Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.019508
Article

Tech Science Press

Hybrid Cloud Security by Revocable KUNodes-Storage with Identity-Based Encryption

S. Saravanakumar[1,*] and S. Chitra[2]

[1]Department of Information Technology, Paavai Engineering College, Namakkal, 637018, India
[2]Department of Computer Science and Engineering, Er. Perumal Manimekalai College of Engineering, Hosur, 63117, India
*Corresponding Author: S. Saravanakumar. Email: researchsaravanan1@yahoo.com
Received: 15 April 2021; Accepted: 14 June 2021

Abstract: Cloud storage is a service involving cloud service providers providing storage space to customers. Cloud storage services have numerous advantages, including convenience, high computation, and capacity, thereby attracting users to outsource data in the cloud. However, users outsource data directly via cloud stage services that are unsafe when outsourcing data is sensitive for users. Therefore, cipher text-policy attribute-based encryption is a promising cryptographic solution in a cloud environment, and can be drawn up for access control by data owners (DO) to define access policy. Unfortunately, an outsourced architecture applied with attribute-based encryption introduces numerous challenges, including revocation. This issue is a threat to the data security of DO. Furthermore, highly secure and flexible cipher text-based attribute access control with role hierarchy user grouping in cloud storage is implemented by extending the KUNodes (revocation) storage identity-based encryption. Result is evaluated using Cloudsim, and our algorithm outperforms in terms of computational cost by consuming 32 MB for 150-MB files.

Keywords: Cloud computing; storage identification based revocation; attribute based access control; encryption; decryption

1 Introduction

Cloud computing is technology that serves resources on demand with well-defined network access for computation and communication. Service providers merely provide resources to users for their applications. In general, cloud storage uses applications of social networking, such as Facebook, WhatsApp, Skype, Zoom, and Twitter. Cloud storage's considerable concern is software for online application, data storage, and processing. Cloud data sharing is a volatile expanding platform with numerous problems. New technological developments, such as mobile Internet, smart cars, and smart city, enables numerous Internet devices to connect to networks. This process results in massive storage during communication over the devices that require dynamic resources for processing. Cloud computing provides enormous virtual resources when users are demanding resources. A new demand integrates the cloud with smart mobile devices or Internet of Things (IoT).

Data collected from various IoT and smart mobile devices are processed using cloud computing infrastructure. This new communication network architecture is controlled using physical networking devices for making reasonable decisions. Further efficiency of the working environment substantially influences the people and helps the majority engage in fast communication. However, these benefits are valid only when technology is significantly secured. Numerous challenges are present in providing security for data privacy and storage [1,2]. Numerous studies have focused on security solutions for cloud computing infrastructure.

Data protection over a network is possible by encryption and decryption techniques while sharing data. Dominant security level involves access control process at the primary stage [3]. Unauthorized data usage is eliminated while sharing data in a cloud network. At present, cloud service providers (CSP) provide significant attention toward ABE [4–7]. It is engrossed owing to its data privacy policy and handling fine-grained, non-interaction based on one-to-many access controls. One of the most popular techniques used is cipher text policy-based attribute encryption (CTP-AE), which is more flexible and feasible compared with general applications [8,9]. Data of organizations must be secured and protected from intruders. Security means owners looking out for data control and knowledgeable access over data stored with privileged access. In large organizations, employee data are stored in private cloud servers or servers [10–12]. Private cloud servers are highly secured because data are accessed and controlled within the premises. Each employee has an access ID and memory in the cooperating private servers. If the number of employees tends to increase, then setting up a private cloud for a minimum number of employees is difficult. Alternatively, organizations plan to request CSP available in the network. This situation creates an integrity problem over a network. Intruders can perpetrate possible attacks on confidential data via internal or external or plaintext attacks.

In recent decades, numerous scholars have focused their research on controlling data access in public cloud servers. The widely accepted scheme is cipher text-policy based attribute encryption (CP-ABE). In this technique, data owners (DO) have direct control over access permission [13–19]. The main motive of the current research is to develop a security of cloud using identity-based cryptographic techniques to achieve high security. Security is an eternal problem in all networks daily. The security of systems is achieved by data authentication and availability. Revocation is considered a main problem while eliminating public key concepts in identity-based cryptosystems. Numerous revocation techniques that have been used include the cloud revocation authorized method key updating-based cloud security provider [20]. Identity-based encryption model creates a separate private key for each user on a weekly or monthly basis. This technique stops generating the private when users are revoked. Good security systems must constantly provide secret keys for users using key generators. This aspect is achieved by introducing an immediate revocation technique. Trusted persons in both sides as mediators tend to share the private keys to users. It reduces the loading of key generators. Another problem raised is that when users are revoked, trusted mediators stop private key generation for user, thereby making users decrypt data using a third person. This study identifies the research solutions to these problems. The main contributions of this study are as follows.

1. A hybrid security technique in cloud computing technology is ensured with high efficiency and performance of systems. It combines considerably established techniques, such as identity-based encryption with revocation methods.
2. Attribute-based cloud security using role hierarchy grouping concept tends to group users based on ID and names, among others. These groups can access their group data. When a user is revoked, the KUNodes (revocation) storage identity-based encryption (RS-IBE) technique is used to ensure forward and backward security.
3. Role hierarchy techniques classify users into certain groups based on attributes in the table. The central authority of ACS is responsible for randomly generating global IDs for users. Simulation is performed using Cloudsim.

The remainder of this paper is organized as follows. Section 2 presents various ideas previously used in identity-based cloud computing and revocation techniques. Section 3 describes the proposed methodology working principle and algorithms. Section 4 explains the simulation and output performance of the proposed scheme. Lastly, Section 5 concludes the research and presents the future scope of this study.

2 Literature Review

This section discusses the studies relevant to the cloud security with attribute-based access control mechanism. Praveen et al. [21] proposed a multi -authority access control with attribute-based encryption. They used role hierarchy algorithm (RHA) and hierarchy access structure (HAS) to protect user data. HAS is used to define access structure based on user-assigned attributes to restrict access to cloud resources. Xue et al. [22] proposed collaboration-based access control strategy to give permission to users with different sets of attributes. This strategy was based on access structure with translation nodes. This collaboration is made with users assigned for the same project.

The proposed an improved cost effecting data sharing model of revocable storage IBE for improving the forward and backward security of the cipher text with user revocation and updation of cipher text. Proposed a cipher text based hierarchical ABE (CP-HABE) based on the assumption of q-parallel bilinear Diffie–Helmen. Proposed a multi authority CP-ABE method that the system not only depends on central authority rather, the attributes authorities also have the rights to issue the user secret key, remove the user from the group under revocation and have the rights to update the secret key and cipher text. proposed a notion with revocable storage IBE with forward and backward security. This work updates the revocation and cipher text simultaneously. The revoked users are not gain access to the data and share the data based on the ℓ-DBHE assumption. The attribute based access control encryption for the data outsourced based on Q-bilinear-Diffie-Hellman Exponent Decision. They implemented the work in Hadoop environment.

Dynamic attribute-based access control method was used to overcome the issues of revocation and updation of policy. This method can support large volume of user attributes-based access mechanism with dynamic nature. An efficient ABE with authorized search scheme (EACAS) is based on anonymous key policy ABE. On the basis of user access structure, the search strategy is also customized and with the secret key sharing enables users to gain access to data. Manas et al. [23] proposed an access control system to overcome the single point execution issue. Central authority (CA) can issue secret keys to authorized users and attribute authorities (AA) who manage the secret key. Instead of individual CA, AA can act as CA if the latter is not found good. If observers found it is correct, then they may remove CA and choose another CA from AA.

Malavika et al. [24] proposed secure data sharing by overcoming the issue of identity revocation with revocable identity-based encryption (IBE) at the server side. The key generation and key updation are handled by the key update CSP. The encryption process includes user authentication and re-encryption. IBE was proposed by [25,26]. The public key of users, such as email and phone numbers, is the identity of the IBE system. The encryption process encrypts the plain text with the receiver's identity to create the cipher text. Zou [27] proposed a hierarchical IBE. Hierarchy positions are denoted by combining users with identity vectors. Users at the high level can distribute the secret key to sublayer users. Bobba et al. [28] proposed recursive set-based structure with user attributes for access control to enable user attributes belonging to the same set to access data. Moreover, attributes present in different sets can be combined with the secret key policy while they have the translation nodes.

Wang et al. [29] proposed an outsourcing security for IBE with key update (KU) called KU-CSP. Key updation is done by KU to reduce the workload of CA. CA can send the user attribute identity to CSP. When unauthorized users attempt to access data, CA can send a message to KU-CSP and prevent them from accessing the data. Shi et al. [30] proposed an authorization strategy with authorized keyword search (AKS) to generate query predicates. Given that DO generates the search policy, the cost of this model is

considerably high. Jiang et al. [31] proposed a public key encryption-based method with authorized cipher text with single keyword. Ciu et al. [32] proposed attribute-based encryption with authorized keyword search. ABE was used to encrypt data, while AKS was used to encrypt keywords. This double encryption method will ensure the security of data sharing in the cloud, although it consumes large computation time and storage. The techniques discussed in the literature have concentrated on keyword search, and the confidentiality of the methods remains an issue. To improve the confidentiality and integrity of cloud access control methods, the current study proposes a hybrid approach with user grouping, encryption and decryption, and revocation.

3 Proposed Hybrid Cloud Security Using Role Hierarchy–KUNodes Revocation Methodology

This study proposed a secure and flexible cipher text-based attribute access control with role hierarchy user grouping (CPACRH) in cloud storage by extending the KUNodes (revocation)-storage identity-based encryption (RS-IBE). The proposed secured cloud storage system model is shown in Fig. 1. User data or DO has the following three categories. (i) privacy not required (PNR), (ii) privacy required with trusted provider (PRTP), and (iii) privacy required with non-trusted provider (PRNTP). This study used RHA [33] to classify cloud users into groups based on their attributes, such as name, age, and employee ID. This grouping leads to efficient use of resources, enables users of the group to access their premises only, and prevents users from accessing data that are irrelevant to them. Once users are grouped, encryption and decryption of data are performed using the cipher text-based encryption and decryption [34] technique for fine grained access control to improve the security of the system. At this end, the revocation storage identity-based encryption (RS-RBE) with KUNodes has been analyzed to grant a forward or backward security of the cipher text. CA has the right to provide global identification to users. Access control system (ACS) encrypts data using CP-ABE because DO does not trust CSP. Encryption and decryption between CSP and DO also follows the same cipher text-based encryption technique.

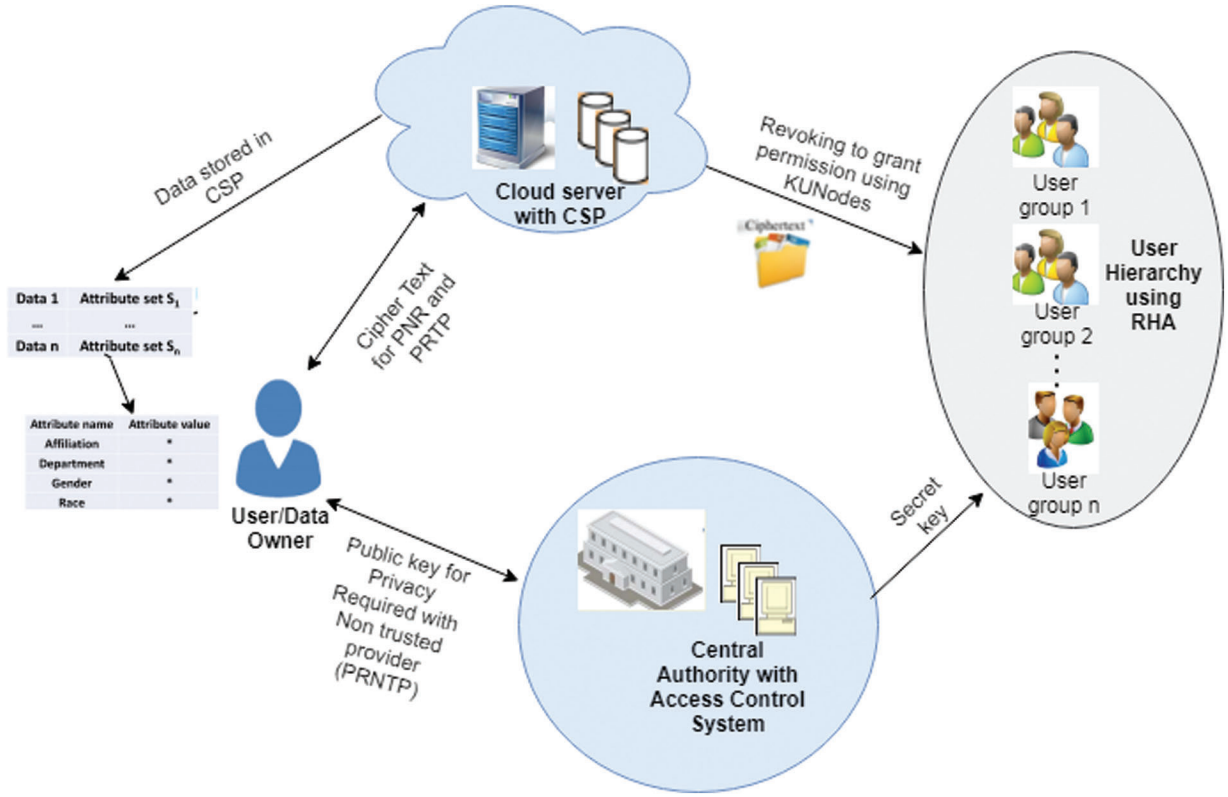

Figure 1: Proposed cloud storage system model

The entities of the system model are described as follows.

CA: CA is the overall controller of the system with access control system to set up the access parameters and share the secret key between users based on their hierarchy levels.

DO: DO is the entity outsourcing data to the cloud server with defined access policies, which are based on user attributes. Data are encrypted before uploading to the cloud server.

User: User is the entity with the interest to access data content from the cloud. These users are arranged based on the hierarchy structure described in Section 3.1. The user has the key to access data based on attribute level. On the basis of the user level, content can be accessed from the cloud using the secret key. The user can also decrypt and encrypt the data content if company policies allow such practices.

Cloud server: Cloud server provides the public with an environment to store and encrypt data for owners. It does not have any access control system for owners. Data stored in the cloud can be accessed by the user.

3.1 Attributed-Based Role Hierarchy Method for User Grouping

Role hierarchy classifies users into certain groups based on their attributes in the attribute table. The central authority of ACS has is responsible for randomly generating a global ID to the user/DO. They encrypt and decrypt data based on the CP-ABE scheme. The algorithm of the role hierarchy-based grouping is as follows:

Algorithm 1: Role hierarchy-based grouping

Input: N users

Output: Hierarchical grouping of N users based on the attributes

Step 1: For each company, each user has a unique employee ID number to access the cloud resources. Company users are arranged in hierarchical order of a binary tree structure based on their attributes and privileges. Users with the highest qualifications, such as admins and CEOs, are considered the root with rights to access all data in the cloud. The hierarchical structure is shown in Fig. 2.

Among the array of N users, a user access list is created based on the user ID as follows:

For i = 1 to n

UA[i]=Uid

Step 2: Based on the user category (user ID), the access list is created and the middle level of the hierarchy is determined and represented as follows:

Middle (Mid)=(L0+Ln)/2 // starting level to number of levels divided by 2.

Thereafter, the entire user ID is arranged into a middle ID list as follows: Middle list[i]=Uid. Lastly, the middle ID is updated as follows:

User middle id [i]=(Uid (first user id)+Lid(last user id) of the level)/2.

Step 3: Repeat step 2 for the sub-tree generation. Compute the sub-tree based on the middle-level user ID and considered a centroid for the next sub-tree split up. The sub-tree generation process is the same as in [21].

Step 4: If the user ID is the last node, then the previous node is considered a root. Users are rearranged in the binary tree based on user attributes.

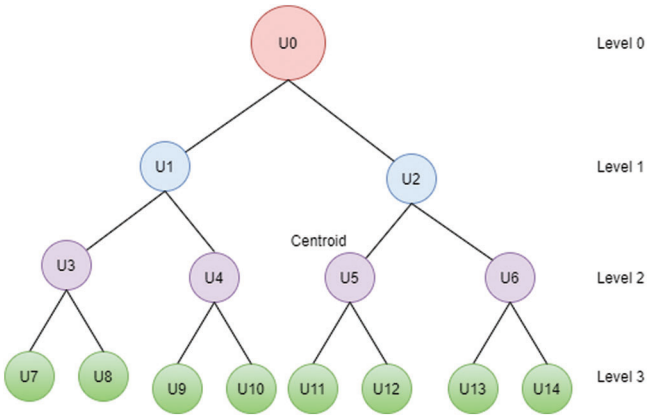

Figure 2: Hierarchical binary tree of users of the employee

The hierarchy structures of users in a cloud network based on their attributes are monitored with cipher text-based encryption and decryption mechanism for fine grained access control. In this research, CA of the access control system monitors user requests to access data. Thereafter, data shared by DO are separated and assigned to the hierarchy of the user access tree using the role hierarchy method. The same category users can access data with same encrypted key, thereby saving time consumption. DO encrypts the data using the CP-ABE method, which is discussed in Section 3.2. User hierarchy can access the data shared by DO based on their hierarchy level. For example, project leaders can have the right to access information related to the project but do not have the right to access personnel information. Senior leaders of companies can have the right to access personnel and official details of users shared by DO. Thus, access control mechanism is managed using the attribute-based role hierarchy approach.

3.2 Cipher Text-Encryption and Decryption with User Attributes

The majority of encryption and decryption method constructs and definitions are the same but not constantly consistent. This study follows the cipher text-based attribute encryption and decryption method, which was first developed in [35]. This section consists of four algorithmic setup: system setup, encryption, key generation, and decryption.

System Setup: Setup *(λ,AD,T,N)->(LPP,MSK,GPP)*: The authority and third-party users setup the parameters. This will take the security parameter λ, attribute description (AD), system time period as total T, and the number of users N as input. The outputs of this algorithm are the local public parameter (LPP), global public parameter (GPP), and master secret key (MSK). This process will also present the revocation list initially as empty. This set has been updated based on Section 3.3.

Encryption: Before uploading the data file to the cloud, DO implements encryption algorithm for security. Encrypt(GPP,A,file,t)->CPT: This algorithm takes input as GPP, access structure A over the attribute set AD, the file that encrypted, and period t. The output of this algorithm is the cipher text of the file at period t. A and t are added to the ciphertext. The user attribute set that satisfies A can decrypt the message.

Key descriptor: This descriptor will generate the secret key to access data in the cloud. For users with global ID and the attribute set $AS = AD_{\tau \in A} S_\tau$, S_τ is the subset of the attribute belonging to CA τ and St_τ is the current state information. From each authority, the secret key is generated as KeyGen(MSK, S, GID, S_τ St_τ)->SK: this algorithm checks the user identity validity with their attributes. If valid, then the secret key is generated for the user and state information is updated.

Decryption: If users satisfy the access policy of the data outsourced in the cloud, then they can have the right to decrypt and access data. The decryption key is generated as DKeyGen(GPP, SK)-> $DK_{GID,S}$. The algorithm for decryption is decrypt (GPP, CT, DKGID), thereby giving access to the file shared by DO.

3.3 Revocation with KUNodes

To improve data confidentiality, this study used the forward and backward secrecy and cost-effective revocation approach with KUNodes [4]. Revocation means that when the authority identifies that user permission has expired, then the user is removed from a particular group to avoid further malicious access. The algorithm for revocation is declared as revoke (GID, RL, St_τ,t)->RL_u : this will take input as the global ID of the user, initial empty revocation list, and current state information of the user at time t. The output will be the updated revocation list with unauthorized user ID. This efficient revocation is performed based on the role hierarchy binary tree using the KUNodes method. The algorithm steps are as follows:

a) While users attempt to access data from the cloud server, CSP asks for the secret key.
b) If users enter the correct secret key, then they can access the data.
c) If users wrongly enter the secret key or the user ID is expired, then the cloud server prepare a revocation list to add the users with time.
d) If the cloud server finds the same user as authorized at a later time, then CSP can update the revocation list by unrevoking them. Revoked and unrevoked users are added to two lists. The revocation tree is shown in Fig. 3.

Algorithm 2: Enhanced KUNode

Input: HBT, GID, RL, St_τ,t

Output: updated revocation list RL_u

The set X,Y<-empty

For all (U_{id},CT_i) ∈RL

  If(U_{id}<=t) then

    Add path(U_{id}) to set X

    Return X

  Else

    Add path(U_{id}) to set Y

    Return Y

  End if

  If Y-> valid then

    Unrevoked the U_{id}

  End if

End for

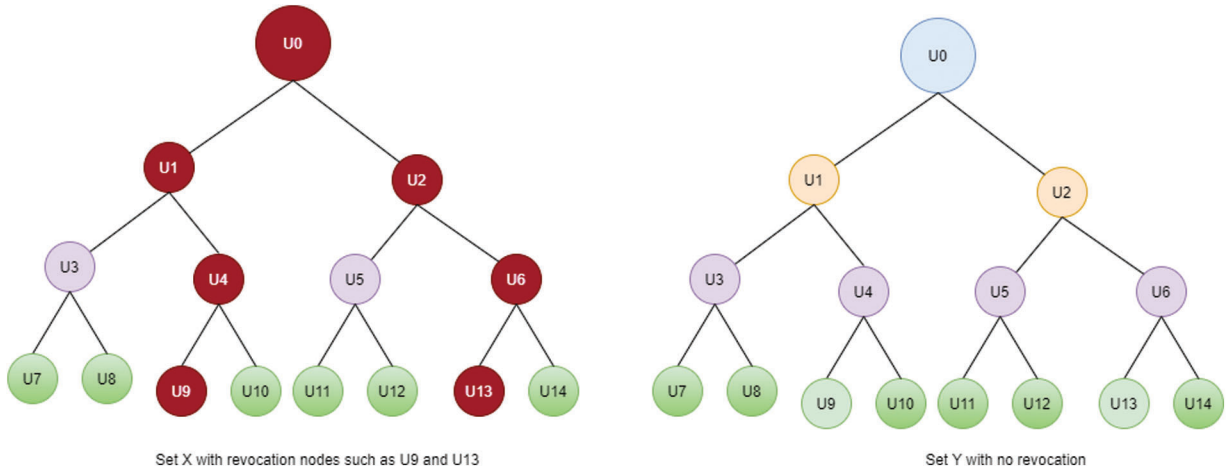

Figure 3: Revocation with enhanced KUNodes

With the combination of role hierarchy, cipher text-based encryption and decryption, and revocation approaches, the security of data and storage of the cloud sever can be efficiently managed. This research can generate the decryption key with the correct secret key. When users are removed from the list using the revocation method, they will no longer have access to data. Accordingly, the proposed scheme ensures the backward security of data sharing in cloud network. Forward security of the system is ensured with the public cipher text update of the owner and the authority.

4 Simulation Results

The proposed algorithm was experimentally tested in a simulation environment called Cloudsim. The performance metrics used for this evaluation are encryption time (time to convert the plain text to cipher text), decryption time (time to convert cipher text to plain text), number of attributes, time consumption (total time for encryption and decryption), storage consumption (capacity of the encrypted data to store the data in the cloud server), and workload of CSP (usage of CPU cycles). Users with attributes for the sample information technology environment will be company details (emp_id, emp_name,emp_desig, emp_dept,prj_id,emp_privileges), project details (Prj_id, Prj_team names,Prj_modules), and HR details (Hr_id,Hr_privileges,Hr_name). The proposed system is evaluated with 100 users, 25 attributes, and 150 files (in MB with different sizes). The number of attributes per authority is 25. All simulations are performed for 15 trials.

The proposed algorithm is compared with the existing literature, such as FH-CPABE [36] and RHA +HAS [21], to test the performance of the proposed system. Time consumption for the encryption and decryption process with respect to the number of attributes and number of files are evaluated. The results are shown in Tabs. 1 and 2.

The time taken to complete the encryption and decryption in terms of number of attributes using the existing and proposed approaches are shown in Fig. 4. The time consumption of the encryption and decryption in terms of the number of files is shown in Fig. 5. Tabs. 1 and 2 and Figs. 4 and 5 show that the proposed scheme obtains less time for encryption and decryption compared with the existing algorithms. The proposed algorithms outperform other algorithms in terms of time. Hence, the proposed cipher text-based attribute encryption with revoked role hierarchy grouping is efficient with less time.

Storage consumption of the proposed system is evaluated by comparing the cipher text storage capacity of the existing algorithms. The evaluated results are shown in Tab. 3.

Table 1: Encryption and decryption times of the proposed *vs.* existing cloud security approaches with respect to the number of attributes

Number of attributes	Encryption time (seconds)			Decryption time (seconds)		
	FH-CPABE	RHA +HAS	Proposed CPACRH	FH-CPABE	RHA +HAS	Proposed CPACRH
5	2.3	2.1	1.2	1.8	1.6	1.2
10	3.5	2.9	1.8	2.2	1.9	1.4
15	4.2	3.8	2.7	2.5	2.1	1.9
20	5.7	4.9	3.2	3.6	3.6	2.1
25	6.9	6.3	3.9	4.7	3.9	2.7

Table 2: Encryption and decryption times of the proposed *vs.* existing cloud security approaches with respect to the number of files

Number of files	Encryption time (seconds)			Decryption time (seconds)		
	FH-CPABE	RHA +HAS	Proposed CPACRH	FH-CPABE	RHA +HAS	Proposed CPACRH
20	5.4	4.8	3.1	4.3	3.8	0.8
40	10.2	8.3	5.2	5.2	4.1	1.4
80	15.6	12.6	9.7	7.03	6.3	1.86
120	20	15.8	11.02	9.81	7.02	2.03
150	25.8	20.4	15.35	12.45	9.72	2.67

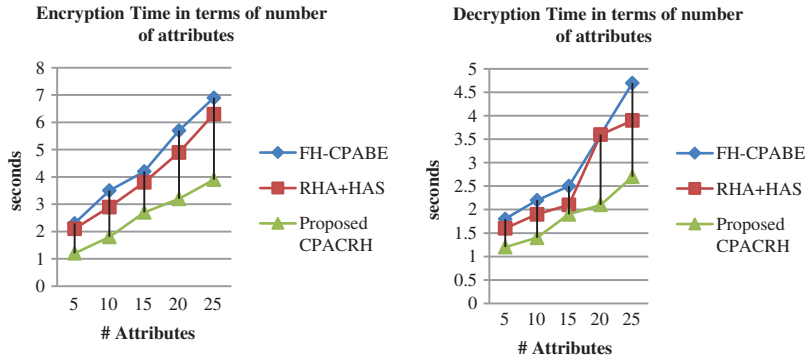

Figure 4: Encryption and decryption times of the proposed *vs.* existing approaches in terms of the number of attributes

Tab. 3 and Fig. 6 evidently show that the proposed algorithm obtains less storage capacity to store the cipher text produced by the proposed approach compared with other existing algorithms. In terms of number of attributes and number of files, the proposed algorithm efficiently used storage to store the cipher text.

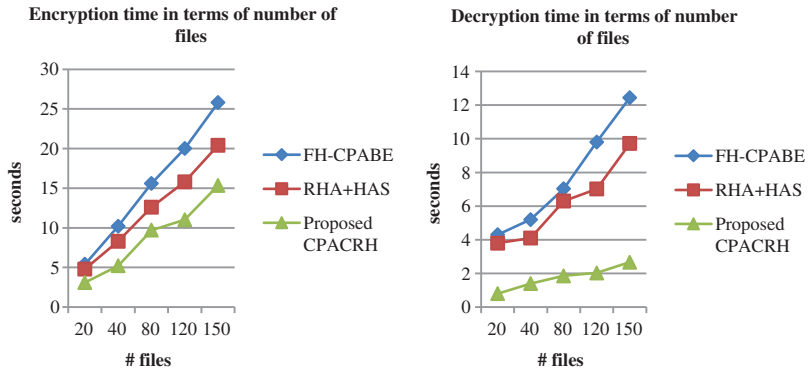

Figure 5: Encryption and decryption times of the proposed *vs.* existing approaches in terms of the number of attributes and number of files

Table 3: Storage cost of the cipher text using the proposed *vs.* existing approaches in terms of the number of attributes and files

Number of Attributes	Storage consumption (MB)			Number of files	Storage consumption (MB)		
	FH-CPABE	RHA +HAS	Proposed CPACRH		FH-CPABE	RHA +HAS	Proposed CPACRH
5	15	10	5	20	32	30	15
10	20	14	8	40	43	39	20
15	28	21	13	80	55	63	23
20	32	28	16	120	78	68	28
25	35	32	23	150	80	75	32

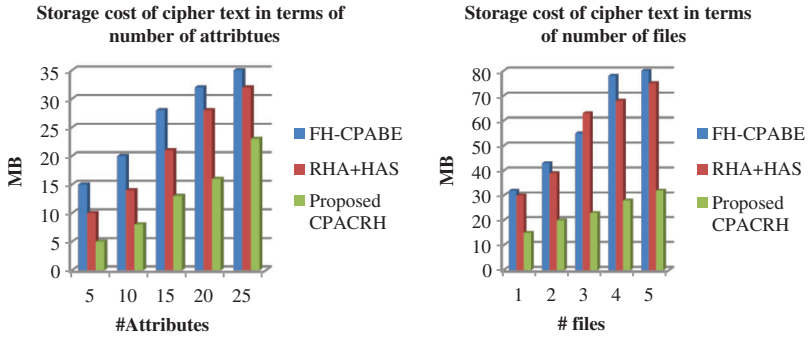

Figure 6: Cipher text storage costs of the existing and proposed approaches

The proposed role hierarchy with attribute-based user grouping and cipher text-based attribute encryption with revocation approach is effective, efficient, and with fine-grained access control method in terms of time and storage. Data confidentiality with forward and backward security is improved with the proposed user grouping technique. This system denies unauthorized users from accessing data outsourced by DO in the cloud server.

5 Conclusions

Security is main concern with high-end technologies, such as cloud computing, big data, and data analytics. This research focused on security solution in a cloud computing platform using identity-based role hierarchy grouping concepts. In this platform, users are grouped based on attribute details, such as name, ID, working project, and place. Thereafter, a group is revoked using the KUNodes-based identity encryption technique. This method provides fine-grained, effective, and efficient security solution to a cloud environment. Encryption and decryption times for the proposed algorithm are highly improved. Security in revocation technique is achieved confidentiality at forward and backward using grouping techniques. Attribute-based role hierarchy method ensures fine-grained security. However, KUNodes-based grouping ensures owners direct access control over shared data in the cloud network. Lastly, computation efficiency is computed for the proposed system; it takes 23 sec in terms of attributes and 32 sec in terms of files. Accordingly, unauthorized users are eliminated by denying access permission other than grouping IDs. However, there remains a limitation with high security in a network. In the future, this research can be enhanced using machine learning algorithms to ensure authorized users at each end.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] I. Lee and K. Lee, "The internet of things (IoT): Applications, investments, and challenges for enterprises,'' *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[2] H. Cai, B. Xu, L. Jiang and A. V. Vasilakos, "Iot-based big data storage systems in cloud computing: Perspectives and challenges,'' *IEEE Transactions on Internet Things*, vol. 4, no. 1, pp. 75–87, 2017.

[3] M. N. Birje, P. S. Challagidad, R. H. Goudar and M. T. Tapale, "Cloud computing review: Concepts, technology, challenges and security," *Cloud Computing*, vol. 6, no. 1, pp. 32–57, 2017.

[4] J. K. Liu, M. H. Au, X. Huang, R. Lu and J. Li, "Fine-grained two factor access control for web-based cloud computing services," *IEEE Transactions on Information Forensics Security*, vol. 11, no. 3, pp. 484–497, 2016.

[5] K. Liang, J. K. Liu, D. S. Wong and W. Susilo,"An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing,"in *Proc. ESORICS*, Guildford, United Kingdom, pp. 257–272, 2014.

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo *et al.*,"K-times attribute-based anonymous access control for cloud computing," *IEEE Transactions on Computer*, vol. 64, no. 9, pp. 2595–2608, 2015.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, Berlin, Germany, pp. 457–473, 2005.

[8] X. Liu, J. Ma, J. Xiong and G. Liu. "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data,"*Network Security*, vol. 16, no. 6, pp. 437–443, 2014.

[9] S. Wang, J. Yu, P. Zhang and P. Wang, "A novel file hierarchy access control scheme using attribute-based encryption," *Applied Mechanics and Materials*, vol. 701, pp. 911–918, 2015.

[10] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen *et al.*, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1265–1277, 2016.

[11] X. Zou, "A hierarchical attribute-based encryption scheme,"*Wuhan University Journal of Natural Sciences*, vol. 18, no. 3, pp. 259–264, 2013.

[12] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferror, L. Zhang *et al.*,"Cipher text-policy hierarchical attribute-based encryption with short cipher texts," *Information Sciences*, vol. 275, pp. 370–384, 2014.

[13] N. Sunanda, N. Sriyuktha and P. Saisankar, "Revocable identity-based encryption for secure data storage in cloud,"*International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 678–682, 2019.

[14] X. Liu, J. Ma, J. Xiong and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data,"*Network Security*, vol. 16, no. 6, pp. 437–443, 2014.

[15] J. Wei, W. Liu and X. Hu, "Secure and efficient attribute-based access control for multiauthority cloud storage," *IEEE Transactions on Systems*, vol. 12, no. 2, pp. 1731–1742, 2018.

[16] J. Wei, W. Liu and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *IEEE Transactions on Cloud Computing*, vol. 6, no. 4, pp. 1136–1148, 2018.

[17] B. SeethaRamulu, H. Balaji and B. Suman, "Attribute based access control scheme in cloud storage system," *International Journal of Engineering & Technology*, vol. 7, no. 4.6, pp. 33–35, 2018.

[18] Z. Liu, Z. L. Jiang, X. Wang, S. M. Yiu, C. Zhang *et al.*, "Dynamic attribute-based access control in cloud storage systems," in *Proc. IEEE Trustcom/Big Data SE/ISPA*, Tianjin, pp. 129–137, 2016.

[19] J. Hao, J. Liu, H. Wang, L. Liu, M. Xian *et al.*, "Efficient attribute-based access control with authorized search in cloud storage," *IEEE Access*, vol. 7, pp. 182772–182783, 2019.

[20] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. SP*, Berkeley, CA, USA, pp. 321–334, 2007.

[21] S. C. Praveen and M. N. Birje, "Efficient multi-authority access control using attribute-based encryption in cloud storage,"in *Proc. ICCIDS*, pp. 840–849, 2020.

[22] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. L. Wei *et al.*, "An attribute-based controlled collaborative access control scheme for public cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2927–2942, 2019.

[23] S. Manasi and S. N. Kini, "Secure and efficient data access control for public cloud storage with multiple attribute authorities," *International Journal of Advance Scientific Research and Engineering Trends*, vol. 3, no. 6, pp. 100–108, 2018.

[24] J. Malavika and G. Ravi, "RS-Ibe: An advanced mechanism for secure data sharing in cloud," *International Journal of Electronics Engineering*, vol. 10, no. 2, pp. 77–81, 2018.

[25] K. Liang, J. K. Liu, D. S. Wong and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Proc. ESORICS*, Guildford, United Kingdom, pp. 257–272, 2014.

[26] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo *et al.*, "K-times attribute-based anonymous access control for cloud computing," *IEEE Transactions on Computer*, vol. 64, no. 9, pp. 2595–2608, 2015.

[27] X. Zou, "A hierarchical attribute-based encryption scheme," *Wuhan University Journal of Natural Sciences*, vol. 18, no. 3, pp. 259–264, 2013.

[28] R. Bobba, H. Khurana and M. Prabhakaran, "Attribute-sets: a practically motivated enhancement to attribute-based encryption," in *Proc ESORICS*, Oakland, CA, USA, pp. 587–604, 2009.

[29] B. Wang, B. Li and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in *Proc. INFOCOM*, Canada, pp. 2904–2912, 2013.

[30] J. Shi, J. Lai, Y. Li, R. H. Deng and J. Weng, "Authorized keyword search on encrypted data," in *Proc. ESORICS*, Oakland, CA, USA, pp. 419–435, 2014.

[31] P. Jiang, Y. Mu, F. Guo and Q. Wen, "Public key encryption with authorized keyword search," in *Proc. ACISP*, Perth, Australia, pp. 170–186, 2016.

[32] H. Cui, R. H. Deng, J. K. Liu and Y. Li, "Attribute-based encryption with expressive and authorized keyword search," in *Proc. ACISP*, Perth, Australia, pp. 106–126, 2017.

[33] J. Wei, W. Liu and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *International Journal of Pure and Applied Mathematics*, vol. 119, No. no. 10, pp. 1617–1625, 2018.

[34] Y. M. Tseng, T. T. Tsai, S. S. Huang and C. P. Huang, "Identity based encryption with cloud revocation authority and Its applications,"*IEEE Transactions on Cloud Computing*, vol. 6, no. 4, pp. 1041–1053, 2018.

[35] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, Barbara, California, pp. 47–53, 1985.

[36] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.