International Journal for Modern Trends in Science and Technology
Volume 9, Issue 02, pages 246-254.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol9issue02.html
DOI: https://doi.org/10.46501/IJMTST0902044

Hierarchal Attribute based Cryptographic Model to Handle Security Services in Cloud Environment: A New Model

N. Raja Rajeswari, Venkata Narayana Reddy, P. Krishnaiah

Department of Computer Science and Technology , Yogi Vemana University, Kadapa, AP

To Cite this Article
N. Raja Rajeswari, Venkata Narayana Reddy and P. Krishnaiah, Hierarchal Attribute based Cryptographic Model to Handle Security Services in Cloud Environment: A New Model, *International Journal for Modern Trends in Science and Technology*, 2023, 9(02), pages. 246-254. https://doi.org/10.46501/IJMTST0902044

Article Info
Received: 22 January 2022; Accepted: 22 February 2022; Published: 28 February 2023.

ABSTRACT

In the present day, information among various clients is being disseminated in the cloud environment. Sharing of information is considered to be a unique element of the cloud to buy and share information among the different clients in the cloud. During this process of sharing information, there is a danger that the information available in the cloud may land with the wrong persons. This always poses a threat to the people whose information is readily available in the cloud. To counter-attack this problem, security-associated methodologies were used to secure the information that was readily available among clients regarding cloud administration purposes. With the presence of this multitude of approaches, one can say that the benefits are very few in the age of key and security information. However, this gives productive/adaptability and dependability in access control strategies between clients in sharing of information. Therefore, keeping the above-mentioned drawbacks in mind, a new method is being proposed in the name of, the Novel Hierarchal Attribute based Cryptographic Security Model (NHACSM) for adaptability, versatility, and solid access control in sharing information in the appropriate climate. This new approach can be considered an extension of ascribe-based encryption concerning figure text and key strategy. The unique feature of this model is, the clients share their information in a hierarchal way which can be used for a productive assessment in access control strategy between shared clients in distributed computing. Our methodology highlights the progressed security. The renouncement of clients, and access consents of clients with versatility and unwavering quality in the age of key design with dynamic credits for rethought information in distributed computing. The analysis of the proposed approach shows adept, compliant, and solid information contributing in the cloud in contrast with the conventional and available methodologies. The NHACSM method is used to reduce the total time values for different user instances compared to conventional approaches i.e. ASBE, KP-ABE, CP-ABE, for 10 instances ASBE is 2.7, KP-ABE is 2.5, CP-ABE is 2.3and also compared to 20, 30, 40, 50 instances , NHACSM is low. The encryption and decryption time evaluation values and performance evaluation of different approaches, ASBE, CP-ABE was taken more time whenever increase the user instance concerning different services. Performance evaluation of memory concerning different approaches also efficient.

I. INTRODUCTION

Distributed computing is a progress perspective constantly science-associated application which includes joined informational collection resources that share flexibility, and capability in sharing of web-subject to customer demands [1]. It is furthermore a promising method for managing to evaluate the restriction of limit and it should be used at any spot whenever [2]. Additionally, because of the strong, flexible resources present in the cloud, it uses to diminish the

computational cost of data owners by conveying data through cloud customers. In disseminated processing, a cloud service provider (CSP) [3] performs organizations that are accessible in the cloud for instance Software as a Service (SAAS), Platform as a Service (PAAS) [4] and Infrastructure as a Service (IAAS) to all of the customers in the cloud [5]. Using these organizations, customers can manage productivity in cloud-based help of regulating projects and composing endeavors. Because of the development of customers and particular security issues in the cloud, figuring relates to cloud offers and evaluates successful and supportive organizations to cloud customers. A piece of the undertakings contains delicate data on cloud laborers and CSP [6] stores that data and plays out the intricate strategies to taking care of data. In light of CSP or absurd might perform exceptional loss of data, because of basic asset present in data which is worked by CSP. Consequently, considering all the insurance issues in the cloud, security [7], and protection of data is the observable issue.

In help organized circulated registering, the protection of data isn't a security essential, fine acquired admittance control is a strongly needed issue [8]. A piece of the clinical benefits and other associated affiliations evaluate specific parts to be a plan/addressed different positions to a social event of customers, instead of delivering different copies are making to each particular individual [9] present in the pack, it is essential to isolate data into sub individual access benefits to all the get-together people reliant upon their endorsement using shared administer permission (SAP) to get to data thoroughly [10]. In SAP, first, it works with and separates data benefits to all of the customers in the bundle, by then, it saves the fundamental affirmation from unnecessary computational cost. Usually, different techniques [11] have analyzed the possibility of individual customer assignments, and pack customer arrangements in sharing of data in the cloud.

Conventional work behind access control strategies in cloud and it is addressed in a brought-together way, attribute-based encryption (ABE) [12] depicts secure verification, this system uses symmetric key-based cryptographic methodology and it isn't furnished productive confirmation with deference key encryption. Zhao et al. uphold validation-based security saving to clients in cloud, this approach utilizes dispersion of key methodology and it upholds just for single key correspondence, if we increment clients in cloud, it isn't support various key ages in conveyed climate [13]. Yang et al. present a decentralized confirmation approach however not help to verify clients can get to cloud as mysterious [14]. Ruj et al. gives a decentralized admittance control strategy approach, it isn't upholds verified clients and it is just store record as understood document and it isn't supported to compose the records, it doesn't give access control by maker just not help to the whole client in cloud [15]. In light of the above methods benefits and bad marks, stretching out the elements connects with security and empower the highlights connects with confirming regarding access control strategy in sharing of information to every one of the clients in disseminated figuring [16].

This paper proposes Novel Hierarchal Attribute based Cryptographic Security Methodology (NHACSM) [17] to give adaptable, versatile and dependable access control in sharing of information in conveyed climate. Our proposed approach safe various kinds of hand-off assaults for example client can supplant old documents with read and compose activities incorporating [18] various tasks. This approach additionally performs renouncement of client for example re-license the tasks of various clients in distributed computing with refreshed activities. The fundamental goal of our proposed approach as follows:

Mainly this article discusses special research for secure authentication for users' shared data. Main contribution behind this research continuously as follows:

a) Stored access control information ought to be imparted to approved clients regarding approve client boundaries in cloud, we likewise check or alter who can get to information, for example, approved clients or unapproved clients.
b) To keep up with the design as a decentralized and incorporated way for effective key administration, in this methodology, no equal clients can get to information for example keep away from impacts regardless of whether any client approved independently.
c) Proposed to use Blockchain related technology in terms of data storage and ensure to discuss the security of data storage in smart computing.

d) Experiments of the proposed approach show versatile and dependable information imparting to various execution measurements in the cloud in contrast with customary methodologies.

2. Implementation and Construction of NHACSM

2.1 Implementation Procedure

This section describes the implementation of security in NHACSM with the following calculation methods:

1. Setup of System: This calculation method is evaluated by the authority of a trusted user, and it is organized by a third-party trusted user, this setup does not contain any input other than security parameters (in the form of attributes) i.e. α, β which are related to global public parameter i.e. *GPK* (global public key)
2. Generation of Key: let us assume as (1)
$$\left(attri\left\{ucpk_{id,k}\middle|k\in\square\right\},\left\{KeyVerif_k\middle|k\in\square\right\},AMSK_d,GPK\right) \quad (1)$$
key generation method for attribute authority is evaluated by AAd, It takes input as following attributes i.e. attri, center-user-public-key (ucpki,k), key relates to verification VKk, master key MKd relates to public global parameters i.e. GPK. It gives output as secret_key SKud of data user (DU) and pair relates to the secret key i.e. $\left(pk_0, sk_0\right)$ of the data owner (DO).
3. Encryption of Files: This encryption procedure is evaluated and performed by domain authority. It takes input as plain text m, GPK, the secret key of DO's, public of DU's i.e. PKU and converted cipher text CTfog_comm. It give all output as cipher text CT1 and CT2 and stores that cipher text into the main cipher text server i.e. cloud service provider.
4. GenTrap: input as $\left(\omega, SK_{id}, PK_0\right)$ Trap door generator calculation method is evaluated by data user i.e. DU, input for this calculation is presented with the search word ω, secret key SK_{ud} and key with the public PK_0 then it generates output as Trapdoor (tw) & key relates to re-encryption value SK_{ud}^{ω}
5. The decryption of Files: This decryption calculation method is evaluated data user and domain authority. It takes input as $\left(C, \Omega RK\right)$ i.e. cipher text which consists of partial decrypted text and key retrieval RK, plain text be the output for this calculation method.

2.2 Proposed NHACSM Schema

This section describes the basic Algorithm implementation procedure of NHACSM [19] which is an extension to attribute set-based encryption to evaluate and handle the dynamic hierarchal structure of different users as described in figure 1. Recall the procedure of domain authority and subordinate domain authorities and different data users concerning corresponding consumers and users relates to data [20]. In our proposed approach authority of the trusted user evaluates privacy-associated master key-assisted parameters that are present in the top-level scenario [21]. Domain SK_d, GPK generates and distributes secure keys to subdomain authorities and users present in next associated level. In our implemented system, every user contains key structure which is generated by attributes with a decrypted key of users.

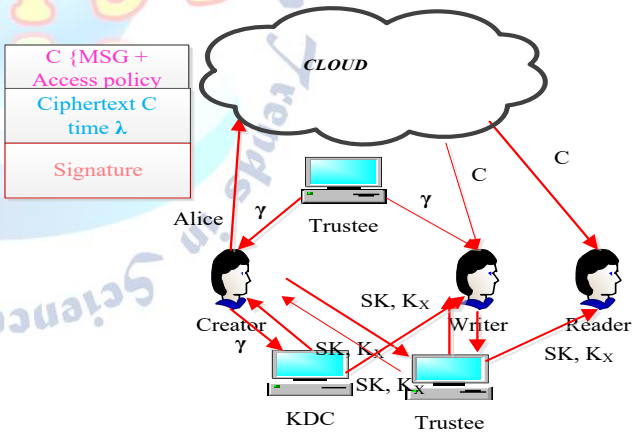

Figure 1. The user is Represented in a Hierarchal Structure.

We describe the basic properties of NHACSM i.e. it consists following methods:

System_setup: setup calculation method is executed by the authority of domain for the creation of key_ public (PK) (2) and key_ master (MK) (3) d is the length of key_structure, by using bilinear map connection C be the prime order p with gen c and then evaluates random parameters $\alpha, \beta \in Z_p, \forall i\left(1,2\right)$. Then a generation of

both master and public keys based on the length of key d is

$$PK=\left(C,c,h_1=c^{\beta_1},f_1=c^{\frac{1}{\beta_1}},h_2=c^{\beta_2},f_2=c^{\frac{1}{\beta_2}},e(c,c)^{\alpha}\right) \quad (2)$$

$$MK=\left(\beta_1,\beta_2,c^{\alpha}\right) \quad (3)$$

Creation and grant of domain authority: Domain authority is organized and associated with recursive attribute relations i.e. $\{X_0,X_1,.....,X_m\},X_i=\{x_{i,1},x_{i,2},.....,x_{i,n}\}$ with ai,j and associated attributes. Creates key for domain authority, select identity no. of keys $r^{\{v\}}$ for the authority of the domain. Random selection of identity keys for each user $a_{i,j},0\le i\le m,1\le j\le n_i$, it is utilized in the authority of the domain (4)

$$DA(MK)=\begin{pmatrix} A,D=c^{\frac{a+r^{\{u\}}}{\beta_1}},D_{i,j}=c^{r_i^{(u)}}.H\left(a_{i,j}\right)^{r_j^{\{u\}}}, \\ D_{i,j}=C^{r_{i,j}^{u}}\ for\left(0\le i\le m,1\le j\le n_i\right), \\ E_i=c^{\frac{r\{u\}+r_i^{\{u\}}}{\beta_2}}\ for\left(1\le i\le m\right) \end{pmatrix} \quad (4)$$

In the above generation of domain authority master key, where Ei is the form of translation unique rule formation $r^{\{u\}}$ relates to attribute set Ai to $r^{\{u\}}$ with associative translating elements Ei & Ei' can be used as E_i/E_i to translator to unique key generations, these details are used again decryption calculation method.

User grant/ selection of novel domain authority:In this scenario, novel user u and subordinate concerning the authority of a domain and it is denoted as DA++, DA joined into cloud system then DA verifies every user then DA generates key structure to every user and user gives grant to other relative users using authorizes which are derived from domain authority.

User Creation (DAMK, u, $\aleph$): This calculation method uses a master key which is generated by the DA with the structure of the key $\aleph$ then evaluates the key structure for the newly generated user $\ddot{\aleph}$ which is the combined key set structure of $\aleph$. Based on unique identifier sequences present in DA master key, evaluates the secret key for user described in the following equation (5)

$$\left(MK_{i+1}\right)=\begin{pmatrix} \ddot{\aleph},\ddot{D}=D.f_i^{\ddot{r}\{u\}},D_{i,j}.c^{\ddot{r}_i^{(u)}}H\left(a_{i,j}\right)^{\ddot{r}_{i,j}^{\{u\}}}, \\ \ddot{D}_{i,j}=D_{i,j}^{1}.c^{\ddot{r}_{ij}^{\{u\}}}\ for\left(a_{i,j}\in\ddot{\aleph}\right), \\ \ddot{E}_i=E.f_2^{\ddot{r}^{\{u\}}+\ddot{r}_i^{\{u\}}}\ for\left(\aleph_i\in\aleph\right) \end{pmatrix} \quad (5)$$

MK_{i+1} are the secret key of user structure, the recipient key is directly removed from the authority of a trusted user.

Encryption of File (PK, m, τ): plain message m is to be encrypted, M be the DEK file, be the tree access structure. τ The encryption calculation method describes as follows (6)

$$Cipher\_Text(CT)=\begin{pmatrix} \tau,\ddot{G}=Me(c,c)^{\alpha.s}.G=h_1^s,G=h_2^s,\forall b\in B: \\ G_b=c^{q(0)},G_b'=H\left(attr(b)^{q^{(0)}}\right), \\ \forall_a\in A:\hat{G}_a=h_2^{q_a^{(0)}} \end{pmatrix} \quad (6)$$

Where *B* defines set of parent node with sub-leaf users in τ and A is the set of the access tree structure τ.

Revocation of User: If any user is revoked from cloud system, then that user not access data owner-shared data at any ware from any side. In our implementation, we solve this problem; perform a re-encryption approach for accessing the association of shared files that are accessed by users related to revoked format. NHACSM extends the properties of attribute set-based encryption for the revocation of different users. Based on the procedure of domain authority security privileges generate the updated key for revoked users if data owner share associated shared files.

File access operations: whenever user sends a request to cloud server the cloud server sends an encrypted request to user then user decrypt the updated data using $Dec(CT,SK_u)$, the decryption procedure as follows:

The decryption of Files: This calculation method takes input as cipher text along with key structure, first decryption procedure verifies user key structure k concerning associative access tree structure τ and cipher text content which is accessed from data owner. Satisfy all the conditions with τ and key structure of user u then

decrypt the entire content, if not satisfy the conditions then evaluate/perform decryption method. The decryption method is described as follows (7)

$$Decr\left(CT, SK_u, i, t\right) = e\left(D_{i,j}, G_t'\right) / \left(D_{i,j}', G_t'\right) = e\left(c,c\right)^{r_i^{\{u\}}} .q_t\left(0\right) \quad (7)$$

The decryption method for all stored encrypted content with translated polynomial interpretation F_z is described as follows (8)

$$F_z = e\left(\hat{G}_z, E_i / E_i\right) F_z' = e\left(c,c\right)^{r\{u\}} .q_2\left(0\right) \quad (8)$$

Based on the above decryption procedure message to be evaluated as $M = \hat{G}.F / e\left(G, D\right)$

3 Experimental Evaluation

In this section, To work out the proficiency of the proposed approach configuration exactly secure cloud with clients which are gotten to by numerous documents from various information proprietors in the cloud [22]. We have carried out NHACSM outline work in light of the working method of property-based encryption (ABE). By utilizing the most recent rendition connects with CloudSim, Java and Netbeans are utilized to set up the most recent cloud climate [23]. For this execution, each host comprises 2.4Hz with 4-8GB RAM and 1TB information stockpiling [24]. Utilizing these prerequisites, our proposed approach investigates the following successions:

Setup_NHACSM: It produces both public and expert key for example PK and MK presumptions

NHACSM_keyGen: Implemented PK and MK create a key that is connected with private tasks with key designs. Key design profundity upholds 1 or 2 help capacities [25].

NHACSM_keyDeleg: Based on PK and MK which are connected with the power of space, this appoints a few strategies for DA's private keys for the recently produced clients. In space authority, a designated key is utilized for the private key [26].

NHACSM_enc: Based on access tree strategy conditions, creates encoded document utilizing PK.

NHACSM_Dec: Using private, decode the documents

NHACSM_rec: utilizing PK, scramble all the record utilizing private key and creates re-encryption process for both encoded and decoded documents [27]. Note that produced privately is utilized to decode the record utilizing encode document tasks [28].

Test after effects of executed methodology concerning the time taken by various activities with various ways to deal with determined [29]. Time taken for various cases during validation in customer cloud with the proposed approach as displayed in after figures [30]. To evaluate the viability of the proposed NHACSM approach with a correlation of various validation approaches like ASBE [31], KP-ABE [32], and CP-ABE [33,34].

The following outcomes which are produced in the proposed approach gives effective security reaction time, encryption for documents, unscrambling for records, access tree age time for various clients, normal precision with memory usage for client tasks like transfer, demands, download demands for proficient and secure capacity of information in disseminated climate.

Table 1 describe total time values for processing different user instances

Table 1. Total Time Values for Different User Instances

Different users	CP-ABE	KP-ABE	ASBE	NHACSM
10	5.3	4.9	5.8	3.9
30	7.4	6.10	7.4	5.4
50	8.6	7.6	7.7	5.9
70	9.5	8.4	9.3	6.8
10	10.6	9.5	8.4	7.5

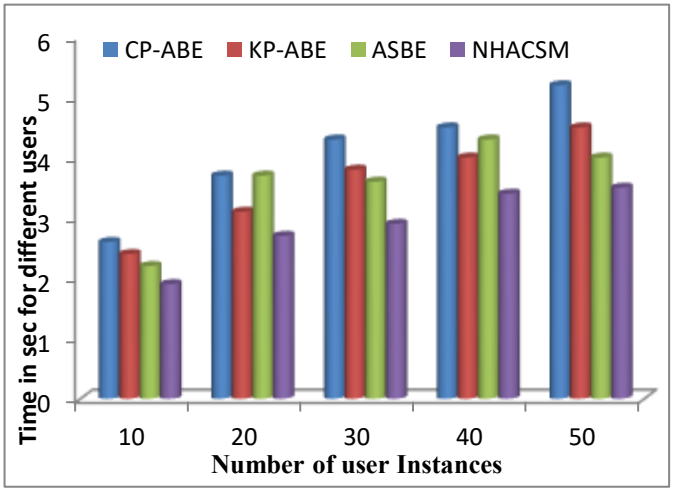

Figure 1. Performance evaluation for cloud setup environment to all the user operations

As shown in table 1, figure 1, compared to traditional approaches i.e. ASBE, KP-ABE taken approximately equal time to explore user instances on cloud whenever user instances increased then those approaches taken more time to execute the services of different users. Where as compared to proposed approach, it was taken by less time compare to existing approaches.

Encryption time for different user instance requests with upload of original content in secure format in cloud with different values described in table 2.

Table 2. Encryption Time Values for Different User Instances

Different users	CP-ABE	KP-ABE	ASBE	NHACSM
10	5.3	4.7	4.6	4.5
20	6.4	5.8	6.3	3.1
30	7.4	7.7	6.3	3.3
40	8.3	7.2	8.2	4.7
50	9.6	8.4	9.4	7.6

Table 2, figure 2 shows the encryption time evaluation values and performance evaluation of different approaches in encryption, ASBE, CP-ABE was taken more time whenever increase the user instance concerning different services. The proposed approach was taken less time for the encryption of files uploaded by different users.

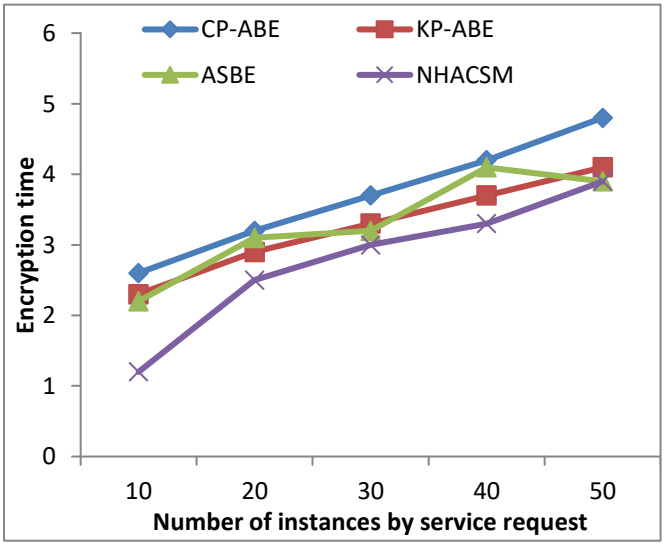

Figure 2. Performance Evaluation Different Approaches with Encryption Time.

Different users want to download shared files from users of data owner the evaluate the decryption time values which are shown in table 3 in secure cloud storage.

Table 3. Description Time Values.

No. of User Instances	CP-ABE	KP-ABE	ASBE	NHACSM
10	4.8	5.8	5.3	4.7
20	5.3	6.7	5.9	3.7
30	4.8	8.5	6.4	3.3
40	7.4	6.9	5.7	3.9
50	6.8	7.5	7.9	6.4

Table 3, figure 3 shows the decryption time evaluation values and performance evaluation of different approaches in decryption also, ASBE, KP-ABE, CP-ABE was taken more time whenever increase the user instance for different services. The proposed approach was taken less time for the decryption of files uploaded by different users with different instant services.

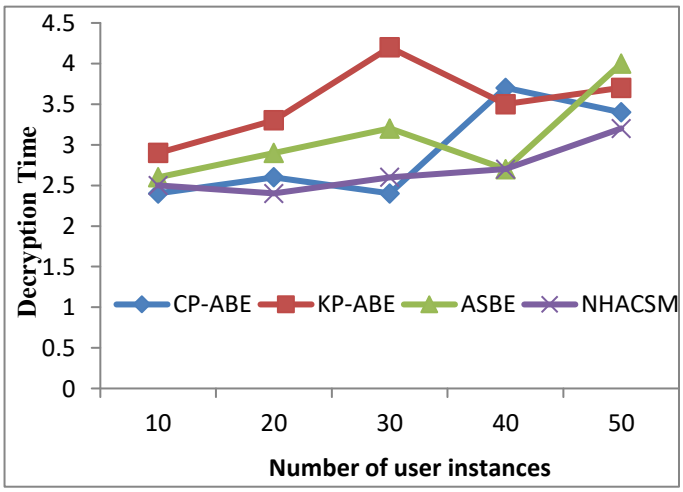

Figure 3. Performance Evaluation of Decryption Time Of Different Approaches.

Table 4; figure 4 shows the performance evaluation of different approaches in the utilization of memory to explore user instance services.

Table 4. Utilization of Memory Values in Processing User Operations in Secure Cloud Storage

Users	CP-ABE	KP-ABE	ASBE	NHACSM
100	4652	3642	4887	4760
200	5327	4326	5226	5626
300	7356	6974	4745	4026
400	22132	5796	6354	5356
500	24553	8964	6785	4324

Utilization of memory with different user operations like store data securely, access tree structure with feasible secure storage described in table 4.

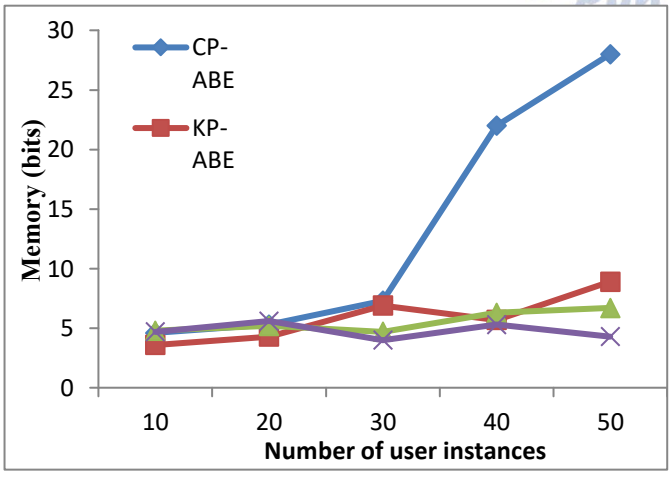

Figure 4. Performance Evaluation of Memory concerning Different Approaches

ASBE, KP-ABE, were taken high amount of memory whenever increase the user instance services. Because of less time complexity proposed approach runs with lowest memory utilization in the processing of users services concerning other approaches.

Figure 4 shows the performance evaluation of the access tree structure concerning different user's tree construction to store data in a secure format.

Table 5 shows the average precision of accuracy values of the proposed approach with different user instances files stored in a secure format in the cloud. Based on the above results, if we increase different user instances, traditional approaches give less accurate results when compare to the proposed approach derived from secure cloud storage.

Table 5. Average Accuracy Values for Different User Instances

Users	CP-ABE	KP-ABE	ASBE	NHACSM
100	4.5	5.9	5.1	3.6
200	5.3	6.6	5.8	4.4
300	4.8	6.3	6.3	3.5
400	7.4	6.8	5.4	4.9
500	6.9	7.2	7.6	5.4

Support of different user instances in exploring data from secure cloud which are described in table 5.

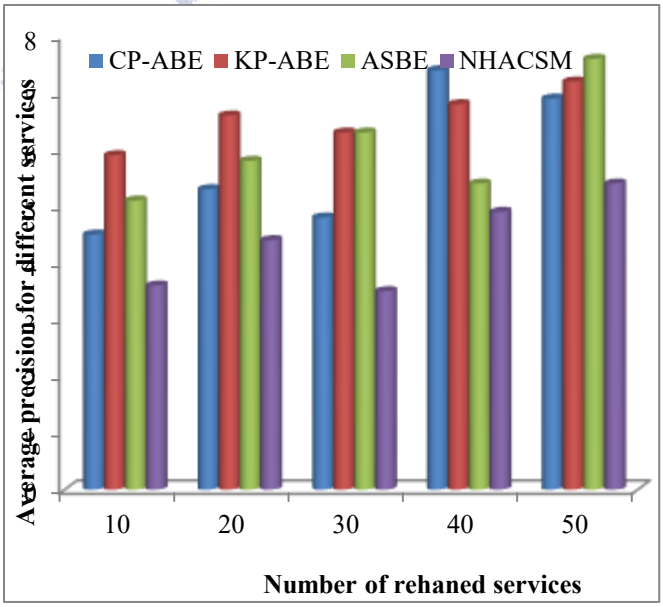

Figure 5. Performance of Accuracy with Different User Secure Operations.

Figure 5 shows the accuracy of different users to perform data security operations in a distributed environment.
Figures from 1-5 show the performance concerning the time of total user instances, time for encryption and decryption concerning memory utilization. The proposed approach gives efficient performance when compared to conventional methods like ASBE, KP-ABE and CP-ABE designed with multi-file sharing cloud environments

4 Conclusion

In this report, we did a novel secure confirmation approach for example NHACSM to give green, adaptable, adaptable client supply get admission to oversee shape in distributed computing. NHACSM practically put into impact hierarchal underlying for approaching individual's documents with the guide of applying realities designation way which is available in trademark set-based encryption. NHACSM does not best help client security and it accomplishes the high-level thought for example disavowal purchaser in measurements sharing assuming more than one venture credit is a gift. We talk security execution system of NHACSM with explicit thought-level estimation methods. The applied trials show green comfortable in general execution assessment and it demonstrates assessment of cutting-edge well-being efficiencies in distributed computing. Further expansion for this is to control the organization's keys, and examine how they might help team-oriented loosened up measurements imparting to relied upon cloud server in distributed computing. The NHACSM method is used to reduce the total time values for different user instances compared to conventional approaches i.e. ASBE, KP-ABE, CP-ABE, for 10 instances ASBE is 2.7, KP-ABE is 2.5, CP-ABE is 2.3and also compared to 20, 30, 40, 50 instances , NHACSM is low. In the encryption time evaluation values and performance evaluation of different approaches in encryption, ASBE, CP-ABE was taken more time whenever increase the user instance concerning different services. In the decryption time evaluation values and performance evaluation of different approaches in decryption also, ASBE, KP-ABE, CP-ABE was taken more time whenever increase the user instance for different services. Where as compared to proposed approach, it was taken by less time compare to existing approaches. The encryption time evaluation values and performance evaluation of different approaches in encryption. The proposed approach was taken less time for the encryption of files uploaded by different users. The decryption time evaluation values and performance evaluation of different approaches in decryption. The proposed approach was taken less time for the decryption of files uploaded by different users with different instant services. The performance evaluation of different approaches in the utilization of memory to explore user instance services. The accuracy of different users to perform data security operations in a distributed environment. Performance evaluation of memory concerning different approaches also efficient. The performance concerning the time of total user instances, time for encryption and decryption concerning memory utilization. The proposed approach gives efficient performance when compared to conventional methods like ASBE, KP-ABE and CP-ABE designed with multi-file sharing cloud environments. Further expansion for this is to control the organization's keys, and examine how they might help team-oriented loosened up measurements imparting to relied upon cloud server in distributed computing.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] R. Ahuja and S. K. Mohanty, "A Scalable Attribute-Based Access Control Scheme with Flexible Delegation cum Sharing of Access Privileges for Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 8, no. 1, pp. 32-44, 1 Jan.-March 2020. doi: 10.1109/TCC.2017.2751471.

[2] S. Xu, G. Yang, Y. Mu and R. H. Deng, "Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2101-2113, Aug. 2018. doi: 10.1109/TIFS.2018.2810065.

[3] Neha Agarwal, Ajay Rana and J. P. Pandey, "Fine-Grained Access Control and Secured Data Sharing in Cloud Computing" cyber security, Advances in Intelligent Systems and Computing, vol 729, pp. 201-214, 2018. https://doi.org/10.1007/978-981-10-8536-9_20

[4] Yaxing Chen, Wenhai Sun, Ning Zhang, Qinghua Zheng, Wenjing Lou, and Y. Thomas Hou, "A Secure Remote Monitoring Framework Supporting Efficient Fine-grained Access Control and Data Processing in IoT", security and privacy in communication

networks, vol 254, pp.3-21,2018. DOIhttps://doi.org/10.1007/978-3-030-01701-9_1,

[5] Jin Sun, Xiaojing Wang , Shangping Wang, Lili Ren "A searchable personal health records framework with fine-grained access control in cloud-fog computing", https://doi.org/10.1371/journal.pone.0207543 November 29, 2018.

[6] Viswanath, G., and P. Venkata Krishna,"Hybrid encryption framework for securing big data storage in multi-cloud environment." Evolutionary Intelligence, vol14, no. 2 pp. 691-698, 2021. DOIhttps://doi.org/10.1007/s12065-020-00404-w

[7] Belguith, Sana, Nesrine Kaaniche, and Mohammad Hammoudeh. "Analysis of attribute-based cryptographic techniques and their application to protect cloud services." Transactions on Emerging Telecommunications Technologies,vol.33, no.3,2022, DOI:10.1002/ett.3667.

[8] Tahir, Muhammad, Muhammad Sardaraz, Zahid Mehmood, and Shakoor Muhammad. "CryptoGA: a cryptosystem based on genetic algorithm for cloud data security." Cluster Computing, vol 24, no. 2, pp. 739-752, 2021. https://doi.org/10.1007/s10586-020-03157-4.

[9] Chinnasamy, P., S. Padmavathi, R. Swathy, and S. Rakesh. "Efficient data security using hybrid cryptography on cloud computing." In Inventive Communication and Computational Technologies, pp. 537-54, 2021. DOI:10.1007/978-981-15-7345-3_46.

[10] Li D, Chen J, Liu J, Wu Q, Liu W,"Efficient CCA2 Secure Revocable Multi-authority Large-Universe Attribute-Based Encryption". in Cyberspace Safety and Security, vol 10581, pp. 103–118,2017. https://doi.org/10.1007/978-3-319-69471-9_8.

[11] Zhang K, Li H, Ma J, Liu X ,"Efficient large-universe multi-authority ciphertext-policy attribute based encryption with white-box traceability". in Science China Information Sciences,vol 61,no. 3,pp. 1-13,2018. https://doi.org/10.1007/s11432-016-9019-8 61: 032102.

[12] Sun W, Yu S, Lou W, Hou T ,"Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grainedOwner-enforced Search Authorization in the Cloud", in IEEE Transactions on Parallel & Distributed Systems, vol 27, no4, pp.1187–1198,2016. DOI: 10.1109/TPDS.2014.2355202.

[13] Cui H, Wan Z, Deng R, Wang G, Li Y ,"Efficient and Expressive Keyword Search Over Encrypted Data in the Cloud" in IEEE Transactions on Dependable & Secure Computing , vol15, no3, PP: 1–1,2016. DOI: 10.1109/TDSC.2016.2599883.

[14] Miao Y, Ma J, Jiang Q, Li X, Sangaiah AK ,"Verifiable keyword search over encrypted cloud data in smart city" in Computers & Electrical Engineering, vol 65, pp 90–101. 2018. https://doi.org/10.1016/j.compeleceng.2017.06.021

[15] Sohal, Manreet, and Sandeep Sharma. "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing." Journal of King Saud University-Computer and Information Sciences, vol 34, no.1, pp 1417-1425, 2022. https://doi.org/10.1016/j.jksuci.2018.09.024.

[16] Adee, Rose, and Haralambos Mouratidis. "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography." Sensors,vol. 22, no. 3, pp.1109., 2022. https://doi.org/10.3390/s22031109.

[17] Li, Jiguo, Fengjie Sha, Yichen Zhang, Xinyi Huang, and Jian Shen. "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length." Security and Communication Networks,vol2017,no.2,pp.1-11,2017. DOI:10.1155/2017/35962052017.

[18] Zhao Z, Wan J ,"Verifiable Outsourced Ciphertext-Policy Attribute-Based Encryption for Mobile Cloud Computing" in Ksii Transactions on Internet & Information Systems,vol.11, no.6, pp. 3254–3272, 2017. DOI:10.3837/tiis.2017.06.024.

[19] Bharath K.Samanthula, YousefElmehdwi,GerryHowser,SanjayMadria, "A secure data sharing and query processing framework via federation of cloud computing" in Information System, vol. 48, pp.196–212, 2015. https://doi.org/10.1016/j.is.2013.08.004.

[20] S. Kumar, G. Karnani, M. S. Gaur and A. Mishra, "Cloud Security using Hybrid Cryptography Algorithms," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM),vol.2021,pp.599-604,2021.doi: 10.1109/ICIEM51511.2021.9445377.