Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI LEVEL ENCRYPTION CIPHERTEXT USING MULTI BLOCKS AND SECURE DATA ACCESS POLICY IN CLOUD COMPUTING

[1*]SAJJA KRISHNA KISHORE, [2]DR. GUDIPATI MURALI, [3]DR. PADMAJA PULICHERLA

[1]Research Scholar, Department of Computer Science & Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India
[1]Assistant Professor, Department of Computer Science & Engineering, P.V.P. Siddhartha Institute of Technology, Vijayawada-520007, Andhra Pradesh, India
[2]Professor, Department of Computer Science & Engineering, KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Guntur, Andhra Pradesh, India
[3]Professor, Department of Computer Science & Engineering, Hyderabad Institute of Technology and Management Hyderabad, Telangana, India
Corresponding Author*: krishnakishoresajja@gmail.com

ABSTRACT

An emerging paradigm in computing that aims to provide customers with the right solutions are cloud computing. Whether multi-layer authentication or multi factor verification makes accessing data stored in a cloud computing environment simple, it relies mostly on many current technologies such as virtualization, grid computing, etc. Results from the simulation show that three-tier authentication is more efficient than competing methods, lending credence to its viability as a cloud authentication solution. To enhance cloud safety and provide effective privacy security, a multi-level micro-access limitation formula is first suggested. Cloud data goes through many layers of indexing. Security is used to varying degrees during data transmission. The advantages listed in the configuration papers are used to assess the customer's requests for reliable accessibility. Data stored in the cloud is similarly encrypted using a key that is owned by the data owner. Both the efficacy and precision of cloud security and privacy protection are improved by this method.

Keywords: *Multi-level, Micro-Access, Privacy, Cloud Data, Security, Authentication, Trusted Access, Encrypted*

1. INTRODUCTION

On the topic of cloud computing, security, and privacy-preserving user profiles, as well as other related topics. We discuss the cryptographic methods and data with attention, including topics like Live Personalised Target Evaluation with Multi Degree Accessibility Restriction to Improve Personal Privacy Preservation performance [1]. A lot of thought has gone into the organising methods, and security and privacy are important factors that have been thoroughly discussed.

When it comes to huge data cloud storage and access, the suggested method provides the highest degree of security for multi-levels environments. To guarantee that only trustworthy consumers are able to purchase and access the data files, the recommended technique employs many layers of security, including authentication, authorization, secrecy, and information honesty [2].

1. uses Characteristic Based Encryption (ABE),
2. System uses Advanced Security Standard (AES),
3. uses a hybrid of ABE and AES, and
4. uses a suggested formula called Secure Dynamic Bit Standard (SDBS), which employs high safety for the data saved by the end user. Additionally, there are other cryptography systems that are utilised for file encryption. Two distinct secrets, one created by the Cloud Service Provider (CSP) and one by the SDLBR method, provide security. The three most important sizes are 128 bits, 256 bits, and 512 bits, all of which are included in the SDLBR formula. Every step of the security process generates a randomly selected opener and session key length. On demand, CSP sends encrypted opener and session essentials to data firms after securing the passkey with session key. After encrypting the data file with the decrypted opener, the information provider uses the session secret to decrypt the master key. The data person must first submit a request to the CSP in order to get the decryption key; only once the information customer has been authenticated and

authorised will the CSP deliver the encrypted opener and session key, allowing the data

The proposed job's goals are briefly outlined in this section. A novel approach to user and service provider security in the cloud computing environment is proposed after research into shadow solution security issues and an analysis of current cloud safety and security-based innovations, methodologies, tools, and protocols. The following are the mounted objectives:

To allow the Cloud Service Provider (CSP) to authenticate and authorize several users through l ogin and registration with their unique details [3].

For the purpose of encrypting and decrypting data documents using the MA-ABE and MA-CP-ABE algorithms. The one-of-a-kind programme when working with data documents in the big data cloud, it is necessary to use Secure Dynamic Little Bit Requirement (SDLBR). SDLBR ensures security using randomly selected three-bit levels, including 128 bits, 256 bits, and 512 bits [4].

Encrypting the master key with the session secret and having the Cloud Provider (CSP) generate the passkey and session secret adds an extra layer of security to the MA-CP-ABE technique. Upon request, CSPs provide encrypted passkeys and session keys to authorised data companies in order to safeguard data documents. After securing the data documents and uploading them, the information provider should decrypt the passkey using the session key [5].

individual to decrypt the documents.

iv. the authorised user may access the Large Information Cloud and download and install files, adding an extra layer of security.

v) To establish a Proof of Ownership (PoW) in order to identify the original file creator and their uploading credentials to the massive data cloud. Anyone who downloads the file will be able to identify the original creator since this reveals where the file came from. For the protection of sensitive information stored in the Large Information Cloud, this system employs numerous layers of authentication [6].

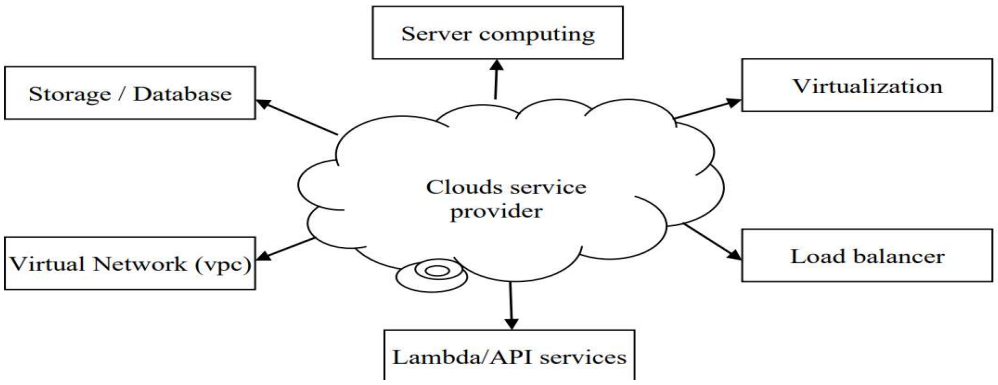


Figure 1: Cloud Computing Services

2. LITERATURE SURVEY

Encryption is a basic technique that is applied to secure sensitive data especially in cloud computing. Cryptographic approaches for securing data in clouds can be generally classified into two types: symmetric and asymmetric encryption methods.

Symmetric Encryption-Based Approaches

Symmetric encryption is based on a single key for encryption as well as decryption purposes. Symmetric encryption-based approaches have been widely explored for secure cloud storage and data protection. Li et al. [7] proposed a technique that supports multiple encryption keys and file partitioning to improve cloud data security. This ensures isolated storage and secure access control. Sookhak et al. [8] incorporated techniques such as "lazy undo," "keychain," and "broadcast encryption" to improve secure data updates and transitions in access permission. Another notable contribution is the Trust Store approach by Liu et al. [9], which uses a specialized key management service provider. This allows different encryption keys for various files and hash-based integrity checks to be included for maintaining data integrity. Symmetric encryption techniques are highly efficient for encryption and decryption, but they suffer from key management and flexibility issues. These issues become more critical in large-

scale cloud environments where there is multi-tenancy and dynamic data sharing.

Asymmetric Encryption-Based Approaches

Asymmetric encryption methods address some of the challenges of symmetric encryption by using separate keys for encryption and decryption. One widely studied approach is Attribute-Based Encryption (ABE), where encryption is performed using predefined attributes as public keys, allowing for fine-grained access control. Wu [10] proposed a hybrid model that combines ABE with symmetric encryption, achieving both secure storage and controlled data access. ABE has been successfully applied to specific domains like healthcare where sharing medical documents in the cloud was made safe in [11].Another type of asymmetric encryption technique for increasing the security level of data within the cloud is Proxy Re-Encryption (PRE). An authorized third party is allowed to re-encrypt the stored data and, in the process, assure secure access control without disclosing the original decryption key [12]. Zhang [13] introduced a fine-grained approach to PRE that involves identity-based encryption and conditional re-encryption mechanisms to enhance the access control policies. Jiang and Guo [14] refined the concept by implementing a confidentiality-preserving access control scheme, while Goyal [15] designed a PRE scheme that supports multi-tenant data sharing through one-time encryption with multiple re-encryption capabilities [16].

Multi-Level Access Control Approaches

Several studies have proposed enhancements to ABE by introducing multi-level access control mechanisms. Works such as [17] extend classical ABE schemes by requiring users to satisfy a structured set of attributes before decrypting data, thereby achieving hierarchical and tiered access control. These approaches improve security by ensuring that different users have access to data based on their level of authorization [18].

Attribute-Based Access Control (ABAC) Models

The formalization of policy-based models is an important feature of secure access control in cloud environments. ABAC has gained significant attention for the ability to mathematically define access policies. Gupta and Sandhu [19] presented a model known as Hierarchical Group and Attribute-Based Access Control (HGABAC) that [20] enables attribute assignment and management by means of three sub-models, namely, User Attribute Assignment (UAA), User-Group Attribute Assignment (UGAA), and User-to-Group Assignment (UGA) [21]. However, their work was mainly on the administrative framework rather than an encryption scheme. In another study, Bhatt et al. [25] proposed a restricted version of HGABAC, which was implemented using the NIST Policy Machine (PM) tool [26]. This work demonstrated practical enforcement of hierarchical access control policies, making it a step toward robust cloud security frameworks.

The proposed scheme, *Multi-Level Encryption Ciphertext Using Multi Blocks and Secure Data Access Policy in Cloud Computing*, introduces a novel approach to enhance data confidentiality and access control in cloud environments. Unlike traditional encryption models, this framework employs a **multi-level encryption mechanism** where data is fragmented into blocks, and each block is encrypted independently using varying cryptographic techniques. This multi-block strategy not only complicates unauthorized decryption but also allows selective encryption based on sensitivity levels, optimizing both security and performance.

A key innovation lies in the **integration of a dynamic data access policy** that ensures only authorized users, based on predefined roles or attributes, can decrypt specific blocks of data. This fine-grained access control model is adaptive, enabling real-time policy updates without re-encrypting the entire dataset. Additionally, the scheme supports secure key management and prevents common vulnerabilities such as key exposure and data leakage.

By combining **block-level encryption, hierarchical security layers, and policy-driven access control**, this approach significantly mitigates threats associated with cloud data breaches and insider attacks. The framework is particularly suited for applications in healthcare, finance, and government, where secure and controlled data sharing is critical. This novel method ensures robust security while maintaining flexibility and scalability in cloud storage systems.

Hypothesis / Conceptual Model: The conceptual model of *Multi-Level Encryption Cipher text Using Multi Blocks and Secure Data Access Policy in* Cloud *Computing* is based on the hypothesis that **dividing data into multiple blocks and applying hierarchical encryption techniques, combined with dynamic access control policies, can significantly enhance data security and access management in cloud environments**.

In this model, data is segmented into logical blocks, each encrypted at different security levels depending on data sensitivity. These encrypted blocks are stored in the cloud, and a **secure access**

policy—based on user attributes, roles, or access levels—governs who can decrypt and access specific blocks. A centralized or distributed **key management system** ensures secure key distribution and revocation.This approach ensures that even if one block or key is compromised, the rest of the data remains secure. The model promotes confidentiality, integrity, and fine-grained access control, addressing critical challenges in cloud data security and compliance.

3. METHODOLOGY

3.1. Data Centers of Cloud Computing

Cloud data is stored in the information centres. It is possible to cluster several storage-capable web servers in closely spaced locations, all of which are accessible over the internet. With virtualization [27], you may create several instances of a single server, reducing the redundant expense that comes with building multiple servers in a single data centre. Cloud storage is housed at the data centres. It is possible to cluster several storage web servers in closely spaced locations, all of which are accessible over the internet. Virtualization [28] allows you to build several instances on a single data web server, which decreases the recurring cost of installing multiple servers in one physical place.

Overview Of Data Security and Privacy Preserving

Everything in today's fast-paced world of informatics is embracing it. Businesses store and make available customer, partner, and product-related data in cloud environments. But many people in your firm, both workers and consumers, have access to it. Atmospheric layers inside a cloud may store and distribute a wide variety of materials. Data security and individual privacy preservation, as shown in Fig 3. Your business and its employees are able to accomplish a great deal thanks to these services. The provider's solution remains accessible in cloud settings [29]. A Third-Party Auditor (TPA) monitors the situation and decides on a course of action. Many people have access to the many pieces of client data that organisations store in their systems and environments. This data contains a variety of sensitive information that has to protect and kept away from other people who should not have access to it. Unauthorised individuals will try to access your private data if you do not access the cloud option. Therefore, security [30] is critical to prevent unauthorised parties from gaining access to sensitive information, maintain the privacy and integrity of individuals' data, and provide consumers with more options for protecting their data.

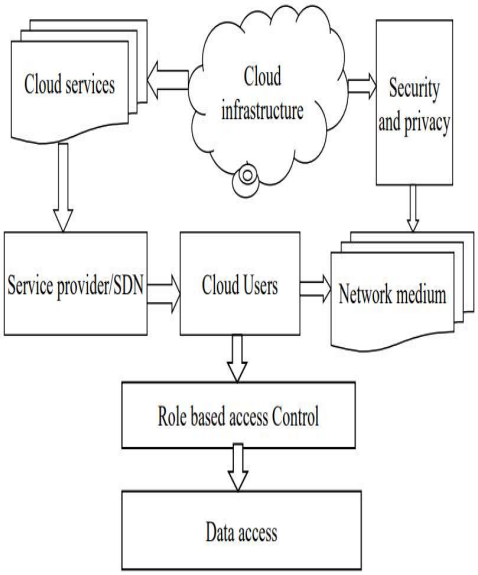


Figure 2: Data security and privacy preserving

3.2. Cryptography Privacy And Security Principles

The incorporation of many robust file encryption techniques into the cloud computing approach enhances privacy security [31]. This method would effectively remove the encryption keys and end the operation when the data needed for encryption is no longer there.

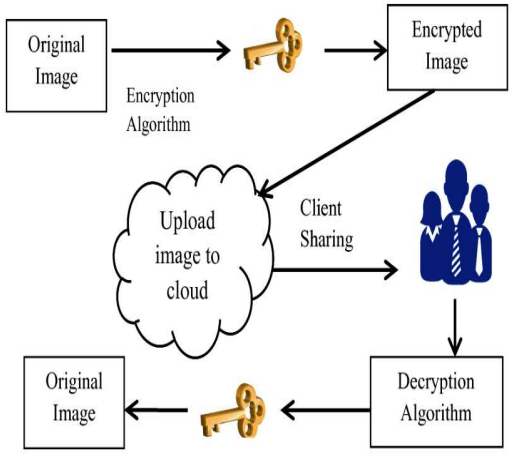


Figure 3: Cloud Encryption Model

3.3. Cipher-Text Policy ABE (CP-ABE)

The CP-ABE gives the person encrypting the files full control over the access plan [32]. The evolved system's public trick is becoming more

complex as the method does, and the system is primarily focused with community concerns. All the calculations take place in these zones, hence access considerations are always important. To make these points resilient enough to fight against vulnerabilities, a beneficial style method is needed so that this technique centres on ensuring structural stability.

3.4. Key-Policy ABE (KP-ABE)

Connected to the process of encrypting and decrypting files, this approach relies heavily on including characteristic collections [33] to specify the cipher-texts. The encryption process for the file is carried out individually by combining the private keys that are supposed to safeguard the communication [34]. However, the consumer is responsible for performing the decryption procedure independently.

3.5. Fully Homomorphic Encryption (FHE)

Prior to decryption, which basically converts the cypher text to plain text, FHE aims at straight calculation of the cypher message, also called the encrypted information. Any kind of mathematical method may be performed directly on the encrypted data. Fig 4 illustrates the Homomorphic security mechanism.

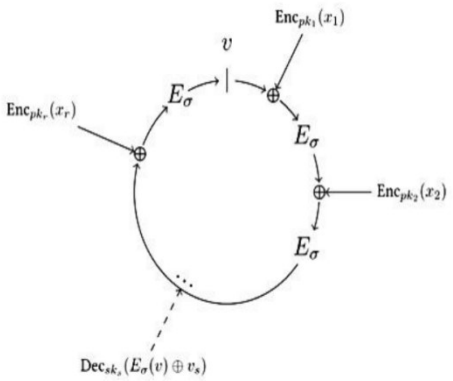


Figure 4: Homomorphic Encryption Process

3.6. Multi-level micro access restriction

People who use the cloud need solutions that provide them access to data organised at different levels and with different capabilities [35]. Accessing the characteristics at each level requires user identification since this technique organises various data at several levels and retains arrangement records. This is how the method zeroes in on the dependent gain access episode for each capability level and calculates the Multi-Level Access Restriction(MLAR). Relying on the value of MLAR, customer access is restricted and corporate accessibility is managed accordingly.

3.7. Analysis Of Cloud Security And Privacy

3.7.1. Data Integrity

Incredible as it may seem, it is a crucial part of every information system. Data security usually refers to preventing data from being made, removed, or altered without authorization.

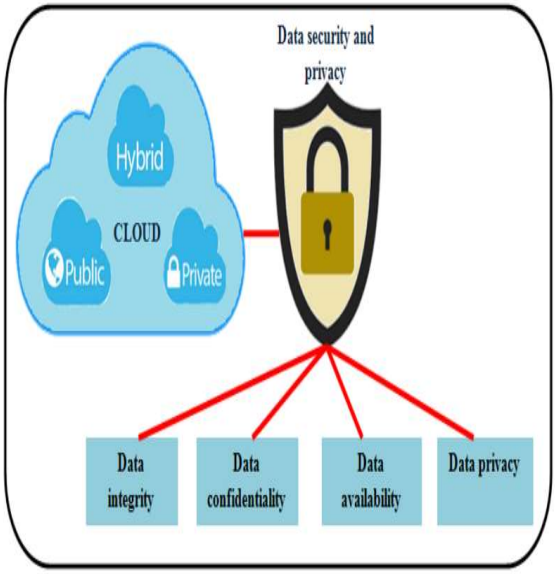


Figure 5:Data privacy and Security In Cloud Computing

The security and privacy of data is stored in the cloud. Ensuring an entity's access and civil liberties to designated venture resources helps prevent the misuse, theft, or overutilization of essential services and information.

3.8. Data Confidentiality

The ability for clients to store sensitive information in the cloud is crucial. The methods for gaining access to control and verification are used to ensure the privacy of information. Increases in cloud reliability and security might address issues with data access control, secrecy, and verification in the cloud.

3.9. Information Accessibility

The users may verify their data by using techniques other than relying on the CSP's guarantee of credit ratings in the event of crashes such as network failures, hard drive damage or IDC fires, and how much data can be recovered or used in such a scenario.

3.10. Personal Information Security

Being able to compartmentalise one's own or one's own exclusive knowledge is a key competence for any organisation or person.

3.10.1. Methods of Privacy Preservation

In reality, a new method is developed to guarantee the confidentiality of user data stored in the cloud. This is accomplished by either restricting access or encrypting the data so that only loyal consumers can access it. In this domain, such methods are located.

3.10.2. The encryption of data files by associates

Access control rules may be fine-grained using attribute-based gain access to control, which is a collection of mechanisms that rely on run-time evaluations of attributes. The main goal of plan enforcement is to ensure that all resources are used and handled according to the established regulations. Some large data platforms, for instance, already implement data expiration schedules. Examining policy compliance and providing evidence are essential components of accountability. Providing automated and scalable control and auditing systems to check the degree of conformance is a pillar of accountability in the context of personal privacy conservation. Explaining how data is collected and used is essential for transparency. Multichannel and split approaches, together with standardised symbols, provide transparency in the era of big data. To establish the legitimacy and origin of information is the foundation of information provenance. Mobility and access facilitate data processing and consumption in many scenarios. The ability to easily access data implies that individuals may verify the information that is kept. Thanks to portability, customers may switch providers without sacrificing any of their data. Specifying and enforcing norms for data use and management is what customer control is all about. Along with individual privacy settings and data storage, consent methods provide for extensive user control.

The data is protected at each attribute level by the attribute-based critical file encryption algorithm. The method commits a details key to the details information and uses it to encrypt data for each claimed characteristic of the information. Once the client has the secret, he may decrypt the data and access the original information.

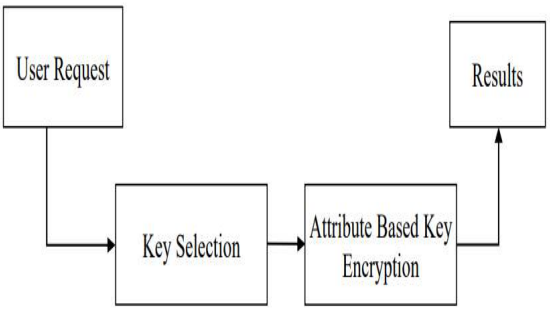


Figure 6: Attribute-Based Data Encryption

We start by identifying the data requested from individual requests. For each attribute, we have a unique key that we already offer to the clients. The cypher text is generated by securing the characteristics using the defined methods. It is the responsibility of the user on the receiving end to decode the data correctly. When a consumer has the essentials from any detailed attribute, they may acquire the original worth of any particular characteristic.

3.11. Block Level Encryption

The approach splits the data into a number of blocks with the same dimension instead of encrypting it at a quality level. Data is encrypted using different methods for each data block. The user would get the encrypted data. The person must be able to identify the size and diversity of blocks. The next step in obtaining the original data is to decode each block using the concern key. data recovery and customer demand are met by the block representation of a block-level file encryption approach. The derived data is partitioned into many blocks, with a unique secret assigned to each block. The user receives an encrypted result based on the selected key. In order to get the results, the user must reverse the process using unique block-specific methods.

3.12. Multiple Layers of File Security

This data is organised into teams using a multi-level method. Data quality is classified at several levels. The strategy would keep different systems and secrets for each level of data. We have therefore selected and protected a secret based on the degree of a characteristic in the data. This outperforms competing approaches in terms of security performance.This kind of data is organised into teams under different levels by the strategy. Various degrees of data characteristics have been recognised.

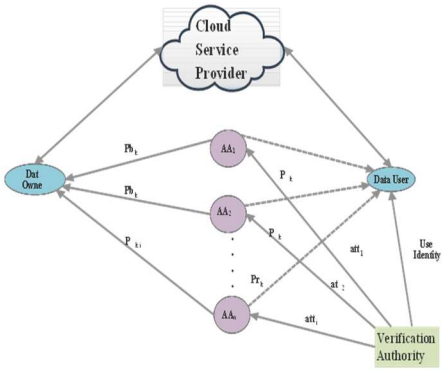


Figure 7:MA-CP-ABE with HC

Different keys and schemes would be preserved for each data level by the method. A key is chosen and secured based on the degree of a data characteristic. Compared to previous ways, this one improves security efficiency even more.

3.13. User-Friendliness, Portability, and Agency Management

Problems with accessibility and trans portability arise when data is transferred from a secure domain name to an unsecured one. In addition, the events participating in access and portability must have faith in one another. Every time a person moves data from one place to another, they must ensure that the data is processed in accordance with their assumptions. A previous agreement between the parties involved is necessary for this to be executed.

3.14. Implementation

In HC, Multi-Authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE) is combined to improve cloud data security. The network model of MA-CP-ABE with HC is composed of the following key entities: 1. Data Owner (DO) 2. Cloud Service Provider (CSP) 3. Data User (DU) 4. Attribute Authority (AA) 5. Verification Authority (VA)

This model will define an attribute-based access control policy by Data Owner (DO) and then encrypt data using a MA-CP-ABE-HCC before uploading it to the cloud. The encrypted data or messages are represented as hyperbolic curve points. Setup, key generation, and key distribution are performed by Attribute Authority (AA) and Verification Authority (VA).

An AA authenticates the attributes of the DU when he is accessing the data hosted in the cloud. If the attributes of the user comply with the access policy set by the DO, then the access policy would allow them to download and decrypt the data. Thus, only authorized persons can get their ciphertext and the security of the cloud is enhanced.

Homomorphic Cryptography

In the cryptographic approach the key generation by using HC based on the public technique for information security, the hyperbola takes a number of points in the hyperbola aeroplane with two fixed vertices in the connectedness. Homomorphic cryptography (HC) is included into the MA-CP-ABE strategy to enhance the security of data transmission in the cloud. For the purpose of creating robust and trustworthy file encryption and decryption methods, the proposed technique employs a novel trick creation mechanism. Computers carry out the confirmation procedure, and the personal secret is used in the reverse process of encryption, known as decryption.

HC and MA-CP-ABE work together to generate public vitals and secret keys. The hyperbolic aeroplane uses a number of parameters to complete the calculations. Two outcomes are considered to be the positive criteria used for public essential selection. Furthermore, the components that are being considered on the hyperbolic plane are provided as the points of emphasis that may be divided into individual cells. It is believed that the junction factor generates hidden tricks for performing encryption and decryption procedures to secure information in hyperbolic aircraft. The Diophantine equation that describes the hyperbolic feature of an aeroplane is given by Pell's formula, which is as follows:

$$x^2 - Ay^2 = 1 \quad (1)$$

From the equation (1) let us consider the coordinates of the aeroplane which is engaged in the public critical generation. It is possible to calculate the hyperbolic formula using Pell's equation. We find the origin of the non-square integer. Not only is Pell's assertion presented with the curve, but its characteristics and elements are also explicitly defined.

So far, the solution sets have two pairs of values (-1,0) and are not NULL.

Specifically, on the finite area, the equation may be described by distinct integers.

By utilising the aforementioned solutions and the subsequent services via the persistent connections, all non-trivial treatments may be computed.

The alternatives may be conveniently produced using the fundamental options based on the numerous algebraic formulas.

The product function is the main activity involved with this.

(f_n), is stated as the point sets that lies over the hyperbolic curve and, the equationwhere, '$\mathbb{Z}$' denotes the random set is given as,

$$(A) = \{(x, y)|x < n, y < n \text{ and } x, y \in \mathbb{Z}\} \quad (2)$$

$$f: HP(A).\ HP(A) \rightarrow HP(A). \quad (3)$$

$$f(< E, F >) = E.F = (x_1, y_1).(x_2, y_2) = (x_1 + y_1\sqrt{A})(x_2 + y_2\sqrt{A})$$
$$(x_1\ x_2 + y_1y_2A) + (x_1\ y_2 + x_2y_1)\sqrt{A} = (x_3, y_3) = R \quad (4)$$

$$E * F = (x_1, y_1) * (x_2, y_2) = (x_1 + y_1\sqrt{A})(x_2 + y_2\sqrt{A}) = R \in HP_n(A) \quad (5)$$

$$E * F = (x_1, y_1) * (x_2, y_2) = (x_1 + y_1\sqrt{A})(x_2 + y_2\sqrt{A}) = F * E \quad (6)$$

$$(E * F) * A = (x_1, y_1) * (x_2, y_2) * (x_3, y_3) = E * (F * A) \quad (7)$$

The unit factor $E = (1,0)$, if $\forall\ E = (x, y) \in HP_n(A)$, then,

$$E * T = (x + y\sqrt{A})(1 + 0\sqrt{A}) = E \quad (8)$$

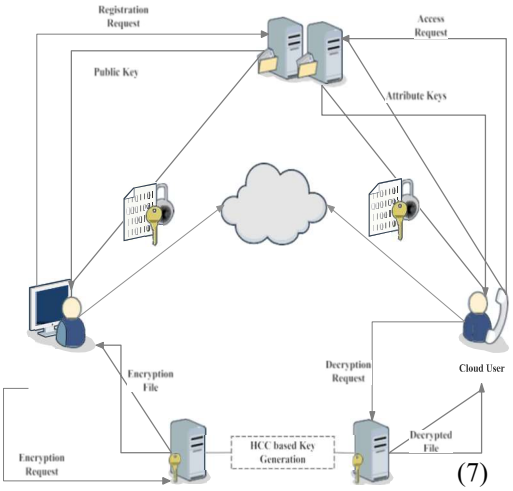
$$E^{-1} * E = (x + y\sqrt{A})(x - y\sqrt{A}) = T \quad (9)$$

$$x_k + y_k\sqrt{A} = \pm(x_0 + y_0\sqrt{A})^k;\ \ k > 1 \quad (10)$$

3.15. Homomorphic Encryption

Moving from somewhat to full encryptions, the issues of limited depths received care. Among the suggested offerings is a service that would significantly reduce background noise. However, homomorphic security systems are not always available, and this method can need a secret key. One possible update would be to encrypt a different version of the key and include it with the cipher-text.

The three homomorphic formulae are tabulated in Table 1 according to their respective categories. All the formulae in the table can calculate encrypted data, as shown in the table. The use of memory is a big problem for HC, even if it can compute on reproduction and improvement. Compared to PHE, SWE is better, although it has a shallow circuit. Multiplication and addition are the only two operations that PHE is capable of doing.



(7)

Figure 8: HC and MA-CP-ABE

Table 1: Comparison of Homomorphic Categories

Description	Partial Homomorphic Encryption (PHE)	Some what Homomorphic Encryption (SWHE)	Homomorphic Cryptography (Hc)
Computation on encrypted data	yes	yes	yes
Limitation	One computation all operation	limited	Large memory requirement
Examples	Pallier RSA and ELGAMAL	Gentry	Gentry

4. RESULTS

Adjustable hyperbolic curve parameters are a part of the suggested system. In order to guarantee safety, the HC's restricted function is split according to various scenarios that may improve the model's order selectivity.

The following metrics are used to evaluate the proposed MA-CP-ABE system with HC:

1. Encryption Time
2. Decryption Time

Based on client attributes, the MA-CP-ABE with HC is assessed and the results are shown. It has also been noted that the time it takes to encrypt a file increases in direct correlation with the number of features and continues to rise over time.

The results show that as the number of characteristics increases, the encryption time also increases. The file encryption time of MA-CP-ABE-HC is lower than that of MA-CP-ABE-ECC. By cutting down on security time, the MA-CP-ABE-HC method outperforms the current systems.

Table 2. Encryption Time with varying number of Attributes

ECC		HC	
No.of Attributes	**Time (in ms)**	**No.of Attributes**	**Time (in ms)**
10	190	10	200
20	200	20	210
30	210	30	220
40	220	40	230
50	230	50	240

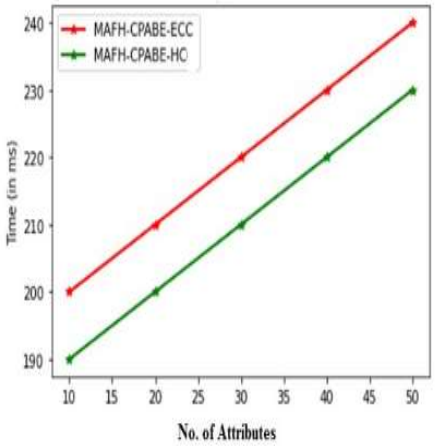


Figure 9: Encryption Time with varying number of Attributes

The decryption time depends on the connections made with customers. The number of attributes also determines the decryption efficiency, just like its effect on security. The decryption time depends on the number of features involved and is directly proportional to the number of characteristics. The decryption time in MA-CP-ABE-HC is much lower compared to the MA-CP-ABE-ECC systems.

Table 3. Decryption Time with varying number of Attributes

ECC		HC	
No.of Attributes	**Time (in ms)**	**No.of Attributes**	**Time (in ms)**
10	200	10	215
20	210	20	220
30	225	30	240
40	235	40	255
50	270	50	280

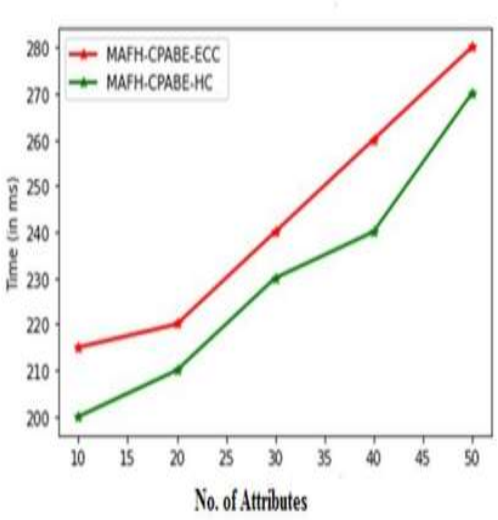


Figure 10 : Decryption Time with varying number of Attributes

The following aspect to be thought about for comparison is storage expense. For the storage space cost of the ciphertext, the proposed MA-CP-ABE-HC plan takes in much less storage than the existing system and it complies with a direct partnership with the variety of characteristics as stood for in. MA-CP-ABE-HC supplies much better results when the varieties of characteristics is increased.

Table 4: Storage Cost with varying number of attributes.

ECC		HC	
No.of Attributes	**Storage in kb**	**No.of Attributes**	**Storage in kb**
10	5800	10	6000
20	7000	20	7200
30	8000	30	8200
40	9000	40	10000
50	9000	50	10000

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

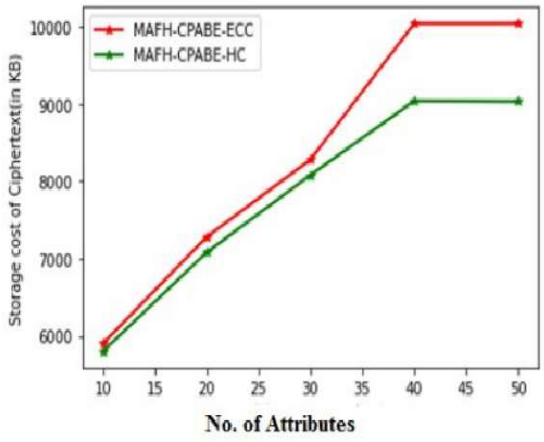


Figure 11: Storage Cost with varying number of attributes.

The performance with respect to the storage cost of ciphertext is enhanced by the suggested systems. The storage cost of the suggested methods is lower than that of the other current solutions. A scale from 1 to 10 represents the range of possible data points. The range of data dimensions is 1–5 megabytes. There is a range of attributes from ten to fifty. The storage space expenditure is shown and compared with respect to the quantity of files and diversity of characteristics in. The MA-CP-ABE-HC offers a better level of security compared to other plans, which is depending on the storage space pricing.

Table 5: Proposed Schemes for Storage Cost with varying number of files and attributes

CPABE (Files, Attributes)		ECC (Files, Attributes)		HC (Files, Attributes)	
No.of	No.of	No.of	No.of	No.of	No.of
28000	23000	25000	22000	24000	21000

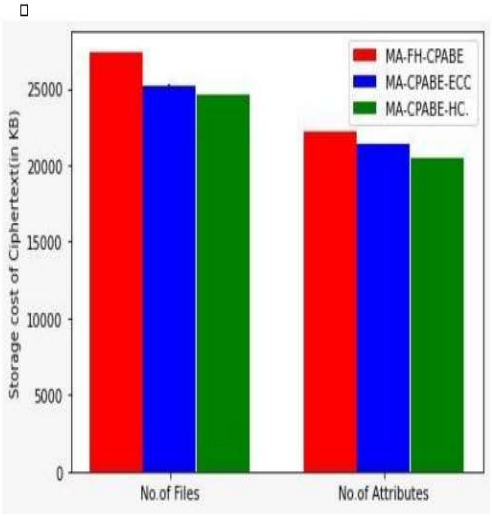


Figure 12: Proposed Schemes for Storage Cost with varying number of files and attributes

5. CONCLUSION

Using a Fully Homomorphic Cryptosystem team, the Homomorphic Cryptosystem (HC) provides a foundational system for crucial generation, decoding, and trademark verification. The proposed system incorporates Homomorphic Cryptography to strengthen the MA-CP-ABE-HC scheme's security. In order to generate important properties, the points in the hyperbolic contour are mapped. The owner of the data uses the hidden feature information access framework to keep it safe. The data is stored in the CSP encrypted. The method keeps a track of service access data from different users, then limits access based on an individualize target analysis that takes into account the user's current service accessibility habits to determine the Trusted Access Rating's value and the technique encrypts data by reliably selecting a random key. The effectiveness of access control and data security will undoubtedly be enhanced by the suggested method. A customer can download and decrypt the requested data only if their qualities match those set by the data owner. In fact, the proposed MA- CP-ABE-HC system is tested in simulation. Time spent encrypting and decrypting is tracked using a wide range of characteristics. When compared to the current systems, the suggested method provides reduced handling time for file encryption and decryption. Using much superior performance, the simulation results have shown that the suggested strategy secures the shared data via the cloud.

Limitations: Despite its advantages, the Multi-Level Encryption Ciphertext Using Multi Blocks and Secure Data Access Policy model has certain

limitations. The complexity of managing multiple encryption levels and keys can increase computational overhead and slow down data processing. Fine-grained access policies require constant updates, which may lead to performance bottlenecks. Additionally, secure and scalable key management remains a challenge, especially in large-scale systems. Synchronizing encryption and access control across distributed cloud environments can be difficult. Lastly, if not properly optimized, the system may become resource-intensive, impacting cloud service efficiency and scalability, particularly for real-time applications or large datasets.

REFERENCES

[1] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, J. Chen, A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment. Futur. Gener. Comput. Syst.88:, 636–643 (2018). https://doi.org/10.1016/j.future.2018.02.050.

[2] M. Qutaibah, S. Abdullatif, and C.T. Viet, "A Ciphertext-Policy Attributebased Encryption Scheme With Optimized Ciphertext Size And Fast Decryption," in Proc. 2017 ACM Asia Conf. Comput, Commun. Secur. (ASIA CCS), Apr. 2017, pp. 230–240.

[3] Bilecki, LF &Fiorese, A 2017, 'A Trust Reputation Architecture for Cloud Computing Environment', IEEE// 14th ACS International Conference on Computer Systems &Applications(AICCSA), IEEE, pp. 614-621.

[4] Casola, V, De Benedictis, A, Eraşcu, M, Modic, J &Rak, M 2017, 'Automatically Enforcing Security SLAs in the Cloud', in IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 741-755, doi: 10.1109/TSC.2016.2540630.

[5] Chandramohan Dhasarathan, A 2017, 'Secure data privacy preservation for on-demand cloud service', Journal of King Saud University - Engineering Sciences, vol. 29, no. 2, pp. 144-150.

[6] Darko Hrestak and Stjepan Picek, "Homomorphic Encryption in the Cloud," Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on , vol., no., pp.1400-1404, 26-30 May 2014, pp. 1400-1404, 26-30, 2014.

[7] R. Li, C. Shen, H. He, X. Gu, Z. Xu, C. -Z. Xu, An lightweights information sharing schemes for cloud computing. IEEE Trans. Cloud Comput.6(2), 344–357 (2017).

[8] M. Sookhak, F. R. Yu, M. K. Khan, X. Yang, R. Buyya, Attribute-based data access control in mobile cloud computing: taxonomy and open issues. Futur. Gener. Comput. Syst.72(C), 273–287 (2017).

[9] B.Liu, X. L. Yu, S. Chen, X. Xu, L. Zhu, in 2017 IEEE International Conference on Web Services (ICWS). Blockchain Based Data Integrity Service Framework for IoT Data (IEEE, 2017), pp. 468–475.

[10] A MULTI LAYER APPROACH TO IMPROVE THE SECURITY AND PROTECTION http://www.journal-iiie-india.com/1_july_23/74_online.pdf

[11] MULTI BLOCKS FILE PROTECTION AND PRIVACY ACCESS POLICY IN https://turcomat.org/index.php/turkbilmat/article/view/5035/4210

[12] Adil Bouti and Jorg. Keller, "Towards Practical Homomorphic Encryption in Cloud Computing," Network Cloud Computing and Applications, pp. 67-74, 2015.

[13] Claude Turner, Pushkar Dahal Monique Ogburn, "Homomorphic Encryption ," Procedia Computer Science , pp. 502-509, 2013.

[14] Mihai Togan and Cezar Plesca, "Comparison-Based Computations Over Fully Homomorphic Encrypted Data," Communications (COMM), pp. 1-6,29-31, 2014.

[15] M. B. Smithamol, S. Rajeswari, Hybrid solution for privacy-preserving access control for healthcare data. Adv. Electr. Comput. Eng.17(2), 31–38 (2017).

[16] Y. He, J. Ni, X. Wang, B. Niu, F. Li, X. Shen, Privacy-preserving partner selection for ride-sharing services. IEEE Trans. Veh. Technol.67(7), 5994–6005 (2018).

[17] H. Cui, R. H. Deng, J. K. Liu, Y. Li, in Australasian Conference on Information Security & Privacy(ACISP 2017). Attribute-Based Encryption with Expressive and Authorized Keyword Search (SpringerCham, 2017), pp. 106–126.

[18] M. Zhang, Y. Jiang, Y. Mu, W. Susilo, Obfuscating re-encryption algorithm with flexible and controllable multi-hop on untrusted outsourcing server. IEEE Access. 5:, 26419–26434 (2017).

[19] L. Jiang, D. Guo, Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage. IEEE Access. 5(99), 13336–13345 (2017).

[20] V. Goyal, et al. Attribute-based encryption for fine-grained access control of encrypted data, in: Proc. of CCS'06, 2006, pp. 89–98.

[21] Z. Li, S. Huan, Multi-level attribute-based encryption access control scheme for big data, in: MATEC Web of Conferences, 173, EDP Sciences, 2018, pp. 03047.

[22] N. Kaaniche, M. Laurent, Attribute based encryption for multi-level access control policies, in: SECRYPT 2017: 14th International Conference on Security and Cryptography, vol. 6, Scite Press, 2017, pp. 67–78.

[23] M. Nabeel, E. Bertino, Privacy preserving delegated access control in public clouds, IEEE Trans. Knowl. Data Eng. 26 (9) (2013) 2268–2280.

[24] M. Gupta, R. Sandhu, The GURAG administrative model for user and group attribute assignment, in: Proc. of NSS'10, Springer, 2016, pp. 318–332.

[25] S. Bhatt, et al., Abac with group attributes and attribute hierarchies utilizing the policy machine, in: Proc. of ABAC Workshop, ACM, 2017, pp. 17–28.

[26] N. I. of Standards, Technology, Policy Machine, Tech. rep., U.S. Department of Commerce, Washington, D.C.

[27] Praveen, S. Phani et al., "Revolutionizing Healthcare: A Comprehensive Framework for Personalized IoT and Cloud Computing-Driven Healthcare Services with Smart Biometric Identity Management", *Journal of Intelligent Systems & Internet of Things*, vol. 13.1, 2024.

[28] Swapna Donepudi, A Madhuri, V Shariff, V Krishna Pratap, S Phani Praveen and Nguyen Ha Huy Cuong, "Security Model for Cloud Services Based on a Quantitative Governance Modelling Approach", Journal of Theoretical and Applied Information Technology 15th April 2023, vol. 101, no. 7, ISSN 1992-8645

[29] C. S. Kodete, V. Pasupuleti, B. Thuraka, V. V. Gayathri, V. S. D. Sundar and V. Shariff, "Machine Learning for Enabling Strategic Insights to Future-Proof E-Commerce," *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2024, pp. 931-936, doi: 10.1109/ICOSEC61587.2024.10722255.

[30] K. V. Rajkumar, K. Sri Nithya, C. T. Sai Narasimha, V. Shariff, V. J. Manasa and N. S. Koti Mani Kumar Tirumanadham, "Scalable Web Data Extraction for Xtree Analysis: Algorithms and Performance Evaluation," *2024 Second International Conference on Inventive Computing and Informatics (ICICI)*, Bangalore, India, 2024, pp. 447-455, doi: 10.1109/ICICI62254.2024.00079.

[31] Veerapaneni, E. J., Babu, M. G., Sravanthi, P., Geetha, P. S., Shariff, V., & Donepudi, S. (2024). Harnessing Fusion's potential: a State-of-the-Art information security architecture to create a big data analytics model. In Lecture notes in networks and systems (pp. 545–554). https://doi.org/10.1007/978-981-97-6106-7_34

[32] S. P. Praveen, P. Chaitanya, A. Mohan, V. Shariff, J. V. N. Ramesh and J. Sunkavalli, "Big Mart Sales using Hybrid Learning Framework with Data Analysis," *2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Pudukkottai, India, 2023, pp. 471-477, doi: 10.1109/ICACRS58579.2023.10404941.

[33] Vahiduddin Shariff, Ruth Ramya K, B Renuka Devi, Debnath Bhattacharyya and Tai-hoon Kim, "A Survey on Existing IP Trace back Mechanisms and their Comparisons", *International Journal of Engineering and Technology*, vol. 7, no. 1.8, pp. 67-71, 2018, ISSN 1314-3395.

[34] Rajkumar, K. V., Vallabhaneni, P., Marlapalli, K., Kumar, T. N. S. K. M., & Revathi, S. (2022). Detection of fake news using natural language processing techniques and passive aggressive classifier. In Smart innovation, systems and technologies (pp. 593–601). https://doi.org/10.1007/978-981-19-0011-2_53

[35] Praveen, S. P., Ghasempoor, H., Shahabi, N., & Izanloo, F. (2023). A hybrid gravitational emulation Local Search-Based algorithm for task scheduling in cloud computing. Mathematical Problems in Engineering, 2023(1). https://doi.org/10.1155/2023/6516482