Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 5164-5175*

Research Article

A Safe and Resilient Cryptographic System for Dynamic Cloud Groups with Secure Data Sharing and Efficient User Revocation

Prerna Agarwal[a], Dr. S.P.Singh[b], Pranav Shrivastava[c]

[a] Research Scholar: Department of Computer Science, Birla Institute of Technology, Mesra, Assistant Professor: Department of Computer Science Engineering, JIMS Engineering Management Technical Campus, Greater Noida
[b]Assistant Professor: Department of Computer Science, Birla Institute of Technology, Mesra
[c] Assistant Professor, Department of Computer Science & Engineering, GLBITM Greater Noida

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: A comprehensive and functional approach is built in cloud computing, which can be used by cloud users to exchange information. Cloud service providers (CSPs) can transfer through server services through powerful data centres to cloud users. Data is protected through authentication of cloud users and CSPs can have outsourced data file sharing security assurance. The continuing change in cloud users, especially unauthenticated users or third parties poses a critical problem in ensuring privacy in data sharing. The multifunctional exchange of information while protecting information and personal protection from unauthorized or other third-party users remains a daunting challenge

Keywords: Cloud Computing Security, Data Security, PKCS, Data Sharing

1. Introduction

The current scenario shows the rapid development of cloud[1][2][3][4][5][6] wireless networks[7][8]and sensor network system [9][10][11], including superior software, on-demand access of data and server services. Explicitly, both individuals and companies used cloud storage services extensively. In cloud computing paradigm, client can remotely access a wide range of shared applications with quality services. Personal computers, in comparison, permit minimal capacity, while the cloud offers scalable capacity. For example, outsourcing of confidential data, health history, private images, videos etc. Nevertheless, the leakage of private / personal data between community members is a significant problem for social network applications. Owing to mentioned reason, the cloud storage data must be encrypted by its owners. Nonetheless, it creates problems such as encrypted data exchange [12]; secure searches for encoded data [1][2][3] and audits of data for outsourced information [4]. This study is aimed at analysing and addressing together; data privacy and protection issues in cloud storage environments faced by clients. This also compares the encryption method, analysing the performance factor, comparing features and computational complexity among current schemes which relate dynamically to group data sharing. From this review, the technology for addressing outsourced data security in cloud systems was explored.

Data sharing has become more common in society in many ways, particularly in real businesses, governments and organizations [2]. As a group, a set of data owners (users) approved as a community shall be recognized. Groups are largely dependent on membership identification. A dynamic group is a group that allows members the rights of joining and exiting the group as necessary.Dynamic membership allows one or more rules to define the membership of a team which checks for certain user attributes [3]. With dynamic membership we can set up teams for certain cohorts of users in any organization. Possible scenarios include:

a A hospital should set up separate coordination groupings for nurses, physicians and surgeons. This is particularly relevant when the hospital is dependent on temp staff.

b A university can set up a group for all faculties within a given college, including an adjunct faculty that frequently changes.

c An airline wishes to set up a group for each flight (like a non-stop flight from Chicago to Atlanta on Tuesday afternoon) and have a constantly changing crew automatically allocated or removed when required.

The four main issues [4] within a dynamic community include user authentication, robustness, load balancing, and cost efficiency [5]. The User Authentication method is an essential aspect of every complex community. Group managers review each new user's identity [6], and verify group data access policies. To do this, it takes an authentication method to limit unauthorized access to the community. We are trying to develop a competent dynamic community system with provision for safe data sharing and successful user revocation [7] to resolve the

aforementioned problems. Following are few of the quintessential prerequisites for a safe and sound information exchange using cloud services:

a The proprietor of the data would be able to identify a user category that can access their data.
b Group member shall remain capable of accessing the information from anywhere, at any time, other than the intervention of the information proprietor.
c Regardless of where the information is kept, the information owner exerts some control on his / her own information.
d Access to information should be restricted to the proprietor of the information and community members.
e The proprietor of the data must be willing to join the new member's party.
f Moreover, the data proprietor must be able to remove any group member's right of access to shared information.
g No community members will be permitted to waive rights or link new participants in the party.

Contribution to the work

The study discussed securities [13][14][15] and privacy issues compared to un-trusted CSPs [16][17] in most of the review articles. Security concerns and challenges of cloud computing environments [5][18][19][20][21][22][23][24]. The main purpose of presented work is addressing relevance of community data sharing in cloud environment (in dynamic groups). Then, a comparative study was carried out of different encryption techniques, especially in cloud environments for security and privacy issues. Finally, assess the comparison of performance, feature and calculation complexity between existing systems relating to group data sharing.

2. Cloud Computing Summary

Cloud computing serves as an online network-based machine, which communicates shared computations of data and assets on request to computers and various gadgets. It's an uncommon way to provide access to common computing resources (for example servers, storage, operating system, software and management) on demand that can be managed and accessed immediately with reduced control. Cloud storage and capacity agreements offer consumers of IT organizations the ability for storing and processing their information of third-party data centres anywhere in the planet. It relies upon asset sharing for achieving stability and economic scale. This is also the product of developing and obtaining current technologies and exemplar models. Its goal is providing consumers with an ability of taking advantage of major advances in cloud computing deprived of actual requirement for profound and extensive cloud knowledge [25].

a. Main features of cloud technology

Within presented segment we deliberate, the crucial features inside cloud frameworks deployed by CSPs. These features comprise comprehensive assortment of facilities which can be availed across internet. Virtualization plays a key part in cloud deployment. Multi-tenant ecosystems have several users or customers and they might not take in or share each other's data. Cloud storage is conserved, administered, and backed up at remote locations; and is made accessible on network where clients can retrieve data. Hypervisor is a significant component for virtualization, and allows execution of many Virtual Machines (VMs) upon a solitary hardware host. Hypervisor administers and manages the diverse operating systems which execute on a shared physical system.

b. Service Cloud Forms

Established upon the requirements of consumers, the cloud system is classified in four types which are:

- Public Cloud –any subscribed user is capable of accessing a public cloud by using a net connection.
- Private Cloud –The rights to access are limited to aspecific clique or establishment.
- Community Cloud - Two or more establishment having the same distinctive cloud requirements share a community cloud.
- Hybrid Cloud - Hybrid cloud refers to a mixed computing, storage, and services environment made up of on-premises infrastructure, private cloud services, and a public cloud with orchestration among the various platforms.

c. Dynamic Group Data Sharing

A group can be described as assortment or set of data users (owners) allocated with a collection of authorizations. They are primarily engrossed on user's individualities. Data sharing in the group has attained more significance in several realms such as governments, corporations, and establishments in the real world [26]. The group leader opens up a sharing area in the cloud to form a group application. Then, he/she grants the group

members the right to implement data management. All the data in this group are available to all the group members, while they remain private towards the outsiders of the group including the cloud provider. The group leader can authorize some specific group members to help with the management of the group, and this privilege can also be revoked by the group leader. When a member leaves the group, he/she will lose the ability to download and read the shared data again.

d. Issues in Data Sharing

The main issues during cloud data sharing are:

i. Confidentiality [26]: The IPO keeps its details or documents in the cloud. Should Cloud-based servers be supervised using cloud-based expert establishments, who are not completely trusted, and might result in unauthorized clients gaining access?
ii. Efficient and Scalable: a cloud has a considerable huge number of clients where the group administrator can include or remove them from concerned group; it is important that group remains flexible and scalable.
iii. User Revocation: In case a customer is expelled within a specified time period, it is important that access to data is restricted exclusive of impacting former group members.
iv. Collusion: After analysing the techniques of information exchange in the cloud, given the fact that when components are conspired, no client would be able to access information exclusive of data owners' consent.

3. Literature Review

In this segment an outline of current reviews on secure cloud data sharing is presented. The analysis surveys and articles discussed, do not concentrate directly upon the sharing of sequence-based group data in the cloud, but on the key requirements. The analysis of safe cloud data sharing is comparatively new and progressively relevant beside growth and emergent recognition of Cloud Computing along with the rising necessity of exchanging information. The analysis papers are classified as follows: group key supervision, cumulative key searchable encryption, and group signature and proxy re-encryption.

a. Group Key Specific Analysis

Group Key Supervision (GKS) Process, focuses mainly on key generation and distribution amongst community members. The safe distribution, formation, and revocation of keys will involve all group members [27]. The Group Controller (GC) accountable for the key creation, dispersal and rekeying of affiliation modification and Key Server (KS), which is accountable for preserving keys and dispensing keys[28] are the entities managing the communications session in group key management. The Group Key Management (GKS) as described in Menezes et al.[29] Is the collection of techniques and procedures used for the development and management of key groups between the group members?

The main group management, according to Menezes et al.[30], can be divided in three consortiums. They are GKS central protocols, GKS decentralization and GKS delivery [28]. Researchers [31][32][33] suggested a GKS approach from the literature review in cloud systems in favour of dynamic group data sharing. Discussed method estimation greatly decreases memory for the use of rekeying messages. It also eliminates overheads of communication and stowage of rekeying schemes with the necessary device overhead. Nonetheless, this research must be enhanced in order to ensure that consumers can interpret the content dynamically. Through monitoring the client and archiving the subtle elements, a log record can be maintained. Data archives are retrieved from the cloud by downloading the solicitation with the client. In addition, studies will concentrate on restricting convictions on the cryptographic server (CS) and resolving within risks.

b. Main Cumulative Searchable Encryption Technique Studies

One conventional modus operandi is using a searchable encryption (SE) system, whereby the information generator is obliged for encoding and uploading potentials of keywords in cloud storage collectively beside encoded data to send the username trapdoor to the cloud in support of the rationale of recovering information which equivalents a keyword. While merging a searchable encryption system next to cryptographic cloud storage makes it capable of handling elementary sanctuary needs of cloud storage, it can still be hindered by employing a large-scale application framework concerning billions of users and trillions of files by real-world problems such as competent encryption key supervision, that are overlooked in earlier studies[34].

Liu[34], Kumar et al. [35] suggested a group sharing strategy using the SE Key Aggregate Scheme. This system is capable of safely storing or sending data by utilizing an exceptionally restricted data storage smart card. They have a detailed safety evaluation of developed device established upon a standard scheme. Under discussed method, the data creator demands that all users be provided with a unique key, focusing upon authentication and search rights around their document sets. The outcomes of the assessment and analysis showed that this method was a successful solution in the public cloud, for creating a realistic data sharing strategy. However, this research will focus more on raising the number of trapdoors in multi-owner settings.

c. Attribute-Based Encryption Analysis

ABE is an effective procedure expended for providing fine grain admittance management in cloud servers for data storage. The Access Control List (ACL) primarily provides links to cloud data. Nevertheless, this was not scalable and offered merely rough-grained admittance [36]. In Goyal et al. [37] ABE offers an additional robust and fine-grained admittance management to data as compared to ACL. ABE is an admittance management procedure in which a data component or user has correlated characteristics. The Admittance Management Policies (AMPs) are demarcated and user must be capable of accessing the database if the characteristics comply with the AMPs [26].Yu et al.[38]aims to obtain secret, fine seeds and scalability data. They supported a KPABE and combined that with PRE and lazy re-encryption for this purpose. In addition, the core security obligations and protection of user access rights have been achieved. Finally, they have shown that the solution suggested by formal safety analysis is more reliable with the traditional cryptographic solution.

Researchers [39][40][41][42][43]proposed the Secure Data Sharing attribute-based encryption process. Encoding and decryption are however inefficient due to the costly pairing operations [42]. If data is encrypted using an ABE program, if a number of users from various backgrounds are involved, key management is difficult. Sun [44]argued that a current key agreement algorithm is necessary for large secure communications through which all customers may contact other customers to make a complete graph. One of these, identical to other nodes which are unprotected, is not protected. Therefore, improvements to key administration algorithms by means of tree structures as well as a trustworthy key centre generation are required in future.

However, the CP-ABE procedure does not aid stringent trust models and is also nonflexible, with very raised costs for keeping keys and is not impermeable to conspiracy attacks, with additional shortcomings[45][46] suffered. In[47] the cancelation technology offers standardized grains for all customer data-sharing systems which necessitate different security requirements, explicitly in absolute removal mode; however, it supports incorporating a single customer repudiation list as a cipher text, thereby making it entirely a fine-grained rejection. Thanks to key screw, Inefficient retroactive security problems as well as problems not relevant to the distributed storage system.

d. Proxy Re-Encryption Analysis

Originally launched by Strauss et al.[48], a proxy re encryption (PRE) permits a semi confidence proxy to convert the code encoded using delegator's public key into another code under the delegate's public key without disclosing the original encrypted messages or the delegated delegator's private key. A particular form of public key encryption gives the impression of an optional candidate for maintaining data sharing security in cloud computing. For example, if the Alice (data owner) wishes of sharing confidential information stored in cloud servers with a given user (for example, Bob). No one apart from Bob will retrieve the stipulated information. This is desirable. Alice is inspired by basic PRE, and afore uploading shared data to the semi-trusted cloud, can encrypt sensible data from its own public key.

As soon as Alice receives the data sharing request from Bob, he uses his private key and public key of Bob to create a proxy reset encryption key and transmits the proxy re-encryption key to the semi trusted cloud server. Consequently, cloud server modifies the encrypted cipher text underneath Alice's secret key into a secret Bob key encryption by utilizing the proxy re-encryption key. When using the PRE primitive, Bob can only decode the transformed text, while the Cloud server cannot know Alice or Bob's plaintext or private keys. Finally, with his own private key, Bob can download and decode necessitated data. It causes the expensive overhead of secure data sharing to be discharged to a semi-confident cloud server possessing plenty of resources .

Investigators [41][49][50]suggested a re-encryption proxy system for the secure sharing of data. They also accomplished a robust exchange of knowledge in the cloud. It provided an easy solution to app revocation problems on the basis of fine-grained approach encryption. The results show that this scheme is successful for cipher text attacks with better collision resistance in the benchmark prototype. Nevertheless, the main challenge with discussed strategy is to take longer to complete the task and to connect the functionality with a client. While they provide a potential change, the consumer has problems as more UAKs demand that different efficient attributes be allowed without modifying UAK numbers, depending on time periods. Improving the level of security is an additional requirement that requires more focus. Qin et al.[51] recommended that the data sharing in the cloud by means of the PRE procedures must be reliable, efficient and secure. A Dharani and Narmatha study[52]only evaluated less data in this sense. The previous study must therefore concentrate more on large data sizes in order to obtain quick encryption and decryption, thus increasing speed and security of the large data set. It rising costs, maintaining processes and low complexity to deal with cloud protection issues.

4. Our Contribution

The utmost critical problem in the Untrusted Public Cloud Environment is the exchange of data in diverse networks, while at the same time preserving data and privacy, due to a regular change in community composition. When discussed above, none of the approaches proposed provide a complete solution to the diverse group management needs and challenges, in particular User Revocation & Key Management. Due to frequent membership changes, sharing data while preserving privacy remains an exigent hindrance, particularly for an insecure cloud because of the collusion attack. However, the safety of key delivery for existing systems is dependent on the protected communications channel, but it is a clear and realistic assumption to provide such a channel. This work aims (as shown in figure 2) to examine the model effectively in terms of:

a) When sharing data, overhead program administrators will be low.
b) Cloud storage system data sharing should be safe.
c) If community membership changes the number of re-encryption keys will be minimal.

For diverse participants, we put forward stable, safe and resilient scheme for data sharing. First, we deliver safe way of transmitting key without reliable means of communication, and Key and Authentication Manager (KAM) allow users to securely access their private keys. Second, our program can achieve a sophisticated access filter, all group members can exercise the cloud sources and revoked members will be unable to re-access the cloud. Also, we should defend the system against manipulation, which ensures that revoked members will be unable to retrieve the previous data file even though they collude with the cloud that is un-

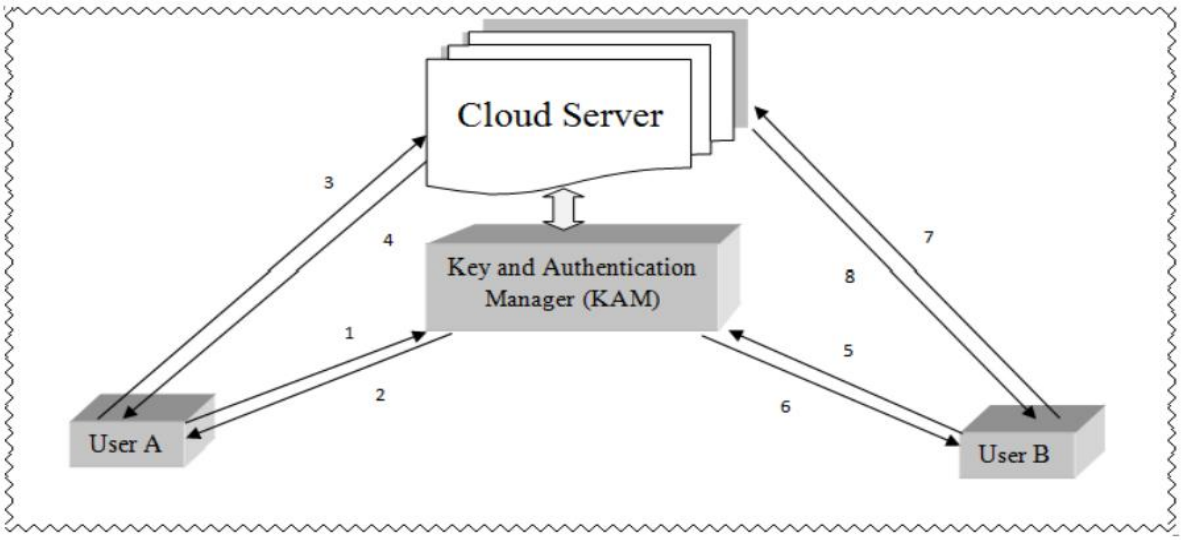

Figure 1 System Model-KAM

trusted. With our method, we are able to achieve a stable, safe and resilient user revocation mechanism by using the Registered User Table (RUT).The following services is provided by the KAM:

i. User Authentication: KAM uses the Public Key Register User Tables (RUT).
ii. User Key Generation: KAM uses randomized feature to create and add them to the user's keyboard user table for further use.
iii. Ticket Generation: To generate these, KAM uses Serialized function.
iv. Encryption Services: KAM eliminates device overhead by delivering messages / file encryption services.

In the table 1, several parameters involved with the proposed scheme are compared with the pre-existing schemes discussed in literature review. It is evident from the theoretical analysis of the proposed scheme that it less risky as compared to pre-existing schemes. The number of encryption keys that needs to be changed in case the membership changes is zero, i.e., if any user leaves the group or he is revoked, it does not affect the encryption and decryption keys of other legitimate users, thereby mitigating the additional overhead incurred in other schemes. The suggested framework tackle concerns such as safe key distribution, fine grain admission management, member revocation and collusion attacks for cloud computing complex classes. We provide a convenient way to share key information without open networks and users can easily access their private keys through the key authentication manager (KAM). Registered users are capable of securely obtaining their public and private keys from KAM that manages and enables the requests after confirmation. Also, users can access the dynamic cloud community when users are enabled and collect their keys. The scheme has sophisticated admittance management, any member in the community may use the cloud source and revoked members would be

unable to access the group again. The KAM performs the following tasks with our proposed program when a new user enters the group or a user has left the group:

- The Registered Consumer Table (RUT) is revised.
- Produce safe and secure keys
- Update cloud storage privileges.

Table 1 Analysis of Various Algorithms

Name of the Algorithm	Risk Factor	In Case of User Revocation		Support For Confidentiality Over Authentication	Analysis of Algorithm
		No of Keys Affected	Overhead on Admin		
Atomic Proxy Re-Encryption	High Risk	Difficult	High	No	High overhead
Proxy Re Encryption (PRE)	High Risk	Difficult	High	No	Revoked user can also access the server
Conditional Proxy Re Encryption (CPRE)	Medium Risk	Difficult	High	No	Encoding keys are created for all members; every time membership of group changes.
Efficient CPRE (E-CPRE)	Medium Risk	Difficult	High	No	Incompetent for securing big data group sharing in cloud environment.
Outsourcing CPRE (O-CPRE)	Medium Risk	Difficult	High	No	The outsourcing server can be a traffic (user request/response) bottleneck.
CP-ABE	High Risk	Difficult	High	No	Hard to support Dynamic group management
KP-ABE	High Risk	Difficult	High	No	Hard to support Dynamic group management
KAM (Proposed Approach)	**LESS RISKY**	**EASY**	**VERY LOW**	**YES**	**A single bit value is changed to achieve efficient handling of user revocation**

KAM maintains the Registered User Table (RUT), used for tracking valid and revoked users. KAM also makes it difficult for revoked users to access the file if they conspire with the server, thus reducing the possibility of conspiracy attacks. The proposed model will offer high performance, which ensures that current members do not need to renovate their private keys in case a new member enters the group or a member is revoked.

a. User Registration Process: User registration is an integral feature of any group. In case any new member wishes to enrol with the group, the group managers must verify their integrity and validate them for group data access. All registered users are maintained by using a Registered User Table (RUT) as shown in Table 2.

Table 2 Registered User Table

S.NO	Type of Cloud	UserID	Public Key	Private Key	Validity of User (0=Revoked User /1=Authorized User)
1	Private Cloud	Unique Email Address	Issued By KAM	Issued By KAM	0/1
2	Public Cloud	Unique Email Address	Issued By CA	Issued By CA	0/1
3	Hybrid Cloud	Unique Email Address	Issued By KAM/CA	Issued By KAM/CA	0/1

b. Keys Generation (public, user keys, and session keys) process: KAM is accountable for the key generation, user registration and user revocation of system parameters. Each registered user receives at registration a set of asymmetric keys using RSA PKCS. Whenever a Member wants to upload data, a serialized function is used to generate a unique session key that corresponds to its request. At the same time, KAM creates a related ticket that is concurrently exchanged between the cloud server and the user. When any user wishes that the data on the cloud server uploaded by some other community member is accessed, KAM provides him with the server pass, the session key and the data generator public key for uploading, encoding and use of the data from the cloud server.

c. Process to Upload Data: At registration, each registered user receives a set of asymmetric keys using RSA PKCS. The public key and private key are added to the corresponding RUT when he enters some new party. If any member wishes to upload data, he / she send a request for data upload (DUR) to the KAM. The KAM uses a serialized method to generate a specific session key corresponding to this order. At the same time, KAM also creates a related ticket (using a random function) that is concurrently shared by the user and the cloud server. The user then encrypts the data by session key and dispatches it together with the ticket to the Cloud Server. The Cloud server compares the member's ticket and the ticket obtained from KAM and recognizes and stores it if they match. The use of tickets allows the network to reduce risks resulting from repetitive attacks. By utilizing the session key for encoding the data, the device keeps the data secure from an abusive cloud server and any malicious user. Both these DUR documents are contained in separate log files by KAM.

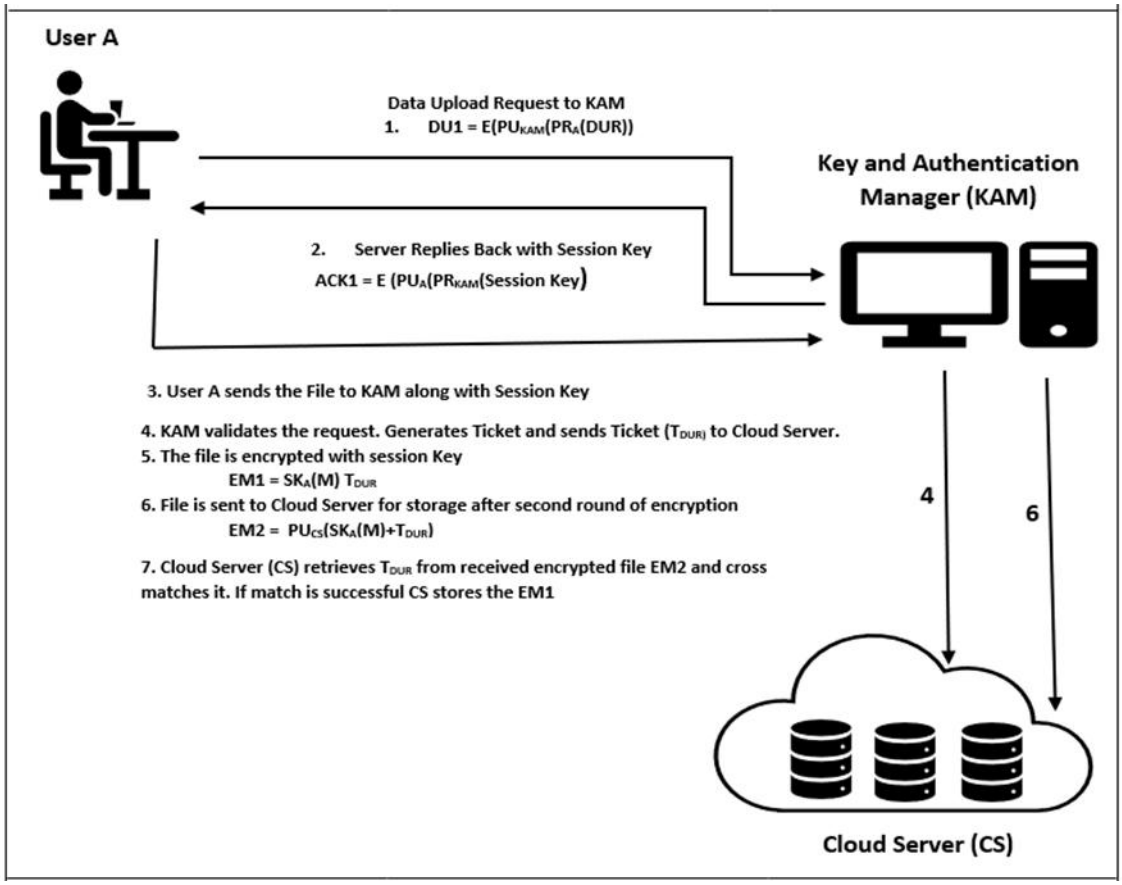

Figure 2 Data Uploading to Cloud Server

d. Data Download Process: Whenever a user wishes to retrieve data from the cloud repository which any other group member has uploaded, he sends a Data Download Request (DDR) to KAM as shown in figure 4. The KAM includes the application ticket, data session key, and the data generator's public key so that the data can be accessed, decrypted and used from the cloud server.

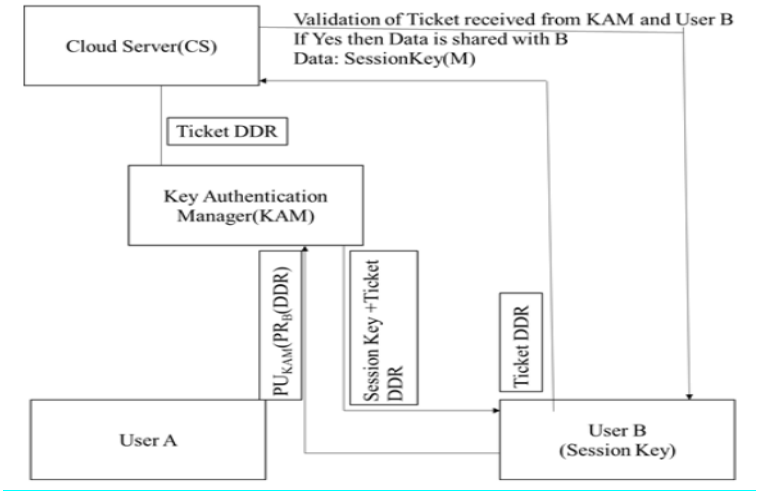

Figure 3 Data Sharing Request Flow between Users

e. User Revocation Process: As shown in Table 1, the event that any group member decides to leave the group, its validity bit will be changed from '1' to '0' in order to revoke its user rights. This streamlined method helps to handle a diverse cloud community effectively. For example, the User 2 in following table has been revoked by changing hi validity bit to '0'.

5. System Configuration and Data Analysis

For evaluating the feasibility of the projected scheme several preliminary experimentations were organized on Windows platform with Intel i3 CPU, 4GB RAM with 2.53 GHz processor to measure overhead in terms of time. In the anticipated arrangement, the complication of encoding the information independent on the file size and the inherent encryption algorithm (3DES& RSA). The over-all number of features in the cipher text is directly related to computational time for encryption. The Data Set is of User 4, User 5, User 6; each user is using 56 Bit of Symmetric Key for Encryption and Asymmetric key of size 256 Bit, 512 Bit & 1024 Bit respectively. Various data file of various format like Doc, PPT, Video, JPEF image Format, CSV, ZIP of sizes varying from 1 to 40000 KB is encrypted using a Symmetric Encryption algorithm namely Triple DES. To maintain Confidentially over Authentication, we are further encrypting the above Symmetric Encrypted Data File with the combination of Asymmetric key of user with servers and/or server and server. We have gathered various Data File(Data Set) of various Type i.e., PPT, Doc, CSV, ZIP, Image and Size ranging from 1KB to 40000KB.For each Data set we are calculating Time(in sec) based on given set of Users. In our model we are calculating time at three stages as stated below:

1. DES Time which is Symmetric Encryption of our data file

DES (Time in Sec) = Total Time Requires to complete the given process [EncryptedSess_Key_56 (Data File of any size)]

Let M= [EncryptedSess_Key_56 (Data File of any size)]

2. RSA time which includes:

a Token bit is appended with the DES encrypted message

Q= M+Token Bit 56 Bit

b Asymmetric encryption time for the above message generated at above step

R=Encryption [PURequest generated for (PRGenerating the request (Q))]

c Copy of 56-bit token generated by KAM will be sent to cloud server for verification.

S=Encryption [PUCS (PRKAM (Token Bit 56 Bit))

3. Upload time include the following:

a Asymmetric Decryption of message R
b Token S received from KAM and above decrypted message is compared and verified.

c If token [Decrypted from message R, S] is verified then the Message M is uploaded to cloud server.

In Figure 4, various file formats are taken in account which is showing that time taken by User 4, User 5, And User 6 is nearly equal. So, the choice of combination i.e., 56 Bit Symmetric Key with 256 Bit Asymmetric Key, 56 Bit Symmetric Key with 512 Bit Asymmetric Key, 56 Bit Symmetric Key with 1024 Bit Asymmetric Key, totally depend on the how important is that data for the organization. If the organization wants to save the data through highly secure channel of communication than he must use 56 Bit Symmetric Key with 1024 Asymmetric key because average time in encrypting a file using 56 Bit Symmetric Key along with 256 Bit/512 bit/1024-bit Asymmetric key is almost equal. Thus, we can say that depending upon the Data of an organization we can select the key size of 56

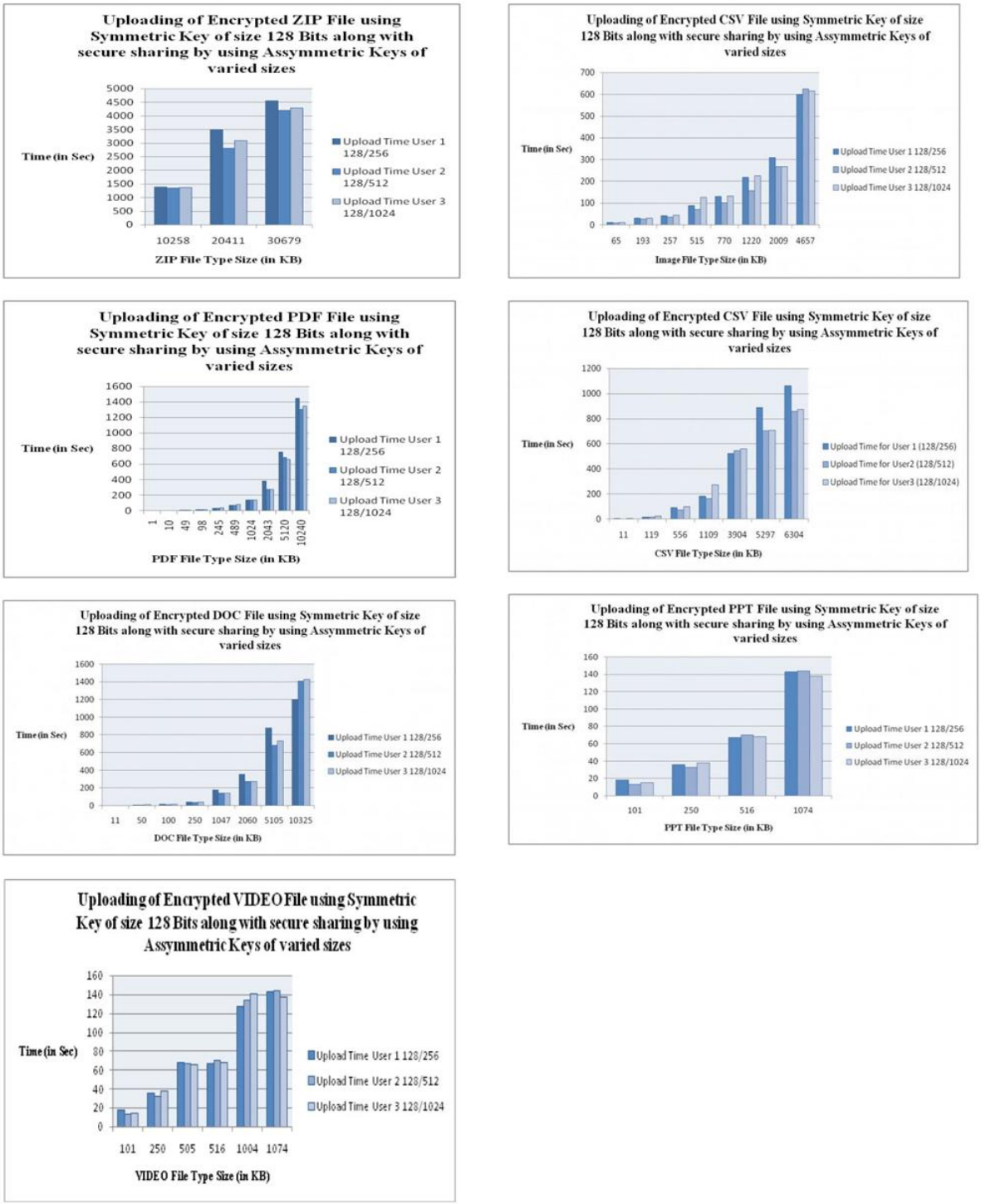

Figure 4 Time Taken to Upload a Particular File Format to Cloud Server using 128 Bit Symmetric Key and 256/512/1024 Bit Asymmetric Key

6. Conclusion

Cloud computing has pushed forward advances in security technology and extensive growth in the usage of internet services. Stable data sharing is an imperative apprehension in cloud-based communities. Data security, traceability, access control and account revocation are primary areas of concern. The use of this cloud infrastructure to reduce costs and boost service efficiency to end users is very useful to e-commerce applications and social networking sites. There are however numerous factors that affect the net profit like (geographical) dispersal of members locations, the accessible internet structure in these geographical zones, the changing existence of use trends and the adaption or changing reconfiguration of cloud services, etc.

We developed a new model framework to boost user revocation in a dynamic group. The new framework proposition with the moderated overhead in the different phases would be sufficient for safe and sound data sharing in the cloud environment. The model proposed fulfils all criteria to withdraw a user efficiently from a dynamic community without disrupting the other users. It decreases customer overhead in some cases until community membership is changed. Core contributions to this arrangement:

- A safe way to transmit key without reliable communication networks.
- Fine grained access control, by means of the user list community, can be accomplished.
- Any community user can use the cloud source
- Revoked users cannot return to the cloud after they have been revoked.
- They can effectively support Dynamic User Management when a new user joins the community or when a user is removed from the user

The proposed cryptographic scheme in this study operates effectively and safely. Through adhering to the authentication security principle, all messages are protected and secure from eavesdroppers and other unauthorized users. The program manages user revocation issues effectively, without overloading Cloud Server, KAM or System Admin. In addition, implementing KAM allows the framework that is proposed to reduce the cloud server overhead by delegating authentication to KAM. It facilitates efficient user revoking and monitoring of fine grains by retaining the individual User Table log. When using private keys, public keys and session keys, users can preserve privacy, transparency and traceability of information. For fact, we would like to expand our existing program to include a number of environments. More work following the introduction of this model will aim to fully improve the cloud scenario. There are two inconveniences of this program evaluated on the basis of the theoretical analysis:

- Higher cost for clients: If a user requests upload or download data from / to the server, it has to be encrypted and decrypted by multiple users. This can hamper customer / client system productivity and results.
- Partial resistance to conspiracy: If any User A conspires to KAM, all uploaded data can be accessed. User B can first encrypt data to be transmitted to the server with a public key and then with the session key for addressing this. It offers growing protection to collaboration but limits data sharing.

7. Future Direction

Protecting data on un-trustful cloud servers poses a challenge and efficient encrypted mechanisms are important. Some of the recommendations for the future are to combine other security methods with cryptography. Future research would also be to find more effective ways to address data protection and Cloud privacy issues.A real-world framework would be useful if the existing data access control schemes could be incorporated into this study. New cryptographic designs are expected to achieve conciliation between security and usability to reduce computational complexity.Another potential approach will be to improve data operating versatility by combining the scheme proposed with other cryptographic primitives, such as homomorphism encryption, to allow computations without decrypting encrypted data.

References

1. W. Q. S. X. W. X. Xia Z, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transaction Parallel Distributed System, Vols. 27:340–352,2016.
2. R. K. S. J. Fu Z, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement," IEEE Transaction Parallel Distributed System volume , Vols. 27:2546–2559,2016.
3. S. X. L. Q. Fu Z, "Achieving Efficient Cloud Search Services: Multi-Keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Transaction Communication, E98, Vols. B:190–200,2015.
4. S. J. W. J. Ren Y, "Mutual verifiable provable data auditing in public cloud storage," JIT, Vols. 16:317–323,2015.
5. L. D. Zissis D, "Addressing cloud computing security issues," FGCS, Vols. 28:583–592,2012.

6. K. Y.-H. R. M. Chang V, "Cloud computing adoption framework: A security framework for business clouds," FGCS, Vols. 57:24–41,2016.
7. H. T. A. Y. K. Mohd B J, "Hardware design and modelling of lightweight block ciphers for secure communications," FGCS, 2017.
8. B. M. A. S. Rahman F, "A privacy preserving framework for RFID based healthcare systems," FGCS, Vols. 72:339–352,2017.
9. W. J. L. B. L. S. Guo P, "A Variable Threshold-value Authentication Architecture for Wireless Mesh Networks," J Internet Technol , vol. 15, p. 929–936, 2014.
10. T. H. W. Shen J, "A novel routing protocol providing good transmission reliability in underwater sensor net-works," J Internet Technol , vol. 16, p. 171–178, 2015.
11. W. Y. Xie S, "Construction of Tree Network with Limited Delivery Latency in Homogeneous Wireless Sensor Networks," Wirel Pers Commun , vol. 78, p. 231–246, 2014.
12. C. S. T. W. Chu CK, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," IEEE Trans Parallel Distrib Syst, vol. 25, p. 468–477, 2014.
13. Z. S. H. R. Pearce M, "Virtualization," ACM Comput Surv , vol. 45, p. 1–39, 2013.
14. S. J. L. R. Perez-Botero D, "Characterizing hypervisor vulnerabilities in cloud computing servers," in Proceedings of the 2013 international workshop on Security in cloud computing - Cloud Computing '13, Hangzhou, China, 2013.
15. Z. Y. B. M. Aguiar E, "an Overview of Issues and Recent Developments in Cloud Computing and Storage Security," High Performance Cloud Auditing and Applications, p. 3–33, 2014.
16. K. V. Subashini S, "A survey on security issues in ser-vice delivery models of cloud computing," J Netw Comput Appl , vol. 34, p. 1–11, 2011.
17. K. S. Abbas A, "A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds," IEEE J Biomed Heal Informatics, vol. 18, p. 1431–1441, 2014.
18. K. S. V. A. V. Ali M, "Security in cloud computing: Opportunities and challenges," Inf Sci (Ny), vol. 305, p. 357–383, 2015.
19. S. L. G. J. V. Fernandes DAB, "Security issues in cloud environments: a survey," Int J Inf Secur, vol. 13, p. 113–170, 2014.
20. R. D. F.-M. E. F. E. Hashizume K, "an analysis of security issues for cloud computing," J Internet Serv Appl , vol. 4, p. 5, 2013.
21. P. D. B. B. Modi C, "survey of intrusion detection techniques in Cloud," J Netw Comput Appl, vol. 36, p. 42–57, 2013.
22. X. Y. Xiao Z, "Security and Privacy in Cloud Computing," IEEE Commun Surv Tutorials , vol. 15, p. 843–85, 2013.
23. C. K. Singh A, "Cloud security issues and challenges: A survey," J Netw Comput Appl 79:88–115, vol. 79, p. 88–115, 2017.
24. S. Y. R. J. Liu Y, "A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions," J Comput Sci Eng. , vol. 9, p. 119–133, 2015.
25. K. G. Sinddhuri P, "The Data Storage and Assured Sharing Methodology among Differing Groups in Cloud Compu-ting," Int J Sci Eng. Adv , vol. 5, p. 313–318, 2017.
26. K. N. B. C. Poornima E, "secure data sharing for multiple dynamic groups in Cloud," in Conference on Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG), 2015.
27. A.-F. J. Z. S. Manz D, "Network Simulation of Group Key Management Protocols," J Inf Assur Secur , vol. 1, p. 67–79, 2008.
28. B. D. D. Ranjani RS, "Current Trends in Group Key Management," Int J Adv Comput Sci Appl, vol. 2, p. 82–86., 2011.
29. O. P. v. V. S. Menezes AJ, "Handbook of Applied Cryptography Discrete Mathematics and Its Applications, illustrate," CRC Press, 1996.
30. H. D. Rafaeli S, "survey of key management for se-cure group communication," J ACM Comput Surv, vol. 35, p. 309–329, 2003.
31. K. P. Reddy RD, "An Efficient Data Sharing Technique in the Cloud," An EDST. Int J Recent Innov Trends Comput Commun 2, 2014.
32. S. D. Bhaurao C, "Privacy Preservation and Secure Data Sharing in Cloud Storage," Int Res J Sci Eng. , vol. 3, p. 231–236., 2015.
33. J. R. Zhu Z, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud. IEEE Trans Parallel Distrib Syst 27:40–50," IEEE Trans Parallel Distrib Syst , vol. 27, p. 40–50, 2016.
34. L. Z. W. L. Cui B, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage," IEEE Trans Comput , vol. 65, p. 2374–2385, 2016.
35. K. R. K. S. Manohar K, "Key Aggregate Search-able Encryption for Group Data Sharing Via Cloud Data Storage," Int J Comput Eng. Res Trends, vol. 2, p. 1132–1136, 2015.

36. Z. G. C. X. Li J, "Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010.
37. P. O. S. A. W. B. Goyal V, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06 Proceedings of the 13th ACM conference on Computer and communications security, New York, 2006.
38. W. C. R. K. L. W. Yu S, "achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings - IEEE INFOCOM, 2010.
39. Z. H. L. H. Yang Y, "Cloud based data sharing with fine-grained proxy re-encryption," Pervasive Mob Comput , vol. 28, p. 122–134, 2016.
40. H. X. L. J. Liu J, "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption," Future Gener Comput Syst, vol. 52, p. 67–76, 2014.
41. L. Q. D. Z. Han K, "Security and efficiency data sharing scheme for cloud storage," Chaos, Solitons & Fractals, vol. 86, p. 107–116, 2016.
42. W. Q. Q. B. Deng H, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," Inf Sci (Ny) , vol. 275, p. 370–384, 2014.
43. C. Z. T. Y. Yao X, "A lightweight attribute-based encryption scheme for the Internet of Things," Future Gener Comput Syst , vol. 49, p. 104–112, 2014.
44. S. L, "Role Based Secure Group Communication and Data Sharing System," Simon Fraser University, 2009.
45. N. D. Hur J, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans PARALLEL Distrib Syst , vol. 22, p. 1214–1221, 2011.
46. W. G. W. J. Liu Q, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inf Sci (Ny) , vol. 258, p. 355–370, 2014.
47. F. D. Z. L. Wang P, "towards attribute revocation in key-policy attribute-based encryption," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), p. 272–291, 2011.
48. B. M. B. G. Strauss M, Divertible protocols and atomic proxy cryptography, p. 127–144, 1998.
49. L. J. Lu Y, "efficient certificate-based proxy re-encryption scheme for data sharing in public clouds," KSII Trans Internet Inf Syst , vol. 9, p. 2703–2718, 2015.
50. R. K. W. J. Wang C, "Secure and practical outsourcing of linear programming in cloud computing," in 2011 Proceedings IEEE INFOCOM, 2011.
51. W. S. X. H. Qin Z, "Strongly Secure and Cost-Effective Certificateless Proxy Re-encryption Scheme for Data Sharing in Cloud Computing," in Strongly Secure and Cost-Effective Certificateless Proxy Re-encryption Scheme for Data Sharing in Cloud Computing, 2015.
52. N. M. Dharani R, "Secured Data Sharing with Trace-ability In Cloud Environment," Int J Invent Comput Sci Eng. , vol. 1, p. 1–9, 2014.
53. S. P, "Secured Group Data Sharing Over Cloud by Using Key Aggregate and Searchable Techniques," Int J Sci Res , vol. 5, p. 499–502, 2016.