International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Data Security in Cloud Using Cipher Text-Policy Attribute-Based Encryption (CP-ABE)

Dr. R. Kaviarasan, G.M. Gayathri, K. Dinesh Kumar, P. Surya Prathap, S. Ashok Kumar

Submitted: 21/11/2024 **Revised:** 28/11/2024 **Accepted:** 05/12/2024 **Published:** 19/12/2024

Abstract: The upward push of cloud-primarly based information garage offerings has captured giant interest from each instructional researchers and enterprise professionals, as a result of their cost-effectiveness and operational performance. As these offerings function over public networks, making sure robust security features is crucial to guard facts integrity and consumer privacy. The get entry to policy is embedded in the cipher textual content itself, ensuring that simplest customers whose attributes satisfy the policy can decrypt the records. Utilizing CP-ABE or Cipher Text-Policy Attribute-Based Encryption, the suggested machine makes sure that the owner of the data cannot be identified when a new report is uploaded. CP-ABE is a popular approach that mixes the strengths of symmetric cryptography with integrates AES algorithm to gain excessive levels of encryption speed and communication cost. The data saved on the cloud stays personal and inaccessible to unauthorized users and the cloud itself. The system consists of a mechanism that lets in the cloud to verify if a statistics person is allowed to download a report without revealing touchy data, such as the user's identification. By the way of integrating these components, the proposed device targets to provide a speed and efficient solution for cloud-based records control and sharing, addressing both the desires for robust statistics protection and powerful get admission to control. Experimental evaluation demonstrates the efficiency of the proposed approach in enhancing facts safety in cloud environments. The consequences indicates reduction in computational cost, development in ordinary machine overall performance in comparison to traditional encryption methods.

Keywords: Cloud-based data exchange, CP-ABE, access control, encryption based on cypher textual content-coverage attributes, redundant residue measurement device, Key management system, symmetric AES, safety.

I. INTRODUCTION

These days, outsourcing services and limitless cloud storage allow businesses and data owners to process and store large amounts of data . The carrier must be of high quality to ensure clean accessibility, availability, and high scalability. Cypher text (CT)-policy characteristic-primarily based encryption (CP-ABE) is a technique used for online social networks like Google Vault[1], Facebook, and many others to encrypt a person's private information. Despite these benefits of cloud servers, there is a rise in serious concerns about confidentiality and data protection in the cloud environment (Vengala et al., 2020]. Numerous strategies had been put in place to provide safety for these private sensitive information. Looking for information that has been outsourced in order to keep it and save it in a cloud environment [2].

However, they are unable to enforce the information that is beneficial for safety, regulate for unique preserved documents, or gain access to them (Xue et al., 2020). Maintaining data, making decisions, maintaining secrecy, and gaining access to policies may be extremely challenging in untrusted cloud environments. As a result, device

Associate Professor,Department of CSE, RGMCET Nandyal, India
kaviarasanr64@ptuniv.edu.in
UG Scholar, Department of CSE, RGMCET Nandyal, India
gmgayathrigayathri@gmail.com
UG Scholar, Department of CSE, RGMCET Nandyal, India
kummaridinesh216@gmail.com
UG Scholar,Department of CSE,RGMCET Nandyal, India
suryaprathap2673@gmail.com
UG Scholar, Department of CSE, RGMCET Nandyal, India
ashokkumar19305@gmail.com

designs and procedures are employed to gain access in order to execute cryptographic activities that offer security for a productive cloud access environment [3].

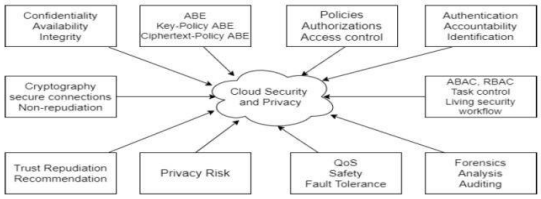


Fig.1. Cloud computing Risks and its Technologies

The above figure shows the technologies used to reduce the dangers associated with cloud computing, including data breaches, unauthorized access, and insecure APIs.

CP-ABE ensures that the identity of the data owner is not revealed when a new file is uploaded. The data stored on the cloud remains confidential and inaccessible to unauthorized users and the cloud itself. Another cloud-computing risk is the unauthorized access of an uploaded file while concealing the identity of the data owner. The data held on the cloud stays confidential, remaining inaccessible to unauthorized users as well as the cloud itself. The system has mechanisms that allow the cloud to verify a user who is allowed to download a file without revealing any sensitive information, which may include the identity of the user himself[4]. Thus, with the combination of the aforementioned components, the proposed system would offer a secure and efficient solution for cloud based data management and sharing, thus addressing the two aspects of strong data security and effective access control.

II. LITERATURE SURVEY

This phase analyzes a plethora of contemporary techniques, advantages, and disadvantages involved with these methodologies. Logesh, K., Subramanian S., et al., (2022) propose a dual access control scheme to secure cloud data storage and file access through QR codes. So, the combination of two-layer access control and cryptographic techniques adds to data security as cloud data is only accessible by those among the users who are authorized to do so. User authentication is done by conventional login credentials along with a QR code that gets sent to the user's device, which is regarded as a dynamic one-time access key. File contents are encrypted with the most recent cryptographic algorithms and QR code provides decryption. RBAC provides further access restriction with user privileges, and audit trails will keep track of records of accesses and actions performed on files[26].

Patil, S., Vhatkar, P., Gajwani, J., et al., (2014).The proposed system allows for integrity checking besides storage challenges and challenge-response protocols using the concept of distributed erasure coding. Accordingly, it lets the user check the integrity and authenticity of their stored data without downloading the entire set[19].

Ren, K., Lou, W., Wang, C., Yu, S., et al. (2010).Key-policy attribute-based encryption (KP-ABE) is the method suggested in this paper for fine-grained data access control. According to predetermined access regulations linked to their attributes, users are given the ability to decrypt data[7].

Li, J., Li, J., Chen, X., Li, Z., Lee, P. P. C., & Lou, W. et al. (2014) .This study presents a secure deduplication solution that combines decentralized key management with convergent encryption. Deduplication saves storage space by preventing duplicate copies of data from being kept in the cloud[15].

Zhou, Z., & Huang, D. et al., (2012) proposes a method secures mobile cloud storage by combining proxy re-encryption with integrity auditing. It allows users to share encrypted data securely and verify its integrity without having to download it[5].

Ren et al. (2015) propose an ingenious solution in the form of a mutual verifiable data-auditing mechanism in which both the clients and the cloud servers can verify the integrity of the data stored in the cloud. With this, accountability is ensured on both ends[6].

Ruj, S., Nayak, A., and Stojmenovic, et al. I propose in November 2011 a decentralized access control system, thus incorporating anonymous authentication and dynamic attribute revocation to secure the data stored on clouds[9].

Al-Yasiri, A., Khan, N., et al. (2016).In order to counter any significant weaknesses, the article offers a comprehensive study of cloud security concerns and suggests a general-purpose architecture for encouraging cloud use through layered defense measures[13].

Zhang et al. (2023) believe that blockchain technology finds application in establishing a secure, trusted, and traceable data-sharing environment basically for cloud settings. With blockchain, every single activity in the data-sharing process is accounted for and no one can alter that activity[23].

Tang et al. The attempts of author to develop such a plan in 2024 are reported. The goal is to create new, safe, and lightweight cloud data deduplication schemes that combine data deduplication with efficient access control and key management tools in a cloud setting. Data deduplication is the process of removing duplicate files from the system so that there is only one useful copy. This allows authorized users to access the data while preventing unauthorized users from doing so by implementing extra public key cryptography-based key management mechanisms[27].

S. No.	Authors	Methodology	Advantages	Disadvantages
1.	Logesh, K., & Subramanian, S. et al., (2022)	Role-based Access Control (RBAC)	Enhanced security, user-friendly, role-based access	Vulnerability to QR Code Attacks,Device Dependency
2.	Patil, S., Vhatkar, P., & Gajwani, J. et al., (2014)	Integrity verifiaction	Ensures data integrity, fault tolerance, transparency.	Increased computational and storage overhead
3.	Ren, K., Lou, W., Yu, S., Wang, C., et al. (2010)	KP-ABE, or Key-Policy Attribute-Based Encryption	Fine-grained access, scalability, reduced key-distribution burden	High complexity in key management and decryption
4.	Li, J., Li, J., Chen, X., Li, Z., Lee, P. P. C., & Lou, W. et al., (2014)	Convergent Encryption	Reduces storage space, ensures data confidentiality	Vulnerable to brute-force attacks for predictable data patterns
5.	Zhou, Z., & Huang, D. et al., (2012)	Proxy-re-encryption	Low computational cost, secure file sharing, integrity verification	Trust dependency on proxies, potential latency
6.	Wang, J., Han, J., Shen, J., Ren, Y. J., & Lee, S. Y. et al. (2015)	Auditing of mutually verifiable data	Transparency, mutual trust, data integrity assurance	Additional communication costs
7.	Jiang, X., Tang, X., Guo, C., Choo, K. K. R., Liu, Y., et al., 2024	Data deduplication scheme	Improved storage efficiency, Reduced Network traffic	Data Recovery, Additional Costs

Table1: Summary Table of Literature Survey

Security and efficiency are proposed in the CP-ABE-AES scheme, which integrates Ciphertext-Policy Attribute Based Encryption (CP-ABE) with AES encryption, in contrast to the systems suggested by Yu et al. (2010) and Li et al. (2013). The method used by Yu et al. gives fine-grained access control using KP-ABE but imposes centralized key management, which can be seen as a single point of failure. In the same way, Li et al.'s secure deduplication system using convergent encryption maximizes storage but loses against dictionary attacks by predictable data. Whereas CP-ABE and AES provide robust encryption: CP-ABE is used for access control over symmetric AES keys, whereas AES provides efficient data encryption. On the other hand, this integration enriches encryption speed, supports dynamic policy updates, and allows additional deduplication while ensuring a high security level. Overall, CP-ABE integrated with AES provides a balance between fine-grained access control and computational efficiency combined with scalable security. This is, therefore, the best option to consider for cloud data management systems.

III. PROPOSED SYSTEM

The study demonstrates how the Ciphertext-policy ABE may guarantee relaxed transmission, safe broadcasting, and efficient access control over data in cloud computing. However, there is a flaw in the current Ciphertext-policy ABE implementation that could cause some sensitive user and data privacy information to be unintentionally revealed by plaintext access policies communicated with ciphertexts. A novel approach is put forth to address this issue, employing hashing techniques to obscure access controls and strengthen security against possible intrusions via verification procedures. The effectiveness of the suggested plan to improve privacy and security in cloud computing settings is demonstrated by the comparison analysis against current frameworks.This work intends to support safe data management practices, hence boosting trust in the cloud computing system, by fixing flaws in Ciphertext-policy ABE and suggesting innovative strategies for the concealment of access policy and security enhancement.

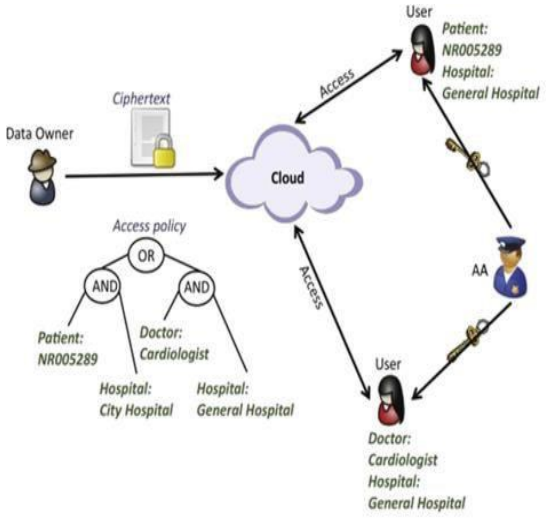


Fig.2. CP-ABE Architecture diagram

The above figure depicts key generation, encryption, and decryption procedures are among the elements of Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

CP-ABE guarantees that the identity of the records proprietor is not found out when a brand new record is uploaded. The statistics stored on the cloud remains confidential and inaccessible to unauthorized customers and the cloud itself. The gadget includes a mechanism that permits the cloud to confirm if a facts user is allowed to download a file with out revealing touchy records, including the user's identification. through integrating these additives, the proposed machine targets to offer a comfy and green answer for cloud-based records control and sharing, addressing both the desires for strong information protection and effective get admission to manage.

1.Establish a set of guidelines

Configuration $(\lambda\lambda) \rightarrow (PK, MSK)$ ----(1)

The primary technological centre is responsible for executing this algorithm. Using a y generator, the

KGC chooses two finite high order P random cyclic symmetric groups, G11 and G22. G11 → G11 × G22 is the description of the bilinear map where $\lambda\lambda$ is taken into account as a public protection parameter.

KGC selects exponents at random, in particular $\psi\psi$ and $\gamma\gamma \in \mathbb{Z}R$ZR.
The protection parameter ($\lambda\lambda$) and exponents ($\psi\psi$, $\gamma\gamma \in \mathbb{Z}R$ZR) are used to construct the general public key (PK) and a master mystery key (MSK).

MSK = (γ, yψ) is the master secret key. ----(2)

2. Generation of keys
KeyGen → SK (PK, MSK, A) ----(3)
In this way, a mystery key is generated for the legitimate user (U*t*t) by running the public key (PK), grasp mysterious key (MSK), and set of attributes (SA) as enter. The secret key is produced mostly using several random integers M*t*t, M*j*j$\in \mathbb{Z}R$ZR.

$$\text{Secret Key } SK_{U_t} = (D = y(\psi + Mt)/\gamma, \forall \text{ in } j \in A: D_j = y^{M_t} * H(j)^{M_t}, D'(j) = y^{M_t}) \quad \text{----(4)}$$

3. Putting the Keygen's signature

The owner of SignKey (sk) → pk records selects a range of x at random from 0 to R − 1 in the C language. The non-public key (x) and public verification key (ok = y*x*x), where y is the G11 generator, are the results of this characteristic.

4. Signing and Encryption Encryption Sign

In our suggested approach, the get right of entrance to control is achieved by inserting the get right of entry to coverage inside the ciphertext. An get entry to structure is the expression for the get right of entry to coverage. Indoor nodes define the brink gates, while leaf nodes describe user credentials and attributes. Algorithm 1 has been used to anonymise the access policy. Prior to initiating the process, the message P is encrypted using the public key. Set of rules 2 with a collection of leaf nodes (L) explains the suggested encryption and signature system.

Algorithm 2: Algorithm for data encryption

```
Function (EncipherSign (PK, P, AP))
Anonymization (AP)
if node = = root then
    for root node W, do
        set q_W(0) = A
    end
end
C' = P. e(y, y)^{ψA};
C = h^A
if node = = leaf then
    for all leaf nodes l ∈ L do
        C_l = y^{q_l(0)}; C'_l = H(att(l))^{q_l(0)}
    end
end
Signing (P, x)
```

5. Verification and Decryption

DecipherVerify → P, success/failure (PK, SK*t*t, C1, $\sigma\sigma$, pk) ----(5)

With regard to policy admittance and cloud user, the decryption process is successful. If not, the ciphertext cannot be decrypted by the cloud person. If you wish to avoid an insider attack, you can use the BLS fast signature to verify whether the owner of the information is authentic.

Algorithm 4: Algorithm for Decryption and Verification

```
Function(DecipherVerify (PK, SK_{u_i}, CT, σ, pk))
DecipherNode (CT, SK, l)
if policy is satisfied by A then
    A = DecipherNode(CT, SK, P) = e (y, y)^{MA}
    C′ = P. e(y, y)^{ψA}; e (C, D) = e (y^{ψA}, y^{(ψ+M/γ)})
    P = C′ / (e (C, D) / A)
end
Verify(σ, pk)
```

Algorithm 5: Algorithm for Node Decryption

```
Function(DecipherNode (CT, SK, l))
for each leaf node l do
    assign j = attr(l)
    if j ∈ A then
        DecipherNode = e (D_j, C_x) / e (D′_j, C′_x)
        return (e (y, y)^{Mq_l(0))}
    end
    else
        return null
    end
end
```

6 Signature Verification

This algorithm takes a message (P), computed hash (σ) and the public key of users (pk) and verifies the signature as shown in Algorithm 6

$$\text{Verify } (P, \sigma, pk) = e(\sigma, y) = e(h(P), y^x)$$
$$e(h(P^x), y) = e(h(P), y^x)$$

Algorithm 6: Algorithm to Verify the Signature

```
Function(Verify (P, σ, pk))
if e (σ, y) = e (h(P), y^x) then
    return Success
    else
        return Failure
    end
end
```

Advancing Data Security with Attribute-Based Encryption:

In the ABE framework, participating entities consist of customers and authority organizations. legal corporations manage attributes and trouble characteristic keys to customers. customers are categorized as message senders and recipients. basic ABE can cope with limit boundary hobby of attributes, and the restriction boundary is ready by using the government[9]. numerous pragmatic programs required to assist 'boundary limit(threshold), 'OR', 'AND' and non-activity of attributes as in line with adaptable get admission to manipulate procedures, so the source can determine get admission to manipulate structures.

ABE is a form of open key encryption wherein the secrets key of a purchaser and ciphertext are subject to attributes. In such a framework, interpreting of cipher textual content is attainable, furnished that the arrangement of key attributed of consumer suits cypher textual content's attributes. Sorts of encryption techniques depending on attributes are: Key-policy ABE[10].

Fig.3. Cipher textual content-coverage ABE

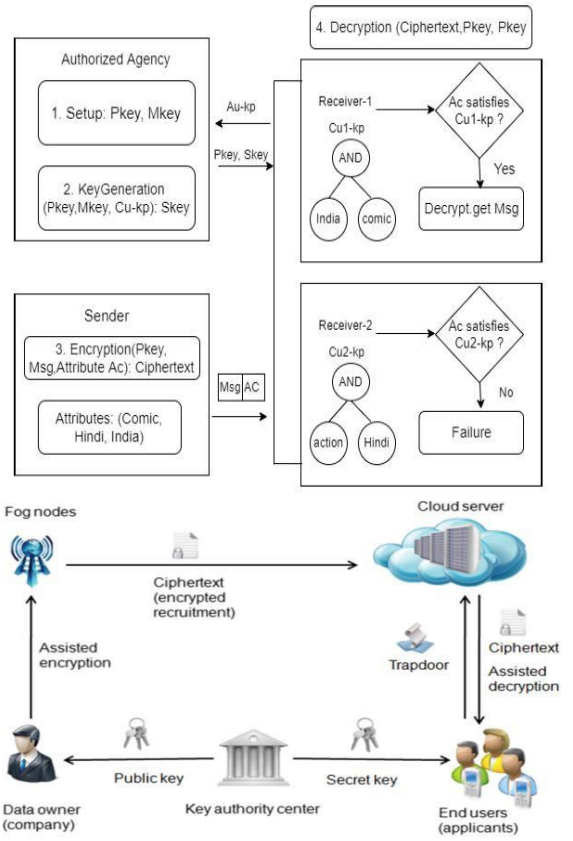


Fig.3. Cipher text-Policy ABE.

The above figure is an illustration of CP-ABE that shows how access rules and characteristics control data encryption and decryption to provide safe cloud storage.

IV. METHODOLOGY

The framework of proposed get right of entry to control approach is outlined in determine five, which offers assurances to carry exceptional-grained get right of entry to manage along protection from insider's attacks. The framework incorporates of 4 distinct elements. records owner is accountable for encryption of all records using access method previous to shifting to the cloud[11]. The Cloud Server stores the records owner's files and allows clients with license to statistics get entry to. patron,

key production machine is accountable for generating a secret key for clients of the cloud. the genuine customer having mystery keys gratifying the policy of access is ready for decryption of statistics. Key production machine (KPS) is chargeable for production and distribution of secret keys to actual customers of the cloud.

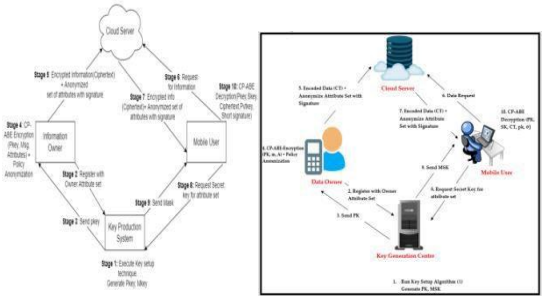


Fig.4. Key Production System

The above figure depicts key generation procedure in the suggested security architecture.

KPS first generates a grasp key and a public key at the initial level. The public key is then sent to the records owner by KPS. In stage three, the facts owner performs the encryption of facts. Statistics owner moves information which can be encrypted to cloud server in degree-4 with anonymously used policies for access. Then in level-five, consumer sends information request to cloud server[12]. The level-6 applied for cloud server to send a ciphertext to purchaser of facts. Then, in stage-7, records user places a request for secret keys for ciphertext obtained. In level- 8, KPS offers reaction to records person with a secret key. on the end, in level-9, information person performs decryption of ciphertexts and verifies for the authenticity of signature[13,14].

.

V. RESULT ANALYSIS:

1. The current study effort that conducted protection metric-based analysis evaluated the following metrics in addition to encryption, decryption, and ultimate touch time. Table 1 illustrates these device requirements for the recommended E-CP-ABE. The following could be used to describe them:
2. Encryption time: The ratio of encrypted basic text in bytes to the encryption time in milliseconds is used to compute the throughput of an encryption method [15,16], which provides an explanation of the encryption time.
3. Decryption time: The decryption time is the amount of time it takes the system to return the encrypted statistics to their original state.
4. Completion time: The total amount of time needed to do a task is known as the crowning glory time.

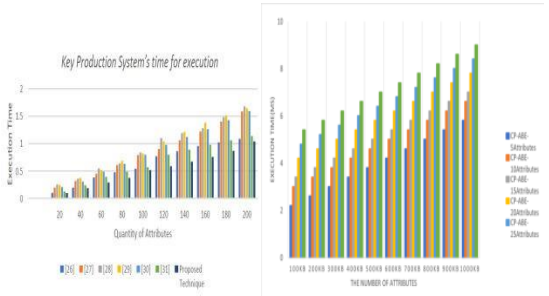
.

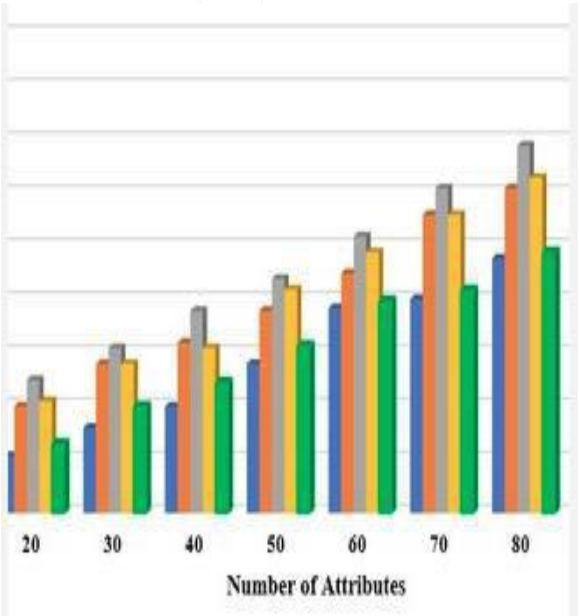
Table 1.

System requirements and their specifications for the proposed E-CP-ABES

System requirements	Specifications
Operating system	Window 10 64 bits
Processor	i9
Central processing unit frequency	3 Ghz
Random access memory	128GB

.





Scheme	Random Oracles	Security Model	Access Structure	Hidden Access Policy	Cipher text Size
CP-ABE	YES	Generic group model	LESS	NO	O(n)
CP-ABE	NO	Selective	LESS	NO	O(n)
CP-ABE +Hidden Access Policy	NO	Selective	AND Gates	YES	O(n)
CP-ABE +Hidden Access Policy	NO	Selective	AND gates	YES	O(n)+G_T
CP-ABE +Partially Hidden Access policy	NO	Selective	LESS	YES	O(n)
CP-AB +Hidden Access Policy	NO	Selective	AND gates	YES	O(n^2)+G_T
CP-ABE +Hidden Access Policy	NO	Selective	LESS gates	YES	O(n)+G_T
Proposed Method	NO	Selective	AND gates	YES	O(1)

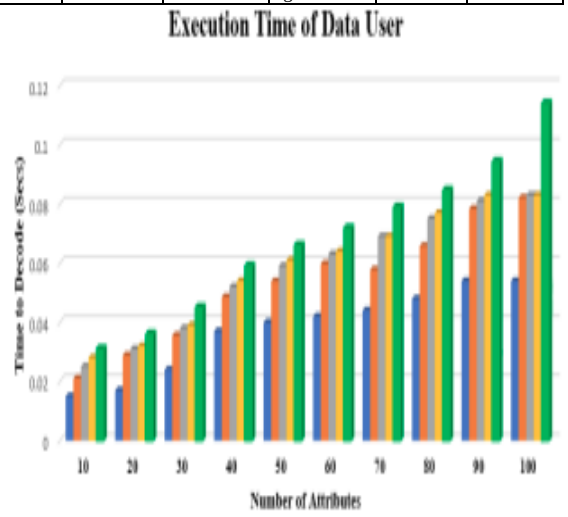


Fig.5.Execution time of key production system.

The above graph illustrates the effectiveness of the suggested strategy by contrasting the execution times for key creation across various cryptographic techniques.

Simulation parameters:

Simulation Parameters	Value
Number of Physical Machines (PM)	2-6
Number of Processing Units (PM)	4 per machine
Scheduling Interval (PM)	30ms
Monitoring Interval (PM)	180ms
No of Users	10-500
Total number of Tasks	100-1000
Number of attributes per User	5-20
Number of iterations	100
Cluster size	1-65

The distinction between Key-policy ABE and primary ABE techniques are Key technology and Decryption mechanisms. KeyGeneration approach can utilize secret sharing device and embody hierarchical method to symbolize an arbitrary polynomial whose remember of times isn't precisely the threshold cost of nodes for every node n in the tree [18].

Ciphertext-policy ABE makes use of get admission to tree for encryption of facts, and customers' secret keys are created over a group of attributes. access manage method is associated with cipher tree, the deciphering keys constrained with the aid of a bunch of attributes which can be depicted, and decoding keys may be gotten while the decrypting birthday party own regulations matched by attributes.

Here, n refers the number of attributes, Gr refers the prime order groups.

Cipher text-coverage ABE mechanism may be very widely known in cloud computing surroundings. to position it plainly, three ABE techniques are very precise, explicit info are displayed in desk-2, basic ABE can utilize boundary restrict policy, the volume of utilization is normally restrained; both Key-policy ABE and Ciphertext -coverage ABE have loads extra considerable programs, yet the weight of encrypting, decrypting and correspondence is extremely weighty.

Table 2 Key-Policy ABE and Ciphertext-Policy ABE comparisons

		Key-Policy ABE	Ciphertext-Policy ABE
SettingUp (λ, U)	Input	Safety Parameters	Safety Parameters
		Size of Attribute space	Size of Attribute space
		Size of User space	Size of User space
	Results	Pkey	Pkey
Encryption (Pkey, Msg, Attributes)	Input	Mkey	Mkey
		Pkey	Pkey
		Message	Message
		Set of Attributes	Structure of Access
	Results	Ciphertext	Ciphertext
Key Generation (Mkey, S)	Input	Mkey	Mkey
		Structure of Access	Set of Attributes
		Pkey	NA
	Results	Ciphertext	Secret Key
Decryption (Pkey, Ciphertext, Skey)	Input	Pkey	Pkey
		Ciphertext	Ciphertext
		Decryption key	Secret Key
	Results	Raw message	Raw message

When the decrypting party can fulfil the necessary strategy to accomplish decryption of the ciphertext, encryption serves no compelling purpose in identifying who decrypts the encrypted facts. The ABE mechanism depends on the difficult-to-interpret bilinear mixing conjecture of the elliptic curve [19]. It is extremely protected in principle and practice because ABE is connected to an access shape in the protection replica, which is difficult to implant into a normal tough assumption because to the complexity of the access structure.

(1) Outsourced statistics confidentiality. Before being uploaded to the cloud, the outsourced records are encrypted in our suggested systems. No one without valid access privileges is allowed to enter them.

(2) The anonymity of exchanging statistics. The anonymity of the owner can be guaranteed in statistics storage and sharing since the cloud server cannot identify the owner of the outsourced records.

(3) Great-grained access to control over encrypted statistics that are outsourced. In particular, a data owner can encrypt his outsourced data under a comprehensive access coverage such that only a select group of legal records users who fit the access coverage can access the data [20].

(4) Control the resistance to EDoS attacks and nameless down load requests. Any machine anyone can send a download request to a cloud server, which can control it and set it to be anonymous. We declare that our systems are safe from EDoS attacks with the manage over download request.

(5) High effectiveness.Our suggested buildings are built on the CP-ABE device's pinnacle. In contrast, they no longer have to deal with the significant additional burden of computation and verbal communication. Because of this, the structures can be used in actual worldwide applications.

The proposed strategies make use of anonymization of rules, further develops the safety approach and signature affirmation of the facts proprietor and distinguishes insider's assaults.To perform this anonymizations of guidelines, SHA1-at ease Hashing algorithm become applied. Be that as it could, stated hashing method provides an inappropriate overhead on the part of clients.

Results:

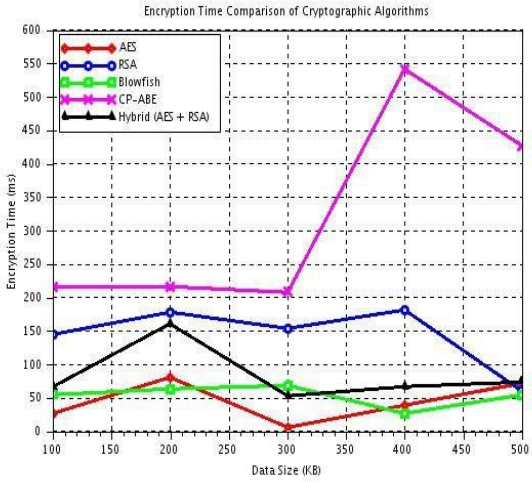


Fig.6.Encryption Time

The above graph displays the performance variations according on data size and compares the encryption times of different cryptographic algorithms.

Increasing the size of the data sets is what this graph evaluates in terms of milliseconds used for different encryption algorithms for five different cryptographic algorithms. CDSS has the highest encryption time, reaching up to 450 ms for larger data sizes with a steep increase at 400 KB. Hybrid Cryptography, Blowfish, and AES are low in their encryption times, which are below 50 ms for all data sizes. RSA comes in with a medium encryption time, varying around 100-200 ms. Hybrid Cryptography, Blowfish, and AES perform better in encryption time, whereas CDSS performs poorly: its encryption times

skyrocket when faced with large data.

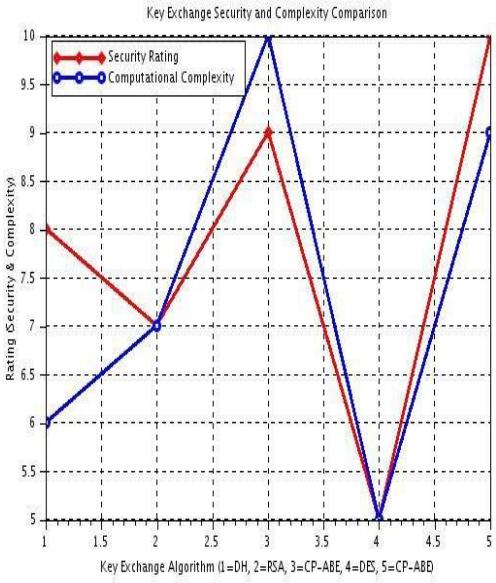


Fig.7.Key Exchange Security

The above graph depicts comparison of security strength and computational complexity of several key exchange techniques.

The graph discusses the comparison of the algorithms of key exchange according to a rating of 5-10 for a combination of algorithmic security and computational complexity. A result of 9 was plotted for RSA in security and moderate in computational complexity. For security and computational complexity. CP-ABE was plotted at the highest rating. DES scores lower for security but also for computational complexity, thus being less demanding in resources. Fair calibrations of moderate rating were shown by DH in security and complexity. CP-ABE is the most secure one but also the most computationally expensive one. DES is left for situations where computational efficiency outweighs the need for security.

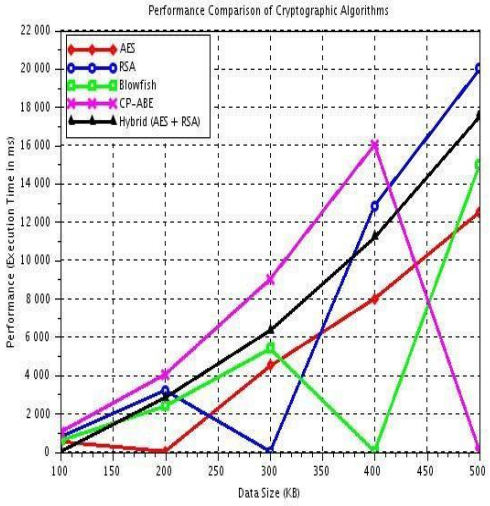


Fig.8.Performance

The above graph compares the effectiveness of several encryption techniques in cloud environments.

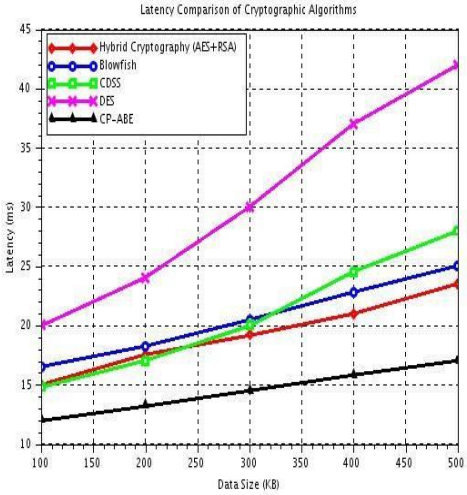


Fig.9.Latency

The above graph is comparison of cryptographic algorithms' latency that shows how various encryption techniques affect the pace at which data is processed.

This graph contrasts the latencies (in milliseconds) for five cryptographic algorithms: Hybrid Cryptography (AES+RSA), Blowfish, CDSS, DES, and CP-ABE- from 100 KB to 500KB data size. CP-ABE has the best performance with less latency, not exceeding 15 ms for any of the data size considered.

Moderate latencies are shown by Hybrid Cryptography, Blowfish, and DES, increasing from 15 ms to about 25 ms linearly.
Meanwhile, the CDSS has the highest latency, starting at 15 ms and then rising steeply to 45 ms as the data size increases. CP-ABE is the best in terms of low latency while the CDSS is the worst as it tends to have very high latency growth with increasing data sizes.

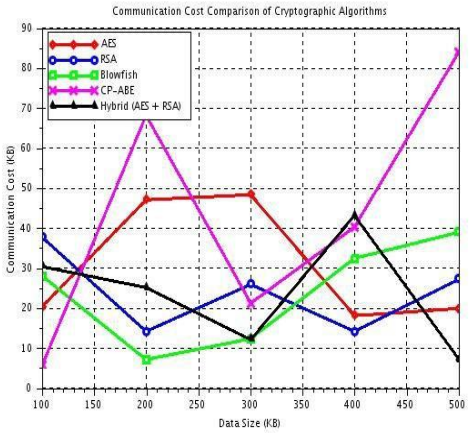


Fig.10.Communication cost

The above graph is analysis of the latency of cryptographic algorithms that demonstrates how different encryption methods impact the speed at which data is processed.

This graph depicts the communication cost (in KB) of five cryptographic algorithms(AES, RSA, Blowfish, CP-ABE, and Hybrid Cryptography) as the data size increases between 100 KB and 500 KB.CP-ABE incurs the highest communication cost and rises sharply with an increase in data size. Hybrid Cryptography by contrast keeps communication costs low and stable for all data sizes. Blowfish and RSA occupy moderate values of communication cost but are steady throughout.AES incurs various communication costs but remains a low-cost algorithm with low cost in comparison to CP-ABE. Hybrid Cryptography offers better trade-offs for communication cost and efficiency, whereas CP-ABE incurs significantly high communication costs, thus rendering it unsuitable for large data communication.

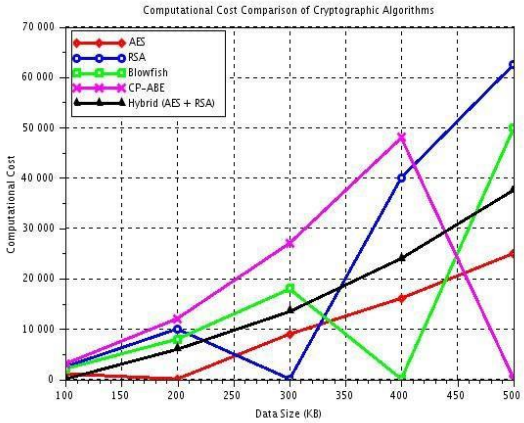


Fig.11.Computational cost

The above graph illustrates the processing load for each cryptographic technique by comparing its computational expenses.

The graph compares the computational costs (in arbitrary units) of AES, RSA, Blowfish, CP-ABE, and Hybrid Cryptography about increases in data size. CP-ABE has shown a computational cost of more than 60,000 units when data sizes go above 400 KB, the maximum so far. Blowfish has had varied computational costs, peaking at about 50,000 units. Hybrid Cryptography has been in the realm of moderate computational costs, increasing linearly to about 30,000 units. AES and RSA have retained the lowest computational costs with all data sizes. AES and RSA, on account of being low-cost, fit well in resource-restricted environments. CP-ABE takes the cake in security; however, it is crippled by exorbitant computational costs, making it almost impossible to use for larger datasets.

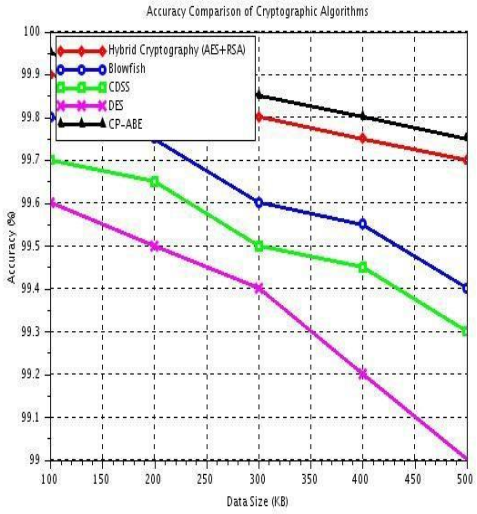


Fig.12.Accuracy

The above graph that shows the efficacy of several cryptography algorithms in securely encrypting and retrieving data by comparing their accuracy.

The graph shows the accuracy (%) comparison of five cryptographic algorithms (Hybrid Cryptography (AES+RSA), Blowfish, CDSS, DES, and CP-ABE) with increasing sizes of data (100 KB to 500 KB). With increasing data sizes, Hybrid Cryptography (AES+RSA) and CP-ABE lie at the upper accuracy range, almost 99.8%. In contrast, CDSS decreases sharply with accuracy, from 99.6% to almost 99.0%, with increasing sizes of data. Blowfish and DES also show a steady decline but are not as pronounced as CDSS.PC-ABE has a steady performance with comparable accuracy with Hybrid Cryptography.

VI. CONCLUSION & FUTURE SCOPE

We provided dual access to manage structures and resolved an intriguing and persistent problem with cloud-based data sharing. Using characteristic-based encryption techniques to encrypt data in cloud computing ensures both security for data that is outsourced and fine-grained access control. In order to improve the privacy of data in the cloud, this study presents a novel plan. The suggested method not only effectively protects data in the cloud but also confirms the accuracy of the data against potential attacks. The technique is printed, the experimental results are shown, and a comparison with six similar current procedures is made through focused discourse in this newsletter. The suggested architectures are impervious to DDoS and EDOS attacks. We claim that other CP-ABE structures can "transplant" the technique employed to obtain the function of control on down load request. In contrast to its underlying CP-ABE building block, our experimental results demonstrate that the suggested structures do not impose any appreciable computational or communication burden. We use the fact that the enclave's private data cannot be retrieved in our upgraded device. However, recent research indicates that Enclave may also divulge some of its secrets to a hostile host using memory access methods or other related aspect-channel attacks. Thus, the model of clear enclave execution is includedIt's an intriguing challenge to build a dual access control system for cloud information sharing from a visible enclave. We can consider the similar technique to the hassle in our upcoming paintings.

VII. REFERENCES

[1] Ahmad, S. A., & Garko, A. B. (2019, December). Hybrid cryptography algorithms in cloud computing: A review. In *2019 15th International conference on electronics, computer and computation (ICECCO)* (pp. 1-6). IEEE.

[2] Biswas C., Gupta U. D and Haque M. M. (2019). An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography. International Conference on Electrical, Computer and Communication Engineering, pp. 1-5. doi:10.1109/ECACE.2019.8679136.

[3] Chandra S., Bidisha M, Sk. S Alam, Siddhartha B. (2015). Content based double encryption algorithm using symmetric key cryptography. 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) doi: 10.1016/j.procs.2015.07.420., Procedia Computer Science 57 (2015) 1228 – 1234.

[4] Elminaam D., Kader H, Hadhoud M. (2010). Evaluation of the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, vol.10 issue3, pp. 216–222

[5] Zhou, Z., & Huang, D. (2012, October). Efficient and secure data storage operations for mobile cloud computing. In *2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualiztion management (svm)* (pp. 37-45). IEEE.

[6] Ren, Y. J., Shen, J., Wang, J., Han, J., & Lee, S. Y. (2015). Mutual verifiable provable data auditing in public cloud storage. *網際網路技術學刊*, *16*(2), 317-323.

[7] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained

Access Control of Encrypted Data. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 89–98. https://doi.org/10.1145/1180405.1180418
[8] Richa, Singla and Richa, Dutta (2017). 'Hybrid Algorithm for Cloud Data Security'. International Journal of IT & Knowledge Management (IJITKM), volume10 issue2, pp 18-26
[9] Ruj, S., Stojmenovic, M., & Nayak, A. (2013). Decentralized access control with anonymous authentication of data stored in clouds. *IEEE transactions on parallel and distributed systems*, *25*(2), 384-394.
[10] Stalling, W. (2014). Cryptography and Network Security. Harlow, United Kingdom: Prentice Hall.
[11] Taha A.A, AbdElminaam D.S, Hosny K.M (2017). 'NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment'. International Journal of Advanced Computer Science and Applications volume8 issue 11.
[12] Timothy D. P. and Santra A. K.,(2017), A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5. doi: 10.1109/ICMDCS.2017.8211728
[13] Khan, N., & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science*, *94*, 485-490.
[14] Two Way factor Authentication, (n.d), retrieved from https://www.imperva.com/learn/application-security/2fatwo-factor-authentication/
[15] Li, J., Chen, X., Li, M., Li, J., Lee, P. P. C., & Lou, W. (2014). Secure Deduplication with Efficient and Reliable Convergent Key Management. *IEEE Transactions on Parallel and Distributed Systems*, 25(6),1615–1625.
[16] Marqas, R. B., Almufti. S. M. and Ihsan, R.R. (2020). Comparing symmetric and asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. Journal of Xi'an University of Architecture & Technology, 12(3), 3110-3116.
[17] Mohan, D. N., Kumar, V. H. and Shashank, N. (2020). Enhancement of cloud computing security with secure data storage using AES. International Journal of Research in Engineering, Science and Management, 3(1), 586–587.
[18] Saeed, Z.R., Ayop, Z., Azma. N. and Baharon. M.R. (2018). improved cloud storage security of using three layers cryptography algorithms. International Journal of Computer Science and Information Security, 16(10),34- 39.
[19] Patil, S., Vhatkar, P., & Gajwani, J. (2014). Towards secure and dependable storage services in cloud computing. *Int. J. Innovative Res. Adv. Eng*, *1*(9), 57-64.
[20] San, M. M. and Win, K. M. (2019). Risk management of secure cloud in higher educational institution. International Journal of Trend in Scientific Research and Development, 3(5), 1314-1319.
[21] Sharma, Y., Gupta, H. and Khatri, S. K. (2019). A security model for the enhancement of data privacy in cloud computing. In: IEEE Amity International Conference on Artificial Intelligence, Dubai, United Arab Emirates, United Arab Emirates, 4-6/02/ 2019. DOI:10.1109/AICAI.2019. 8701398
[22] Singh, B. and Sharma, S. (2019). Enhancing data security using encryption and splitting technique over multicloud environment. International Journal of Scientific Research & Engineering Trends, 5(3),1041-104.
[23] Zhang, F., & Al-Turjman, F. (2023). Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. *Applied Soft Computing*, 132, 109909.
[24] Venkateswaran, N., Vidhya, K., Ayyannan, M., Chavan, S. M., Sekar, K., & Boopathi, S. (2023). A Study on Smart Energy Management Framework Using Cloud Computing. In *5G, Artificial Intelligence, and Next Generation Internet of Things: Digital Innovation for Green and Sustainable Economies* (pp. 189-212). IGI Global.
[25] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.
[26] Logesh, K., & Subramanian, S. (2022). Secure and Efficient Dual Access Control Scheme in Cloud Based Data Storage and File Access with QR Code. *Child Studies in Asia-Pacific Contexts*, *12*(1), 53-63.
[27] Tang, X., Guo, C., Choo, K. K. R., Jiang, X., & Liu, Y. (2024). A secure and lightweight cloud data deduplication scheme with efficient access control and key management. *Computer Communications*, *222*, 209-219.