Abstract: Cloud computing plays a key role in the implementation of commercial systems. It helps companies like Microsoft, Amazon, IBM, and Google deliver their services to their customers on a large scale. A third-party service company operates the cloud computing-centric network and applications. The Cloud Service Provider (CSP) is an entity that works in both all organizations. It, therefore, suffers from systemic defects, including internal and external attacks. So, its organizational mission is to secure a provider of cloud services while ensuring the quality of service. A hierarchical Multi Authority ABE (HMA-ABE) framework to provide oversight of fine-grained access is proposed here. But the scalability and versatility of these systems are missing. Encryption based attributes could also be used for data protection with Key Policy Attribute-Based Encryption (KP-ABE) or Text Policy Attribute-Based Encryption (CPABE) encryption. Finally, it uses the triple encryption and decryption algorithm.

Keywords: CP-ABE, Access policy, ABE, Public Key cryptography, Hierarchy, Multi Authority.

I. INTRODUCTION

Virtualized tools are used in Cloud Computing for accessing centralized infrastructure and applications [12]. Abstraction and virtualization are two core concepts of the cloud. Abstraction refers to the covering of program implementing information, user data storage. Virtualization means creating virtual network resources which provide scalability instantly [13]-[17]. The use of cloud computing has rendered knowledge searchable globally and conveniently. An organization, within the framework of an entity, may create a cloud. Network services in the cloud may be either physical or virtualized [18]. The cloud computing platform provides access to shared network infrastructure and storage space for remote users, as the customer needs. The information is available through the internet to a user at any time [19]. Cloud computing plays a major role in commercial IT systems development. This allows companies like Microsoft, Amazon, IBM and Google to offer large-scale services to their customers [20]-[26]. The benefits of cloud computing include on-demand service, platform-independent network access, cost reduction, ease of use. Cloud computing load balancing capability has made this more reliable [27]-[33]. Storage in cloud computing is internet dependent, and data security and privacy are the main security concern. Cloud service provider (CSP) does all the user and data management online. Data sharing is a very secure cloud technology [34].
It is used for photo sharing on social networking sites, consisting of billions of users, the electronic health record system, etc. Authentication and authorization are used in the proposed research to solve flexible and modular access control and data security for security system encryption in cloud storage [35]-[41]. Authorization here ensures that the consumer accesses only information for which he or she is allowed [42]. The program's contribution includes key generation attributes, reduced complexity and secret key size, and improved search efficiency [43]-[57].

II. RELATED WORK

The NVO-CP-ABE scheme by outsourcing encryption and decryption computations to the proxy server increases the computational performance of the CP-ABE scheme for big data [58]. Furthermore, the NVO-CP-ABE scheme tests the accuracy of the encrypted message along with outsourced computations and supports limited user access to data [59]. In the standard model, user conspiracy attack, and proxy attack, the NVO-CP-ABE scheme is proven safe against CPA. Theoretical analysis and experimental results indicate that the NVO-CP-ABE scheme is in all respects more effective than current schemes [1]. Therefore, the NVOCP-ABE scheme is more suitable for Big Data privacy and cloud access control [60-65]. We will be continuing this research with revocation in our future work to provide effective control of access. A new method called multiple-value linear secret sharing, which can greatly improve the interpretation of access policy [66]-[71]. In addition, every attribute is broken down into two parts, namely the name of the attribute and its meaning [72]. The most obvious advantage of the proposed scheme is that important values of the attributes can be concealed [73]. And in PHR, it can well protect the privacy of the users [2]. The size of the public parameters is constant in the proposed scheme, and the decryption cost is just two pairing operations, making it more practical [74]-[79]. Eventually, using the dual system encryption method, we prove the complete security of the proposed scheme within the standard model under static assumptions [80]-[91].

To address the question of malicious user tracing in a multi-domain context, a CP-ABE scheme that supports both white-box tracing for domains and intra domain users is proposed in this paper. With the leaked user private key, the scheme first uses the tracing method to establish the domain from which the user private key falls [92-111]. It then uses the link flag of the linkable ring signature to locate the malicious user in the domain [3]. The authority performs the domain tracing, and the domain manager performs user tracing in a domain [112-134]. The two-layer tracing relieves a single authority's workload and increases system performance; meanwhile, this paper uses the domain attributes instead of the user attributes. This decreases the size of attributes in the system and further improves performance [135-155]. Our two-layer traceable CP-ABE scheme is primarily generated and simulated in theory [156-171].

This paper investigated an essential property that we call "key-delegation violation" in ABE schemes, which could severely affect health when implemented in Fog Computing. It means users could divide their SAA privilege and share it with others by generating new private keys from their own rather than from the trusted authority when an ABE system is adopted, which is not resistant to key delegation abuse [172-185]. More precisely, it is possible to generate the new derivative keys for attribute setting as 0 from a private key set for as long as 0 is available. We noted that most of the current ABE schemes in the literature are suffering from this problem. Given its relevance for adopting ABE in the real situation, it is noteworthy that this topic has not been studied well in the literature [4]. A security notion for the key-delegation abuse property introduced a new CP-ABE scheme that is key-delegation abuse-resistant. We also proved the scheme's security in both the traditional limited CPA model and the proposed model [186-191]. Furthermore, we have proposed extending our CP-ABE scheme to a traceable CP-ABE scheme,
allowing traceability of the "traitors" in the system. Our scheme is the first CP-ABE scheme that is immune to harassment by key delegations [192-196].

CP-ABE is a very useful scheme for mitigating the risks associated with Cloud data protection. This offers a degree of flexibility and scalability in that it eliminates the need for data owners to handle every single request. Alternatively, the data owner has an access policy and will gain access if the user has the correct attributes. This survey aimed to explain how CP-ABE's inherent computational complexity and communication costs are a major concern in MCC and IoT and may impede its adoption. The survey also identified several innovative schemes to address these concerns, including offline/online algorithms, computation delegation by proxy server processing, computation and communication-limiting schemes utilizing constant size cipher texts and security keys, and risk management and scalable solutions defined in multi-authority schemes [5]. ABE's application to IoT, and especially CP-ABE, is creating its paradigm. While some work in this field is based on previous mobile device research, it does not appear that a significant amount is being extended to the IoT from mobile device schemes. On the one hand, there is consensus that computing needs to be more effective and, on the other, hardware and network changes need to be made to see real advantages in IoT.

Device-to-device (D2D) connectivity is gaining significant attention due to its applicability in network-less infrastructure environments such as mobile multi-hop networks. Nevertheless, existing D2D authentication protocols cannot be used in multi-hop networks because they are vulnerable to inside attacks such as man-in-the-middle attacks or replay attacks by relaying nodes. This paper suggested D2D authentication protocols that use CP-ABE to resolve issues related to the secure exchange of the initial secret information under attack [6]. In addition, by introducing a message integrity code, the proposed schemes guarantee the validity of the messages. Although the proposed schemes are based on the Bluetooth protocol, the proposed schemes fix initial key setup and integrity concerns in the presence of inside adversaries in multi-hop networks. Therefore, the existing schemes can be extended to the other D2D protocols, such as Wi-Fi Direct.

Automated trust negotiation (ATN) through various cryptographic authentication mechanisms and protocols provides useful features in various negotiation scenarios. The ATN system includes Attribute-based Trust Negotiation Language (ATNL). This policy language enables negotiators to define authorization criteria and Extended Trust Target Graph (ETTG), the ATN protocol to coordinate negotiation targets and use authentication techniques to satisfy defined authorization requirements. Yet gradual dependence on certificates and their policies will fail negotiations [7]. But all of the above-listed schemes are well adapted for applications within the same permitted domain, service providers and data source. Therefore, data source and service provider problems in different areas need to be solved in cloud computing. So Sahai and Waters introduced attribute-based encryption (ABE). ABE notes that the collection of attributes can describe both the user's private key and the ciphertext. The user-assigned attributes can be used to compute the private key for a computer. If a user's private key and cipher text suit the attributes, then that particular ciphertext can be decrypted. Yet ABE isn't ideal for larger systems [8]. Policies of access control characterize the issue of integrity security. In this security strategy, issues of honesty are defined. But the model has addressed the data integrity issue of data owners and service providers within the same sphere of trust [9]. Here is proposed a general policy model and terminology for security policy definition and reconciliation. Through designing and implementing Ismene's policy vocabulary, the writers have demonstrated expressiveness. The writers agreed that by limiting the vocabulary, a compromise between two policies would become tractable. But it remains intractable to limit the language reconciliation of three or more policies [10].
To develop a system to protect data in cloud storage, by implementing protection using encryption, authentication and authorization, we have implemented Hierarchical CP-ABE by introducing a key generation algorithm attribute that reduces the complexity and size of the key [11]. We've improved search efficiency using blowfish algorithms. Scalability and versatility have been introduced to provide control over fine-grained access. We also stopped the framework from using a stored procedure to target SQL injection.

III. PROPOSED METHOD

Existing methods for key detection in multi-authority schemes are no longer applicable without a central authority, as there is no such centralized authority to tie all the components together. In this paper, without using a global authority, we develop an effective Hierarchical multi-authority CPABE process and suggest a multi-authority access control framework for cloud storage systems. Throughout our process, we enforce a certificate authority (CA) for assigning a global user identifier (UID) and an identification authority (AID) to each authority. The UID can uniquely identify a user in the network and is used for data decryption following the secret keys provided by specific authorities. Two users can't conspire to gain illegal data access. We also propose a new technique in multi-authority CP-ABE systems for solving the Complexity problem. To improve the efficiency of ABE, we transfer the function of re-encrypting the ciphertext to the server using the method of attribute encryption so that the server does not need to decrypt the ciphertext before re-encryption (i.e., the server cannot get the content key).

Hierarchical Multi Authority ABE (HMA-ABE)

We find a control system for access to multi-authority cloud storage as defined in Fig.1. There are five categories of entities in the system: data masters (owners), cloud servers (servers), data users (users), attribute authorities (AAs), and a certificate authorities (CA). The owners define the access policies and encrypt their data before the policy stores them in the cloud. The server gathers proprietors' data and provides services for users to access data. Each attribute authority is a trusted entity responsible for creating, revoking, and modifying user attributes within its administrative domain. The CA is a completely trusted agency supplying a global UID for each network customer and an AID for each AA (figure 1).

![Hierarchical Multi Authority ABE (HMA-ABE)](image-url)
In particular, PK is a public parameter published by the Attribute Authority. Cph is data owner encrypted cipher text and includes three parts: 1) keyword list WD is encrypted to construct keyword index, namely index; 2) encryption key ck is encrypted to get ciphertext CT’; 3) file M is symmetrically encrypted using encryption key ck to obtain Eck (M). Finally, the data owner uploads Cph to the cloud server with a text cipher. OK is used afterwards to indicate the intermediate key created by the data user attribute provided by the attribute authority and sent to the key generating serve. The key generation server determines the partial secret key of the data user based on OK, i.e. the outsourced SK1 secret key sent to the authority attribute. The attribute authority then generates the data user's local secret key SK2 and obtains the data user's secret key SK= (SK1, SK2), sent to the data user. Tok denotes a token created by the data consumer based on the desired keywords that match the keyword index. The cloud server executes search results, and the cloud server sends the stored text cipher Cph to the data usage if the token meets the index effectively. Then, the data user first decrypts text cipher Cph with SK secret key to get ck encryption key, and then symmetric decrypts text cipher with ck for M code. Moreover, when an attribute has to be removed, the authority attribute sends instructions for updating ciphertext to the cloud server.

**Attribute Authority (AA)**

The AA is the attribute administrator responsible for setting up the system initially and creating the local secret key for data users. At the same time, according to the list of attributes, it distributes the respective secret key for data usage. When an attribute is deleted, AA creates an update key and completes partial changes to the secret key.

**Cloud Server provider (CSP)**

The CSP stores ciphertext containing keyword indexes created by encrypted files and data owners. When a data user tries to search for ciphertext, CS completes a match of the data user's token and keyword index. If the matching succeeds, it sends cipher text to the data recipient. In addition, CS is responsible for altering ciphertext in the attribute revocation process.

**Key Generation Server (KGS)**

For data users, the KGS produces a partial secret key, namely an outsourced secret key, which essentially decreases the computational burden on AA. Additionally, when an attribute is revoked, KGS is responsible for completing the outsourced hidden key update.

**Data Owner**

The Data Owner encrypts the list of keywords and shared data, transferring ciphertext to the cloud server. Only the data user attributes that wish to access the data follow the ciphertext access scheme, i.e. the encrypted data will be exchanged with the data consumer. Essentially, the encryption method to be performed by the Data Owner includes the production of keyword indexes, encrypted file encryption and encrypted key encryption, so the ciphertext forms of three sections.

**Data User**

If the data user's attribute set meets the access specification in ciphertext, then Data User can access encrypted data and retrieve the original plaintext. Data User generally creates and sends the requested keyword token to the CSP cloud server; the CSP matches the search token with the keyword index. If the matching succeeds, the Data User can access the relevant cipher text. In other words, the Data User has to produce a keyword token that he is interested in and decrypt text by the cipher.

**Triple encryption and decryption**

Triple encryption and decryption of data using RSA and Triple encryption algorithm preserve data
confidentiality and data security. The program used encryption to encrypt all the user-assigned attributes to preserve data integrity. The main key is used throughout encryption, and decryption is performed using both public and private keys. Use of private and public key pair RSA is created during registration for every user.

The Base Construction of KP-ABE

They define, for the first time, a scheme for a universe $U$ of attributes where a polynomial is in $1 U$. Is Next, we'll clarify how to adjust this construction to suit the broad universe of the random oracle model $U= \{0, 1\}$. We mean this version when referring to our base construction in a setting where vast universes are believed. Email Space is GT.

Setup ($\pi, U$): Instead (PK, MK). Next, the configuration algorithm selects a prime order $p$ bilinear group $G [2^y]$. It opts for a random generator $g[G]$. First, it selects the random values $h1$. $H \alpha$ and $G$ and $Zp$. Then, the keys are set to:

$$PK = (G, p, g, g(g,g)\alpha, h1, \ldots, h|U|), MK = (PK, \alpha) \ldots \ldots (1)$$

Encrypt (PK, M, S) $\rightarrow$ CT. The encryption algorithm takes the public parameters PK, an M message to encrypt GT, and a set of S attributes as its input. It selects a Zp random s. The ciphertext is written in the form of $CT = (S, C, C, \{Cx\})$

Decrypt (SK, CT) $\rightarrow$ M: The decryption algorithm takes as its input a key SK= $(PK,(D1, R1, \{Q1,d\}))$. $(D', R', \{Q',d\})$ for the control structure $(W, \Delta)$ and the text cipher $CT= (C, C, \{Cx\}xS)$ for the set S. Let $W$ be a’ section n’ matrix.' Attributes are associated with W rows by the function y. If S fails to satisfy the access structure, some will be generated. Suppose S follows the access specification, and let me $\{1,2, \ldots\}$. Be an index set, and be a set of constants $\{i\} i|Zp|$ such that:

1. For all $i \in I$, $\rho(i) \in S$.
2. $P I \in I \omega i \cdot Wi = (1, 0, 0 \ldots 0)$.

Then we're defining the default=$\{x: I=, I= x\}$. I am the set of indexes that correspond to the rows used in one way to decipher the ciphertext, and I am the set of different attributes associated with those rows. Typically one will want to will the size of I. Recall where S is the attributes used to encrypt the cypher text and where S is the set of attributes used to construct the private key. Next, we define the f function, which transforms a set of attributes into a G-element, as:

$$f(\Delta) = Yx \in \Delta hx \ldots \ldots (3)$$

The algorithm initially will do a pre-processing step for decryption on the private key. The value is estimated for each I,

$$D_i^* = D_i \cdot Y x \in \frac{\Delta}{\rho}(i)Qi, x = g if(\Delta)ri \ldots \ldots (4)$$
By calculating the meaning, the algorithm performs a pre-processing step for the ciphertext,

\[ L = Yx \in \Delta Cx = Yx \in \Delta k s x = f(\Delta)s \]  \hspace{1cm} (5)

The algorithm now recovers by calculating the value \( e(g, g) \) as

\[ \frac{e(C, Y i \in I D \omega i i)}{e(Y i \in I R \omega i i, L)} = \frac{e(g s, Y i \in I g \lambda i i f(\Delta) r i o i)}{e(Y i \in I g r i o i, f(\Delta)s)} = e(g, g) \alpha s \cdot e(g, f(\Delta)s) \]

\[ P i \in I \frac{r i o i}{e(g, f(\Delta)s)} P i \in I r i o i = e(g, g) \alpha s \ldots... \ldots. (6) \]

The decryption algorithm will then divide this value out of \( C \) and get the message \( M \). The decryption algorithm only involves estimating two pairing operations.

**IV. EXPERIMENTAL RESULTS**

The proposed overall system was developed with MySQL database HTML. The developed model was evaluated in execution time and varied task scheduling for scalability and performance. Two modules have been developed for complete system realization, where the first module enables user authentication and security features. In contrast, the second module introduces the triple encryption and decryption algorithm for data security and confidentiality. The Cloud Cipher framework can save the data in its encrypted form and even seamlessly retrieve it in its original form, using the minimum possible use of the CPU. Often, the user has enough freedom to choose the encryption protocol he/she wants to use, and the system works smoothly with all the algorithms and standards it supports. Fig 2 shows, if the user is new, Cipher Cloud will request permission from the user to create a new account using the Google Account to which he/she has signed in.

After the user has successfully signed in to Cipher Cloud, the user will have access to his/her account. It highlighted the link in Figure 2. Users can then upload the encrypted files and import them to their accounts. Cipher Cloud will seek permission to create a new account using the Google Account they signed into if the user is new. On this page, the user has been offered a choice of the algorithm that he/she would like to use for this specific account. Once the algorithm has been chosen, it cannot be changed. Once the user clicks the upload button, the file is transmitted using HTTPS via an encrypted connection to Cipher Cloud and then decrypted on the server side again. Afterwards, it is encrypted again using a symmetric key algorithm chosen by the owner. These algorithms are used for the security of the data. Users can select the algorithm according to their preferences, which is selected according to the data.
Figure 3 reveals that the traditional CP-ABE method has the greatest storage cost, which rises when the number of files is increased from 1 to 4. Because FH-CP-ABE uses file hierarchy and centralized policy maintenance costs. However, the proposed Hierarchical Multi Authority ABE (HMA-ABE) has the lowest storage cost since its weighted policy consumes far smaller amounts. As a result, the percentage increase in (HMA-ABE) schemes over FH-CP-ABE and CP-ABE is 3.7% and 15.8%, respectively.

Figure 4 shows that the conventional CP-ABE scheme has the highest decryption period, which rises from 2 to 2.5 when the number of attributes rises from 2 to 10. Since FH-CP-ABE uses file hierarchy and centralized procedure, its decryption time only falls within 1–5.4. However, the suggested (HMA-ABE) scheme achieves the lowest decryption time within the range of 5.81–7.05 s, as it can get all the content keys when the protocol matches the set of attributes. Therefore, the percentage improvement of Hierarchical Multi Authority (HMA-ABE) over FH-CP-ABE and CP-ABE schemes is 8.3 percent and 67 percent, respectively.
The cost of storage for the ciphertext is measured according to the size of the encrypted files. Figure 5 shows storage cost outcomes measured for attribute numbers 2–8.

V. CONCLUSION

Cloud computing is a technology that is in rapid growth. Security in the cloud is the main issue of cloud computing (i.e. unauthorized users accessing data or changing data); for this purpose, the data is first encrypted and hiding the data inside the text using triple encryption. This process ensures Cloud computing security. This paper focuses mainly on the various security problems in the cloud and explores cloud protection measures using HMA-ABE and triple encryption methods. Such methods have produced the best results when compared with existing methods.
Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES


31. Ratnam Kamala Sarojini, Palanisamy Kaliannan, Yuvaraja Teekaraman, Srete Nikolovski, Hamid Reza Baghaee, "An Enhanced Emulated Inertia Control for Grid-Connected PV Systems with HESS in a Weak Grid"" Energies 2021, 14(06), 1455 (1-21);


38. Hariprasath Manoharan, Yuvaraja Teekaraman, Irina Kirpichnikova, Ramya Kuppusamy, Srete


64. Żywiołek, J.; Schiavone, F. The Value of data sets in Information and Knowledge Management as a Threat to Information Security, Garcia-Perez, Alexeis; Simkin, Lyndon (red.). European Conference on Knowledge Management:2021, pp 882–891.

65. Żywiołek, J.; Nedeliakova, E. Analysis of the information security system when ordering furniture online: Sustainability of Forest-Based Industries in the Global Economy (red.) JELACIC Denis. In 2020 ; pp 95–99.

66. Żywiołek, J. Monitoring of information security system elements in the metallurgical enterprises.


131. Aakanksha Singhal and D.K. Sharma, “Generalized ‘Useful’ Rényi & Tsallis Information Measures,


145. S. Sudhakar and S. Chenthur Pandian, “Authorized Node Detection and Accuracy in Position-Based


