ISSN 2515-8260 Volume 8, Issue 11, 2021

An Anti-Collusion Information Sharing Scheme Provides Secure Scheme for Data Privacy in Cloud Computing

[1] V Veeresh, [2]L. Rama Parvathy
[1]*Research Scholar*, [2]*Professor*,
[12]*Department of Computer Science and Engineering,*
[12]*Saveetha School of Engineering, Chennai, Tamilnadu, India.*
[12]*Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India.*
[1]vaddeveeresh@gmail.com, [2]ramaparvathyl.sse@saveetha.com

Abstract:
In cloud computing, the cloud service providers provide space for shoppers to network with other information management system by moving native management system into cloud services. This provides a strong and effective use of resources and, also cuts down the expenditure for the providers. There is a limitation for the cloud suppliers in preserving the information more secure and economically within the cloud. They also have to encrypt the information before transferring into the cloud to maintain privacy. The suppliers have found a crypto graphical storage system to share secure and economical information based on the following technique, in which the files are divided and encrypted into groups within a file-block key. These file-block keys were driven to be updated and shared for user revocation. There are complications when alternative schemes used for information sharing with un-trusted servers. The revocation in these schemes measure lengthy with the information from the suppliers and also call back the users. An Anti-Collusion Information Sharing Scheme provides secure private keys to consumers on the addition or revocation of a customer. The new customers can obtain the keys from team manager through certified authorities and secure communication channels. Thus a revoked customer won't be able to retrieve usual data documents even if they plot with un-trusted cloud.
Keywords: Native management system, Cloud services, Crypto graphical storage, File-block keys, Cloud Computing, Cloud Security, Secure private keys, Un-trusted cloud

1. INTRODUCTION

Cloud computing is known technology, which delivers and maintains its computing resources through server virtualization using the internet. Cloud computing transfers, stores, manages and processes information to providers securely with a customer controlled policy. Based on customer demand the cloud offers infrastructures, computing power, applications and services. Cloud computing is not a single technology, it is primarily comprised of three services Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). It provides information based on the user needs which are stored in different locations with cost advantages. Clod computing stores data and users can access it through the internet rather storing it in the hardware, this method helps users to access data at a maximum utilization.

It operates on a principle where the users can access all

features and files as per their demand instead of storing them in bulk in their own system.

Cloud computing is classified based on its location and services offered as;

Private cloud: The cloud infrastructure is allocated to a single client and the data is not shared with others and thus enhances the security and privacy.

Public cloud: The cloud infrastructure and services are available in public where all users can have access to it.

*Hybrid cloud***:** It is a blend of private and public cloud

The organizers keep more sensitive data in a private cloud and maintained privacy whereas operations that do not use sensitive data are maintained in public cloud.

Community cloud: Community cloud is an attractive option for companies with common goals and the infrastructure is designed to meet community needs.

The research is presented in the following order, Introduction to cloud computing system followed by Literature

ISSN 2515-8260 Volume 8, Issue 11, 2021

reviews of cloud computing. Then Cloud computing system architecture is explained with Simulation tools and results and concluded.

2. LITERATURE REVIEW

To build trust and confidence among the service providers and data owners a secured network is structured with various resources in different locations as clouds. Data coloring and watermarking method provide authenticated data, single cloud based on demand, strong access control for data cloud in public and private. Due to increased growth in cloud computing the business is also evolving with the model that delivers security as a service (SECaaS) and data protection as a service (DPaaS) [1].

The cloud computing services are debated for the security challenges which stresses on storage layer and data layer. The paper also discusses about the Map Reduce in Hadoop security in processing large data which are divided and presented parallel with independent tasks. Lastly, the XACML application for Hadoop is discussed and it provides fine access to data control and created safe cloud computing using trusted applications from non-trustworthy server [2].

The data security is well managed by RSA algorithm where the concern user can only access the data. The encryption is performed by the cloud service provider and decryption is safely done by the cloud user only. Thus, data security is provided by implementing the RSA algorithm [3].

The data is protected before storing in the cloud by a new encrypted technique method as explains; it compares 3xAES with AES and T-DES algorithms by calculating encryption, decryption time and key generation time. The security of data is higher based on the key length, i.e. 3xAES has a refined security than AES and 3DES because it encrypts the data 3 times with new key for each encrypt and decrypt [4].

A framework is implemented to show the security levels by performing risk assessment, analysis and mitigation, by covering all cloud service models and cloud deployment models. The reason for accepting this framework is because of the successful secured information execution or alteration of data for cloud computing environment. It is implemented in the logistics Software as a Service (SaaS) is developed and applied to Infrastructure as a Service (IaaS) environment and Platform as a Service (IaaS) to testing this framework [5].

The consumers have accepted the cloud computing services mainly for data storage and privacy safety measures. A brief discussion about the cloud computing process particularly safety issues with few solutions are discussed. The current scope of cloud computing in sharing data lays far behind expectation and the future research work on privacy and security challenges in the cloud are discussed [6].

A cohesive security system offers “Security as a Service” to the organizers as a single-tier or multi-tier based on their need. The safety of the data is evaluated in the cloud at each macro and micro level. This provides an effective solution to the cloud application and to the consumers with similar goals or requirements [7].

The system holds different methods and specific action to present the data from start to the end that is structured based on three cryptographic constraints provided by the user, such as, Confidentiality (C), Availability (A) and Integrity (I). The data in cloud storage are guarded by procedure like the SSL (Secure Socket Layer) 128-bit encryption and also uplifted up to 256-bit encryption on requirement, the authenticity of the data is verified by MAC (Message Authentication Code), searchable encryption and data is divided into three segments in the cloud. Hence, the consumer is provided with a login identity and password to access the data that is secured after data conversion in Section 1, Section 2, and Section 3 [8].

Scholars have conducted numerous surveys about data safety and privacy from software and hardware where data are stored in clouds at different locations. They have also suggested many methods to achieve the highest level of data security in the cloud which has created trust between cloud service provider and users [9].

At present users are concerned about data security issues, mainly virtualization security and data security have been the major problem, thus cloud computing is facing challenges with regard to security issues. Users have stored their information in a cloud and keep transferring from one cloud to another cloud which risks the security of the data. The elliptic curve cryptography technique is used for a faster and more efficient cryptographic key to offer better security, privacy and quality of data in the clouds [10].

The data safety process for cloud computing is improvised by studying the cloud architecture and three solutions are presented. The software is applied to boost the security for cloud computing and recently used in the Amazon EC2 Micro instance [11].

Many studies are conducted to analyze the performance and quality of data processing, secured data storage, data recovery and data collection in IIoT. An efficient and secured data storage and recovery in IIoT is suggested by a structured framework to provide solutions after studying the fog computing and cloud computing. Based on the latency need the data are transferred and stored by the edge server or the cloud server [12].

ISSN 2515-8260 Volume 8, Issue 11, 2021

Two algorithms AES (Advanced Encryption Algorithm) and Blowfish Algorithms are studied which provided double security for the data in the cloud. It mainly offers safety against unauthorized data access. This research paper discusses only about the early proposal and the technical details and data analysis are not briefed [13].

A productive and secured access control environment is created for cloud computing using Attribute Based Encryption (ABE), Distributed Hash Table (DHT) network, and Identity Based Timed Release Encryption (IDTRE). Based on the consumer needs the data is encrypted, segregated and compressed into cipher text and extracted cipher text. IDTRE algorithm is installed to encrypt the decryption key. Cipher text key and extracted cipher text are clubbed to generate cipher text shares, that are distributed into DHT network and the compressed cipher text are stored in the cloud servers [14].

The cloud data are audited using a public key based on homomorphic authenticator with arbitrary camouflaging. It mainly results in privacy-preserving of data in the cloud and focuses on multiple auditing with a method of bilinear aggregate signature resulting in multiple user setting. For this action TPA is applied to conduct countless auditing tasks simultaneously. Thus, a study revealed that this technique is highly secured and effective [15].

A new approach is presented to the resource users, who trust the cloud services for storage of data efficiently and secured deletion of data. The method includes All-Or-Nothing-Transform for strong, secure resource storage and securely divides the resources to finally decentralize the data allocated in the storage network. The resource owners use this model to control their settings that are available and secured [16].

The recent evolving technology is cloud computing, which offers many advantages to the users. But this technology challenges security issues and many solutions are presented to develop secured cloud services. Creative or supported encryption methods along with suitable management systems can be implemented to attain safe data storage and recovery from the cloud. This would allow data access only by enrolled users [17].

A classification technique is presented which describes numerous scopes for data safety at different levels. It provides required safety to the data at each stage that are segregated and stored. Its success is analyses with the sample data stored in the cloud [18].

Cipher text-Policy Attribute-Based Hierarchical document collection Encryption scheme called CP-ABHE is a combination and construction of access tress. This tree is at regular rise and rose by merging the smaller ones. Each leaf on the tree has a similar secret number that is used for encryption of data, resulting in the enhanced performance. CP-ABHE expressed his work effectively with regard to safety and storage size of the cipher text [19].

A superior control measure and privacy protection in a multi-authority cloud storage structure is provided by PMDAC-ABSC data access control system which is built on Cipher text-Policy ABSC. The authorities and cloud servers are aware of the characteristics of the sign-cryptor and de-sign cryptor. Hence this method is confirmed to be safe for normal model by delivering privacy, unidentified validation and public verification [20].

A classified multi-authority attribute-based encryption has a multi-centre attribute authorization arrangement along with a combined attribute index. This method is presented on larger group and identified by its characteristic to structure a dual tree. Based on the child node in an attribute access tree the value of the parent node is identified. In this study the attribute-based encryption calculatedly decreases the volume for decryption and compresses the unwanted data in the cipher text at a greater extend. This encryption method has a hypothetical and real-world significance in the system of "large universe" constructions [21].

Mediated Constant Cipher text-Policy ABE (MCCP-ABE) and a mediated revocation are constructed to give solutions for storage and deletion. Third-party servers are designed using these methods for enabling file transmission in semi trusted pattern for access control. The performance is evaluated that resulted in holding a constant-length numeric ABE cipher text and limited duration in conducting selective and partial revocation [22].

3. PROPOSED METHOD

3.1 Cloud Computing System Structure

The cloud offers space for data storage for user has pay-as-you-go manner. At times the cloud service providers become untrusted, hence the cloud analyses the content of the data stored. The Group Manager is the leader who is trusted by the users. He is in-charge of the system parameters generation, user registration and user revocation. The registered users who have stored their own data in the cloud do share them with others. All registered users become the group members and the membership keeps changing because of new user registration and revocation.

3.2 File Security Module

Encryption of data file – The Group Manager or the data owner (i.e., the member who uploaded the file into the server) can delete the file stored in the cloud.

3.3 Group Signature Module

On securely maintaining one's identity, the member of the group can sign messages through the group signature

ISSN 2515-8260 Volume 8, Issue 11, 2021

scheme. The member's identity can be revealed by the assigned group manager when an issue arises to indicate the originator.

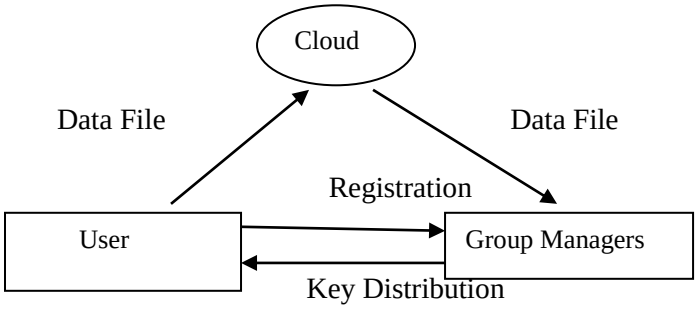


Fig.1: Structure of Proposed System of Group Signature Module

3.4 User Revocation Module

The group manager performs User revocation through a publicly available revocation list (RL).The group members do encrypt the data files through this model by ensuring confidentiality against revoked members.

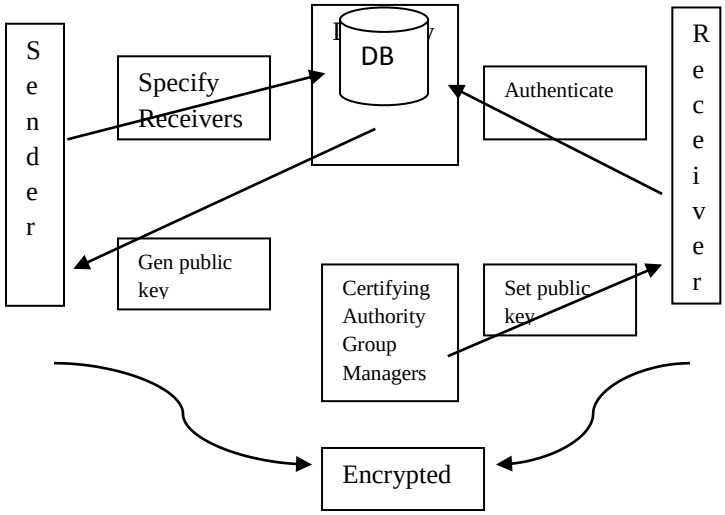


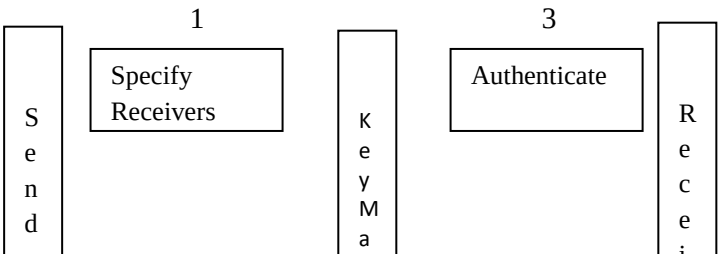
Fig.2: Proposed System of User Revocation Module

3.5 A New Method to Key Management

In 1984 a new method of public key algorithm named Specific Identity-Based Encryption (SIBE) was introduced. This algorithm mathematically produces the receiver's public key from their own identity and the key server calculates the desired private key. SIBE algorithm pulls out the requirement for public key queries or certificates, because the key recovers doesn't need a separate private key database, since the key server generates its private key.

SIBE algorithm wholly simplifies key management so that the sender receives the encrypted key derived from the receiver's identity without contacting the key server. The receiver contacts the key server once by which it generates the receiver's decryption key mathematically and produces key recovery exceptionally simple. This makes the partner's key server simple and the sender's policy order which key server to be ordered to secure a message. This server is controlled by a single sender's organization, processed by a single outside server or stored at a single receiver's organization.

Design Goal



ISSN 2515-8260 Volume 8, Issue 11, 2021

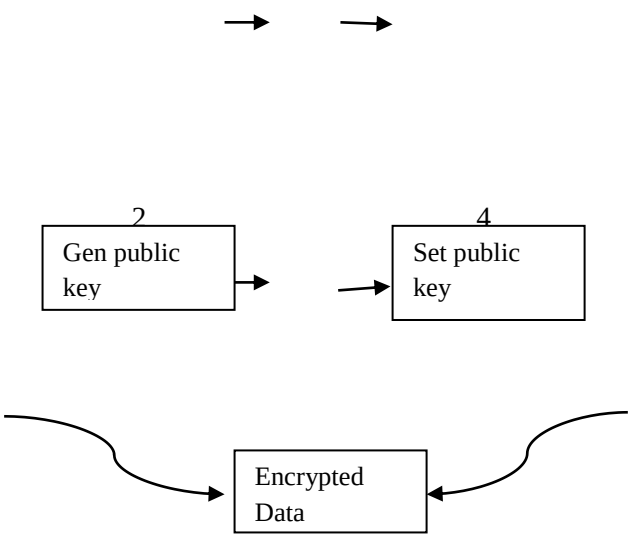


Fig.3: Proposed Key Management System

3.5.1) Key Distribution:

A secured communication channel is achieved when the users receive their private keys from the group manager without any approval from certified authorities. While with other schemes the security is only assumed.

3.5.2) Access Control:

The group members have access to the cloud resource for data storage and sharing, while the revoked users on the revocation and unauthorized users cannot access the cloud resources at all.

3.5.3) Data Confidentiality:

Maintaining Data confidentiality for dynamic group yet remains an important and challenging issue. The revoked users on the revocation and unauthorized users will not be able to learn or decrypt the stored data.

3.5.4) Efficiency:

The data can be stored and shared in the cloud by any of the group members. There is no necessity for members to update their private keys when an user is revoked from the group.

ISSN 2515-8260 Volume 8, Issue 11, 2021

ALGORITHM:

The algorithm design includes various methods and theorems as follows;

Bilinear Maps

Complexity Assumption

Table 1: Notation and Description of Algorithms

Notation	Description
IDi	The identity of user I
IDdatai	The identity of data I
pK	Public key of user
sK	Corresponding private key to pK
KEY=(xi,Ai,Bi)	The private key which is distributed to user from the group manager and used for data sharing.
Enck()	Symmetric algorithm used the encryption key k
AEnck()	Asymmetric algorithm used the encryption key k
UL	Group user list
DL	Data list

The algorithm consists of the following segments

System Initialization

User Registration for existing user

File Upload

Registration for new user

File Download

System Initialization:

The system is initiated by the group manager

$$S = \left(q, G_1, G_2, e(\cdot,\cdot)\right)$$

The formula briefs that S is a bilinear System, where two random elements from group are selected i.e. P,G € G1 and consider the number γ € Zq*

From the above consideration, we can find that

W= γ.P, Y= γ.P and complex number Z=e(G,P).

In the end, the group manager publishes the equation with some parameters

(S,P,W,Z,f,f1, Enc())

Where f is a hash function {0,1}*-> G1 , Enc() is a symmetric encryption algorithm.

The group manager will keep the parameter (γ,G) for secret key computation.

User Registration

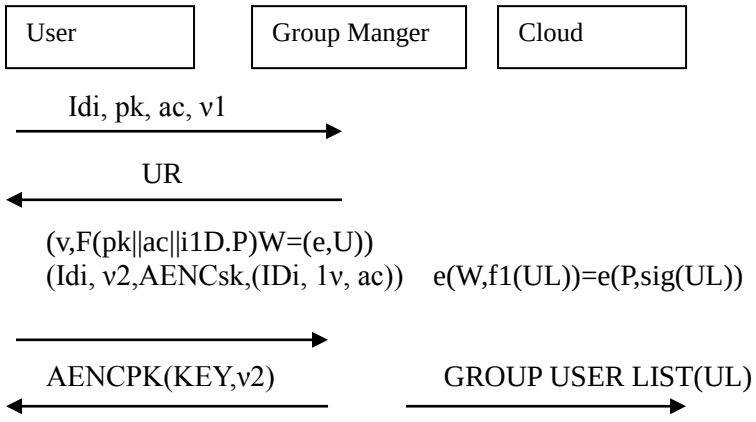


Fig.4: Data Flow of User Registration Module

User sends Idi, pk, v1 as request, the group managers where IDI – Identify of the ith user.

Pk – public key used in asymmetric encryption algorithm

ac – account user used to pay for registration

v1- random number selected by user

r- random number selected by group managers

compute

R= e(P,P)r,

U = (r+γ.v1.f(Pk ‖ ac ‖ IDi)).P

Lately group managers send the verification for U and R for user verification and the verification performed by the

ISSN 2515-8260 Volume 8, Issue 11, 2021

user as,

R.e(v1. f (pk ‖ ac ‖ IiDi) P.W= e(U,P).

The user sends the message to the group manager

Idi, v2,AENCsk,(IDi, 1v, ac)

In this AENC is a symmetric encryption algorithm

Sk is the private key and pk is a public key;.

The group managers receive the message, compare the received ID from decryption of AENCsk,(IDi, 1v, ac)

Then confirms the decrypted v1 is same as random number v1. Then the group manager selects a number and an another manager selects another random number x

This computes the following elements

Ai=(1 / (𝛾 + xi)).P € G1

Bi=(xi/ (𝛾 + xi)).G € G1

V1m= f(Bi)

(xi, Ai,Bi) constructs the message key.

Thus the group manager sends the encrypted message AENCPK(KEY, v2) to the user and stores (xi, Ai,V,IDi) in the local storage space. And he adds (Ai,xi) to the group user list UL, which is illustrated in the Table 1. Frequently the group

manager updates the time stamp tUL for each user listed. Finally the group manager signs, sig(UL) = 𝛾f1(UL) and sends the group user list, to the cloud.

Only on successful verification e(W,f1(UL))=e(P,sig(UL)) is available in the cloud and it stores the group user list

The user can decrypt the file by applying the following equation AENCPK(KEY,v2) with his private key (x, A, B). On successful registration, the user becomes a group member.

IDgroup	A1	X1
	A2	X2
	*	*
	Ar	Xrtulsig(UL)

File Upload

On choosing the unique data file identity IDdata and the random number k € Z*q the group user can upload a file.

After calculation

C1=k.Y€ G1

C2=k.P€ G1

K=Zk€ G2

C=Enck(M)

The group member can encrypt the data with private key Bi, for this real time stamp tdata

EncBi(IDdata,C1,C2,C,tdata)

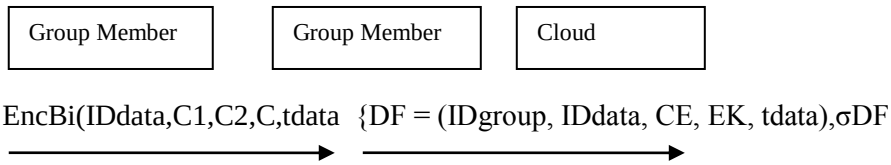


Fig.5: Key Encryption Data Flow

CE is encrypted by the key {DF = (IDgroup, IDdata, CE, EK, tdata),σDF}

And the signature of the group is σDF= 𝛾f1(DF)

The group manager then sends the data list to the cloud.

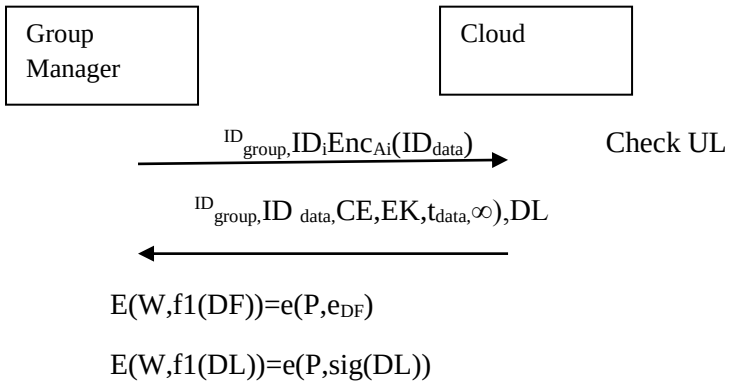
In the table 2 real time stamp and data list are presented

ISSN 2515-8260 Volume 8, Issue 11, 2021

Table 2: Real Time Stamp and Data List

Group Id	Data List	Time Stamp For Encypt	Time Stamp For Data List	Signature Of Data List
ID_{group}	ID_{data1}	t_{data1}		
	ID_{data2}	t_{data2}		
	ID_{datar}	t_{datar}	t_{DL}	Sig(DL)

File Download:



On receiving the file, the member can decrypt the encrypted the file

K^ =e(C1,A)e(C2,B)
=e(k. Y,1/(𝛾+x). P)e(k. P,1/(𝛾+x). G)
=e(G,P)ky/𝛾+x e(P,G)ky/𝛾+x
=Zk= K
Finally the group member can decrypt the data.

4. RESULTS AND IMPLEMENTATION

New models are tested with NS2 and compared with Mona in [20] and the original dynamic broadcast encryption (ODBE) Scheme in [21]. Earlier we considered p=160 and the elements in G1 and G2 is 161 and 1,024 bits respectively.

The following are the framework design of the nodes NS2.
The data identity = 16
Group capacity of 216 data files.
Size of user =16 bits
The group identity = 16 bits
This model is configured with latest i7 processor and 8 GB of Ram that operates using Ubuntu OS and an elliptic curve with 160 bits group order is chosen.

Table 3: Comparison on user computation cost for file creation (10 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The number	ODBE-computation	RBAC	MONA	Anti-Collusion

ISSN 2515-8260 Volume 8, Issue 11, 2021

of revoked users	of member-side			Information Sharing Scheme
10	0.4	0.39	0.32	0.35
20	0.5	0.35	0.33	0.33
30	0.6	0.34	0.34	0.34
40	0.7	0.36	0.32	0.35
50	0.8	0.39	0.33	0.36
60	0.9	0.37	0.34	0.35
70	1	0.36	0.32	0.34
80	1.1	0.35	0.33	0.35
90	1.2	0.37	0.31	0.34
100	1.3	0.39	0.32	0.35

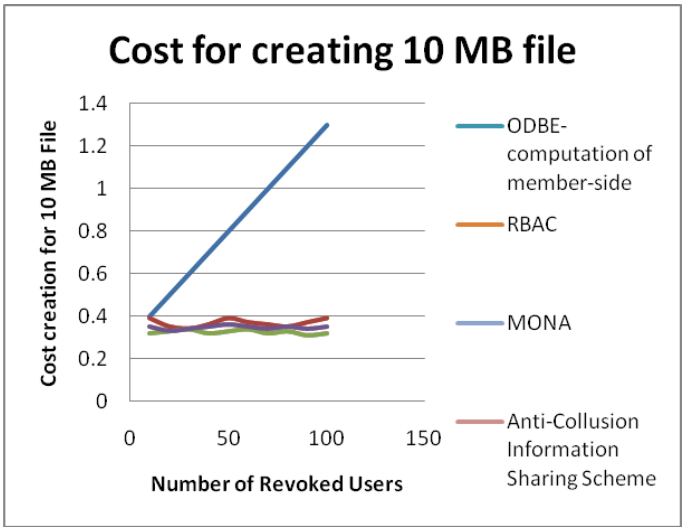


Fig.6: Comparison on user computation cost for file creation (10 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

Table 3 and Fig.6illustrated, according to the X axis value that represents the number of revoked users and Y axis depicts cost creation for a 10 MB file. The cost creation for a 10 MB file is created using the different available algorithm along with the propose algorithm. During file creation the proposed cost model is higher than the existing ones. The estimation is higher because the upload and download to format, duration is longer to encrypt and decrypt files

Table 4: Comparison on user computation cost for file creation (100 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The number of revoked users	ODBE-computation of member-side	RBAC	MONA	Anti-Collusion Information Sharing Scheme
10	1.3	1.39	1.32	1.35
20	1.4	1.35	1.33	1.33
30	1.5	1.34	1.34	1.34
40	1.6	1.36	1.32	1.35
50	1.7	1.39	1.33	1.36
60	1.8	1.37	1.34	1.35
70	1.9	1.36	1.32	1.34

ISSN 2515-8260 Volume 8, Issue 11, 2021

80	2	1.35	1.33	1.35
90	2.1	1.37	1.31	1.34
100	2.2	1.39	1.32	1.35

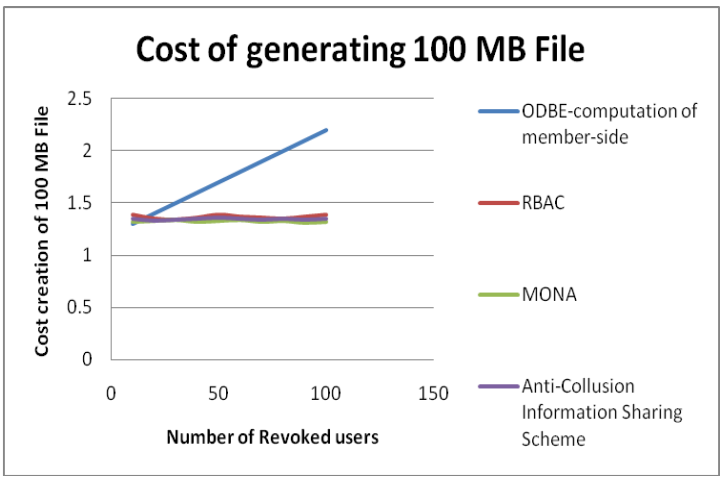


Fig.7: Comparison on user computation cost for file creation (100 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The Table 4 and Fig.7illustrates the cost to create 100 MB file using different algorithms including the proposed algorithm. The duration involved in formatting the uploads and downloads of a file with encryption and decryption has increased the cost of the model during file creation. This graph is plotted based on the x axis value, which is the number of revoked user and the y axis is creation of cost for a 100 MB file.

Table 5: Comparison on user computation cost for file download (10 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The Number Of Revoked Users	ODBE-Computation Of Member-Side	RBAC	MONA	*Anti-Collusion Information Sharing Scheme*
10	0.4	0.39	0.32	0.86
20	0.6	0.35	0.38	0.83
30	0.8	0.34	0.44	0.8
40	1	0.36	0.5	0.77
50	1.2	0.39	0.56	0.74
60	1.4	0.37	0.62	0.71
70	1.6	0.36	0.68	0.68
80	1.8	0.35	0.74	0.65
90	2	0.37	0.8	0.62

ISSN 2515-8260 Volume 8, Issue 11, 2021

100	2.2	0.39	0.86	0.59

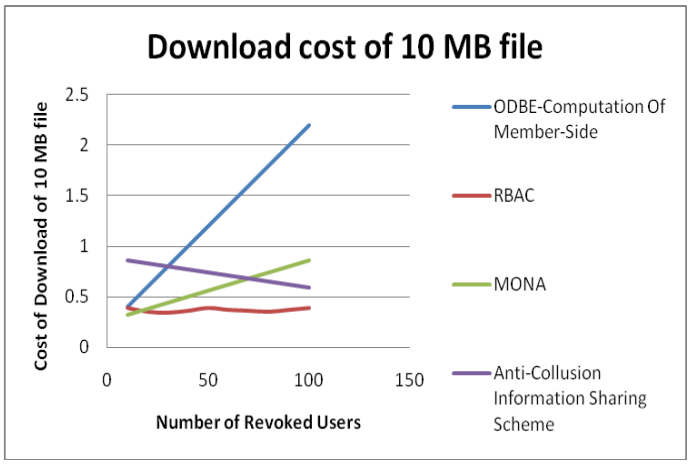


Fig.8: Comparison on user computation cost for file download (10 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The Table 5 and Fig.8 explains the cost involved to download 10 MB file using various exiting algorithms including the proposed algorithm. Due to the duration taken to upload and download the file with encryption and decryption during file creation the cost is on the rise. The graph is plotted based on the value of the x axis, which represents the number of revoked user and the y axis explains the uploading cost of 10 MB file. The graph shows that the RBAC cost is lower because there is no encryption and decryption algorithm. The cost rises, if the number of the user increases. But this model is not designed based on the number of users

Table 6: Comparison on user computation cost for file download (100 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The number of revoked users	ODBE-computation of member-side	RBAC	MONA	*Anti-Collusion Information Sharing Scheme*
10	1.6	1.64	1.6	2
20	1.8	1.63	1.66	1.97
30	2	1.74	1.72	1.94
40	2.2	1.63	1.78	1.91
50	2.4	1.62	1.84	1.88
60	2.6	1.65	1.9	1.85
70	2.8	1.66	1.96	1.82
80	3	1.65	2.02	1.79
90	3.2	1.63	2.08	1.76
100	3.4	1.64	2.14	1.73

ISSN 2515-8260 Volume 8, Issue 11, 2021

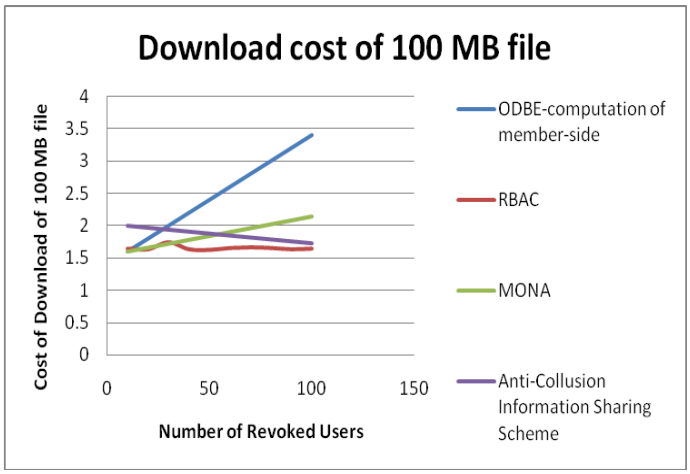


Fig. 9: Comparison on user computation cost for file download (100 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The Table 6 and Fig.9presents the estimation to download 100 MB file using various exiting algorithms along with the proposed algorithm.Due to the duration taken to upload and download the file with encryption and decryption during file creation the cost is on the rise. The graph is plotted based on the value of the x axis, which represents the number of revoked user and the y axis explains the downloading cost of 100 MB file.The graph shows that the RBAC cost is lower because there is no encryption and decryption algorithm. The cost rises, if the number of the user increases. But this model is not designed based on the number of users.

Table 7: Comparison on user computation cost for file upload (10 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The number of revoked users	RBAC	MONA	Anti-Collusion Information Sharing Scheme
10	0.02	0.043	0.04
20	0.024	0.083	0.044
30	0.021	0.098	0.041
40	0.022	0.113	0.044
50	0.0223	0.128	0.0443
60	0.0211	0.143	0.0411
70	0.024	0.158	0.044
80	0.025	0.173	0.045
90	0.023	0.188	0.043
100	0.021	0.203	0.041

ISSN 2515-8260 Volume 8, Issue 11, 2021

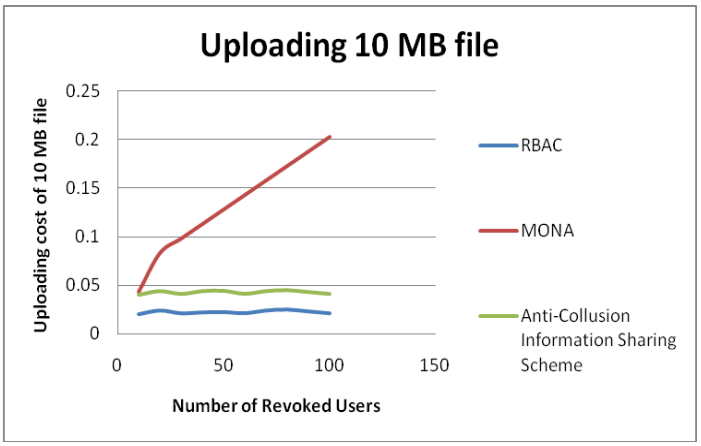
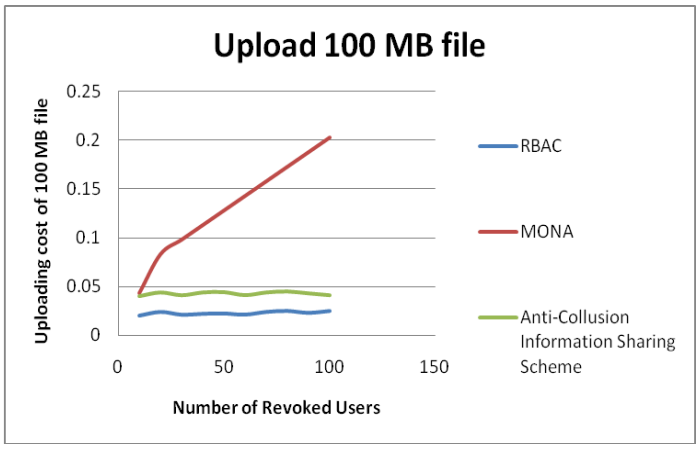


Fig.10: Comparison on user computation cost for file upload (10 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The Table 7 and Fig.10 explains the cost involved to upload 10 MD file using various exiting algorithms including the proposed algorithm. Due to the duration taken to upload and download the file with encryption and decryption during file creation the cost is on the rise. The graph is plotted based on the value of x axis, which represents the number of revoked user and the y axis explains the uploading cost of 10 MB file. The graph shows that the RBAC cost is lower because there is no encryption and decryption algorithm. The cost rises, if the number of the user increases. But this model is not designed based on the number of users.

Table 8: Comparison on user computation cost for file upload (100 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The number of revoked users	RBAC	MONA	Anti-Collusion Information Sharing Scheme
10	0.02	0.043	0.04
20	0.024	0.083	0.044
30	0.021	0.098	0.041
40	0.022	0.113	0.044
50	0.0223	0.128	0.0443
60	0.0211	0.143	0.0411
70	0.024	0.158	0.044
80	0.025	0.173	0.045
90	0.023	0.188	0.043
100	0.025	0.203	0.041



ISSN 2515-8260 Volume 8, Issue 11, 2021

Fig.11: Comparison on user computation cost for file upload (100 MB) among ODBE, RBAC, MONA and Anti-Collusion Information Sharing Scheme

The Table 8 and Fig.11 explains the cost involved to upload 100 MB file using various exiting algorithms including the proposed algorithm. Due to the duration taken to upload and download the file with encryption and decryption during file creation the cost is on the rise. The graph is plotted based on the value of x axis, which represents the number of revoked user and the y axis explains the uploading cost of 100 MB file. The graph shows that the RBAC cost is lower because there is no encryption and decryption algorithm. The cost rises, if the number of the user increases. But this model is not designed based on the number of users.

CONCLUSION

The Information sharing on un-trusted servers is planned to use alternative schemes. But there are challenges for the user involvement and revocation in the schemes. The quantity of information about the owners and the revoked users are increasing progressively. The cloud with an Anti-Collusion Information Sharing Scheme for dynamic companies had secured private keys for the users, obtained from the team managers through certified authorities and secured communication channels. When a new user is registers or a user is revoked from the group, the scheme is equipped to support powerful companies by providing secured private keys, which are not required to be recomputed or updated in this process. The scheme also protects the data effectively, when a revoked user cannot retrieve the data even if they try to process using an un-trusted cloud, as a result this scheme handles revoked user at ease.

REFERENCES

[1]. Hwang, Kai, and Deyi Li. "Trusted cloud computing with secure resources and data coloring." IEEE Internet Computing 14, no. 5 (2010): 14-22.

[2]. Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." International Journal of Information Security and Privacy (IJISP) 4, no. 2 (2010): 36-48.

[3]. Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." International Journal of research in computer and communication technology, IJRCCT, ISSN (2012): 2278-5841.

[4]. Ahmed, Farah Qasim, and Lect Dr Amin Salih Mohammed. "ENHANCING THE DATA SECURITY IN CLOUD COMPUTING BY USING NEW ENCRYPTION METHOD." Qalaai Zanist Journal 3, no. 1 (2018).

[5]. Zhang, Xuan, Nattapong Wuwong, Hao Li, and Xuejie Zhang. "Information security risk management framework for the cloud computing environments." In 2010 10th IEEE international conference on computer and information technology, pp. 1328-1334. IEEE, 2010.

[6]. Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In 2012 International Conference on Computer Science and Electronics Engineering, vol. 1, pp. 647-651. IEEE, 2012.

[7]. Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34, no. 1 (2011): 1-11.

[8]. Sood, Sandeep K. "A combined approach to ensure data security in cloud computing." Journal of Network and Computer Applications 35, no. 6 (2012): 1831-1838.

[9]. Sun, Yunchuan, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu. "Data security and privacy in cloud computing." International Journal of Distributed Sensor Networks 10, no. 7 (2014): 190903.

[10]. Gampala, Veerraju, Srilakshmi Inuganti, and Satish Muppidi. "Data security in cloud computing with elliptic curve cryptography." International Journal of Soft Computing and Engineering (IJSCE) 2, no. 3 (2012): 138-141.

[11]. Mohamed, Eman M., Hatem S. Abdelkader, and Sherif El-Etriby. "Enhanced data security model for cloud computing." In 2012 8th International Conference on Informatics and Systems (INFOS), pp. CC-12. IEEE, 2012.

[12]. Fu, Jun-Song, Yun Liu, Han-Chieh Chao, Bharat K. Bhargava, and Zhen-Jiang Zhang. "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing." IEEE Transactions on Industrial Informatics 14, no. 10 (2018): 4519-4528.

[13]. Gupta, Utkarsh, Mrs Shivani Saluja, and Mrs Twinkle Tiwari. "Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms." (2018).

[14]. Namasudra, Suyel. "An improved attribute-based encryption technique towards the data security in cloud computing." Concurrency and Computation: Practice and Experience 31, no. 3 (2019): e4364.

[15]. Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for data storage security in cloud computing." In 2010 proceedings ieee infocom, pp. 1-9. Ieee, 2010.

[16]. Bacis, Enrico, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. "Securing resources in decentralized cloud storage." IEEE Transactions on Information Forensics and Security 15 (2019): 286-298.

ISSN 2515-8260 Volume 8, Issue 11, 2021

[17]. Rao, R. Velumadhava, and K. Selvamani. "Data security challenges and its solutions in cloud computing." Procedia Computer Science 48 (2015): 204-209.

[18]. Shaikh, Rizwana, and M. Sasikumar. "Data Classification for achieving Security in cloud computing." Procedia computer science 45, no. C (2015): 493-498.

[19]. Fu, Junsong, and Na Wang. "A practical attribute-based document collection hierarchical encryption scheme in cloud computing." IEEE Access 7 (2019): 36218-36232.

[20]. Xu, Qian, Chengxiang Tan, Zhijie Fan, Wenye Zhu, Ya Xiao, and Fujia Cheng. "Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption." IEEE Access 6 (2018): 34051-34074.

[21]. Zhang, Zhiyong, Cheng Li, Brij B. Gupta, and Danmei Niu. "Efficient compressed ciphertext length scheme using multi-authority CP-ABE for hierarchical attributes." IEEE Access 6 (2018): 38273-38284.

[22]. Figueroa, Kathleen Gay, and Susan Pancho-Festin. "An access control framework for semi-trusted storage using attribute-based encryption with short ciphertext and mediated revocation." In 2014 Second International Symposium on Computing and Networking, pp. 507-513. IEEE, 2014.