\sigma_{\geq}^{*}(x_l)} \right)^{\lambda_l} \psi_l^{\gamma l} \tag{4}$$

$$L_{M2}^{t} = h2 \prod_{l \in t\left(\sigma_{\geq}^{*}(x)\right)} \left(i_l v_l^{\sigma_{\geq}^{*}(x_l)} \right)^{\psi_l} \psi_l^{\tau l} \tag{5}$$

$$L_{M3}^{t} = h^{\alpha} \tag{6}$$

$$L_{M4}^{t} = h^{\alpha} \tag{7}$$

$$L_{M5}^{t} = h^{-\sum l \in t\left(\sigma_{\geq}^{*}(x)\right)^{(w_l \alpha + ul\beta)}} \tag{8}$$

In the same way, the DD produces a token $U_{q\leq}$ by utilizing the query vector $\sigma_{\leq}^{*}(X)$ in the following manner:

- Select a random $\alpha^{'}, \beta^{'} \in A_q$, and generate $\lambda_{l'}, \psi_{l'} \gamma_{l'}, \tau_{l'} \in A_q$ such that $\lambda_{l'} z_1 + \psi_{l'} z_2 = \alpha^{'}, \gamma_{l'} z_1 + \tau_{l'} z_2 = \beta^{'}$.
- Compute the token $U_{Q\leq}$ as (9) to (13).

$$L_{S1}^{t} = h1 \prod_{l \in t\left(\sigma_{\geq}^{*}(x_{Mt})\right)} \left(i_{l^{'}} v_{l^{'}}^{\sigma^{*}\left(x_{mtl^{'}}\right)} \right)^{\lambda_l} \psi_{l^{'}}^{\gamma l^{'}} \tag{9}$$

$$L_{S2}^{t} = h2 \prod_{l^{'} \in t\left(\sigma_{\geq}^{*}(x_{Mt})\right)} \left(i_{l^{'}} v_{l^{'}}^{\sigma^{*}\left(x_{mtl^{'}}\right)} \right)^{\psi_l} \psi_{l^{'}}^{\tau l^{'}} \tag{10}$$

$$L_{S3}^{t} = h^{\alpha^{'}} \tag{11}$$

$$L_{S4}^{t} = h^{\beta'} \tag{12}$$

$$L_{S5}^{t} = h^{-\sum l' \in t(\sigma^{*}(x_{mt}))\left(w_{l'}\alpha' + u_{l'}\beta'\right)} \tag{13}$$

If $U_{q\geq} = (L_{M1}^{t}, L_{M2}^{t}, L_{M3}^{t}, L_{M4}^{t}, L_{M5}^{t})$ given by (4) to (7) and $U_{q\leq} = (L_{S1}^{t}, L_{S2}^{t}, L_{S3}^{t}, L_{S4}^{t}, L_{S5}^{t})$ given by (9) to (13) are both present, the DD given by (14) will save a record $(ID_t, U_{q\geq}, U_{q\leq})$ in its database and send $U_{q\geq} and U_{q\leq}$ to the authorized requester T as tokens.

$$DD \rightarrow T: [U_{q\geq}, U_{q\leq}] \tag{14}$$

3.8. Matching phase

After receiving the index number and token generation from the user, the DO uses it to identify each user. During the matching phase, the user's identity is confirmed using their username and index number. If the match is successful, the DO provides the user with the hash of their data stored in the blockchain. Whenever the user requests the data again, it is retrieved from IPFS, decrypted, and made available for use. The data matching phase represents therefore as critical step where DO and DU are granted permission for data accessibility secure data resource sharing. To enhance this function, authentication mechanisms are implemented, ultimately ending in MA by the DO to confirm the link between the DU and the system. First, at the stage of matching, the data provider and the DU certify data access rights, making sure the DU has the required credentials for the data retrieval. Following the verification, mutual identification is initiated, where the DO checks the actuality of the DU's identity against the blockchain. This process encompasses reviewing user credentials stored on the blockchain including the one's blockchain address or private key to validate the legitimacy. Through MA, the DO reinforces the trustworthiness of the data abuser and guarantees that only authorized and true users with privileged access rights can progress to participate in the encrypted data in the cloud, thus, strengthening the entire security position of the system.

Let M stand for the matching phase given by (15) which is the verification of access permissions of the DO to the DU. The AU stands for authentication process, through which the DO performs MA to validate the link between DU and the blockchain. The whole process can be represented as (15).

$$M \rightarrow AU \tag{15}$$

Here sequential phase execution is denoted as →, the DU is denoted as U_D, block chain is denoted as B. The process of MA can be mathematically represented as and is given in (16).

$$AU = O_D \leftrightarrow B \leftrightarrow U_D \tag{16}$$

Here $O_D \leftrightarrow B$ stands for the DO, the process of authenticating the link between the blockchain and itself by the DO is deliberately done to ensure that the blockchain records are free from errors. Also, $B \leftrightarrow U_D$ symbolizes DO checking the relationship between blockchain and DU, which makes it possible to verify if the DU's credentials stored on the blockchain are authentic.

The mathematical model expresses the succession of phases. First matching and then MA which guarantees that the process of accessing and using the data is secure and authentic. The complete procedure of matching phase is as shown in the Figure 6.

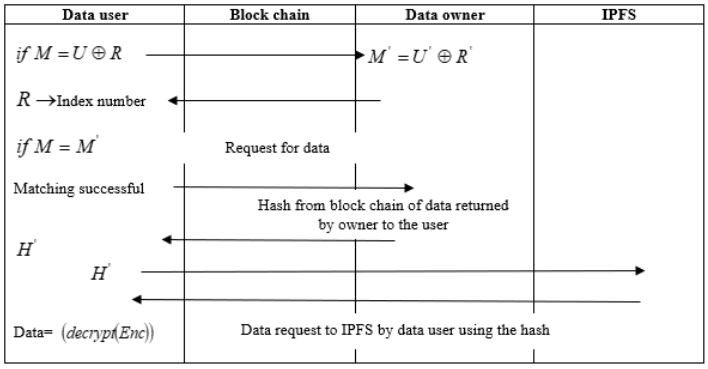

Figure 6. Matching phase

4. RESULTS AND DISCUSSION

The purpose of this research is to create a reliable access control system using a hybrid AES-RSA based MA model. To evaluate the efficiency of this model, its performance will be compared with that of other existing models. The existing models used various access control schemes such as blockchain-based access, trusted control access, lightweight dual blockchain, attribute-based access.

4.1. Experimental setup

The Python programming language is conducting an experiment on a Windows 10 system, which possesses 8 GB of memory, to test the MA model. The Ganache an Ethereum blockchain framework is used to develop, test, and debug the code creating a smart contract between DU and DO. A decentralized, peer-to-peer distributed file system IPFS is used for storing, sharing, and accessing data in content-addressed manner rather than by location. IPFS overcome on-chain storage limitations of blockchain.

4.2. Comparative methods

In order to showcase the efficiency of the Hybrid AES-RSA based MA model, researchers are conducting a comparison analysis. They are evaluating different methods such as blockchain based access control protocol [1], lightweight dual block chain [30], decentralized trusted control access scheme [32], and attribute-based access control scheme [33] as part of this investigation. The dataset used are education dataset [34] and medical dataset [35].

4.2.1. Comparative analysis based on education

The effectiveness of the hybrid AES-RSA based MA in ensuring secure access control is being assessed in comparison to other methods. This evaluation includes analyzing decryption time, encryption time, gas usage, information loss, memory usage, privacy ratio, and transaction time with a set number of 250 users. The overall comparative analysis based on education is presented in Figure 7.

In Figure 7(a), the hybrid AES-RSA based MA model is demonstrated to be effective in enhancing secure access control, achieving a decryption time of 0.025 with a number of users (NOU) of 250. Moreover, this model surpasses the attribute-based access control model by 25.25%. The hybrid AES-RSA based MA model shown in Figure 7(b) exhibits strong performance in secure access control, with an encryption time of 0.35 at NOU of 250. It outperforms the attribute-based access control model by a significant margin of 17.96%. In Figure 7(c), the hybrid AES-RSA based MA model demonstrates strong performance in secure access control, achieving a gas usage of 120.56 at NOU of 250. Additionally, this model shows a 2.58% improvement over the attribute-based access control model. Figure 7(d) illustrates the efficiency of the hybrid AES-RSA based MA model in ensuring secure access control, with an information loss of 0.12 at NOU 250. Additionally, this model surpasses the attribute-based access control model by 1.74%. Figure 7(e) highlights how the hybrid AES-RSA based MA model is successful in ensuring secure access control, with a lower memory usage of 214.63 at NOU 250 compared to the attribute-based access control model, showing a 1.96% improvement. The hybrid AES-RSA based MA model is shown to be effective in ensuring secure access control with a privacy ratio of 1.44 at NOU 250 in Figure 7(f). Additionally, the hybrid AES-RSA based MA model outperforms the attribute-based access control model by 3.55%. The hybrid AES-RSA based MA model is shown in Figure 7(g) to be successful in ensuring secure access control with a reduced transaction time of 2.53 at NOU 250, furthermore, this model outperforms the attribute-based access control model by 0.51%.

4.2.2. Comparative analysis based on medical

The overall comparative analysis based on medical dataset are presented in Figure 8. In Figure 8(a), the hybrid AES-RSA based MA model is demonstrated to be effective in enhancing secure access control, achieving a decryption time of 0.026 with a NOU of 250. Moreover, this model surpasses the attribute-based access control model by 14.69%. The hybrid AES-RSA based MA model shown in Figure 8(b) exhibits strong performance in secure access control, with an encryption time of 0.36 at NOU of 250. It outperforms the attribute-based access control model by a significant margin of 15.97%. In Figure 8(c), the hybrid AES-RSA based MA model demonstrates strong performance in secure access control, achieving a gas usage of 120.73 at NOU of 250. Additionally, this model shows a 2.81% improvement over the attribute-based access control model. Figure 8(d) illustrates the efficiency of the hybrid AES-RSA based MA model in ensuring secure access control, with an information loss of 0.12 at NOU 250. Additionally, this model surpasses the attribute-based access control model by 10.78%. Figure 8(e) highlights how the hybrid AES-RSA based MA model is successful in ensuring secure access control, with a lower memory usage of 207.25 at NOU 250 compared to the attribute-based access control model, showing a 6.39% improvement. The hybrid AES-RSA based MA model is shown to be effective in ensuring secure access control with a privacy ratio of 1.51 at NOU 250 in Figure 8(f). Additionally, the hybrid AES-RSA based MA model outperforms the attribute-based access control model by 7.35%. The hybrid AES-RSA based MA model is shown in Figure 8(g) to be successful in

ensuring secure access control with a reduced transaction time of 0.48 at NOU 250, furthermore, this model outperforms the attribute-based access control model by 12.04%.

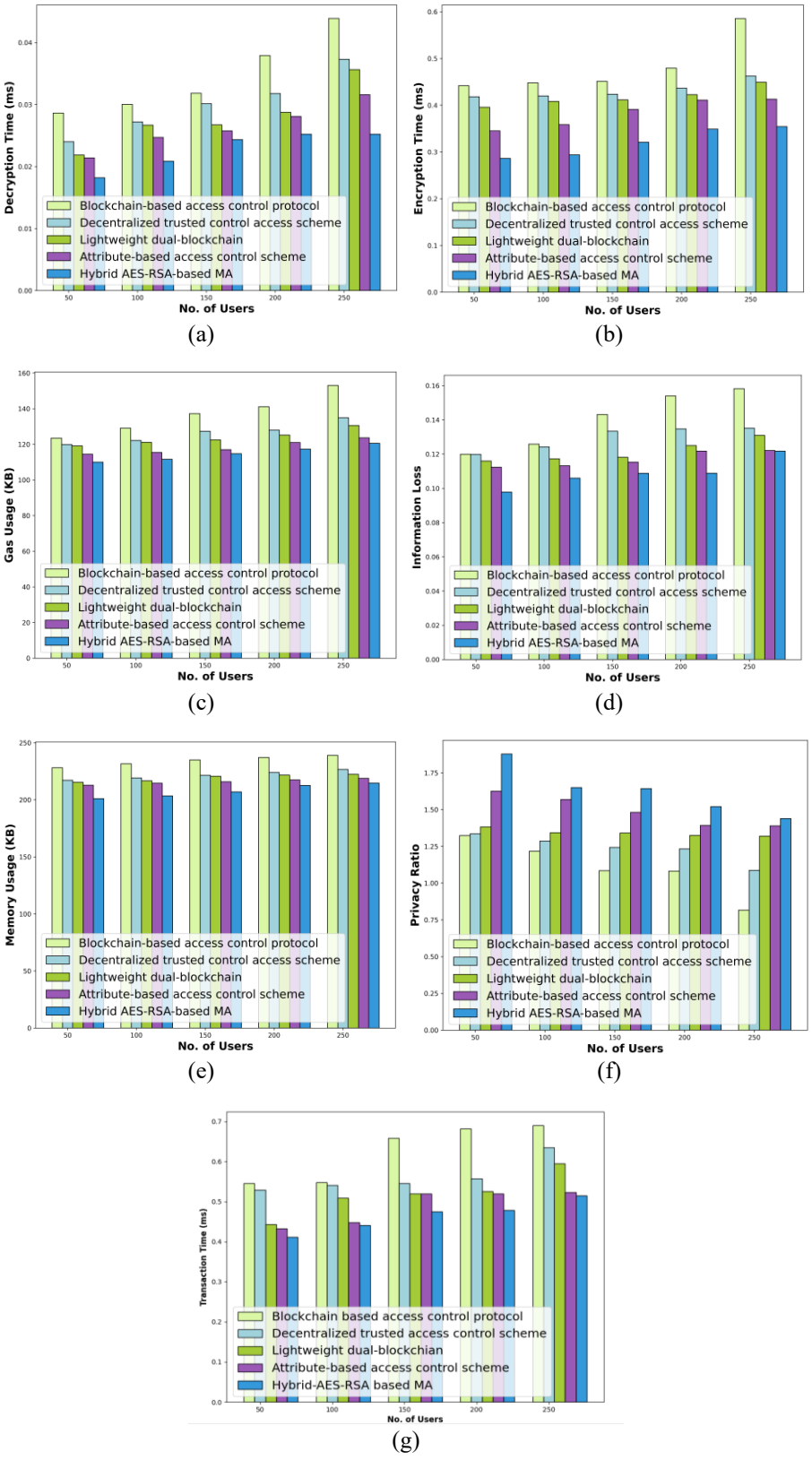

Figure 7. Comparative analysis based on education (a) decryption time, (b) encryption time, (c) gas consumption, (d) data loss, (e) memory usage, (f) privacy ratio, and (g) transaction time

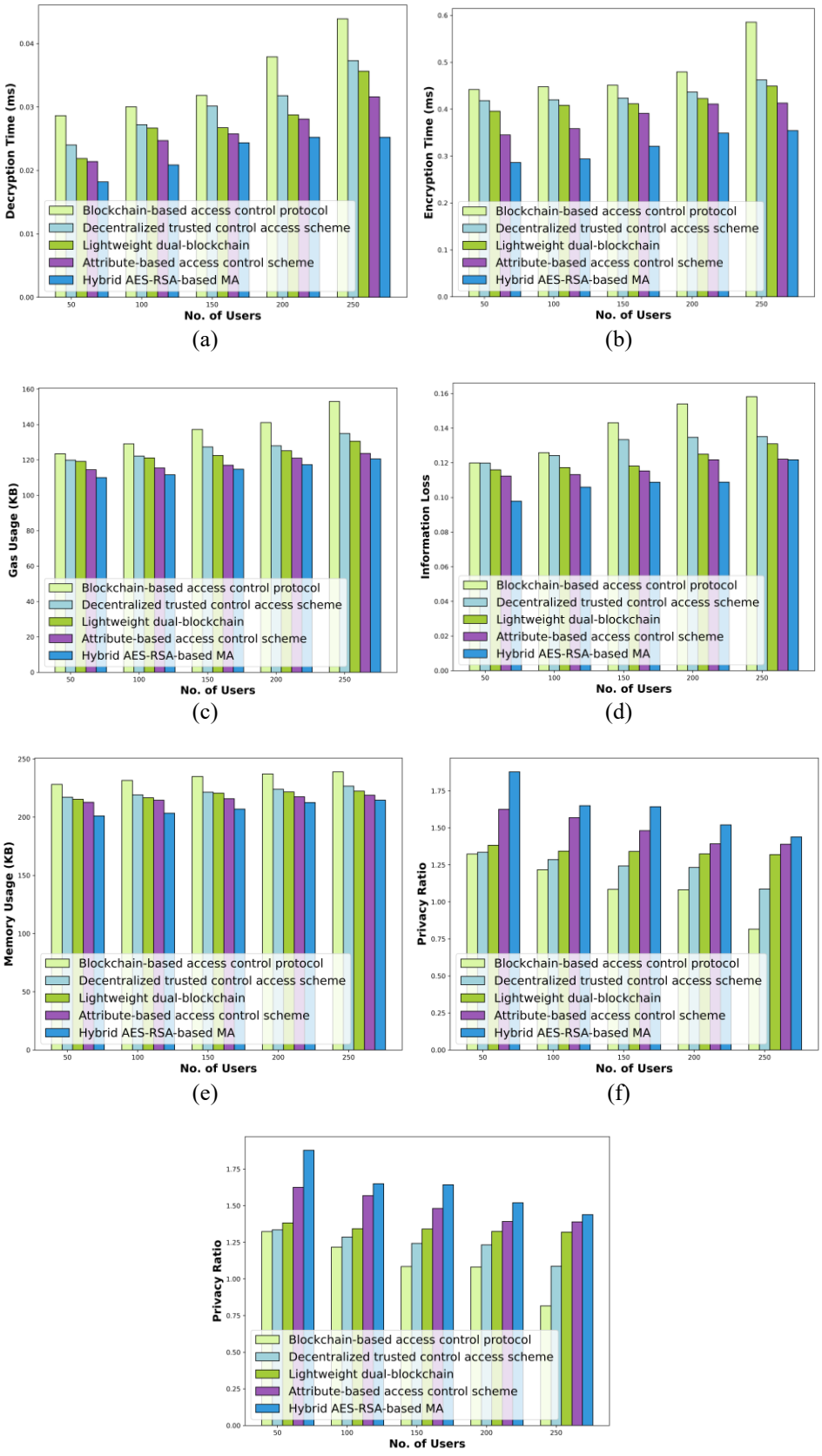

Figure 8. Comparative analysis based on medical (a) decryption time, (b) encryption time, (c) gas consumption, (d) data loss, (e) memory usage, (f) privacy ratio, and (g) transaction time

4.3. Comparative discussion

The proposed hybrid AES-RSA based MA model demonstrates superior performance compared to existing approaches, primarily due to its innovative use of encryption techniques and authentication protocols. AES handles large data volumes efficiently, while RSA manages secure key transmission, reducing the computational workload for both encoding and decoding operations. As a result, the model supports faster data processing and overall improved system performance. The MA stage further enhances security by simplifying the authentication process without compromising its robustness. This ensures secure data access while keeping authentication time to a minimum. Additionally, the integration of blockchain technology strengthens the system's security framework. Blockchain provides a decentralized, tamper-resistant method for verifying user connections, adding another layer of reliability to the model. Results shown in Table 2 revealed significant improvements in all tested areas. At an NOU of 250, the model achieved values of 0.025 for decryption time, 0.35 for encryption time, 120.56 for gas consumption, 0.12 for data loss, 214.63 for memory usage, 1.44 for privacy ratio, and 0.51 for transaction time.

Table 2. Comparative discussion for education analysis and medical analysis

Models	Domain	Decryption time	Encryption time	Gas usage	Info loss	Memory usage	Privacy ratio	Transaction time
Blockchain-based access control	Education	0.044	0.59	152.99	0.16	238.92	0.82	0.69
	Medical	0.044	0.63	146.83	0.19	241.95	1.00	0.64
Decentralized trusted control	Education	0.037	0.46	134.89	0.14	226.62	1.09	0.63
access scheme	Medical	0.033	0.48	133.31	0.15	233.57	1.11	0.60
Lightweight dual-blockchain	Education	0.036	0.45	130.56	0.13	222.38	1.32	0.60
	Medical	0.033	0.44	129.89	0.14	226.02	1.39	0.58
Attribute-based access control	Education	0.032	0.41	123.67	0.12	218.84	1.39	0.52
scheme	Medical	0.030	0.42	124.13	0.13	220.5	1.40	0.54
Hybrid AES-RSA-based MA	Education	0.025	0.35	120.56	0.12	214.63	1.44	0.51
	Medical	0.026	0.36	120.73	0.12	207.25	1.51	0.48

5. CONCLUSION

In summary, the research offers a complete assessment of the authentication and access control processes in distributed storages by determining main problems and providing smart solutions. The hybrid AES-RSA encryption model, which exploits the strengths of both algorithms, is presented as the most effective option to protect data integrity. In addition, the establishment of a MA phase post-matching process provides additional data access security and integrity through the verification of a connection between the DU and the blockchain. These contributions significantly advance secure access control for decentralized data storage systems. Moving forward, further research and development efforts will build upon these achievements to enhance the security, efficiency, and usability of authentication procedures. The superiority of the hybrid AES-RSA based MA model is demonstrated in comparison to other models. This comparison involves evaluating metrics at a NOU of 250. The findings indicate that at NOU of 250, the models demonstrate significant improvements in decryption time, encryption time, gas usage, information loss, memory usage, privacy ratio, and transaction time, with scores of 0.025, 0.35, 120.56, 0.12, 214.63, 1.44, and 0.51 for education, respectively, compared to the current models.

FUNDING INFORMATION

The authors states no funding received.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Abhijeet Cholke	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Vaishali V. Mandhare		✓				✓		✓		✓	✓	✓		
Pratap S. Vikhe				✓	✓		✓			✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare no competing interests.

ETHICAL APPROVAL

The authors declare that this research was conducted in accordance with accepted ethical standards. The study does not involve human participants, animals, or personal/sensitive data. All methods, analyses, and results are reported honestly and transparently. Any sources of data, tools, or software used in this work have been properly cited. The authors declare no conflict of interest related to this study.

DATA AVAILABILITY

The data that support the findings of this study are openly available in Kaggle at:

- https://www.kaggle.com/datasets/rohithmahadevan/students-marksheet-dataset, reference [34]
- https://www.kaggle.com/datasets/imdevskp/corona-virus-report?select=country_wise_latest.csv, reference [35]

REFERENCES

[1] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021, doi: 10.1109/JIOT.2020.3030308.

[2] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, Mar. 2020, doi: 10.1109/TDSC.2017.2764083.

[3] O. Naseer, S. Ullah, and L. Anjum, "Blockchain-based decentralized lightweight control access scheme for smart grids," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8233–8243, Sep. 2021, doi: 10.1007/s13369-021-05446-5.

[4] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2629–2640, Jun. 2018, doi: 10.1109/TII.2018.2789442.

[5] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions," *IEEE Access*, vol. 7, pp. 62962–63003, 2019, doi: 10.1109/ACCESS.2019.2913984.

[6] R. Sharma, M. Wazid, and P. Gope, "A blockchain based secure communication framework for community interaction," *Journal of Information Security and Applications*, vol. 58, May 2021, doi: 10.1016/j.jisa.2021.102790.

[7] S. Saha, A. K. Sutrala, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "On the design of blockchain-based access control protocol for IoT-enabled healthcare applications," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, IEEE, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148915.

[8] S. Algarni *et al.*, "Blockchain-based secured access control in an IoT system," *Applied Sciences*, vol. 11, no. 4, Feb. 2021, doi: 10.3390/app11041772.

[9] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020, doi: 10.1109/ACCESS.2020.2996093.

[10] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-preserving mechanism in smart home using blockchain," *IEEE Access*, vol. 9, pp. 103651–103669, 2021, doi: 10.1109/ACCESS.2021.3098795.

[11] K. -D. Kim and P. R. Kumar, "Cyber–physical systems: a perspective at the centennial," *Proceedings of the IEEE*, vol. 100, pp. 1287–1308, May 2012, doi: 10.1109/JPROC.2012.2189792.

[12] R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, "Smart grid technologies and applications," *Renewable and Sustainable Energy Reviews*, vol. 66, pp. 499–516, Dec. 2016, doi: 10.1016/j.rser.2016.08.002.

[13] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "Fog computing for smart grid systems in the 5G environment: challenges and solutions," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 47–53, Jun. 2019, doi: 10.1109/MWC.2019.1800356.

[14] D. Chattaraj, S. Saha, B. Bera, and A. K. Das, "On the design of blockchain-based access control scheme for software defined networks," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, Jul. 2020, pp. 237–242, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162669.

[15] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[16] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019, doi: 10.1109/ACCESS.2019.2920682.

[17] D. Chattaraj, B. Bera, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing fine-grained access control for software-defined networks using private blockchain," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1542–1559, 2022, doi: 10.1109/JIOT.2021.3088115.

[18] H. Zhang, J. Wang, and Y. Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid," *Energy*, vol. 180, pp. 955–967, Aug. 2019, doi: 10.1016/j.energy.2019.05.127.

[19] C.-W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4405–4425, Sep. 2018, doi: 10.1109/TSG.2017.2656068.

[20] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, Jun. 2019, doi: 10.1016/j.future.2019.01.018.

[21] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, Jun. 2019, doi: 10.1016/j.jnca.2019.02.027.

[22] M. Banerjee, J. Lee, and K. K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018, doi: 10.1016/j.dcan.2017.10.006.

[23] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014, doi: 10.1007/s11276-014-0761-7.

[24] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, 2013, doi: 10.1109/MWC.2013.6704479.

[25] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," *Future Generation Computer Systems*, vol. 91, pp. 475–492, Feb. 2019, doi: 10.1016/j.future.2018.09.017.
[26] M. Wazid, A. K. Das, V. Bhat K, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *Journal of Network and Computer Applications*, vol. 150, Jan. 2020, doi: 10.1016/j.jnca.2019.102496.
[27] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42–52, Aug. 2018, doi: 10.1016/j.jnca.2018.05.005.
[28] B. Bera, A. K. Das, M. S. Obaidat, P. Vijayakumar, K.-F. Hsiao, and Y. Park, "AI-enabled blockchain-based access control for malicious attacks detection and mitigation in IoE," *IEEE Consumer Electronics Magazine*, vol. 10, no. 5, pp. 82–92, Sep. 2021, doi: 10.1109/MCE.2020.3040541.
[29] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and privacy-preserving energy trading based on blockchain and ABE in smart grid," *Journal of Parallel and Distributed Computing*, vol. 147, pp. 34–45, Jan. 2021, doi: 10.1016/j.jpdc.2020.08.012.
[30] K. Li, Y. Yang, S. Wang, R. Shi, and J. Li, "A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid," *Computers & Security*, vol. 103, Apr. 2021, doi: 10.1016/j.cose.2021.102189.
[31] J. Li *et al.*, "A secured framework for SDN-based edge computing in IoT-enabled healthcare system," *IEEE Access*, vol. 8, pp. 135479–135490, 2020, doi: 10.1109/ACCESS.2020.3011503.
[32] Y. Ye, L. Zhang, W. You, and Y. Mu, "Secure decentralized access control policy for data sharing in smart grid," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484474.
[33] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.
[34] R. Mahadevan, "Students marksheet dataset: a sample dataset of students marks," *Kaggle*. Accessed: Aug. 15, 2025. [Online]. Available: https://www.kaggle.com/datasets/rohithmahadevan/students-marksheet-dataset
[35] K. P. Devakumar, "COVID-19 dataset: number of confirmed, death and recovered cases every day across the globe," *Kaggle*. Accessed: Aug. 15, 2025. [Online]. Available: https://www.kaggle.com/datasets/imdevskp/corona-virus-report?select=country_wise_latest.csv

BIOGRAPHIES OF AUTHORS



Abhijeet Cholke received the B.E. degree in Computer Engineering from University of Pune, India, in 2009, and M.Tech. from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, Madhya Pradesh in 2015 and pursuing Ph.D. degree in Computer Engineering, from Matoshri College of Engineering, Nashik, affiliated to Savitribai Phule Pune University, Pune from 2022. He is currently working as assistant professor in Computer Engineering at School of Computing, MIT Art, Design and Technology University, Pune. His current research interest includes blockchain technology, cryptography, and data mining. He is member of Indian Association of Engineers (IAENG), Society of Digital Information and Wireless Communications (SDIWC), and Computer Society of India (CSI). He can be contacted at email: abhijeet.cholke@gmail.com.



Dr. Vaishali V. Mandhare holds her Ph.D. in Information Technology from SGGS Institute of Engineering and Technology, affiliated to Swami Ramanand Teerth Marathwada University, Nanded and received her M.Tech. in Computer Engineering from Dr. Babasaheb Ambedkar Technological University in 2009. She works as head and associate professor in the Department of Artificial Intelligence and Data Science, at the Pravara Rural Engineering College, Loni. She is board of studies member in Computer Engineering in Savitribai Phule Pune University. Her research interests include computer network, artificial intelligence, blockchain technology, published several papers in peer reviewed journals and conferences. She is life member of ISTE, CSI, IAENG, and AIMEE. She can be contacted at email: vaishalivikhe@gmail.com.



Dr. Pratap S. Vikhe holds a Ph.D. (2018) in Instrumentation Engineering from SGGS Institute of Engineering and Technology, Nanded, affiliated with Swami Ramanand Teerth Marathwada University and M.Tech. (2009). He completed his bachelor's degree in Instrumentation Engineering from Padmashri Dr. Vithalrao Vikhe Patil, Ahmednagar (University of Pune) in 2003. Currently, he is an associate professor in the Department of Instrumentation and Control Engineering at Pravara Rural Engineering College, Loni, affiliated with the University of Pune. His research focuses on biomedical signal and image processing. He has published several papers in national and international journals and conferences. He is a life member of ISTE, IETE, IAENG, IARA, and ISA. He can be contacted at email: Pratap.vikhe@gmail.com.