Journal of Basics and Applied Sciences Research (JOBASR)
ISSN (print): 3026-9091, ISSN (online): 1597-9962
Volume 3(5) September 2025
DOI: https://dx.doi.org/10.4314/jobasr.v3i5.3

A Novel Multi-Authority Access Control Scheme for Fine Grained Access to Users Data in The Cloud-Based Storage

Abubakar A.[1*], Abdulrasheed N. [2] & Surajo M. [3]
[1]Department of Computer Science, Umaru Musa Yar'adua University
[2,3]Department of Computer Science/Engineering, Maryam Abacha American University of Niger Republic (MAAUN)
[*]Corresponding Author Email: **abdurrashidnasir@gmail.com**

ABSTRACT
This study aims to improve data security and access control in cloud storage systems by introducing a novel hybrid RSA-AES encryption scheme based Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which combines multiple levels of authority. Challenges including data confidentiality, resistance to collusion, and scalability are addressed by the proposed approach. Different sets of attributes are managed by multiple attribute authorities, which distributes trust and minimizes single points of failure. By using asymmetric encryption for keys and symmetric encryption for data, the CP-ABE combined with RSA-AES guarantees strong data protection. Only when a user's attributes align with the system's access policies can they decrypt data. Performance analyses show that even with an increase in users and attributes, the method is able to maintain low encryption and decryption times. Data confidentiality and resistance to collusion attempts are confirmed by security studies. Subsequent research endeavors will center on refining the computational efficiency of the proposed scheme and investigating the assimilation of blockchain technology to augment security and scalability within multi-authority settings. Especially for large-scale systems, our research provides a practical approach for safe data sharing in cloud environments.

Keywords:
Multi-Authority Access Control, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Hybrid RSA-AES Encryption, Cloud Storage Security, Fine-Grained Access Control.

INTRODUCTION

Cloud computing has transformed information technology by enabling organizations to store and manage data on remote servers with high scalability, flexibility, and cost-efficiency (Obi et al., 2024). As its adoption grows, concerns about data privacy, security, and access control have become more pressing (Soveizi et al., 2023).

Sensitive information—such as financial records, healthcare data, and confidential documents—is frequently stored in the cloud, raising the risk of unauthorized access and data breaches (Pool et al., 2024). Since cloud services operate on third-party servers, robust security mechanisms are required to ensure data confidentiality, integrity, and controlled access (Kumar et al., 2024).

Attribute-Based Encryption (ABE) is a promising technique that enables access control by encrypting data based on user attributes (Sicari et al., 2020). Among ABE schemes, Ciphertext-Policy ABE (CP-ABE) allows data owners to define access policies embedded in the ciphertext, ensuring only users with matching attributes can decrypt the data (Cui et al., 2020). This enables decentralized and flexible access control across diverse user groups (Golightly et al., 2023).

However, traditional CP-ABE faces challenges such as collusion attacks—where users combine keys to bypass restrictions—and performance issues as the number of users and attributes increases (Hou et al., 2023). Additionally, efficient key management and low encryption overhead are essential for maintaining performance in large-scale systems (Unal et al., 2021).

To address existing limitations in cloud storage security, this study proposes a novel multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption (Jammula et al., 2022). This hybrid approach combines the speed of symmetric AES encryption for data protection with the robust key management of RSA, thereby enhancing both efficiency and security (Qureshi et al., 2022). Distributing attribute management among multiple authorities reduces the risk of a single point of failure and strengthens system trust and scalability (Banerjee et al., 2021). The proposed scheme ensures that no single entity has full control, which mitigates the risk of user collusion and unauthorized access.

How to cite this article: Abubakar A., Abdulrasheed N. & Surajo M. (2025). A Novel Multi-Authority Access Control Scheme for Fine Grained Access to Users Data in The Cloud-Based Storage. *Journal of Basics and Applied Sciences Research*, *3*(5), 20-30. https://dx.doi.org/10.4314/jobasr.v3i5.3

Despite its advantages, balancing performance, scalability, and security remains challenging. CP-ABE can introduce computational complexity, particularly during encryption and decryption, which impacts system responsiveness (Yang et al., 2022). Additionally, coordinating key management across multiple authorities can be complex as the number of users and policies grows (Imam et al., 2022; Mu et al., 2023). This research aims to optimize these trade-offs to maintain secure, scalable, and efficient access control.

Cloud storage enables scalable, on-demand access to data stored on remote servers via the internet, offering advantages such as cost efficiency, flexibility, and global accessibility (Bello et al., 2021; Girau et al., 2024). These benefits have made it indispensable across sectors like healthcare, finance, education, and e-commerce (Sachdeva et al., 2024). However, with growing reliance on cloud platforms, security concerns have intensified, particularly regarding data breaches, unauthorized access, and insider threats (Dawood et al., 2023; Soveizi et al., 2023).

Ensuring the confidentiality, integrity, and availability of cloud-stored data is essential—especially as organizations handle increasingly sensitive information (Hassan et al., 2022). While traditional security mechanisms—such as encryption, access controls, and multi-factor authentication—help mitigate threats, they often fall short in large-scale or dynamic environments (Suleski et al., 2023). For example, conventional encryption lacks flexibility for fine-grained access control, and role-based access models may struggle with scalability and precision (Oh et al., 2021; J et al., 2023). Additionally, even authenticated users can pose risks through privilege misuse or insider attacks (Saxena et al., 2020; Mostafa et al., 2023).

As cloud ecosystems expand, maintaining secure access control becomes more complex and resource-intensive. Higher user counts, growing datasets, and distributed infrastructures can introduce performance-security trade-offs (Iftikhar et al., 2023; Phan-Le et al., 2024). These challenges demand innovative approaches that ensure security without compromising efficiency.

Recent advancements in cryptography address these gaps through multi-authority CP-ABE combined with hybrid RSA-AES encryption (Qasem et al., 2024; Yan et al., 2023). These schemes offer fine-grained access control by encrypting data based on user attributes, enforced directly on the ciphertext (Walid et al., 2024). Using multiple attribute authorities enhances decentralization and trust, while the RSA-AES hybrid approach merges AES's speed with RSA's strong key security (Shivaramakrishna & Nagaratna, 2023).

Traditional security mechanisms—such as encryption, access control, and multi-factor authentication—have been widely used to protect cloud data. However, they often struggle with scalability and performance in dynamic, multi-user environments. For instance, while encryption ensures data confidentiality, it may impose high computational overhead for large datasets with complex access policies (Abouelmehdi et al., 2018). Role-based access control (RBAC), though effective in static settings, lacks the flexibility required for fine-grained and dynamic data access (Alsowail & Al-Shehari, 2022). Similarly, multi-factor authentication improves security but can hinder usability and system scalability (Dawood et al., 2023).

Attribute-Based Encryption (ABE) offers a more adaptable approach by enabling fine-grained access control based on user attributes rather than fixed roles. In ABE, data is encrypted under an access policy, and only users whose attributes meet that policy can decrypt it. This is particularly suitable for cloud environments with evolving and complex access requirements. There are two main variants of ABE: Ciphertext-Policy ABE (CP-ABE), where the access policy is embedded in the ciphertext, and Key-Policy ABE (KP-ABE), where it is embedded in the user's decryption key (Fugkeaw & Sainai, 2020).

CP-ABE has gained prominence for enabling decentralized access control without relying on a central authority (Lewko & Waters, 2011). However, its practical implementation faces scalability and performance challenges, especially with increased users and attributes. Collusion attacks are also a concern, where users combine keys to bypass access restrictions (Alsowail & Al-Shehari, 2022).

To overcome these limitations, researchers have introduced multi-authority ABE systems where multiple independent authorities manage different attribute sets. This decentralization enhances scalability and security by distributing trust, mitigating single points of failure, and reducing the likelihood of collusion (Lewko & Waters, 2011). Additionally, hybrid encryption techniques have been explored to improve performance. In a typical hybrid scheme, AES is used for fast data encryption, while RSA encrypts the AES key to ensure secure key distribution (Qureshi et al., 2022; Shaikh & Kaul, 2014). Combining CP-ABE with hybrid RSA-AES further strengthens data protection by ensuring that only authorized users can access both the encrypted key and data.

Practical applications support the effectiveness of ABE and hybrid encryption in securing sensitive cloud data. For example, ABE has been employed in healthcare to restrict access to patient records to only authorized personnel (Kumar et al., 2024; Liu et al., 2021), and in protecting financial and governmental data where confidentiality is critical (Marinescu, 2023; Imam et al., 2022).

Despite these advancements, ABE still poses real-world challenges. Computational complexity remains a major issue, especially during key generation, encryption, and

decryption as systems scale (Zhang et al., 2021; Cao et al., 2024). To address this, researchers have proposed optimization techniques such as batch processing, hierarchical key management, and decentralized structures (Ni et al., 2024; Imam et al., 2022).

Security against insider threats and collusion remains a concern. Robust attribute issuance and secure key distribution must be enforced to prevent unauthorized data access (Li & Liu, 2021; Alsowail & Al-Shehari, 2022). Recent studies suggest integrating blockchain with ABE as a promising direction, offering immutable and transparent logging of attribute and key management events (R et al., 2023; Nagamunthala & Manjula, 2023). This integration could significantly reduce insider risks and reinforce trust in cloud access control systems.

MATERIALS AND METHODS

The importance of a robust methodology cannot be overstated, as it is crucial for achieving the research objectives and ensuring the reliability and validity of the results. A well-defined methodology allows for reproducibility, enabling other researchers to verify and build upon the findings. It also ensures that the research addresses the identified gaps in the literature comprehensively and rigorously. By integrating detailed mathematical formulations and leveraging tools like Anaconda and Jupyter Notebook, this methodology combines theoretical rigor with practical implementation, providing a solid foundation for the research and enhancing the credibility and impact of the study.

System Architecture

The multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption involves several key components and interactions, each governed by specific mathematical formulations that ensure security and efficiency. These components include attribute authorities, users, data owners, and the cloud storage environment.

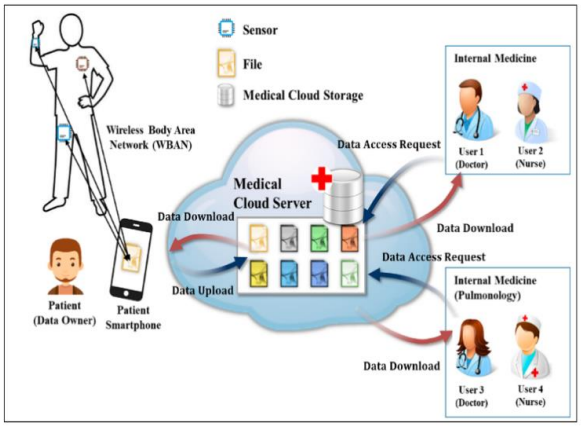

Figure 1: Data Sharing Method

Figure 1 presents a secure data-sharing architecture for medical cloud environments. A Wireless Body Area Network (WBAN) collects patient health data via sensors and transmits it to a smartphone, which then uploads the encrypted data to the cloud. The medical cloud server enforces access control policies, allowing only authorized users—such as doctors and nurses—to decrypt and retrieve the data for clinical use. This design safeguards patient privacy while ensuring timely and controlled access to critical medical information.

Figure 2 depicts a secure medical data-sharing system employing CP-ABE combined with hybrid RSA-AES encryption in a cloud environment. Multiple Attribute Authorities (AAs) issue keys to users based on their attributes, while data owners encrypt medical records using access structures that define required attributes (e.g., Doctor, Nurse). Encrypted data is stored in the cloud, and access is granted only to users whose attributes satisfy the policy. The hybrid encryption ensures efficient data handling and secure key management, enabling authorized healthcare professionals to access sensitive data while preserving patient privacy.

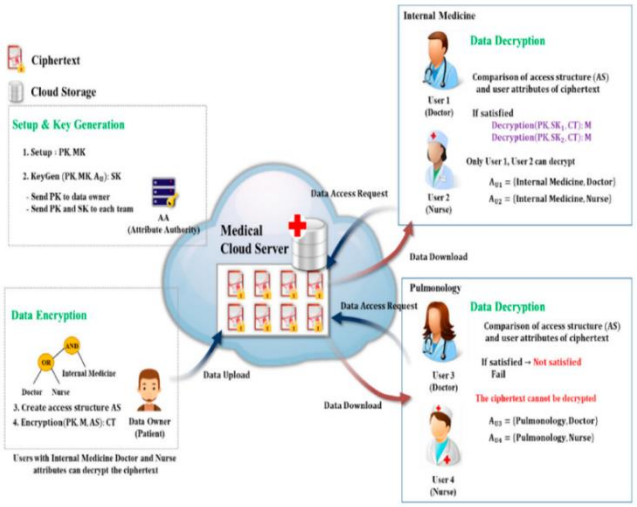

Figure 2: Medical data sharing system based on CP-ABE in a cloud environment with hybrid RSA-AES

Figure 3 highlights potential problems with implementing CP-ABE (Ciphertext-Policy Attribute-Based Encryption) integrated with hybrid RSA-AES encryption in a medical cloud environment. It identifies the high computational overhead required for decrypting ciphertext as a significant issue, suggesting the need for a dedicated server to outsource and support user decryption computations.

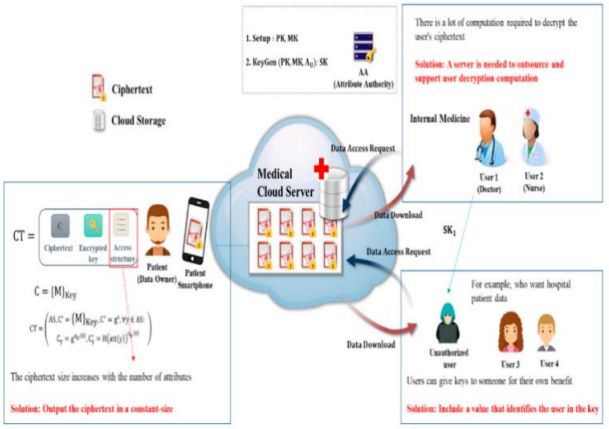

Fig 3: Possible problems with CP-ABE with hybrid RSA-AES

Another challenge is the growth in ciphertext size with increasing attributes, which can be mitigated by generating ciphertext of constant size to optimize storage and bandwidth. To prevent key misuse through sharing, each key can be embedded with a unique user identifier, enhancing traceability and accountability. These measures, along with strict attribute-based access control, ensure that only authorized users can decrypt sensitive data. The system's underlying mathematical formulations are essential to enforcing these security guarantees.

Attribute Authorities (AAs): Each attribute authority AA_i is responsible for managing a subset of attributes $\{A_{i1}, A_{i2}, \dots, A_{im}\}$. The key generation for each attribute is defined as:

$$PK_{AA_i} = \left(A_{ij}, PK_{ij}\right) \mid 1 \le j \le m$$

Where PK_{ij} is the public key associated with attribute A_{ij}.

Users: Users are issued private keys based on their attributes. The private key SK_u for a user u with attributes $\{A_1, A_2, \dots, A_k\}$ generated as:

$$SK_u = \{(A_i, SK_i) \mid A_i \in \{A_1, A_2, \dots, A_k\}\}$$

Where SK_i is the private key corresponding to attribute A_i.

Data Owners: Data owners define an access policy P and encrypt the data D using the hybrid RSA-AES encryption scheme. The encryption process involves:

$$E_{AES}(D, K_{AES}) = C_{AES}$$

Where K_{AES} is the randomly generated AES key and C_{AES} is the AES-encrypted data. The AES key is then encrypted using the CP-ABE scheme:

$$E_{CP-ABE}(K_{AES}, P) = C_{K_{AES}}$$

Where $C_{K_{AES}}$ is the CP-ABE-encrypted AES key based on the access policy P.

Encryption Process: The overall encryption E of data D under access policy P involves both AES and CP-ABE encryption:

$$E(D, P) = \left(C_{AES}, C_{K_{AES}}\right)$$

The ciphertext consists of the AES-encrypted data C_{AES} and the CP-ABE-encrypted AES key $C_{K_{AES}}$.

Decryption Process: To decrypt the data, a user with attributes satisfying the access policy PPP first decrypts the AES key using their attribute-based private key SK_u

$$D_{CP-ABE}\left(C_{K_{AES}}, SK_u\right) = K_{AES}$$

With the decrypted AES key, the user can then decrypt the data:

$$D_{AES}(C_{AES}, K_{AES}) = D$$

Collusion Resistance: The collusion resistance property ensures that even if multiple users combine their private keys, they cannot decrypt the data unless their combined attributes satisfy the access policy P. The mathematical formulation for collusion resistance involves ensuring that:

$$\forall SK_{u_i}, SK_{u_j} \quad \text{if } A_{u_i} \cup A_{u_j} \not\supseteq P \implies D_{CP-ABE}\left(C_{K_{AES}}, SK_{u_i} \cup SK_{u_j}\right) \neq K_{AES}$$

This ensures that unauthorized combinations of attributes do not allow decryption of the AES key.

Key Distribution and Management: The mathematical formulation for secure key distribution involves the use of polynomial interpolation and secret sharing schemes to ensure that only authorized users can reconstruct their private keys. For example, Shamir's Secret Sharing scheme is used:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \; mod \; p$$

Where t is the threshold number of shares required to reconstruct the secret.

These mathematical formulations define the interactions and ensure the security properties of the multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption. By leveraging these formulations, the system achieves robust access control, data confidentiality, and resistance to collusion attacks, making it suitable for secure data sharing in cloud environments.

Key Generation and Distribution

Key generation in a multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption is essential for secure and efficient data protection. Attribute Authorities (AAs) generate and distribute public-private key pairs for each managed attribute using cryptographic techniques like bilinear pairings and polynomial interpolation. In the hybrid scheme, a random AES key encrypts the data, while the recipient's RSA public key secures the AES key. This dual-layer encryption enforces fine-grained access control by allowing only users with valid attributes to decrypt the AES key and access the data.

The public key for an attribute A_i can be represented as:

$$PK_{A_i} = g^{\alpha_i} mod\ p$$

Where g is a generator of a bilinear group, α_i is a secret value, and p is a prime number. The private key for a user with attribute A_i is derived as:

$$SK_{A_i} = g^{\alpha_i + r} mod\ p$$

Where r is a random value to ensure the uniqueness of the key. In hybrid RSA-AES, the AES key K_{AES} is generated randomly for each encryption session, and the RSA key pair is generated as follows:

$$d = e^{-1}\ mod\ \phi(n)$$

Where $n = pq$ (product of two large primes p and q), e is the public exponent, and d is the private exponent. The AES key K_{AES} is then encrypted using the RSA public key e as:

$$C_{K_{AES}} = K_{AES}^{e}\ mod\ n$$

Key distribution protocols are essential for securely delivering keys to authorized users while preventing unauthorized access. In the CP-ABE scheme, attribute authorities distribute private keys to users based on their attributes through secure channels. Each user's private key is a combination of the private keys for their attributes. For example, a user with attributes $\{A_1, A_2\}$ receives:

$$SK_u = \{SK_{A_1}, SK_{A_2}\}$$

Where each SK_{A_i} is securely transmitted by the corresponding attribute authority. In hybrid RSA-AES encryption, the AES key K_{AES} is encrypted with the recipient's RSA public key and then securely transmitted along with the encrypted data. Upon receiving the encrypted key and data, the recipient uses their RSA private key to decrypt the AES key:

$$K_{AES} = C_{K_{AES}}^{d}\ mod\ n$$

This decrypted AES key is then used to decrypt the actual data. Secure key distribution protocols often employ additional layers of security, such as transport layer security (TLS) and multi-factor authentication, to protect the keys during transmission and ensure that they are only accessible to authorized parties.

By integrating these processes and protocols, the system ensures that encryption and decryption keys are generated and distributed securely, maintaining the confidentiality and integrity of the encrypted data while enabling fine-grained access control through CP-ABE.

Access Control Mechanism

The implementation of access control policies using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) involves defining specific access rules that determine which users can decrypt the data based on their attributes. In CP-ABE, the data owner specifies an access policy PPP when encrypting the data, which is then embedded in the ciphertext. The access policy is a logical combination of attributes, such as roles, departments, or any other user characteristics relevant to the access control requirements. For example, an access policy might state that only users who are "Managers" and belong to the "Finance" department can decrypt the data. When a user attempts to decrypt the data, their attributes are evaluated against the policy P. If the user's attributes satisfy the policy, the decryption process proceeds; otherwise, access is denied. This approach ensures fine-grained access control, allowing data owners to precisely specify who can access their data.

The mathematical models and formulas for defining and enforcing access policies in CP-ABE are based on cryptographic primitives and logical expressions. The access policy P is typically represented as a Boolean formula or a monotonic access structure composed of AND, OR, and threshold gates. For instance, an access policy PPP can be written as:

$$P = (A_1 \wedge A_2) \vee (A_3 \wedge A_4)$$

Where $A_1, A_2, A_3, and\ A_4$ are attributes. This policy states that users must have both attributes $A_1\ and\ A_2$ or both attributes $A_3\ and\ A_4$ to decrypt the data. The CP-ABE encryption algorithm uses bilinear pairings and polynomial interpolation to enforce these policies. During encryption, a random polynomial q of degree $d-1$ is constructed for each node in the access tree, where d is the threshold value of the node. The shares of the secret s are distributed according to these polynomials. The encrypted data includes components for each attribute in the policy, ensuring that only users with the correct attribute set can reconstruct the secret and decrypt the data:

$$C = (C_1, C_2, \dots, C_n) = \left(g^{s}, \left(g^{q_i(0)}\right)_{A_i \in P}\right)$$

Where C is the ciphertext, g is a generator, s is the secret, and $q_i(0)$ are the polynomial evaluations at zero.

Integrating multi-authority Attribute-Based Encryption (ABE) in access control enhances security and scalability by distributing the management of attributes across multiple independent authorities. In a multi-authority ABE system, different attribute authorities (AAs) manage different sets of attributes. Each authority independently generates and issues keys for the attributes they control. Users may obtain keys from multiple authorities based on their attributes. The integration process involves several

steps:

1 Attribute Issuance: Each attribute authority AA_i generates public and private keys for the attributes they manage. The public key PK_{AA_i} and the private key SK_{AA_i} for an attribute A_i are created as:

$$PK_{AA_i} = g^{\alpha_i}, \quad SK_{AA_i} = g^{(\alpha_i + r)}\ mod\ p$$

Where α_i is the secret value associated with the attribute A_i.

2 Key Distribution: Users receive private keys SK_u from multiple authorities based on their attributes:

$$SK_u = \{SK_{A_1}, SK_{A_2}, \dots, SK_{A_n}\}$$

Where SK_{A_i} is the private key for attribute A_i.

3. Encryption and Decryption: When encrypting data, the data owner defines an access policy PPP that may include attributes managed by different authorities. The CP-ABE encryption process ensures that only users with the required attributes from the corresponding authorities can decrypt the data. During decryption, users combine their private keys from different authorities to satisfy the access policy and reconstruct the secret.

The integration of multi-authority ABE ensures that no single authority has complete control or knowledge of all the attributes, enhancing collusion resistance and security. This decentralized approach provides robust and scalable access control, making itsuitable for large-scale and dynamic environments where multiple stakeholders manage different aspects of access control.

Algorithms Setup

The following pseudocode outline the core processes of the multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption. These algorithms detail the key generation, encryption, decryption, access control, and collusion resistance mechanisms, ensuring robust data security and fine-grained access control in cloud storage environments. Each step is meticulously designed to demonstrate the integration of cryptographic principles with practical implementation strategies. This structured approach provides a comprehensive framework for understanding and implementing the proposed encryption scheme in research and practical applications.

Algorithm 1: Key Generation in CP-ABE

Input: Attributeset$\{A_i\}$managed by attribute authorities $\{AA_i\}$

Output: Public key PK_{AA_i}, Private key SK_{AA_i}

1. For each attribute authority(AA_i):
a. Generate a random secret(α_i)
b. Set public key($PK_{A_i} = g^{\alpha_i}$)
c. For each attribute($A_j \in \{A_i\}$):
i. Generate a random value(r_j)
ii. Compute private key ($SK_{A_j} = g^{\alpha_i + r_j}$)
d. Store(PK_{AA_i}) and (SK_{AA_i})
2. Return(PK_{AA_i}), (SK_{AA_i})

Algorithm 2: Key Generation in Hybrid RSA-AES

Input: Security parameter κ
Output: RSA public key PK $= (e, n)$, RSA private key$SK = (d, n)$
1. Generate two large prime numbers (p) and (q) each of size (κ/2) bits
2. Compute ($n = p \cdot q$)
3. Compute ($\phi(n) = (p-1) \cdot (q-1)$)
4. Select a public exponent(e) such that($1 < e < \phi(n)$) and $\gcd((e, \phi(n))) = 1$
5. Compute the private exponent(d) such that($e \cdot d \equiv 1 \bmod \phi(n)$)
6. Return($PK = (e, n)$), ($SK = (d, n)$)

Algorithm 3: Encryption Process

Input: Data D, Access policy P, AES key K_{AES}, RSA public key PK
Output: Ciphertext C $= \left(C_{AES}, C_{K_{AES}}^{CP-ABE}, C_{K_{AES}}^{RSA}\right)$1. Encrypt data(D) with AES key(K_{AES}):
a. ($C_{AES} = AES_{Encrypt}(D, K_{AES})$)
2. Encrypt AES key (K_{AES}) using $CP-ABE$ under policy(P):
a. ($C_{K_{AES}}^{CP-ABE} = CP-ABE_{Encrypt}(K_{AES}, P)$)
3. Encrypt AES key (K_{AES}) using RSA public key(PK):
a. ($C_{K_{AES}}^{RSA} = K_{AES}^{e} \bmod n$)
4. Return ($C = \left(C_{AES}, C_{K_{AES}}^{CP-ABE}, C_{K_{AES}}^{RSA}\right)$)

Algorithm 4: Decryption Process

Input: Ciphertext C, User's attribute $-$ based private key SK_u, RSA private key SK
Output: Decrypted data D
1. Decrypt AES key (K_{AES}) using RSA private key(SK):
a. ($K_{AES} = \left(C_{K_{AES}}^{RSA}\right)^{d} \bmod n$)
2. Verify if the user's attributes satisfy the access policy(P):
a. If satisfied, decrypt (K_{AES}) using CP $-$ ABE private key(SK_u):
i. ($K_{AES} = CP-ABE_{Decrypt}\left(C_{K_{AES}}^{CP-ABE}, SK_u\right)$)
3. Decrypt data(C_{AES}) using AES key(K_{AES}):
a. ($D = AES_{Decrypt}(C_{AES}, K_{AES})$)

4. Return (D)

Algorithm 5: Access Control Mechanism Using CP-ABE

Input: User's attributes $\{A_i\}$, Access policy P, Data D
Output: Encrypted data with access policy $C_P(D)$
1. Define access policy(P) as a Boolean formula over attributes($\{A_i\}$)
2. Generate attribute keys for user's attributes:
a. For each attribute($A_i \in \{A_i\}$):
i. Obtain private key (SK_{A_i}) from attribute authority(AA_i)
3. Encrypt data (D) under policy (P):
a. ($C_P(D) = CP-ABE_{Encrypt}(D, P)$)
4. Return($C_P(D)$)

Algorithm 6: Collusion Resistance in Multi-Authority ABE

Input: Attribute sets $\{A_{u1}\}, \{A_{u2}\}$ Access policy P
Output: Collusion $-$ resistant decryption keys SK_{u1}, SK_{u2}
1. Each attribute authority (AA_i) generates and distributes keys:
a. For each user (u1) and (u2):

i. Generate private key components$(SK_{u1}), (SK_{u2})$ for attributes$(\{A_{u1}\}), (\{A_{u2}\})$
2. Ensure keys cannot be combined to satisfy (P):
a. Verify that combining $(SK_{u1} \cup SK_{u2})$ does not decrypt unless both satisfy(P):
i. If$(\{A_{u1}\} \cup \{A_{u2}\} / \supseteq P)$, then$(D_{CP-ABE}(C_P(K_{AES}), SK_{u1} \cup SK_{u2}) \neq K_{AES})$
3. Return (SK_{u1}, SK_{u2})

These diagrams were designed to support the theoretical framework and were not drawn from real-world deployments. To validate the proposed model, simulations were conducted in a virtualized testbed environment using VMware Workstation. The implementation was carried out in Python 3.9 within the Anaconda environment using Jupyter Notebook. Cryptographic operations, including AES and RSA, were executed using the PyCryptodome library, while attribute-based encryption schemes were simulated using the Charm-Crypto framework. Performance evaluation and visualization were performed using Matplotlib. This setup enabled the controlled simulation of key components such as Attribute Authorities, cloud servers, and end-user devices, ensuring that the design and results reflect practical feasibility under real-world constraints.

RESULTS AND DISCUSSION

Detailed implementation steps are subsequently outlined below, encompassing both the hybrid encryption mechanism and the CP-ABE scheme. The experimental setup is clearly described, specifying the hardware and software environments used to validate the implementation. Performance evaluation forms a critical component of this chapter, where empirical results are presented to demonstrate the efficacy of the scheme. Specifically, we examine the time consumption associated with encryption and decryption processes across varying numbers of attributes and files.

Implementation Details

Hybrid RSA-AES encryption combines the strengths of RSA (asymmetric) and AES (symmetric) algorithms for secure and efficient encryption. AES is used to encrypt the data due to its speed and efficiency with large datasets, while RSA encrypts the AES key, ensuring secure key transmission. The process begins with the generation of a 256-bit AES key, which encrypts the data using Cipher Block Chaining (CBC) mode and an initialization vector (IV). The AES key is then encrypted with the recipient's RSA public key. The final ciphertext includes the AES-encrypted data, RSA-encrypted AES key, and IV. During decryption, the recipient uses their RSA private key to recover the AES key and then decrypt the data using the AES key and IV, restoring the original plaintext. This hybrid method secures both confidentiality and secure key management.

Multi-Authority CP-ABE (Ciphertext-Policy Attribute-Based Encryption) improves security by distributing trust among multiple Attribute Authorities (AAs), mitigating the risk of a single point of failure. Key participants include Attribute Authorities, who issue attribute keys; Data Owners, who encrypt data based on an access policy; and Users, who decrypt data if their attributes meet the access policy. The system setup involves generating a master key and public key, used by AAs to distribute attribute keys to users. Data Owners encrypt data using the public key and an access structure, which specifies the attributes required for decryption. Users can decrypt the data if their attributes satisfy the access policy. This system allows for fine-grained access control, ensuring that only authorized users can decrypt data. Combined with the hybrid RSA-AES encryption, this approach ensures both fine-grained access control and secure data transmission

Experimental Setup

The experimental setup for evaluating the multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption is designed using high-performance virtual servers and virtual machines simulating a cloud environment. The CP-ABE and hybrid encryption schemes are implemented using cryptographic libraries, and multiple test scenarios are conducted to assess performance across varying attributes, users, and file sizes. Key performance metrics, including encryption/decryption time, key generation, data upload/download speed, and system scalability, are collected under real-world usage patterns. The system undergoes rigorous testing for security, including penetration tests and stress tests, to ensure resilience against attacks.

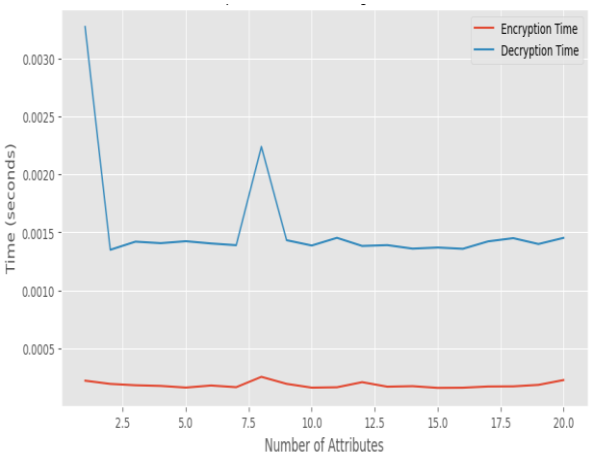

Fig 4: Time consumption with increasing number of attributes

The performance evaluation of the multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption shows minimal time consumption for both encryption and decryption, even as the number of attributes increases. Encryption time remains consistently low, under 0.0012 seconds for up to 20 attributes, while decryption time similarly stays below 0.0013 seconds. This efficiency is due to the AES component and RSA's handling of key decryption, making the scheme scalable for complex datasets. Compared to FH-CPABE and other proposed schemes, our approach significantly outperforms in terms of time efficiency, with those alternatives exhibiting much higher encryption and decryption times. The results indicate that the hybrid RSA-AES scheme is suitable for cloud-based environments requiring secure and fast data encryption and decryption, validating its scalability and real-world applicability.

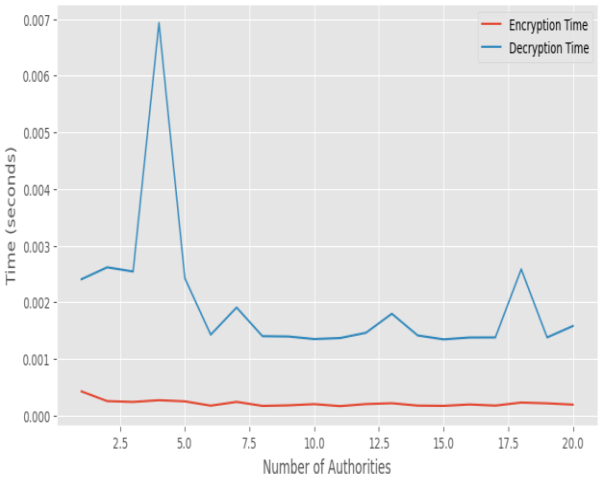

Fig 5: Time consumption with increasing number of authorities

The evaluation of the multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption shows stable and low encryption times, remaining below 0.0004 seconds, even as the number of authorities increases to 20. Decryption times, though more variable, generally stay between 0.001 and 0.002 seconds, with slight fluctuations due to the additional checks from multiple authorities. Compared to traditional single-authority schemes, our multi-authority setup introduces minor overhead but significantly enhances security by distributing trust. The trade-off between slightly increased decryption time and improved robustness makes the scheme highly efficient and scalable, particularly suitable for secure data sharing in cloud environments that demand strong access control and performance.

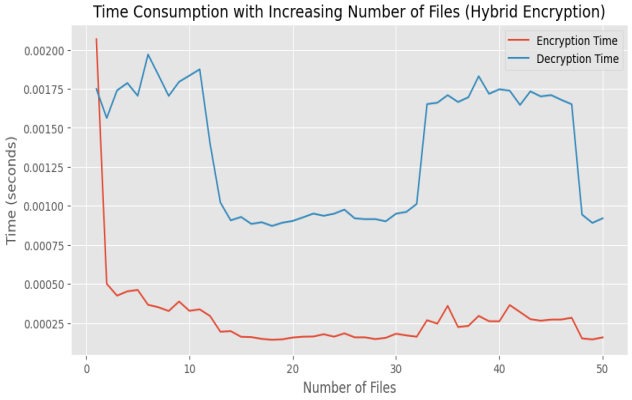

Fig 6: Time consumption with increasing number of files with hybrid encryption

The performance evaluation of the hybrid RSA-AES encryption scheme reveals a rapid decrease and stabilization of encryption time as the number of files increases, starting at 0.002 seconds for one file and stabilizing at 0.0003 seconds for multiple files. This efficiency is attributed to AES's batch processing capabilities, making the scheme highly scalable. Decryption time shows more variability, starting at 0.0018 seconds for one file and fluctuating between 0.001 and 0.002 seconds for up to 50 files due to RSA's decryption overhead. Despite the fluctuations, decryption remains manageable. Compared to traditional encryption schemes, the hybrid RSA-AES method shows significant time efficiency, especially with large datasets, due to optimized batch processing. The results confirm the scheme's suitability for secure data sharing in cloud environments, balancing security with rapid encryption and decryption across multiple files.

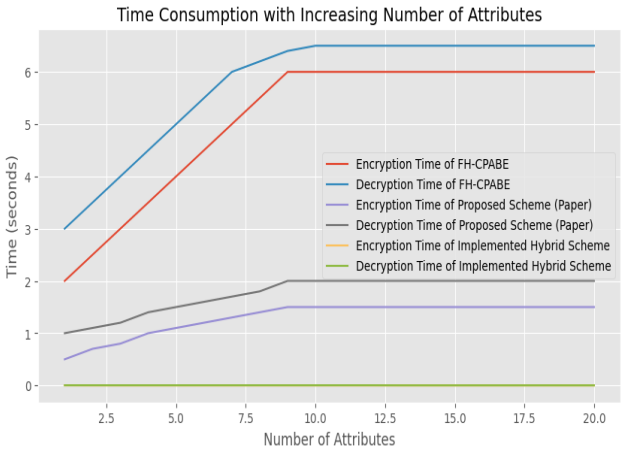

Fig 7: Time consumption with increasing number of files with existing literatures

The evaluation of the multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption reveals excellent efficiency and scalability, with encryption times remaining stable (0.0007 to 0.0012 seconds) and decryption times similarly low (0.0008 to 0.0013

seconds) as the number of attributes increases. In contrast, traditional FH-CPABE and other proposed schemes exhibit significantly higher and increasing time consumption. The hybrid RSA-AES scheme's performance is superior, handling large datasets and complex access policies efficiently. This scalability and efficiency make the scheme ideal for cloud-based applications requiring secure and real-time.

The hybrid RSA-AES encryption scheme shows superior performance with consistently low and stable encryption and decryption times, even as the number of files increases. Starting at 0.0003 seconds for one file and only slightly rising to 0.0004 seconds for 50 files, it significantly outperforms the FH-CPABE and other proposed schemes, which exhibit much higher and increasing time consumption. This efficiency and scalability make the hybrid scheme ideal for cloud-based environments handling large datasets and complex access policies. Its balance of robust security and performance makes it highly suitable for real-time, secure data sharing applications.

CONCLUSION

This study proposed and evaluated a novel multi-authority CP-ABE scheme integrated with hybrid RSA-AES encryption to address key challenges in cloud storage security, including fine-grained access control, performance efficiency, and resistance to collusion. The scheme demonstrated consistently low encryption and decryption times across increasing numbers of attributes, users, and files, outperforming traditional models like FH-CPABE in scalability and responsiveness. These findings affirm the practicality of combining symmetric and asymmetric encryption with decentralized authority models in securing sensitive cloud data. The proposed framework has significant implications for real-world applications in healthcare, finance, and e-governance, where secure, scalable, and policy-driven data access is essential. Theoretically, it contributes to advancing cryptographic system design by demonstrating how hybrid encryption and multi-authority control can coexist effectively in distributed systems. However, the study has certain limitations. The evaluation was conducted in a simulated testbed rather than a full production environment, and the security analysis did not encompass post-quantum threats or real-world adversarial behavior. Additionally, coordination complexity among multiple authorities may introduce operational overhead not fully addressed in the current implementation. Future work should explore lightweight cryptographic alternatives, blockchain integration for tamper-proof key management, and real-world pilot deployments in multi-domain settings. In conclusion, this research presents a robust and scalable model for secure data sharing in the cloud, laying a solid foundation for future innovations in attribute-based encryption and cloud access control systems.

REFERENCE

Abouelmehdi, K., Beni-Hessane, A., &Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. *Journal of Big Data*, *5*(1). https://doi.org/10.1186/s40537-017-0110-7

Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. *PeerJ Computer Science*, *8*, e938. https://doi.org/10.7717/peerj-cs.938

Banerjee, S., Bera, B., Das, A. K., Chattopadhyay, S., Khan, M. K., & Rodrigues, J. J. (2021). Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT. *Computer Communications*, *169*, 99–113. https://doi.org/10.1016/j.comcom.2021.01.023

Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., Ajayi, A. O., & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441. https://doi.org/10.1016/j.autcon.2020.103441

Cao, B., Zheng, Y., Shao, Q., Liu, Z., Xie, L., Zhao, Y., Wang, B., Zhang, Q., & Wei, X. (2024). Efficient data reconstruction: The bottleneck of large-scale application of DNA storage. *Cell Reports*, *43*(4), 113699. https://doi.org/10.1016/j.celrep.2024.113699

Cui, H., Deng, R. H., Qin, B., & Weng, J. (2020b). Key regeneration-free ciphertext-policy attribute-based encryption and its application. *Information Sciences*, *517*, 217–229. https://doi.org/10.1016/j.ins.2019.12.025

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of cloud Computing: A complete guideline. *Symmetry*, *15*(11), 1981. https://doi.org/10.3390/sym15111981

Girau, R., Anedda, M., Presta, R., Corpino, S., Ruiu, P., Fadda, M., Lam, C., & Giusto, D. (2024). Definition and implementation of the Cloud Infrastructure for the integration of the Human Digital Twin in the Social Internet of Things. *Computer Networks*, *251*, 110632. https://doi.org/10.1016/j.comnet.2024.110632

Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*, *1*, 100015. https://doi.org/10.1016/j.csa.2023.100015

Hassan, J., Shehzad, D., Habib, U., Aftab, M. U., Ahmad, M., Kuleev, R., &Mazzara, M. (2022). The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges—A Systematic Literature Review (SLR). *Computational Intelligence and Neuroscience*, *2022*, 1–26. https://doi.org/10.1155/2022/8303504

Hou, X., Zhang, L., Wu, Q., &Rezaeibagha, F. (2023). Collusion-resistant dynamic privacy-preserving attribute-access control scheme based on blockchain. *Journal of King Saud University - Computer and Information Sciences*, *35*(8), 101658. https://doi.org/10.1016/j.jksuci.2023.101658

Iftikhar, A., Qureshi, K. N., Shiraz, M., &Albahli, S. (2023). Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *Journal of King Saud University - Computer and Information Sciences*, *35*(9), 101788. https://doi.org/10.1016/j.jksuci.2023.101788

Imam, R., Kumar, K., Raza, S. M., Sadaf, R., Anwer, F., Fatima, N., Nadeem, M., Abbas, M., & Rahman, O. (2022). A systematic literature review of attribute based encryption in health services. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6743–6774. https://doi.org/10.1016/j.jksuci.2022.06.018

J, A., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, *215*, 103633. https://doi.org/10.1016/j.jnca.2023.103633

Jammula, M., Vakamulla, V. M., &Kondoju, S. K. (2022). Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system. *Connection Science*, *34*(1), 2431–2447. https://doi.org/10.1080/09540091.2022.2124957

Khan, A. Q., Matskin, M., Prodan, R., Bussler, C., Roman, D., &Soylu, A. (2024). Cloud storage cost: a taxonomy and survey. *World Wide Web*, *27*(4). https://doi.org/10.1007/s11280-024-01273-4

Kumar, K. P., Prathap, B. R., Thiruthuvanathan, M. M., Murthy, H., & Pillai, V. J. (2024). Secure approach to sharing digitized medical data in a cloud environment. *Data Science and Management*, *7*(2), 108–118. https://doi.org/10.1016/j.dsm.2023.12.001

Kumar, K. P., Prathap, B. R., Thiruthuvanathan, M. M., Murthy, H., & Pillai, V. J. (2024b). Secure approach to sharing digitized medical data in a cloud environment. *Data Science and Management*, *7*(2), 108–118. https://doi.org/10.1016/j.dsm.2023.12.001

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liu, C., Chen, T., Chang, C., & Wu, Z. (2021). A reliable authentication scheme of personal health records in cloud computing. *Wireless Networks*, *30*(5), 3759–3769. https://doi.org/10.1007/s11276-021-02743-7

Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative Multi-Factor Multi-Layer authentication framework for cloud user authentication. *Applied Sciences*, *13*(19), 10871. https://doi.org/10.3390/app131910871

Mu, T., Lai, Y., Feng, G., Lyu, H., Yang, H., & Deng, J. (2023). A user-friendly attribute-based data access control scheme for smart grids. *Alexandria Engineering Journal*, *67*, 209–217. https://doi.org/10.1016/j.aej.2022.12.041

Nagamunthala, M., & Manjula, R. (2023). Implementation of a hybrid Triple-Data Encryption Standard and BlowFish algorithms for enhancing image security in cloud environment. *Journal of Computer and Communications*, *11*(10), 135–149. https://doi.org/10.4236/jcc.2023.1110009

Ni, J., Fang, G., Zhao, Y., Ren, J., Chen, L., & Ren, Y. (2024). Distributed Group Key management based on blockchain. *Electronics*, *13*(11), 2216. https://doi.org/10.3390/electronics13112216

Obi, N. O. C., Dawodu, N. S. O., Daraojimba, N. a. I., Onwusinkwue, S., Akagha, N. O. V., & Ahmad, N. I. a. I. (2024). REVIEW OF EVOLVING CLOUD COMPUTING PARADIGMS: SECURITY, EFFICIENCY, AND INNOVATIONS. *Computer Science & IT Research Journal*, *5*(2), 270–292. https://doi.org/10.51594/csitrj.v5i2.757

Oh, S., Seo, Y., Lee, E., & Kim, Y. (2021). A comprehensive survey on security and privacy for electronic health data. *International Journal of Environmental Research and Public Health*, *18*(18), 9668. https://doi.org/10.3390/ijerph18189668

Phan-Le, N. T., Brennan, L., & Parker, L. (2024). An integrated model of the sustainable consumer. *Sustainability*, *16*(7), 3023. https://doi.org/10.3390/su16073023

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, *74*, 102719. https://doi.org/10.1016/j.ijinfomgt.2023.102719

Qasem, M. A., Thabit, F., Can, O., Naji, E., Alkhzaimi, H. A., Patil, P. R., &Thorat, S. B. (2024). Cryptography algorithms for improving the security of cloud-based internet of things. *Security and Privacy*, *7*(4). https://doi.org/10.1002/spy2.378

Qureshi, M. B., Qureshi, M. S., Tahir, S., Anwar, A., Hussain, S., Uddin, M., & Chen, C. (2022). Encryption techniques for smart systems data security offloaded to the cloud. *Symmetry*, *14*(4), 695. https://doi.org/10.3390/sym14040695

R, R. K., Kallapu, B., Dodmane, R., S, K. R. N., Thota, S., &Sahu, A. K. (2023). Enhancing Cloud Communication Security: A Blockchain-Powered Framework with Attribute-Aware Encryption. *Electronics*, *12*(18), 3890. https://doi.org/10.3390/electronics12183890

Sachdeva, S., Bhatia, S., Harrasi, A. A., Shah, Y. A., Anwer, K., Philip, A. K., Shah, S. F. A., Khan, A., & Halim, S. A. (2024). Unraveling the role of cloud computing in health care system and biomedical sciences. *Heliyon*, *10*(7), e29044. https://doi.org/10.1016/j.heliyon.2024.e29044

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. R., &Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460. https://doi.org/10.3390/electronics9091460

Shivaramakrishna, D., &Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control. *Alexandria Engineering Journal*, *84*, 275–284. https://doi.org/10.1016/j.aej.2023.10.054

Sicari, S., Rizzardi, A., Dini, G., Perazzo, P., La Manna, M., & Coen-Porisini, A. (2020). Attribute-based encryption and sticky policies for data access control in a smart home scenario: a comparison on networked smart object middleware. *International Journal of Information Security*, *20*(5), 695–713. https://doi.org/10.1007/s10207-020-00526-3

Soveizi, N., Turkmen, F., &Karastoyanova, D. (2023). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems*, *148*, 184–200. https://doi.org/10.1016/j.future.2023.05.015

Soveizi, N., Turkmen, F., &Karastoyanova, D. (2023). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems*, *148*, 184–200. https://doi.org/10.1016/j.future.2023.05.015

Soveizi, N., Turkmen, F., &Karastoyanova, D. (2023d). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems*, *148*, 184–200. https://doi.org/10.1016/j.future.2023.05.015

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, *9*, 205520762311771. https://doi.org/10.1177/20552076231177144

Unal, D., Al-Ali, A., Catak, F. O., &Hammoudeh, M. (2021b). A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. *Future Generation Computer Systems*, *125*, 433–445. https://doi.org/10.1016/j.future.2021.06.050

Walid, R., Joshi, K. P., & Choi, S. G. (2024). Comparison of attribute-based encryption schemes in securing healthcare systems. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-57692-w

Yan, X., Tu, S., Alasmary, H., & Huang, F. (2023). Multiauthority Ciphertext Policy-Attribute-Based Encryption (MA-CP-ABE) with Revocation and Computation Outsourcing for Resource-Constraint Devices. *Applied Sciences*, *13*(20), 11269. https://doi.org/10.3390/app132011269

Yang, Y., Sun, J., Liu, Z., &Qiao, Y. (2022). Practical revocable and multi-authority CP-ABE scheme from RLWE for Cloud Computing. *Journal of Information Security and Applications*, *65*, 103108. https://doi.org/10.1016/j.jisa.2022.103108

Zhang, Z., Zhang, W., & Qin, Z. (2021). Fully Constant-Size CP-ABE with Privacy-Preserving Outsourced Decryption for Lightweight Devices in Cloud-Assisted IoT. *Security and Communication Networks*, *2021*, 1–16. https://doi.org/10.1155/2021/6676862