Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE CLOUD DATA STORAGE USING CONTEXTUAL ENTROPIC CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

NAGA SWETHA DHULIPUDI[1], BALAJI SAVADAM[1]

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana, India

E-mail: [1]mailsforswetha@klh.edu.in, [2]balajis@klh.edu.in

ABSTRACT

Cloud computing delivers a centralized platform for data storage and commercial applications. To ensure security, the cloud system effectively manages all connected devices, applications, and data. Various existing algorithms fail to optimize the operational delay during data encryption because of ineffective key management, which affects overall security. To overcome this issue, this research proposes Contextual Entropic Ciphertext-Policy Attribute-Based Encryption (CE-CPABE) for secure cloud data storage. CE-CPABE provides improved security and flexibility for cloud data storage by applying attribute-based access control and contextual validation. Integrating entropy-based key generation ensures that every encryption and decryption process is unique and resistant to key reuse, thereby securing data access in dynamic and distributed environments. This approach enhances the integrity, confidentiality, and access efficiency of the sensitive information stored in the cloud. CE-CPABE optimizes cryptographic operations while reducing computational overhead and resource utilization in cloud environments. The experimental results show that CE-CPABE achieves an encryption time of 2.28s and a processing time of 0.62s for a data size of 30MB, which is better than that of existing methods.

Keywords: *Attribute-Based Encryption, Attribute-Based Access Control, Contextual Entropic, Cloud Computing, Secure Cloud Data Storage*

1. INTRODUCTION

Cloud computing is based on a high-bandwidth broadband infrastructure, most prominently the Internet, which remains vulnerable to a wide range of traditional security risks. This vulnerability is mainly because cloud computing introduces multiple technologies into the unity of functioning [1] [2]. It has significantly transformed the IT field by enabling virtualization and offering services such as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [3]. As a relatively new development in data technologies, cloud computing is defined as the storage of data and the development of software through a networked system of interconnected computers. Users use the Internet to design, control, and store applications and information in a cloud environment [4] [5]. Virtualization is a fundamental element of cloud computing, which is related to a programmable mechanism of physical computing resources such that various virtual computing environments operate on one shared hardware platform [6]. Data are stored in distant data centers handled by cloud services under the decentralized architecture managed by the service provider [7]. However, this information is transmitted over networks, processed, and stored externally, several security issues emerge, such as data breach, interception of information, information loss, and malicious insider threats [8]. Location transparency is a unique feature of cloud computing and a major threat to security. The lack of a clear understanding of the physical location of the data may lead to a lack of compliance with the laws pertinent to that particular country in relation to data protection, which may result in a violation. Therefore, user privacy is of primary importance to the cloud environment [9] [10].

Moreover, there are several access points to the cloud, which predispose it to more attacks that can impair the performance of an application in the future [11]. Physical protection measures also form the basis of data security, and cannot be easily obtained through cloud services. In personal cyber cloud environments, the service provider provides the required security measures virtually, regardless of whether the application has a physical

implementation [12]. The most relevant threats to cloud computing are authentication, authorization, trust, and phishing, as well as data loss and leakage [13]. Often, authentication processes are attacked in which unauthorized access requests are falsified in an attempt to enter confidential information [14]. The existing methods of cloud data security are, to some degree, based on subjective information and instincts thereby making it difficult to monitor security with basis consistencies [15] [16]. Furthermore, due to the dynamic and open nature of cloud systems, there is a high risk of inefficient resource utilization, inability to assign and retrieve resources, prioritization of users, and significant energy wastage [17]. Cryptographic mechanisms, such as encryption protocols, digital signatures, and hash functions, have been extensively used to protect sensitive data [18]. Symmetric encryption uses a similar key for encrypting and decrypting the message, whereas asymmetric algorithms use different keys [19]. Symmetric, asymmetric, or hybrid cryptographic algorithms can be used in cloud storage to apply encryption and decryption functions [20]. Although various cryptographic frameworks such as ABE, blockchain based security and hybrid encryption methods have been developed which suffer from higher computational overhead, latency and less adaptability to dynamic contents. Furthermore, most existing models lacks effective revocation and context-aware access control thereby leaving sensitive cloud data which is vulnerable to misuse thereby leading to create the need for secure and scalable encryption framework.

1.1 Aim of the research

The main aim of this research is to design and estimate the novel Contextual Entropic Ciphertext-Policy Attribute-Based Encryption (CE-CPABE) to enhance the efficiency, security and scalability of cloud data storage systems. The proposed method overcome limitations of existing cryptographic approaches through integrating contextual parameters into encryption process by entropy-based key generation to provide secure, unique and non-reusable keys. The contextual entropic denotes to the use of environmental randomness to enhance key unpredictability while the CP-ABE is an encryption where the data access is managed by policies embedded within the ciphertext.

The contributions of this research are as follows.

- The Contextual Entropic Ciphertext-Policy Attribute-Based Encryption (CE-CPABE) is proposed in this research, which integrates contextual information with traditional CPABE to create dynamic, fine-grained access control that enhances data protection against unauthorized access.
- CE-CPABE ensures future-proof security against quantum computing threats that apply attribute-based access, thereby creating a robust framework for secure data in cloud.
- CE-CPABE provides less key generation time, encryption time, decryption time, and computational overhead compared to traditional methods because of its entropy-based key generation and context filtering, reduced redundant cryptographic operations, and enhanced scalability for cloud environments.

This research is organised as follows: Section 2 examines literature review and Section 3 provides system model, Section 4 explains results analysis, and Section 5 concludes the research with future work.

2. LITERATURE REVIEW

Sundar et al. [21] presented a Quantum Cryptography-based Cloud Security Model (QC-CSM) that utilized the Quantum Key Distribution Protocol (QKDP) for secret key sharing among parties in accessing and storage. Attribute Based Encryption (ABE) was applied to ensure data owner in terms security of the data over cloud. Moreover, the data were accessed through an authenticated user who had decryption access through a key from a secure quantum channel.

Patil et al. [22] developed a Blockchain-Integrated Optimized Cryptographic Framework (BIOCF) for dynamic cryptographic key generation and management. BIOCF included Paillier Homomorphic Encryption (PHE) with hybrid Greylag Goose Optimization (GGO) and Crayfish Optimization (CO) for data privacy. The incorporation of blockchain in decentralized key management enables cryptography for key sharing, thereby improving security and minimizing dependency on the central authority. Furthermore, cryptographically hashed encrypted data are stored in a blockchain to provide a secure data integrity check.

Sivakumar and Ganapath [23] introduced a Hybrid Encryption System (HES) and QKD for secure data communication in the cloud. HES is a cryptography algorithm called Advanced Encryption Standard (AES) and RSA for efficient encryption and decryption processes. QKD provides secure data communications through producing and allocating keys to authorized users. Furthermore, it ensures

reliable key distributions among users and maintains data through a secure HES.

Rao and Sujatha [24] presented a Hybrid Elliptic Curve Cryptography (HECC) for data encryption in cloud security. The HECC makes a key through a lightweight Edwards curve, where user identity-based encryption is applied to modify generated private key. Key reduction was applied to shorten keys to enhance AES encryption. Furthermore, public keys are replaced through Diffie Hellman key exchange.

Chithanya and Reddy [25] presented a DL with cryptographic transformation to improve data security in the cloud. The sensitive data were separated from the collected data through DL and named SqueezeNet. To enhance the SqueezeNet performance, the hyperparameters are selected optimally using the rat optimization algorithm (ROA). Then, the sensitive data were encrypted using a Light-Weight Transformation Model (LWTM).

Ahmad and Mehfuz [26] introduced an effective Time-Oriented Latency Approximation-Based Data Encryption (TLADE) for secure data encryption in cloud storage. This method focuses on optimal encryption technique selection at various times based on latency approximation, where the optimal values are selected based on Quality of Service (QoS) values. Various encryption techniques are used, and each is estimated for QoS support Values (QoSV) based on latency.

From the above analysis, the existing approaches have limitations in terms of encryption and decryption time because of computationally demanding procedures of QKD, homomorphic encryption, and hybrid RSA and AES. Delays in secure key dispensation and encryption enhance system latency, allowing unauthorized systems to use access rules and preserve privacy. The involvement of optimization algorithms and blockchain includes a further increase in the computational overhead and the number of resources consumed. These mechanisms also lack context-aware and an efficient revocation process, which limits their flexibility and scalability within cloud environments. This demonstrates that there is a research required for a security framework that not only provides better cryptographic protection but also handles less computational overhead and adaptability in dynamic cloud systems. Cloud platforms remains exposed to latency issues, credentials misuse and insufficient policy enforcement which severely compromise the data confidentiality and integrity. Therefore, CE-CPABE is designed in this research to provide fine-grained, context-aware, and entropy-driven secure data access control that minimizes running time and increases security without affecting the performance. These findings clearly highlight that the existing approaches address cloud data security but it fails to meet the requirements of less latency, reduced computational overhead and dynamic fine-grained access control. This creates a research need that not only strengthens data confidentiality and integrity but also adapts evolving conditions of distributed cloud systems.

3. SYSTEM MODEL

This paper provides a security model capable of surviving cyber-attacks and quantum computing threats in the future. This model is intended to develop secure data communication. Cryptography in the cloud focuses on encrypting a process that ciphers plaintext (original message) to ciphertext and secure mechanisms for distributing keys to achieve successful decryption. A decryption key is vital for decoding the ciphertext as plaintext. Although some traditional cryptographic protocols provide multiple techniques for securing sensitive data, such systems are exposed to quantum attacks. Thus, the model combines both QKD to share keys securely and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to control access in a fine-grained manner. To provide trusted encryption, the presented architecture uses a quantum communication channel to safely deliver a symmetric encryption key to authorized users. The goal of this system is to enhance data security and control accessibility without affecting transmission efficiency. The system model is depicted in Figure 1, and consists of quantum key generation, attribute-based key wrapping, and secure data encryption for its workflow.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

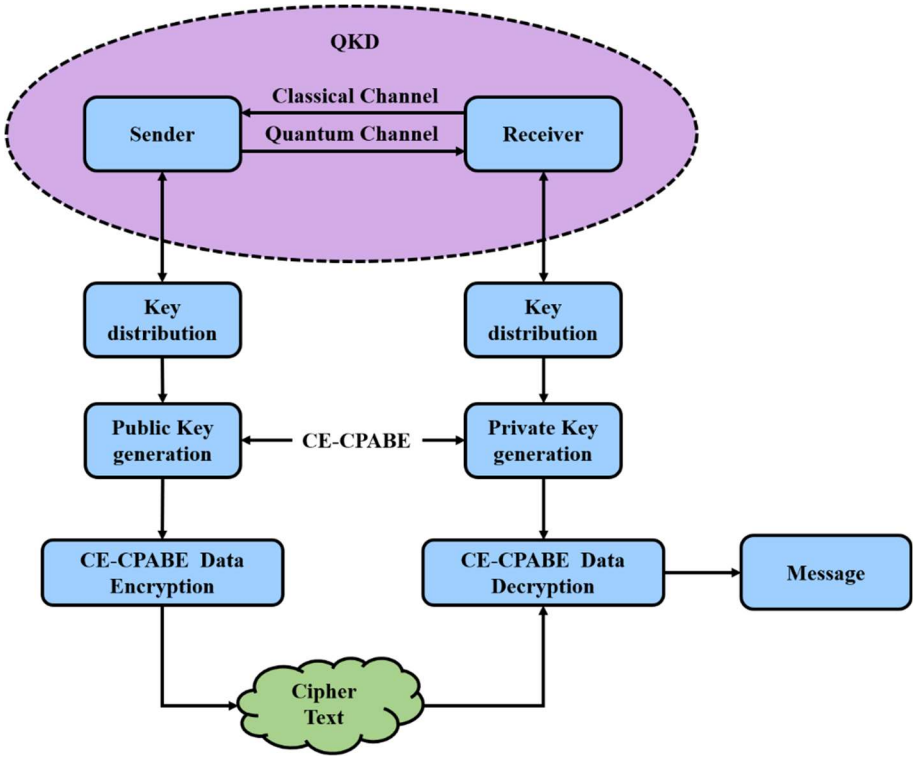

Figure 1: System model for cloud data security

A quantum channel is obtained between the key authority and user using the system architecture to distribute symmetric encryption keys. A random key is obtained by analyzing the polarization of photons that oscillate in four directions. These quantum states are sent securely to a particular recipient. When an eavesdropper attempts to intercept a transmission through incorrect detector polarization, the quantum states of the photons become disrupted. The sender and receiver are notified when they check for transmission errors.

Once the symmetric key is securely established through QKD, the encryption mechanism transitions to the CP-ABE phase, replacing conventional hybrid encryption with a policy-driven cryptographic approach. In this model, actual data are encrypted using a symmetric key obtained through QKD, whereas the key itself is encrypted under an access control policy using CP-ABE. This ensures that users whose attribute sets satisfy the access structure decrypt the symmetric key and subsequently access data. Unlike RSA, which relies on a fixed public-private key pair for key encapsulation, CP-ABE dynamically enforces access control through attribute-based secret keys issued by a trusted authority. This approach not only secures communication, but also ensures that data access is strictly limited to authorized users based on predefined attribute conditions. Thus, the proposed framework establishes a robust, post-quantum-secure system for storing and transmitting cloud data while providing scalable and flexible access control.

3.1 Proposed Methodology

CE-CPABE is a complex encryption scheme that offers fine-grained, context-aware, encryption-based data access control. Similar to traditional CP-ABE, information is encrypted according to a set of attributes, and access is achieved based on predefined policies. CE-CPABE further combines contextual parameters (time, location, and device) and entropy-improved randomness during key generation and encryption functions. The main advantage is that it allows dynamic, up to the second enforcement of policies, and CE-CPABE is especially effective when highly sensitive or time-constrained access is required, such as in cloud storage, e-health, or edge computing systems. The other major reuse vulnerabilities and insider threats are also mitigated with CE-CPABE because cryptographic keys are bound to traits and situations in addition to attributes. This binding ensures that even if credentials are compromised, decryption fails when the context is invalid at the time of access. Over traditional CP-ABE schemes, CE-CPABE

allows stronger policy flexibility, an adaptive revocation key, and entropy sources that resist attacks on quantum computers. It provides privacy-enhancing collaboration, data protection, and enhanced compliance with data-protection laws.

3.1.1. Setup

The CE-CPABE system initialization involves a trusted authority/server carrying out the setup phase, which is executed only once. It involves scalar multiplication, pairing operations, and exponentiation, with an important extension, the integration of context-dependent entropy to produce secure, unpredictable key components. The result of this stage is the master keys MK and the public key PK. Whereas MK is kept secret, the key PK is shared with every user. The algorithm starts with the generation of bilinear groups G, G_T where G is of order r and contains generator g and both groups are of order r. Instead of using random values, CE-CPABE uses an entropy-aware method, that is, select contextual entropy $\alpha, \beta \leftarrow \text{EntropicRandom}(Z_r, \text{context})$. Then, estimate the master and public keys as equations (1) and (2),

$$MK = (\beta, g^{\alpha}) \quad (1)$$

$$PK = (G, g, h, f, v) \quad (2)$$

Where, $h = g^{\beta}, f = g^{\beta^{-1}}, v = e(g,g)^{\alpha}$ and $e = G \times G \rightarrow G_T$ is a bilinear pairing map.

3.1.2. Key generation

The key-generation algorithm is executed by a trusted party or authority for every user. In contrast to the traditional CP-ABE, CE-CPABE incorporates contextual entropy into the process to ensure that the secret key of each user is bound not only to the attributes but also to environmental conditions such as time, location, and device identity. This stage uses MK and attribute set $A = \{att_1, att_2, \ldots\}$ with contextual metadata as inputs to estimate the user's secret key SK. Initially, this algorithm selects the contextually bound random value $\gamma \in Z_r$ by using an entropy extractor in the user context. Then, every attribute $i \in A$ selects a unique value $\gamma_i \in Z_r$ derived from context-aware entropy. This scheme utilizes the hash-to-curve function $H: \{0,1\}^* \rightarrow G$ to map attributes. The SK is computed using equation (3),

$$SK = (D, \{D_i, D_i'\}_{\forall i \in A}) \quad (3)$$

Where, $D = g^{(\alpha+\gamma)\beta^{-1}}$, $D_i = g^{\gamma} \cdot H(i)^{\gamma_i}$ and $D_i' = g^{\gamma_i}$.

3.1.3. Encryption

The encryption process is performed by data owner or sender which ensures that the data is encrypted before uploading it to the cloud. CE-CPABE augments a generic CP-ABE encryption scheme with contextual attributes, such as the time window, location, and device identity to the access policy. The algorithm utilizes a PK, message M and context-extended access policy T for user attributes and contextual conditions. Users whose keys ensure T under contextual conditions are used to decrypt data. Consider $s \in Z_r$ is randomly selected to encrypt a secret. The polynomial q_t is selected for every node t in the access tree T. Set the $q_R(0) = s$ for root node R, consider $q_t(0) = q_{par(t)}(ind(t))$ for each node t. The leaf node in T includes contextual constraints, which are denoted by L. Each node denotes the contextual condition or attribute by a function att(t). The cipher text CT is generated by T as in equation (4),

$$CT = (T, \tilde{C}, C, \{C_l, C_l'\}_{\forall l \in L}) \quad (4)$$

Where, $\tilde{C} = M \cdot e(g,g)^{\alpha s}$, $C = h^s$, $C_l = g^{q_l(0)}$ and $C_l' = H(att(l))^{q_l(0)}$.

3.1.4. Decryption

The descriptor uses the decryption algorithm to obtain the encrypted message M. This is supplemented in the case of CE-CPABE with contextual validation in CE-CPABE, where the attributes of the user and current context such as location, device ID, and time of access, both meet the access policy T. The decryption process only occurs when both the context and attributes are verified, otherwise, access is denied even if the attributes match. This ensures the data security of invalid applications using valid credentials, as in equation (5),

$$dec\_node(CT, SK, t) = \begin{cases} \frac{e(D_i, C_t)}{e(D_i', C_t')} & \text{if } i \in A \\ \text{null} & \text{if } i \notin A \end{cases} \quad (5)$$

The $dec\_node(CT, SK, t)$ performance on leafless node t as following: The algorithm calls $dec\_node(CT, SK, t)$ for every child node cand saves result in F_c. The A_t is a list of children c where the $F_c \neq$ null. Otherwise, it returns null. Else, subsequent estimation is achieved as in equations (6) and (7),

$k = ind(c), \quad A'_t = \{ind(c), \forall_c \in A_t\}$

$$\Delta_{k,A'_t(0)} = \prod_{j \in A'_t, j \neq k} \frac{-j}{k-j} \quad (6)$$

$$F_t = \prod_{c \in A_t} F_c^{\Delta_{k,A'_t(0)}} = \prod_{c \in A_t} \left(e(g,g)^{\gamma q_c(0)}\right)^{\Delta_{k,A'_t(0)}} = \prod_{c \in A_t} \left(e(g,g)^{\gamma q_{par(c)}(ind(c))}\right)^{\Delta_{k,A'_t(0)}} = \prod_{c \in A_t} e(g,g)^{\gamma q_t(k) \Delta_{k,A'_t(0)}} = e(g,g)^{\gamma q_t(0)} \quad (7)$$

If attribute A matches tree access policy T, the algorithm is called as dec_node(CT, SK, t) as in equation (8):

$$\tilde{A} = dec_{node(CT,SK,t)} = e(g,g)^{\gamma q_R(0)} = e(g,g)^{\gamma s} \quad (8)$$

Then, the ciphertext is decrypted using equation (9),

$$M = \frac{\tilde{C}}{\frac{e(C,D)}{\tilde{A}}} \quad (9)$$

CE-CPABE improves on the traditional CP-ABE by incorporating both context awareness and the use of entropy to generate keys. This ensures that not only the user characteristics, but also real-time contextual situations, such as the time, location, or identity of the device, needs to satisfy the access policy for successful decryption. This method is more secure when it comes to access control because the system can block unauthorized access even when legitimate credentials are used in an inappropriate environment. CE-CPABE helps share data safely in a cloud setting through the implementation of fine-grained and dynamic access policies.

Pseudocode for proposed CE-CPABE:

Algorithm: CE-CPABE $(\lambda, context, A, M, T)$
Input: Security parameter λ, context, Attribute set of user A, Message to be encrypted M and Access policy tree T.
Output: Ciphertext CT, Secret key SK, and decrypted message M
Phase 1: Setup
Generate bilinear groups G, G_T of prime order $r, g \in G$
$\alpha, \beta \leftarrow EntropicRandom(Z\_r, context)$ using Equation (1),
$h = g^{\beta,f} = g^{\beta^{-1}}, v = e(g,g)^{\alpha}$ using Equation (2),
Set public key $PK = (g, h, f, v)$, master key $MK = (\beta, g^{\alpha})$
Phase 2: Key Generation
$\gamma \leftarrow ContextualEntropy(Z\_r, context)$
for each $i \in A$:
$\gamma\_i \leftarrow EntropyPerAttribute(Z\_r, i, context)$
$D_i = g^{\gamma} \cdot H(i)^{\gamma_i}$
$D'_i = g^{\gamma i}$
end for
$D = g^{(\alpha+\gamma)\beta^{-1}}$ using Equation (3),
Output $SK = (D, \{D_i, D'_i\}\ for\ all\ i \in A)$
Phase 3: Encryption
Select random $s \leftarrow Z_r$
for each node $t \in T$:
if t is root:
$q_t(0) = s$
else
$q_t(0) = q_{par(t)}(ind(t))$
end if
end for
for each leaf node $l \in L$:
$C_l = g^{q_l(0)}$
$C'_l = H(att(l))^{q_l(0)}$
end for
$C = h^s, \tilde{C} = M \cdot e(g,g)^{\alpha s}$
$CT = (T, \tilde{C}, C, \{C_l, C'_l\}_{\forall l \in L}$ using equation (4),
Phase 4: Decryption
Validate user context against contextual attributes in T
if context invalid
return $\perp$
end if
for each node $t \in T$:
if t is a leaf and $i \in A$:
$F_t = \frac{e(D_i, C_t)}{e(D'_i, C'_t)}$ using Equation (5),
else
for each child $c \in A_t$:
Compute Lagrange coefficient $\Delta_{k,A'_t(0)}$ using Equation (6)
$F_t = F_c^{\Delta_{k,A'_t(0)}}$ using Equation (7),
end for
end if
end for
At root node R:
$\tilde{A} = dec_{node(CT,SK,t)} = e(g,g)^{\gamma s}$ using Equation (8),
Compute $M = \frac{\tilde{C}}{\frac{e(C,D)}{\tilde{A}}}$ using Equation (9),
Output M

4. RESULT ANALYSIS

The experimental setup was performed in Python 3.10, CloudSim with an i7 processor, 16GB RAM

and Windows 10 OS. Data sizes of 10, 15, 20, 25, and 30MB were used for performance analysis. Performance metrics include Key Generation Time, encryption time, decryption time, processing time, latency, computational overhead, and resource utilization. This comparative and experimental research design was chosen as it is a direct approach to solving the main goals of this research to improve security, efficiency and scalability of cloud data storage. The design allows systematically assessing its efficiency by designing and testing the proposed CE-CPABE model in a controlled simulation setting and comparing it with current cryptographic methods, such as RSA, AES, ABE, and CPABE. The key performance metrics are well aligned to the research questions as they are used to portray the capability of the model to minimize the cost of computation, enhance operational performance and enhance security of access. This makes the research design not only appropriate but adequate to ensure that the CE-CPABE addresses the desired research goals.

All experiments were performed under the same and controlled conditions to provide the stability of the results. The environment, simulation settings and hardware remained the same in the course of the evaluation and the tests were repeated severally with averaged outcomes taken to analyze them. The input data sizes from 10MB to 30MB are considered and evaluation processes were compared with various cryptographic techniques. These control measures were necessary to ensure that the performance variations were only a result of the proposed CE-CPABE model and no external factors or uncontrolled variations.

Figure 2 shows the key generation time of CE-CPABE and compares it with RSA, AES, ABE, and CPABE with various sizes of data, such as 10, 15, 20, 25, and 30 MB.

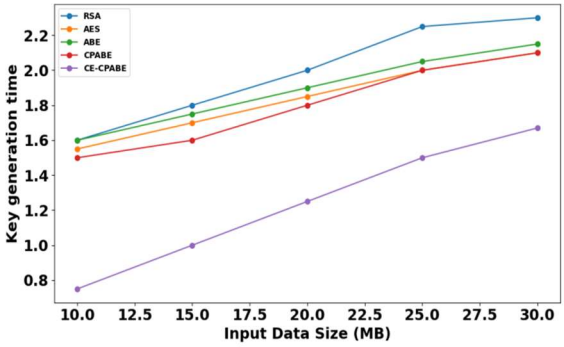

Figure 2: Key generation time (s) of cryptographic methods over varying data sizes from 10MB to 30MB

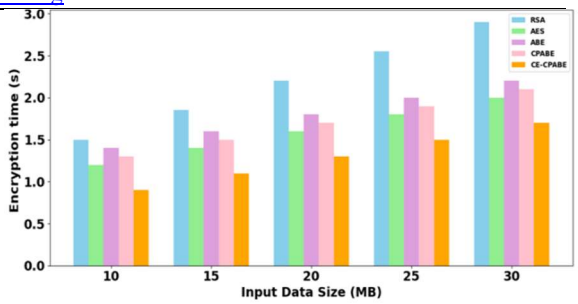

Figure 3: Encryption time (s) of cryptographic methods over varying data sizes from 10MB to 30MB

The key generation times achieves 0.75s, 1.00s, 1.25s and 1.50s, 1.67s of with varied sizes of data such as 10MB, 15 MB, 20 MB, 25 MB and 30 MB respectively of CE-CPABE. This is because the key generation ability of CE-CPABE is context-aware and utilizes entropy-based randomness that depends on environmental conditions. In contrast to RSA or ABE, in CE-CPABE, keys are bound to user attributes as well as context and do not require a separate heavy cryptographic round. This reduces the number of calculations and accelerates the delivery of keys without loss of security.

Figure 3 shows the encryption time of CE-CPABE and other existing methods for the same set of data sizes. CE-CPABE achieves fast encryption of 0.90s, 1.25s, 1.65s, 2.00s and 2.28s for 10MB, 15 MB, 20 MB, 25 MB and 30 MB respectively. This ensures that the process is enhanced by its ability to incorporating contextual constraints directly into the encryption policy, thereby eliminating the need to perform policy translation. Furthermore, polynomial assignments are optimized across access tree nodes to be traversed in the minimum possible manner. Compared with RSA and CPABE, CE-CPABE makes it easier to eliminate unnecessary encryptions.

Figure 4 specifies the encryption time of CE-CPABE of 1.00s, 1.40s, 1.85s, 2.20s and 2.53s for 10MB, 15 MB, 20 MB, 25 MB and 30 MB respectively. Compared to traditional CPABE and RSA, CE-CPABE verifies the attribute and context before performing full traversal and attribute matching, thereby preventing unnecessary decryption attempts when a mismatch is found. This short-circuited assessment helps avoid unwanted cryptographic operations. A limited scope of decryption is also achieved using the fine-grained control policy implemented in ciphertext, which gives it a performance advantage over having a broadened domain of access control.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

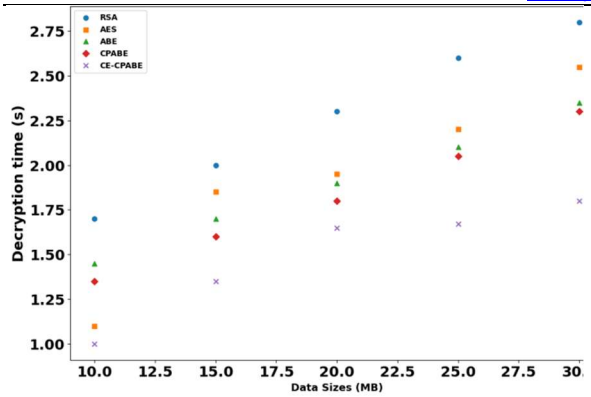

Figure 4: Decryption time (s) of cryptographic methods over varying data sizes from 10MB to 30MB

Figure 5 illustrates that the processing time of CE-CPABE achieves decryption times of 0.28s, 0.35s, 0.45s, 0.55s, 0.62s for 10MB, 15 MB, 20 MB, 25 MB and 30 MB respectively. This is because it has an efficient lightweight cryptographic flow and does not engage in any re-validation or elaborate key derivations.

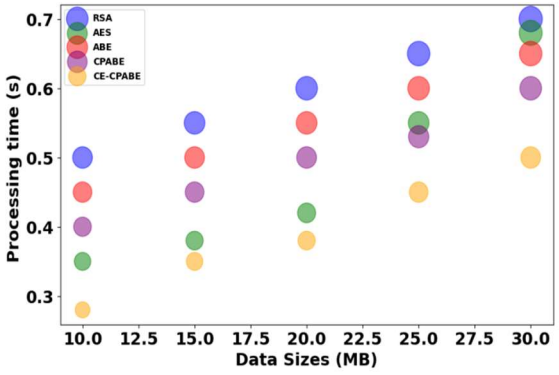

Figure 5: Processing time (s) of cryptographic methods over varying data sizes from 10MB to 30MB

The context is filtered by entropy; therefore, the useless keys are filtered out before processing, and the effective volume of data for the CPU is lower. Policy and attribute mapping in CE-CPABE is performed once per cryptographic cycle, resulting in a shorter computation delay. Figure 6 provides the latency of CE-CPABE with 0.85s, 1.00s, 1.25s, 1.45s, and 1.65s for 10MB, 15 MB, 20 MB, 25 MB and 30 MB, respectively as compared to RSA and ABE. This is because CE-CPABE verifies the context used to execute the data operations with fast validation and processing. It can eliminate repetitive checks during encryption and decryption processes, thereby reducing latency in secure data management.

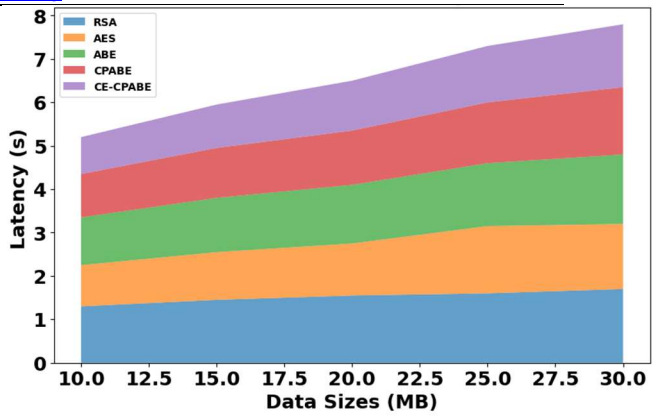

Figure 6: Latency (s) of cryptographic methods over varying data sizes from 10MB to 30MB

Figure 7 shows the computational overhead of CE-CPABE of 1.80%, 2.20%, 2.80%, 3.20%, and 3.72% for 10, 15, 20, 25, and 30 MB, respectively. It can optimize policy matching logic and context-aware key generation, thereby reducing the computational overhead. CE-CPABE does not require the comparison of all attribute types and the unnecessary process of encrypting decryption, as in the case of CPABE and ABE. There is also a limitation in cryptographic depth per operation, which minimises the number of resources used.

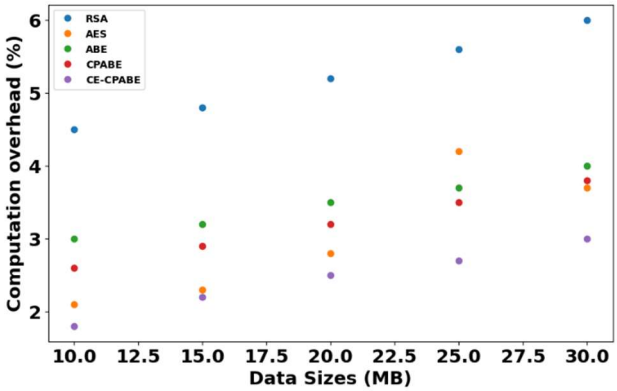

Figure 7: Computation overhead (%) of cryptographic methods over varying data sizes from 10MB to 30MB

Figure 8 illustrates the resource utilization of CE-CPABE at 49.0%, 52.0%, 54.5%, 56.0%, and 57.2% for 10, 15, 20, 25, and 30 MB, respectively. This enhancement is due to its entropy-based key and selective validation of access, which does not introduce overhead processing in the case of a context mismatch. Existing methods such as RSA and ABE are utilized to reduce computational cost due to the extensive arithmetic operations or policy evaluation operations.

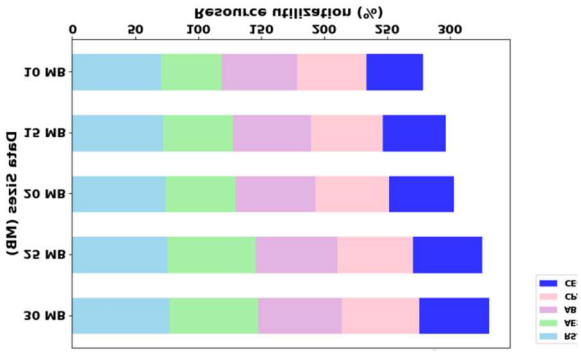

Figure 8: Resource utilization (%) of cryptographic methods over varying data sizes from 10MB to 30MB

Table 1: Time complexity analysis of various cryptographic methods

Method	Time Complexity
RSA	$O(n^3)$
AES	O(n)
ABE	$O(n^2)$
CPABE	O(n log n + m)
CE-CPABE	O(n log n + m + k)

Table 1 provides a complexity analysis of the proposed CE-CPABE using various cryptographic methods, such as RSA, AES, ABE, and CPABE. As a combination of (n log n + m) input and (k) context-aware constraints, CE-CPABE attains O(n log n+m+k). This indicates a trade-off between a balanced framework with fine-grained access control and effective cryptographic algorithms. In contrast, $O(n^3)$ in RSA and $O(n^2)$ in ABE achieved scalable performances in the cloud. CE-CPABE optimizes the access tree construction and ciphertext size for better performance.

4.1 Comparative analysis

A comparative analysis of the existing PHE-HGCCF method [22] and the proposed CE-CPABE method is presented in Table 2 with regard to a data size of 30MB. The CE-CPABE provides better performance when assessed over all measurements, and key generation time, encryption time, decryption time, processing time, latency is 1.67s, 2.28s, 2.53s, 0.62s, and 1.65s, while the computational overhead and resource utilization are 3.72% and 57.2 respectively. CE-CPABE can secure the system better because it adds contextual constraints, thereby enabling dynamic access control.

Table 2: Comparative analysis with the data size of 30 MB

Metrics	PHE-HGCCF [22]	CE-CPABE
Key generation time (s)	2.103	1.67
Encryption time (s)	2.649	2.28
Decryption time (s)	2.81	2.53
Processing time (s)	0.745	0.62
Latency (s)	1.785	1.65
Computational overhead (%)	4.01	3.72
Resource utilization (%)	64.1	57.2

4.2 Research Implications

The proposed CE-CPABE has various research implications for secure and effective cryptographic frameworks as follows: (1) Enhancing fine-grained access control through context awareness: The proposed CE-CPABE improves access security through decryption to user attributes, but also real-time contextual parameters such as time, location, and device. This model significantly reduces unauthorized access and threats to misused credentials. (2) Improving key generation robustness through entropy integration: Entropy-based randomness in key generation enhances the randomness and flexibility of quantum analysis. This ensures that each key is unique to the context and environmental state, thereby enhancing cryptographic stability. (3) Enhancing revocation and dynamic policy adaptability: Unlike ABE, CE-CPABE provides dynamic policy and adaptive key revocation-based context violations to improve data security. (4) Enabling post-quantum secure and cloud storage systems: Using QKD, CE-CPABE is integrally resilient to quantum-based attacks, thereby providing future-proof encryption for distributed cloud environments. Overall, the evaluation criteria for validating the research problem includes key generation time, encryption time, decryption time, processing time, latency, computational overhead, and resource utilization. These metrics are selected because it directly reflects the scalability, efficiency, and security of cryptographic in cloud environments. The results demonstrate that CE-CPABE achieves less computational cost and high performance among all the metrics compared to existing methods thereby ensuring that the proposed model effectively address the research problem to secure and efficient cloud data storage.

4.3 Difference from Prior Literature

The proposed CE-CPABE approach presents the explicit differences with the previous literature due to its ability to resolve the essential shortages of the current attribute-based encryption approaches in clouds. Although the previous literature mainly emphasizes on either security or efficiency, the proposed solution is capable of maximizing several performance metrics at the same time, such as key generation time, encryption and decryption time, latency, computational overhead, and resource consumption. This end-to-end optimization is the guarantee of scalability and strength in real-world cloud storage. Moreover, CE-CPABE proposes a attribute-based encryption scheme that does not violate data privacy and performance, which is a drawback in most earlier works. The advantage of the proposed work is proven in the results of the experiment that showed comparative improvements to the existing methods and hence the validity of the novelty and practical importance of the proposed work.

5. CONCLUSION

This research proposes a novel Contextual Entropic Ciphertext-Policy Attribute-Based Encryption (CE-CPABE) to address the security and performance challenges of cloud data storage. By combining contextual parameters with entropy-enhanced key generation, CE-CPABE provides dynamic and fine-grained access control. Compared to CPABE, CE-CPABE includes attributes and environmental context into keys, thereby making unauthorized decryption virtually impossible with valid credentials. CE-CPABE ensures future-proof security against quantum computing threats, which applies attribute-based access, thereby generating a robust framework for secure data in the cloud. The performance evaluation shows that CE-CPABE outperforms the existing models in terms of key generation time, encryption time, decryption time, processing time, latency, computational overhead, and resource utilization, thereby making it scalable for large-scale cloud environments. The results indicate that CE-CPABE not only enhances cloud security but also maintains operational efficiency. The CE-CPABE achieves significant improvements in encryption and decryption time, latency, computational overhead, and resource utilization thereby validating its significance as a solution to the identified research problem. Therefore, this model provides a better solution for secure, privacy-preserving, and context-sensitive data sharing in the cloud, particularly for sensitive data. Future work will focus on trust-based access control mechanisms to further improve the data security in decentralized cloud environments.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES:

[1] X. Dong and Y. Xie, "Research on cloud computing network security mechanism and optimization in university education management informatization based on OpenFlow," *Systems and Soft Computing*, Vol. 2, 2025, p. 200225.

[2] R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooie, "An integrated architecture for maintaining security in cloud computing based on blockchain," *IEEE Access*, Vol. 9, 2021, pp. 69513–69526.

[3] C. Tamizshelvan and V. Vijayalakshmi, "Cloud data access governance and data security using distributed infrastructure with hybrid machine learning architectures," *Wireless Networks*, Vol. 30, No. 4, 2024, pp. 2099–2114.

[4] N. Krishnamoorthy and S. Umarani, "Implementation and management of cloud security for industry 4.0 data using hybrid elliptical curve cryptography," *The Journal of High Technology Management Research*, Vol. 34, No. 2, 2023, p. 100474.

[5] B. Rahul and K. Kuppusamy, "Efficiency analysis of cryptographic algorithms for image data security in cloud environment," *IETE Journal of Research*, Vol. 69, No. 9, 2023, pp. 6053–6064.

[6] H. Farshadinia, A. Barati, and H. Barati, "A secure and energy-efficient architecture in Internet of Things–cloud computing network by enhancing and combining three cryptographic techniques via defining new features, areas, and entities," *The Journal of Supercomputing*, Vol. 81, No. 8, 2025, p. 944.

[7] D. Shivaramakrishna and M. Nagaratna, "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*, Vol. 84, 2023, pp. 275–284.

[8] S. Guan, C. Zhang, Y. Wang, and W. Liu, "Hadoop-based secure storage solution for big data in cloud computing environment," *Digital*

Communications and Networks, Vol. 10, No. 1, 2024, pp. 227–236.

[9] S. Gadde, J. Amutharaj, and S. Usha, "A security model to protect the isolation of medical data in the cloud using hybrid cryptography," *Journal of Information Security and Applications*, Vol. 73, 2023, p. 103412.

[10] N. M. Reddy, G. Ramesh, S. B. Kasturi, D. Sharmila, G. Gopichand, and L. T. Robinson, "Secure data storage and retrieval system using hybridization of orthogonal knowledge swarm optimization and oblique cryptography algorithm in cloud," *Applied Nanoscience*, Vol. 13, No. 3, 2023, pp. 2449–2461.

[11] G. Visalaxi and A. Muthukumaravel, "IoT monitoring membrane computing based on quantum inspiration to enhance security in cloud network," *Measurement: Sensors*, Vol. 27, 2023, p. 100755.

[12] H. Mahajan and K. T. V. Reddy, "Secure gene profile data processing using lightweight cryptography and blockchain," *Cluster Computing*, Vol. 27, No. 3, 2024, pp. 2785–2803.

[13] S. Mohammed, S. Nanthini, N. B. Krishna, I. V. Srinivas, M. Rajagopal, and M. A. Kumar, "A new lightweight data security system for data security in the cloud computing," *Measurement: Sensors*, Vol. 29, 2023, p. 100856.

[14] I. Qiqieh, J. Alzubi, and O. Alzubi, "DNA cryptography based security framework for health-cloud data," *Computing*, Vol. 107, No. 1, 2025, p. 35.

[15] S. D. Dhamdhere, M. Sivakkumar, and V. Subramanian, "Cloud data security with deep maxout assisted data sanitization and restoration process," *High-Confidence Computing*, Vol. 5, No. 1, 2025, p. 100238.

[16] U. Gowrisankar and V. Vennila, "Adaptive elephant herding optimization and enhanced advanced encryption standard algorithm for dynamic task scheduling and security over cloud computing," *Journal of Electrical Engineering & Technology*, 2025, pp. 1–14.

[17] F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," *International Journal of Intelligent Networks*, Vol. 2, 2021, pp. 18–33.

[18] N. M. Sultana and K. Srinivas, "Data privacy protection in cloud computing using visual cryptography," *Multimedia Tools and Applications*, 2024, pp. 1–21.

[19] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing," *International Journal of Intelligent Networks*, Vol. 3, 2022, pp. 16–30.

[20] S. Bashir, Z. Ayub, and M. T. Banday, "Cloud data security for distributed embedded systems using machine learning and cryptography," *International Journal of Information Technology*, 2024, pp. 1–12.

[21] K. Sundar, S. Sasikumar, C. Jayakumar, D. Nagarajan, and S. Karthick, "Quantum cryptography based cloud security model (QC-CSM) for ensuring cloud data security in storage and accessing," *Multimedia Tools and Applications*, Vol. 82, No. 27, 2023, pp. 42817–42832.

[22] R. S. Patil, G. S. Biradar, and S. Terdal, "Blockchain-integrated optimized cryptographic framework for securing cloud data," *Knowledge-Based Systems*, 2025, p. 113830.

[23] J. Sivakumar and S. Ganapathy, "An effective data security mechanism for secured data communications using hybrid cryptographic technique and quantum key distribution," *Wireless Personal Communications*, Vol. 133, No. 3, 2023, pp. 1373–1396.

[24] B. R. Rao and B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security," *Measurement: Sensors*, Vol. 29, 2023, p. 100870.

[25] K. V. K. Chithanya and V. L. Reddy, "A novel deep learning technique with cryptographic transformation for enhancing data security in cloud environments," *Multimedia Tools and Applications*, Vol. 84, No. 8, 2025, pp. 5149–5173.

[26] S. Ahmad and S. Mehfuz, "Efficient time-oriented latency-based secure data encryption for cloud storage," *Cyber Security and Applications*, Vol. 2, 2024, p. 100027.