International Journal of Engineering & Technology, 7 (2) (2018) 646-656

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i2.9770
Research paper

Review on dynamic group data sharing in cloud environment

Sathish Easwaramoorthy [1], Chunduru Anilkumar [2] *, Usha Moorthy [3], Sravankumar B [4]

[1] *Independent Researcher*
[2] *SCOPE, Vellore Institute of Technology, Vellore, India*
[3] *School of Computer science, Galgotias University, Noida*
[4] *Assistant Professor, QIS Institute of Technology, Ongole, India*
**Corresponding author E-mail: chunduru.anilkumar@vit.ac.in*

Abstract

Information sharing or exchange of data within entities plays a significant role in cloud storage. In cloud computing, a robust and practical methodology is developed which can be utilized by cloud users for sharing information among multiple group members in the cloud with lowered maintenance and management costs. Furthermore, a service provider in the cloud does not share data with anyone other than the Trusted Third Party (TTP) sources due to the semi-trusted characteristics of the cloud. In this way, there is no global security mechanism for dynamic group data sharing over the cloud. Subsequently, the Cloud Service Providers (CSPs) can convey different services to cloud users through powerful data centres. Hence, data is secured through the validation of users in the cloud. Meanwhile, CSPs should offer outsourced security assurance for data file sharing. Assuring privacy in data sharing is still a critical issue due to continuous change in cloud users, particularly, for unauthenticated or third party users because of the risk of collusion attacks. However, security concerns turn into a major restraint as outsourcing storage data is perhaps a delicate concern for cloud providers. Additionally, sharing information in a multi-proprietary approach while protecting information and individual security to the data from unauthorized or third party users is still a challenging task as there is a frequent change in cloud members. In this regard, previous studies are reviewed and discussed which are related to dynamic group data sharing using cloud computing.

Keywords: *Cloud Computing; Group Data Sharing; Security; Privacy; Data Storage; Encryption and Decryption.*

1. Introduction

In the present scenario, the rapid growth of network platforms and infrastructure which includes the cloud computing [1–6], wireless communications [7], [8] and wireless sensor networks [9–11], have high-quality applications, on-demand data access and services. Specifically, the cloud storage systems have been used comprehensively as both individuals and organizations. Here, the user able to access a vast set of applications with quality services which are shared amongst customers as remotely. In contrast, personal computers have limited storage, but the cloud has infinite storage space. So, the outsourcing of sensitive information, for instance, personal photos, videos, health histories and so on are explosively increased. However, the private/personal data leakage amongst group member is the significant issue in social network applications. For this purpose, the data on the cloud server must be encrypted through their possessors. Still, it causes the issues like encrypted data sharing [12], conducting secure searches of encrypted data [1–3] and provable data auditing for outsourced data [4]. Therefore, the study aimed to review and discuss both the data security and privacy issues which are faced by the clients in cloud storage environments. Moreover, it provides a comparison of encryption approach, performance factor analysis, feature and computation complexity comparison amongst existing schemes which are related to group data sharing in a dynamic manner. From this, the study explored the techniques that trend towards addressing the protection of outsourced data in cloud frameworks.

2. Contribution of the study

From the analysis, most of the review article has discussed security [13–15] and privacy concerns against untrusted cloud service providers [16], [17]. Security issues and challenges of cloud computing environments [5], [18–24]. The primary objective of this paper is to discuss the significance of group data sharing (both static and dynamic manner) in cloud frameworks. Then, provided a comparative analysis of different encryption techniques, especially for security and privacy concerns in cloud environments. Finally, evaluate the performance factor, feature and computation complexity comparison amongst existing schemes which are related to the group data sharing.
The rest of the paper is organized as follows: section 2 discussed the overview of cloud computing, types, significance, and issues in data sharing. Section 3 examines the previous literature related to the examination of the aforementioned issues in group data sharing. A brief discussion of methods, inclusion, and exclusion criteria of the study is discussed in section 4. In section 4, preliminaries with various methods with evaluation of performance are discussed. Conclusions with the recommendation of the survey are presented in Section 6.

3. An overview of cloud computing

Cloud computing is more of an online system based computing that transmits shared computation of assets and data to computers

and different gadgets on request. It is an unusual path for empowering an all-inclusive, on-demand access to shared computing resources (like servers, stockpiling, computer system, applications, and administration), which can be immediately arranged and discharged with the decreased administration. Cloud computing and capacity arrangements give users among IT firms the potential to store and process their data in third-compel data focuses that might be found anywhere around the world. Cloud computing depends on sharing of assets to get consistency and scale in the economy. Moreover, it is the consequence of the improvement and procurement of existing innovations and ideal models. The objective of cloud computing is to give users a chance to benefit from the majority of the advancements in cloud computing, without the real need of in-depth information and knowledge on the cloud [25].

3.1. Primary components of cloud computing

In this section, deployed the essential components in cloud frameworks. These components consist broad range of services that we can use all over the internet. Here we discuss some important elements [26]:

- Virtualization: It plays a major role in deploying the cloud. It is the strategic component in the cloud, which allows the use of physical resources through multiple consumers. Also, it creates the virtual instance of resource/device like servers, storage devices, operating system and network resources wherein the framework utilizes the resources in more than one execution environment [16].
- Multi-tenancy: Multi-tenant environment can have multiple customers or users who do not see or share each other's data but can share resources or applications in an execution environment, even if they may not belong to the same organization. Multi-tenancy results in the optimal utilization of hardware and data storage mechanism [27].
- Cloud storage: It is a component, which is maintained, managed, backed up remotely and it is made available over the network where the users can access data [28].
- The hypervisor: It is a key module of virtualization. Also, it permitts multiple Virtual Machines (VMs) to run on a single hardware host. Moreover, it controls and manages and controls the different operating systems that executed on a shared physical scheme [29].
- Cloud Network: It can work more than one traditional data centre; a typical data centre contains hundreds or thousands of servers. To efficiently build and manage the storage of the system where the cloud requires a secure network infrastructure called cloud networking. It requires an internet connection that is similar to a virtual private network which enables the user to securely access printers, applications, files and so on.

3.2. Types of clouds system

Based on the user needs, the cloud system are categorized into four types named as public, community, private and hybrid cloud [30]. These are discussed as follows:

- Public Cloud - any subscriber can access a public cloud with an internet connection
- Private Cloud - A particular group or organization and limits its access to just that group.
- Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
- Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

3.3. Significance of group data sharing

A group is defined as a set or collection of data owners (users) assigned to a set of permissions. Groups are mainly focused on user's identities. Data sharing in the group has achieved greater importance in multiple domains such as businesses, governments and organizations in the real world [31].

3.4. Requirements of data sharing in a group

The primary requirements of group data sharing are discussed as follows:

1) The data owner should define who get to access the data within a group or list of users.
2) In a group, a user should get the permission from data owner to access data.
3) In a cloud, the group members and data owner should have authorization to store data
4) The data owner should have powers to restrict access to users in a group

3.4.1. Problems in data sharing

The primary issues while sharing data in cloud computing are discussed as follows:
Confidentiality [31]: The information proprietor stores his information or records in the cloud. In the event that the servers in Cloud are taken care by Cloud specialist organizations, which are not entirely trusted, then unapproved clients may end getting access.
Scalable and Efficient: A cloud has large numbers of clients, where any client in a group can include or remove from a group; it is basic to keep up the effectiveness and versatility of the framework.
User Revocation: When a client is expelled from a group in a specified time, it is important to restrict access to information, without affecting other clients in the group.
Collusion between substances: When we examined information sharing strategies in the cloud, despite the fact that when elements conspire, none of the clients ought to have the capacity to get information without the consent of the proprietors of information.

4. Literature review

This section aims to present a summary of existing review articles related to secure data sharing in the Cloud. The review articles and surveys presented in this section do not focus specifically on secure group data sharing in the Cloud, rather the main requirements that will enable it. The study of secure data sharing in the Cloud is relatively new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people. We categorize the existing review articles in six aspects: group key management, key aggregate searchable encryption, group signature, attribute-based encryption, and proxy re-encryption, group Diffie-Hellman. All the aforementioned studies are discussed as follows:

4.1. Studies related to group key

Management (GKM) Method
GKM focusses mainly focusing on key generation and distribution of key among group members. All group members need to participate in the secure distribution, creation, and revocation of the keys [32]. Two entities manage the communication session in group key management: Group Controller (GC), responsible for key generation, distribution and rekeying for membership change and Key Server (KS), responsible for maintaining the keys and distributing the keys [33].
As defined in Menezes et al. [34], Group Key Management (GKM) is the set of techniques and procedures used for the estab-

lishment and maintenance of keys among members to form the group. According to Menezes et al. [35], group key management can be classified into three categories. These are Centralized GKM Protocols, Decentralized GKM and Distributed GKM Protocols [33]. From the review of literature, Researchers [36–43] proposed a GKM method for dynamic group data sharing in cloud systems. Through this approach computation, memory with the usage of rekeying messages is reduced significantly. Additionally, it reduces the communication overheads and storage in the rekeying schemes with suitable computational overhead. However, these studies need to improve to ensure that the client is able to view the content on dynamically receiving confirmation. A log record can be managed by keeping track of the client and archive subtle elements. By discharging the solicitation with the client, data archives are recaptured from the cloud. Additionally, the studies require focusing on restricting the conviction levels in the Cryptographic Server (CS) as well as to cope up with insider threats.

4.2. Studies related to key aggregate searchable encryption technique

A common solution is to employ a searchable encryption (SE) scheme in which the data owner is required to encrypt potential keywords and upload them to the cloud together with encrypted data, so that, for the purpose of retrieving data that matches a keyword, the user will send the corresponding keyword trapdoor to the cloud for performing search through the encrypted data. Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the basic security requirements of a cloud storage, implementing such a system for large-scale applications that involves millions of users and billions of files may still be hindered through practical issues like efficient key management with encryption, which are ignored in the literature [44].

Cui et al. [44] and Manohar et al. [45] and Snehal [46] proposed a technique for sharing data in a group using Key Aggregate SE scheme. This scheme was able to store or send data using a smart card with exceptionally restricted data storage in a secure manner. They deliver a formal safety exploration of this scheme based on a typical design. In this approach, the data owner requires dispensing a unique key to other users based on verification and search privileges over their document sets. The evaluation and analysis results proved that this approach was an efficient solution to develop a practical data sharing technique in the public cloud. However, these studies need to focus more towards reducing the number of trapdoors under multi-owners setting.

4.3. Studies related to group signature

The author Chaum and van Heyst first introduced the concept of group signatures. In general, a group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. The variant of the short group signature scheme [47] will be used to achieve anonymous access control, as it supports efficient member-ship revocation [48].

Researchers [49–55] suggested a technique using group signature for sharing the data in dynamic groups through cloud computing. Additionally, few of them have focused towards proxy signature referred in [56–63] for sharing data over the cloud. By this method, the group key was retrieved only through cloud members; however, an unapproved client is not permitted to recover the group key. Further, the study exploited the group signature towards ascertaining confirmation on shared information. This was verified through a third-party auditor and additionally did not disclose the unique nature of the sign of the user. This approach is independent of revoked users in terms, storage overhead and computation cost. Though this study does not concentrate on key management; the focus is towards private key cancellation among group members. Also, to reduce the computation overhead for improving efficiency as well as to preserve the data from malicious activities.

4.4. Studies related to attribute-based encryption

Attribute-Based Encryption (ABE) is a powerful technique used to provide fine-grained access control to data stored in the Cloud. Primarily an Access Control List (ACLs) is maintained, which contains access to data in Cloud. However, this was not scalable and only provided coarse-grained access to data [64]. Attribute-Based encryption first proposed by Goyal et al. [65] provides a more scalable and fine-grained access control to data in comparison to ACLs. Attribute-Based Encryption is an access control mechanism where a user or a piece of data has attributes associated with it. An access control policy is defined, and if the attributes satisfy the access control policy, the user should be able to get access to the piece of data [31].

Yu et al. [66] goal of the study are to obtain the data confidentiality, fine grainedness and scalability. For this purpose, they proposed a KPABE as well as combining it with lazy re-encryption and proxy re-encryption. Further, they achieved the user secret key accountability and confidentiality of user access privilege. Finally, they proved, the proposed approach is more secure in standard cryptographic approach via Formal security analysis.

Researchers [67–75] proposed attribute-based encryption method for secure sharing of data. However, their encryption and decryption lack efficiency because of the expensive pairing operations involved [73], [76]. When data is encrypted using an ABE scheme, key management becomes difficult if there is a huge number of users from diverse backgrounds. Sun [77] claimed that for large secure communications, the current key agreement algorithm is required through which all the clients can contact with other clients to make a complete graph. Among these, one of the nodes is not protected, similar to other nodes that are not protected. Therefore, in future, improvements are required in the key management algorithms using tree structures with a trusted key generation center.

Additionally, the CP-ABE technique does not support strict confidence model, and is also inflexible, with high-costs towards maintaining keys and is not impervious to anti-collusion attacks, apart from suffering from additional inadequacies [78–80]. In [81], the cancellation technique achieves refined grains for all clients data sharing that have various secure standards specifically in direct removal mode; yet it helps towards backings to insert only one client repudiation list in the form of cipher text, thus is considered completely fine-grain disavowal. Because of key escrow, inefficiency backward security issues as well as not connected to distributed storage framework.

4.5. Studies related to proxy re-encryption

Proxy re-encryption (PRE), initially introduced by Blaze et al.[82], enables a semi-trusted proxy to transform a cipher text encrypted under the public key of delegator into another cipher text under the public key of delegate without leaking the underlying encrypted messages or private keys of delegator/delegate to the proxy. This particular kind of public key encryption seems to be an optimal candidate to ensure the security of sharing data in cloud computing. For instance, a case where the data owner (say, Alice) intends to share the sensitive data stored in the cloud with another granted user (say, Bob). It is desirable that nobody other than Bob can access the requested data. Inspired by the primitive of PRE, Alice can encrypt the sensitive data under her own public key before uploading the shared data to the semi-trusted cloud. After receiving the request for data sharing from Bob, Alice generates a proxy re-encryption key using her own private key and Bob's public key and sends this proxy re-encryption key to the semi-trusted cloud server. Equipped with this proxy re-encryption key, cloud server can transform the cipher text encrypted under the public key of Alice into an encryption under the public key of Bob. By utilizing the PRE primitive, the transformed cipher text can only be decrypted by Bob whereas the cloud server is unable to learn the plaintext or private keys of Alice or Bob. Finally, Bob can download and decrypt the requested data with his own private

key. In this way, the costly burden of secure data sharing can be offloaded to the semi-trusted cloud server with abundant resources [83].

Researchers [70], [84–88] proposed a proxy re-encryption method for secure data sharing. They achieved fine-grained information sharing in the cloud. This provided the effective solution towards user revocation issues based on the fine-grained encryption approach. The demonstrated results show this scheme to perform effectively for cipher text attacks with improved collision resistance in the standard model. However, the biggest issue of this approach is taking more time for executing the task as well as associate the features with a client. Even though they offered possible enhancement, the client will have issues as more UAKs requires permitting various efficient attributes based on time periods without altering UAK number. Also, there is a need to concentrate more on improving the security level. Qin et al.[89] Suggested a robust, effective and secure approach for data sharing in the cloud using certificates PRE technique. A study by Dharani and Narmatha [90] tested only fewer data size in this context. So the previous study needs to focus more towards large data size to obtain fast encrypt and decrypting, thereby enhancing speed with the security of the big data set. This will minimize the cost, security mechanism and low complexity towards dealing with security problem over the cloud.

4.6. Studies related to group diffie-hellman

The Diffie-Hellman key exchange protocol [91] is the first public key based key management scheme. In the public-key based cryptosystem, the public-key authentication is one of the main challenges. The PKI based public key cryptosystem achieves the public key authentication by binding the certificate with the public key. In this service mode, the certificates are issued and managed by trusted third party entity CA, but it also brings the huge cost of managing the certificate list to the CA [92].

Lee et al. [93] suggested a TGDH procedure towards enhancing the computational effectiveness through the use of pairing-based cryptanalysis. They minimized the computational cost without demeaning the communication complexity. Lee et al. [94] suggested sharing of data with the multi-owner method, but this system does not support dynamic groups. The system supports only static groups [66], [94], [95]. Also, the previous study uses group signature where each user signs their messages without revealing their identity [94]. Here broadcast encryption approach was used to handle static groups. Gadge [96] reviewed the ABE technique with different access procedure which secured the system. Furthermore, they overcome the key escrow issues using the 2-pc procedure. Also, the issues on fine cancellation problems are resolved. However, the security of the distribution scheme is a major issue nowadays. Further, there is a need to maintain the system with more secure and secrecy based concepts, so as to resist external attackers. This implies the need to focus on finding the solution for the system lacking reliability factor and operates with multimedia data.

Adusumilli et al. [97] proposed a technique and analyzed sharing information, multiple leave operations and working out the cost for join, multi-join, leave. The TGDH approach was [98] most distinctive among CGKA procedures regarding scalability as well as efficiency. Accordingly, future studies should concentrate on TGDH and DGKD. The DGKD approach is more resistant towards failure, network congestion, and delay than TGDH. The key generation is self-governing and for synchronization among other members of the group using TGDH. The DGKD robust technique uses simple substantiation. A new key does not depend on old keys which make it a collision-free network. Therefore, it is genuinely secure at both DGKD and TGDH approaches which require two circles for client leave and join operations. Subsequently, the DGKD method utilized the secret key and public key encryption for distribution of keys (Distributors- Members) and co-distributors as respectively. From the review, the DGKD is practically identical and in few cases superior to TGDH as far as correspondence and calculation costs.

Adusumilli et al. [99] proposed a ternary tree based TGDH protocol for dynamic group data sharing in healthcare cloud that could be used by a healthcare organization to share their data in dynamically secure groups containing other health organizations. Safe and reliable group communication in healthcare organizations is an increasingly active research area by growing popularity in group-oriented and collaborative applications. Ternary tree approach covers other healthcare members (organizations) in a subgroup and height of ternary tree will increase when the number of members in a group increase, where the height of the tree is the number of iterations required to compute a group shared key. However, this study needs to focus towards strong auditing and security techniques which are used to enhance the internal security of this framework.

Based on the aforementioned researchers, Table 1 specifically describes the methodology and the limitations of all the studies that have been considered for the purpose of review. Table 2 discusses the review of performance factor analysis, segregated into the method, data confidentiality, quality of being authentic and anonymity. Table 3 comparatively discussed the computational complexity of various existing schemes, such as the group key management technique, key aggregate searchable encryption, Group signature method, Attribute-based encryption, Proxy re-encryption, Group Diffie-Hellman.

5. Methods

An extensive literature search on Dynamic Group Data Sharing in Cloud Computing was conducted using Google Scholar, IEEE transaction, other international journals such as Springer, Elsevier, ACM, and so on. These searches are limited to the period between 2004 to 2017. In this research, the review papers and reference sections of the individual articles were manually searched. Also, some studies report that a well-defined data sharing method with encryption method in cloud computing were included. As seen in this review, 117 suitable records are retrieved which provides relevant results about security in group data sharing. Also included are the original research studies that developed and evaluated data sharing over the cloud in a secure manner, including summarization of the text document. We excluded studies that met any of the following criteria: (1) Data sharing outside the group over cloud; (2) Security and privacy access control without group data sharing; and (3) Not written in English wherein the present research may have missed systems that are discussed in other languages.

5.1. Inclusion and exclusion criteria

The inclusion and exclusion criteria were applied to all the retrieved studies from the Scopus database. The criteria used for including/excluding papers are as follows:

- Peer-reviewed articles —excluded keynotes, editorials, reviews, tutorial summaries, position papers and panel discussions.
- Studies related to empirical research using various approaches such as experimental research, survey and case studies.
- Augmented papers—If two papers from a similar research on a similar subject were distributed in various scenes (e.g., Journal and conference), only the journal article was incorporated.
- All copied reviews found from different sources were identified and removed.

5.2. Search string

We framed our search string via three compartments as shown in Table 2. We chose to incorporate a condition for picking exact reviews in our search string amid the survey procedure. Given the

assortment of research techniques, having that condition could have made our search string mind-boggling. Running a pilot check for considering the papers, we were mindful of the fact that, we exploited the final search string as obtainable as follows:

Table 1: Details of the Search String Ran On Scopus

Digital Library	Scopus
Years	2000–2017
Language	Only English
Subject Areas	"Computer Science", "Cloud computing, Web intelligence", "Information technology", "Computational science"

6. Study selection

Our search in Scopus returned 2720 outcomes. We separated the papers through evaluating the abstract and title of the research. At the point when there were a few papers that we could not settle on by perusing the titles and abstract, these papers were held for the following round of assessment. We barred the papers that were seen as unrelated, or whose full content was not accessible. Since we were keen on experimental reviews, we rejected papers that were not bolstered with observational information. Besides, we included the articles related to group data sharing as both static and dynamic manner. Also, have avoided the duplicate research article. At the end of progression, it was found that 77 papers met all the incorporation criteria. Having settled the rundown of our essential reviews, we in the long run added 6 studies to our rundown which were either not found by our search or we had rejected them in the light of title/abstract surveys. In the choice procedure, 117 papers were conveyed between two initial writers and they separated the papers by perusing the full content of the papers. In this stage, 62 studies were chosen as essential reviews. At that point, the references of these 62 selected articles were checked, keeping in mind the end goal to discover more potential essential reviews. We found 35 conceivably significant articles by title from the references of these 62 articles.

7. Results

The present study has reviewed 117 articles, of which 16 were from Springer digital library, 32 from IEEE digital library, 13 from Elsevier, 9 from ACM, 31 from the specific journal and international journal and 14 from Google scholar (Figure 1). Of these studies, the following aspects are addressed: Group Key Management method (15 articles), Key Aggregate Searchable Encryption technique (8 articles), Group Signature (19 articles), Attribute-Based Encryption (13 articles), Proxy Re-encryption (6 articles), Group Diffie-Hellman (13 articles). The pictorial representation of the previous method is provided in Figure 2. From the analysis, it is revealed that most of them have focused on group signature method to share data through cloud source securely.

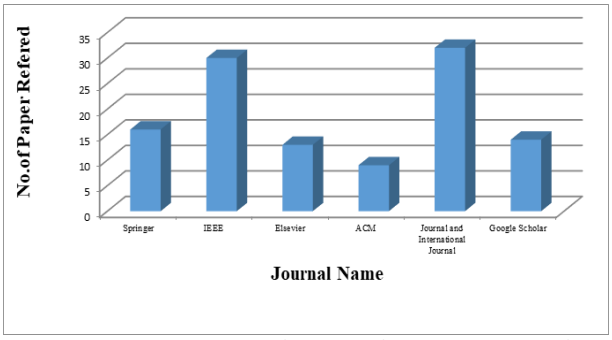

Fig. 1: Pictorial Representation of Number of Research Article Referred.

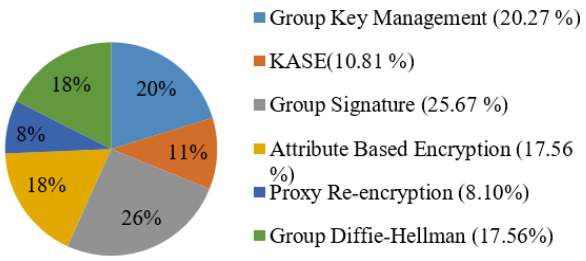

Fig. 2: Pictorial Representation of Existing Methods.

From the aforementioned review, privacy and security is an important concern, with respect to outsourcing data to the cloud service provider. Moreover, the privacy of the data is affected once the illegitimate users infer something from the cloud data. Firstly, the primary issue of the cloud is building a secure environment for the implementation, and web management of business software and email service. It provides enormous potential for a reliable, available, and agile infrastructure in autonomic, distributed and grid computing environments [100], [101]. On the other hand, a lot of personal information and potentially sensitive data that people store on their computers are now being transferred to the cloud. This makes it critical for you to understand the security measures that your cloud provider has in place, and it is equally important to take personal precautions to secure your data [102], [103]. The author has classified cloud computing security issues into two main categories: security issues faced by the providers and security issues faced by the users [104]. Security issues are holding back the growth of cloud computing market. Some companies are returning back to their own platforms since they do not wish to be exposed to security risks [105]. Also, other major cloud security issues are as follows: wrapping XML signature, Browser Security, Cloud middleware attacks, and Flooding attacks [106].

Secondly, the privacy of users (their identity and data in the cloud) is another crucial issue with cloud computing; and with the growth of cloud storage, concerns about privacy are becoming important [107], [108] . However, reaching the peak in providing and assuring privacy data access in cloud computing is in progress and needs further attention to achieve users' goals (refer to previous sections and discussions). On the other hand, data privacy is about the security of the Personally Identifiable Information (PII). Personal information should be managed as a part of the data usage. The PII was found lacking in the cloud computing service because of the privacy issues [110]. Moreover, privacy issues exist for a long time in computing literature, and many acts have been passed to protect individual privacy of users and secrecy. Nevertheless, these have passed and are inapplicable to new scenarios, where a new relationship between users and providers (that means three parties) rises [111]. To be more specific, privacy issues include access, compliance, storage, retention, destruction, audit and monitoring [100]. Moreover, in the past decade, many methods were proposed to preserve privacy. In this review, we have described some of these methods and approaches as shown in Table II. Subsequently, Table II specifically describes the methodology and the limitations of all the studies that have been considered for the purpose of review. Table III discusses the review of performance factor analysis, segregated into the method, data confidentiality, quality of being authentic and anonymity. Table IV comparatively discussed the computational complexity of various existing schemes, such as the group key management technique, key aggregate searchable encryption, Group signature method, Attribute-based encryption, Proxy re-encryption, Group Diffie-Hellman.

The suggested solutions to the above-mentioned security issues are discussed as follows:

1) Authentication: When unauthorized users access the service and users' information, identity management system should be applied.
2) Access control: Using SLA with access control to identify only authorized users of the cloud.

3) Policy integration: Accessing different cloud providers by different nodes may raise a conflict between their policies; hence, a solution is needed to work out the inconsistencies between those policies.
4) Service management: Composed service by many cloud providers are produced to meet customers' needs, it thus needs a service integrator to offer accurate service.
5) Trust management: The approach of trust management should be used as the negotiation factor of the users and provider of the cloud. Some level of trust should exist interchangeably between cloud providers and users.

The suggested solutions to the privacy issues are discussed as follows:

1) The cloud user should carefully read the privacy policy before placing their information in the cloud. If a cloud user does not understand any of the policies, it should be clarified with the provider or the user may consider other service providers.
2) Cloud users should pay close attention regarding the rights to use, disclose, or make public cloud user information.
3) Suppose the cloud user wants to remove any data from the cloud, the cloud provider should take necessary steps to remove the data. Cloud users should possess the rights to check whether the data is still retained by the cloud provider.
4) Cloud users should not place any important data which may be helpful for their competitors, government, and others.
5) Cloud users should always consult their technical support group about the advisability of keeping their data in the cloud.

8. List of abbreviations

TTP	Trusted Third Party
CSPs	Cloud Service Providers
VMs	Virtual Machines
GKM	Group Key Management
GC	Group Controller
KS	Key Server
CS	Cryptographic Server
SE	Searchable encryption
ABE	Attribute-Based Encryption
ACLs	Access Control List
PRE	Proxy re-encryption
PII	Personally Identifiable Information

9. Conclusion

In this paper, several existing techniques were reviewed and classified based on three categories: key management and encryption approaches, searching over encrypted data and access control schemes. From the classification, it was concluded that there is a need to enhance security, and privacy and also need to provide as strong-as-possible protection mechanisms, without computational overheads from cloud data owner. Moreover, the solutions should take into consideration the performance and pay attention to the speed of searching and decrypting since the amount of data in the cloud is huge, whereas the technique will be inefficient if it takes too long a time to retrieve data for users. Finally, the limitations and challenges that require future researchers to handle them are discussed.

10. Future scope

The proposed solutions should cover the following:

1) Enable storing the keys safely while preventing cloud-based service and unauthorized parties
2) Permit the Cloud Service Provider towards participating in the process of searching and to decrease computational overheads on the owner's side.
3) Needs to focus more towards advanced and refined attributes for securely sharing data and implement the same. Furthermore, the path and data encryption need to be secured from the unapproved access of information. On the other hand, the two-factor authentication offers highly reliable validation; however, the verification procedure is recommended during user login with username, password, and OTP confirmation.
4) Prevention of collusion attack. Revoked user should not violate the data confidentiality, and he should not be able to decrypt the data even if he receives it
5) To extend the traceability, which means only the original user can reveal the identity of the signer in order to preserve data from the malicious activities of users in the group.

Table 2: Survey of Previous Studies

Author	Method	Results	Limitation/ future scope
Kim et al. (2011)	Layered platform architecture	Enhanced expandability and proven efficiency of avionic contents through SaaS and application layer.	Need to focus towards executing service based on IACSS; specifically, different avionic services as well as to share the useful data as required.
Wang et al. (2011b)	Hierarchical attribute-based encryption technique	Effectively canceled the access rights from the client side.	Need to concentrate more towards encryption scheme, which can be improving security level
Dharavath and Bhima (2011)	Group Key Management	Strong authentication with LIDs, CIDs for cluster formations. Further, provided client source substantiation with RSA keys	They planned to extend this method towards cluster communications, to disjoin or merge information over dynamic networks
Mallaiah et al. (2015)	Multi-user multi-key Encryption Search	Data stored in a shared table under one or other columns of database server	1. Need to focus towards support proximity search on encrypted relational databases. 2. Try to explore possibility of doing some of the proxy functionality in the cloud where the service provider does not have the access control to plain data while performing operations.
Tu et al. (2012) Han et al. (2016)	CP-ABE	They solved key escrow issues through key generation with distributed semi-trusted parts	Need to enhance the effectiveness of encrypted data with decryption process
Yuan et al. (2013)	Multi-User Public key timed-release searchable encryption method	1. The sender transmits encrypted information to cloud server over the group. 2. At the same time, the receiver cannot decrypt the cipher text till present time.	Only low set of data is tested and not appropriate for a huge group of authorized users
Reddy and Saritha (2014)	Group Key Management	They employed secure communication over the group as well as access the procedure over the cloud	Need to focus towards designing a framework for formal technical communication within the group over the network
Malarvizhi et al. (2014)	Group Signature with encryption	1. They shared the information over the group without canceling their identity. 2. Also, supports new client joining and cancellation.	Need to reduce the computation overhead for improving the efficiency of the system.

Author	Method	Results	Limitation/ future scope
Xue and Hong (2014)	Mona	They shared the information over the group without canceling their identity.	Need to concentrate on filing the key updations for improving the security level of the system
Devi and Kanimozhi (2014)	Dynamic broadcast encryption method and security Elliptic Curve Cryptography	They shared the data in a secure manner amongst dynamic groups without cancelling their identity members.	Require focusing on key management schemes, specifically to revoke the group members private keys.
Reddy and Kiran (2014)	Efficient Data Sharing Technique	Without exhibiting, privacy details of the cloud user can be shared among others in a group.	1. Only focused on text document 2. Need to concentrate on various types of data being uploaded to the cloud server like video and audio information.
Liu et al. (2014b)	Time-based proxy re-encryption	1. The data was associated with the attribute, access structure and access time for identification of feature. 2. Additionally, eligible time periods denote the period of validity of user's access right	Need to allow different effective time periods for various features of the users without modifying UAKs numbers.
Liu et al. (2014a)	Fine-grained access control with encryption	Digital signature and encryption were combined as a single method for providing data confidentiality, authenticity, unforgeability, anonymity and collusion resistance of the system.	Need to work on attribute-based signcryption for user/attribute revocation.
Wang et al. (2014a)	certificateless PRE method	1. Resolved the key escrow issues using identity-based public key cryptography. 2. public key validity is assured in the proposed approach.	Need to focus towards improving the efficiency and provably secure CL-PRE schemes in the standard model
Mercy and Srikanth (2014)	Group Key Management	1. Contributed towards efficient control for user access to revoked system coordinator group. 2. Authenticated user were able to view and upload the document in the cloud.	1. Need to concentrate on improving the user access or view the data after receiving authentication from the data owner 2. Through a description of the user request, the documented data are required to be regained from the cloud.
Dong et al. (2014)	CP-ABE	This approach aids the effective and secure dynamic operations that involve unlimited data creation, alteration of client features and user cancellation.	Need to focus towards improving the privacy and security of data sharing in real time cloud application.
Ranjith and Kathiravan (2014)	Dynamic group data sharing	1. Data items were shared in dynamic groups which remain for a long time in the system considerably reducing the security and privacy of system with increased complexity in managing data files. 2. All records are removed automatically once there is no usage of data.	1. Planned to extend this work for the recovery of destroyed information when needed. 2.This system needs to be adapted for dealing with Big Data analysis with slight modifications.
Wang et al. (2014b)	Multi-user Searchable Encryption	Using this approach, efficient user revocation in a dynamic manner is achieved.	To minimize the computation and complexity of the system
Jin and Peng (2009)	Tree-based key management scheme	The shared secret data permits various reconstructed keys using different shares activation for information which is prepositioned.	1. All the key belongs to future groups are encrypted with existing keys or same keys. 2. Additionally, there is no aid on multicast group once the rekeys are needed from one of the group members
Malarvizhi et al. (2014)	Group Signature and encryption method	Efficient user cancellation was achieved by revoked public list without altering private keys on the new users and remaining users for decrypted information among users.	High computation overhead
Cheng-Kang Chu et al. (2014)	Key-Aggregate Cryptosystem for Scalable Data Sharing	In cloud storage for flexible ciphertext in cloud for aggregator key by release of secret key, however, the information available other than encrypted information remains confidential.	Limited data storage
Lu and Li (2015)	Certificate-based Proxy re-encryption	1. This proposed Proxy re-encryption technique provides significant security in random oracle model for Diffie-Hellman computation. 2. To avoid the time-consuming bilinear pairing operations, this scheme significantly reduces the computation cost. Computation cost is minimized by incorporating time-consuming bilinear pairing operations.	1. It provides security in random oracle model alone. 2. For this purpose, need to focus towards CB PRE method without incorporating bilinear pairing scheme.
Lin et al. (2015)	Threshold crypto sharing with group signature	Prevent the subdivided and merged information from being tampered	Need to focus more towards applying this technique for preventing attacks in the cloud or developing various networks for strengthening the security in the platform.
Ruan et al. (2015)	Novel online auditing method	Considerably improved the performance of auditing tasks efficiency compared with existing vehicle-based communication.	Need to concentrate on collusion attacks which exist between proxy and user. Also, information should not be altered for the proposed algorithm.
Dhanshri and Raut (2015)	Secure data sharing method	1. Less key size cannot hack the information as easily. 2. It provides effective revocation schemes for private key after updation of user's details.	Need to focus towards group key management. Specifically, on how private keys are revoked from group members.
Vinupriya et al. (2015)	Secure group sharing a framework	1. Computation load is distributed among many hosts. 2. Also, support forward and backward secrecy	1. Need to focus towards proposing a new key agreement protocol which will support for increasing the subgroup over the data sharing system. 2. Also, construct a tree in log(n) steps using effective group key agreement algorithm in future
Liang et al.	CP-ABPRE	This approach supports the access structure mono-	Need to concentrate towards improving the effi-

Author	Method	Results	Limitation/ future scope
(2015)		tonically for a composite bilinear group order. By this, they proved the adaptively of the CCA-secure standard model without affecting the access policy.	ciency in re-encrypted key generation over various phases.
Shi et al. (2015)	ABE	Permits trusted authority towards canceling the client detail through updating cancellation list without contact non- revoked users and cancelled user are not able to decrypt the ciphertext successfully. Additionally every auditor confirms the TTP updated ciphertext in a proper manner.	Need to concentrate towards constructing revocable cipher text-policy ABE with verifiable ciphertext delegation approach for improving the efficiency of the system over cloud server.
Poornima et al. (2015)	Reviewed data sharing approach	Share the data in a secure manner using multiple dynamic groups over the cloud server.	They suggested to concentrate on data sharing and collaboration in cloud. Also, this review states that issues related to user revocation are still challenging.
Bhaurao and Swati (2015)	Privacy preservation and secure data sharing	1. The proposed scheme provides the advantage without revealing secret or private key user, to enable transmission of data among the group. 2. Furthermore, the user can easily join in the group and decrypt shared data in the cloud which provides ease of access.	Need to focus more towards advanced and sophisticated features for secure data sharing for implementation.
Ali et al. (2015)	SeDaSC methodology	The use of SeDaSC methodology provides data sharing security without any encryption mechanisms, for malicious insiders access control mechanisms were developed, and it provides access control in both forward and backward systems.	1. This research can be further extended by limiting cryptographic server trust level and the need to analyze the performance for insider threats. This study needs to focus towards limiting the trust level in the cryptographic server as well as helping the system cope with insider threats. 2. Moreover, the response of the methodology with varying key sizes needs to be evaluated.
Cui et al. (2015), Manohar et al. (2015), Snehal (2016)	Key Aggregate Searchable Encryption	Offered a solution towards real-time data sharing over public cloud storage.	Need to focus towards decreasing the usage of trapdoors beneath multi-owners setting by enhancing and achieving security of the system.
Akanksha and Patil (2016)	Mona	Any user securely shares the data in the group with others over untrusted cloud system.	This system has only one group manager. Once the group manager fails, another backup group manager will replace the failed one.
Shahina (2016)	TGDH scheme	Cloud-based data share security requirement scheme for achieving higher efficiency.	Need to focus towards extending this scheme to handle more than one group on the cloud.

Table 3: Review of Performance Factor Analysis

S. No	Reference	Method	Data Confidentiality	Quality of being authentic	Anonymity
1	Liu et al. (2014a)	Cipher text-Policy Attribute-Based Signcryption	Yes	Yes	Yes
2	Mercy and Srikanth (2014)	Group Key Management	No	Yes	No
3	Bhaurao and Swati (2015)	Privacy preservation and secure data sharing	Yes	Yes	No
4	Trueman and Narayanasam (2015)	Homomorphic Authenticable Ring Signature	No	Yes	No
5	Chaudhary et al. (2014)	Homomorphic encryption	No	Yes	No
6	Harn and Lin (2010)	Group key transfer protocol	No	Yes	No
7	Abdalla and Pointcheval (2006)	Constant-round password-based group key exchange protocol	No	Yes	No
8	Pandranki and Krishna (2012)	Authenticated key transfer protocol	Yes	Yes	No
9	Xu et al. (2012)	Certificate-less proxy re-encryption	No	Yes	No
10	Ma and Zhang (2015)	Group Signature	No	No	Yes
11	Margret (2013)	Secure Multi-Owner attributes method	No	No	Yes
12	Devi and Kanimozhi (2014)	Group signature, with ECC algorithm	Yes	No	Yes
13	Rao and Ahamed (2015)	Secure Multi-Owner data sharing scheme	No	No	Yes
14	Wei et al. (2014)	EFADS protocol	No	No	Yes
15	Swarna and Maryam (2016)	ID-Based Ring Signature	No	No	Yes

Table 4: Feature and Computation Complexity Comparison among Existing Schemes

	Group key management Technique	Key aggregate searchable encryption	Group signature method	Attribute-based encryption	Proxy re-encryption	Group Diffie-Hellman
Major principle adopted	Dynamic group data sharing with encryption	Multi- owner data sharing with encryption	Group signature and dynamic broadcast encryption techniques	Cipher text-policy attribute-based encryption	Re- encryption technique	Group key agreement with encryption approach
Efficient for very large group	Yes	No	Yes	No	No	No
Scalable to massively adding and removing members	Yes	Yes	Yes	No	No	Yes
Member computational complexity	Decryption	Decryption	Decryption with group signature	Decryption	Simple operation	Group key protocol
Group controller computational complexity	Combination of data and key encryption	Encryption	Encryption with group signature	Encryption	Simple operation	Shared key protocol

References

[1] Xia Z, Wang X, Sun X, Wang Q (2016) A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data. IEEE Trans Parallel Distrib Syst 27:340–352. https://doi.org/10.1109/TPDS.2015.2401003.

[2] Fu Z, Ren K, Shu J, et al (2016) Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement. IEEE Trans Parallel Distrib Syst 27:2546–2559. https://doi.org/10.1109/TPDS.2015.2506573.

[3] Fu Z, Sun X, Liu Q, et al (2015) Achieving Efficient Cloud Search Services: Multi-Keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing. IEICE Trans Commun E98.B:190–200. https://doi.org/10.1587/transcom.E98.B.190.

[4] Ren Y, Shen J, Wang J, et al (2015) Mutual verifiable provable data auditing in public cloud storage. J Internet Technol 16:317–323. doi: 10.6138/JIT.2015.16.2.20140918.

[5] Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Futur Gener Comput Syst 28:583–592. https://doi.org/10.1016/j.future.2010.12.006.

[6] Chang V, Kuo Y-H, Ramachandran M (2016) Cloud computing adoption framework: A security framework for business clouds. Futur Gener Comput Syst 57:24–41. https://doi.org/10.1016/j.future.2015.09.031.

[7] Mohd BJ, Hayajneh T, Ahmad Yousef KM, et al (2017) Hardware design and modeling of lightweight block ciphers for secure communications. In: Futur. Gener. Comput. Syst. http://linkinghub.elsevier.com/retrieve/pii/S0167739X17304661.

[8] Rahman F, Bhuiyan MZA, Ahamed SI (2017) A privacy preserving framework for RFID based healthcare systems. Futur Gener Comput Syst 72:339–352. https://doi.org/10.1016/j.future.2016.06.001.

[9] Guo P, Wang J, Li B, Lee SY (2014) A Variable Threshold-value Authentication Architecture for Wireless Mesh Networks. J Internet Technol 15:929–936. doi: 10.6138/JIT.2014.15.6.05

[10] Shen J, Tan H, Wang J, et al (2015) A novel routing protocol providing good transmission reliability in underwater sensor networks. J Internet Technol 16:171–178. doi: 10.6138/JIT.2014.16.1.20131203e.

[11] Xie S, Wang Y (2014) Construction of Tree Network with Limited Delivery Latency in Homogeneous Wireless Sensor Networks. Wirel Pers Commun 78:231–246. https://doi.org/10.1007/s11277-014-1748-5.

[12] Chu CK, Chow SSM, Tzeng WG, et al (2014) Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage. IEEE Trans Parallel Distrib Syst 25:468–477 https://doi.org/10.1109/TPDS.2013.112.

[13] Pearce M, Zeadally S, Hunt R (2013) Virtualization. ACM Comput Surv 45:1–39. https://doi.org/10.1145/2431211.2431216.

[14] Perez-Botero D, Szefer J, Lee RB (2013) Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the 2013 international workshop on Security in cloud computing - Cloud Computing '13. Hangzhou, China, p 3 https://doi.org/10.1145/2484402.2484406.

[15] Aguiar E, Zhang Y, Blanton M (2014) an Overview of Issues and Recent Developments in Cloud Computing and Storage Security. In: High Performance Cloud Auditing and Applications. Springer New York, New York, NY, pp 3–33 https://doi.org/10.1007/978-1-4614-3296-8_1.

[16] Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34:1–11. https://doi.org/10.1016/j.jnca.2010.07.006.

[17] Abbas A, Khan SU (2014) A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds. IEEE J Biomed Heal Informatics 18:1431–1441. https://doi.org/10.1109/JBHI.2014.2300846.

[18] Ali M, Khan SU, Vasilakos A V. (2015) Security in cloud computing: Opportunities and challenges. Inf Sci (Ny) 305:357–383. https://doi.org/10.1016/j.ins.2015.01.025.

[19] Fernandes DAB, Soares LFB, Gomes J V., et al (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13:113–170. https://doi.org/10.1007/s10207-013-0208-7.

[20] Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) an analysis of security issues for cloud computing. J Internet Serv Appl 4:5. https://doi.org/10.1186/1869-0238-4-5.

[21] Modi C, Patel D, Borisaniya B, et al (2013) A survey of intrusion detection techniques in Cloud. J Netw Comput Appl 36:42–57. https://doi.org/10.1016/j.jnca.2012.05.003.

[22] Xiao Z, Xiao Y (2013) Security and Privacy in Cloud Computing. IEEE Commun Surv Tutorials 15:843–859. https://doi.org/10.1109/SURV.2012.060912.00182.

[23] Singh A, Chatterjee K (2017) Cloud security issues and challenges: A survey. J Netw Comput Appl 79:88–115. https://doi.org/10.1016/j.jnca.2016.11.027.

[24] Liu Y, Sun YL, Ryoo J, et al (2015) A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. J Comput Sci Eng 9:119–133. https://doi.org/10.5626/JCSE.2015.9.3.119.

[25] Sinddhuri P, Kumar GR (2017) The Data Storage and Assured Sharing Methodology among Differing Groups in Cloud Computing. Int J Sci Eng Adv 5:313–318.

[26] Singh S, Jeong Y-S, Park JH (2016) A survey on cloud computing security: Issues, threats, and solutions. J Netw Comput Appl 75:200–222. https://doi.org/10.1016/j.jnca.2016.09.002.

[27] Tan X, Ai B (2011) the issues of cloud computing security in high-speed railway. In: Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. IEEE, pp 4358–4363 https://doi.org/10.1109/EMEIT.2011.6023923.

[28] Feng J, Chen Y, Summerville D, et al (2011) Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol. In: 2011 IEEE Consumer Communications and Networking Conference (CCNC). IEEE, pp 521–522 https://doi.org/10.1109/CCNC.2011.5766528.

[29] Li J, Li B, Wo T, et al (2012) CyberGuarder: A virtualization security assurance architecture for green cloud computing. Futur Gener Comput Syst 28:379–390. https://doi.org/10.1016/j.future.2011.04.012.

[30] Huth AJC (2011) the Basics of Cloud Computing. Pittsburgh.

[31] Poornima E, Kasiviswanth N, Bindu CS (2015) secure data sharing for multiple dynamic groups in Cloud. In: 2015 Conference on Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG). IEEE, pp 326–331 https://doi.org/10.1109/PCCCTSG.2015.7503928.

[32] Manz D, Alves-Foss J, Zheng S (2008) Network Simulation of Group Key Management Protocols. J Inf Assur Secur 1:67–79.

[33] Ranjani RS, Bhaskari DDL, Dr.P.S.Avadhan (2011) Current Trends in Group Key Management. Int J Adv Comput Sci Appl 2:82–86.

[34] Menezes AJ, Oorschot PC van, Vanstone SA (1996) Handbook of Applied Cryptography Discrete Mathematics and Its Applications, illustrate. CRC Press, United States.

[35] Rafaeli S, Hutchison D (2003) a survey of key management for secure group communication. J ACM Comput Surv 35:309–329 https://doi.org/10.1145/937503.937506.

[36] Reddy KSK, Saritha SJ (2014) Accountable Contract Signing Protocol for Secure Data Sharing In Multiuser Untrusted Clouds. IJARCCE 3:8138–8141. https://doi.org/10.17148/IJARCCE.2014.31013.

[37] Ranjith K, Kathiravan PG (2014) A Self-Destruction System For Dynamic Group Data Sharing In Cloud. IJRET Int J Res Eng Technol 3:265–270 https://doi.org/10.15623/ijret.2014.0319048.

[38] Reddy RD, Kiran PR (2014) An Efficient Data Sharing Technique in the Cloud: An EDST. Int J Recent Innov Trends Comput Commun 2:

[39] Mercy SS, Srikanth GU (2014) an efficient data security system for group data sharing in cloud system environment. In: International Conference on Information Communication and Embedded Systems (ICICES2014). IEEE, pp 1–4 https://doi.org/10.1109/ICICES.2014.7033956.

[40] Ali M, Dhamotharan R, Khan E, et al (2015) SeDaSC: Secure Data Sharing in Clouds. IEEE Syst J 1–10. https://doi.org/10.1109/JSYST.2014.2379646.

[41] Sonar PG, Shinde PD, Patil VA, et al (2015) A Novel Approach for Secure Group Sharing in Public Cloud Computing. Int J Comput Appl 127:47–50.

[42] Bhaurao C, Swati D (2015) Privacy Preservation and Secure Data Sharing in Cloud Storage. Int Res J Sci Eng 3:231–236.

[43] Zhu Z, Jiang R (2016) A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud. IEEE Trans Parallel Distrib Syst 27:40–50. https://doi.org/10.1109/TPDS.2015.2388446.

[44] Cui B, Liu Z, Wang L (2016) Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage. IEEE Trans Comput 65:2374–2385. https://doi.org/10.1109/TC.2015.2389959.

[45] Manohar K, Kumar RA, Kumar SP (2015) Key Aggregate Searchable Encryption for Group Data Sharing Via Cloud Data Storage. Int J Comput Eng Res Trends 2:1132–1136.

[46] Snehal P (2016) Secured Group Data Sharing Over Cloud by Using Key Aggregate and Searchable Techniques. Int J Sci Res 5:499–502.

[47] Armbrust M, Stoica I, Zaharia M, et al (2010) A view of cloud computing. Commun ACM 53:50. https://doi.org/10.1145/1721654.1721672.

[48] Sowjanya SL, Ravikiran D (2014) Secure Data Sharing for Dynamic Groups in the Public Cloud. Int J Comput Eng Res Trends 1:PP 428–435.

[49] Margret MK (2013) Secure Policy Based Data Sharing for Dynamic Groups in the Cloud. Int J Adv Res Comput Eng Technol 2:2073–2076.

[50] Devi JK, Kanimozhi S (2014) Efficient User Revocation for Dynamic Groups in the Cloud. Int J Eng Comput Sci 3:3938–3942.

[51] Trueman TE, Narayanasamy P (2015) Ensuring Privacy and Data Freshness for Public Auditing of Shared Data in Cloud. In: 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM). IEEE, pp 22–27 https://doi.org/10.1109/CCEM.2015.36.

[52] Priyanka S, Sonali R, Kanchan S, Gayatri T (2015) Data Sharing in Cloud Using Identity Based Ring Signature. Int Res J Eng Technol 2:885–889

[53] Rao DV, Ahamed SA (2015) Multi Owner Data Sharing for Dynamic Groups in the Cloud Securely. Int J Electr Electron Comput Syst 3:56–62

[54] Akanksha S, Patil BM (2016) A Secure Multiowner Dynamic Groups Data Sharing In Cloud. Int J Adv Eng Technol 9:32–39.

[55] Malarvizhi M, Sujana JAJ, Revathi T (2014) secure file sharing using cryptographic techniques in cloud. In: Proceeding of the IEEE International Conference on Green Computing, Communication and Electrical Engineering, ICGCCEE 2014. IEEE, Coimbatore https://doi.org/10.1109/ICGCCEE.2014.6921421.

[56] Kishore S, Lakshmi N, Rao T (2015) Secure Multi-Owner Data Sharing for Dynamic Groups using Proxy-Signature in the Cloud. Int J Comput Appl 132:42–46.

[57] Valli K, Punitha A (2016) Multi Proxy Resignature with Public Auditing of Shared Cloud Data for User Revocation. Int J Res Emerg Sci Technol 3:74–76.

[58] Mari AP, Basha MJ (2015) A mechanism of user revocation based public auditing for shared data in the cloud. Int J Sci Eng Appl Sci 1:351–358.

[59] Kamble SM, Lomte A. (2014) Homomorphic Authenticable Ring Signature (HARS) mechanism for Public Auditing on Shared Data in the cloud. Int J Eng Res Gen Sci 6:812 –816.

[60] Anantula J (2016) A Study on Proxy Re-Signatures for Public Auditing of Shared Data on the Cloud. Int J Adv Res Comput Commun Eng 5:692 –694.

[61] Reddy PN, Reddy J, Kumar P (2015) Efficient User Revocation in Dynamic Cloud Using Proxy Server. Int J Comput Eng Res Trends 2:552–557.

[62] Chang Y-F, Chang C-C (2007) An RSA-based (t, n) threshold proxy signature scheme with freewill identities. Int J Inf Comput Secur 1:201 –209 https://doi.org/10.1504/IJICS.2007.012250.

[63] Belekar Y, Verma M, Tormal P (2015) Efficient User Revocation in Cloud Using Proxy Server. Int J Adv Found Res Comput 2:435–440.

[64] Li J, Zhao G, Chen X, et al (2010) Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing. In: 2010 IEEE Second International Conference on Cloud Computing Technology and Science. IEEE, pp 89–96 https://doi.org/10.1109/CloudCom.2010.44.

[65] Goyal V, Pandey O, Sahai A, Waters B (2006) 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. ACM, New York, pp 89–98 https://doi.org/10.1145/1180405.1180418.

[66] Yu S, Wang C, Ren K, Lou W (2010) achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proceedings - IEEE INFOCOM.

[67] Fu JY, Huang QL, Ma ZF, Yang YX (2014) secure personal data sharing in cloud computing using attribute-based broadcast encryption. J China Univ Posts Telecommun 21:77–51. 10.1016/S1005-8885(14)60344-7 https://doi.org/10.1016/S1005-8885(14)60344-7.

[68] Yang Y, Zhu H, Lu H, et al (2016) Cloud based data sharing with fine-grained proxy re-encryption. Pervasive Mob Comput 28:122–134. https://doi.org/10.1016/j.pmcj.2015.06.017.

[69] Liu J, Huang X, Liu JK (2014) Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption. Futur Gener Comput Syst 52:67–76. https://doi.org/10.1016/j.future.2014.10.014.

[70] Han K, Li Q, Deng Z (2016) Security and efficiency data sharing scheme for cloud storage. Chaos, Solitons & Fractals 86:107–116. https://doi.org/10.1016/j.chaos.2016.02.010.

[71] Hu D, Xu W, Qu R (2014) Electromagnetic design optimization of single-sided linear induction motor for improved drive performance based on linear metro application. In: 2014 Australasian Universities Power Engineering Conference (AUPEC). IEEE, pp 1–6. https://doi.org/10.1109/AUPEC.2014.6966564.

[72] Liang K, Au MH, Liu JK, et al (2015) A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. Futur Gener Comput Syst 52:95–108. https://doi.org/10.1016/j.future.2014.11.016.

[73] Deng H, Wu Q, Qin B, et al (2014) Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Inf Sci (Ny) 275:370–384. https://doi.org/10.1016/j.ins.2014.01.035.

[74] Yao X, Chen Z, Tian Y (2014) A lightweight attribute-based encryption scheme for the Internet of Things. Futur Gener Comput Syst 49:104–112. https://doi.org/10.1016/j.future.2014.10.010.

[75] Shi Y, Zheng Q, Liu J, Han Z (2015) Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation. Inf Sci (Ny) 295:221–231. https://doi.org/10.1016/j.ins.2014.10.020.

[76] Zhang Y, Chen X, Li J, et al (2016) Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. In: Information Sciences. Elsevier.

[77] Sun L (2009) Role Based Secure Group Communication and Data Sharing System. Simon Fraser University.

[78] Bethencourt J, Sahai A, Waters B (2007) Cipher text-policy attribute-based encryption. In: 2007 IEEE Symposium on Security & Privacy. IEEE, pp 321–334 https://doi.org/10.1109/SP.2007.11.

[79] Hur J, Noh DK (2011) Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Trans PARALLEL Distrib Syst 22:1214–1221 https://doi.org/10.1109/TPDS.2010.203.

[80] Liu Q, Wang G, Wu J (2014) Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Inf Sci (Ny) 258:355–370. https://doi.org/10.1016/j.ins.2012.09.034.

[81] Wang P, Feng D, Zhang L (2011) towards attribute revocation in key-policy attribute based encryption. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Berlin Heidelberg, pp 272–291 https://doi.org/10.1007/978-3-642-25513-7_19.

[82] Blaze M, Bleumer G, Strauss M (1998) Divertible protocols and atomic proxy cryptography. pp 127–144 https://doi.org/10.1007/BFb0054122.

[83] Qin Z, Xiong H, Wu S, Batamuliza J (2016) A Survey of Proxy Re-Encryption for Secure Data Sharing in Cloud Computing. IEEE Trans Serv Comput 1–1. https://doi.org/10.1109/TSC.2016.2551238.

[84] Lu Y, Li J (2015) efficient certificate-based proxy re-encryption scheme for data sharing in public clouds. KSII Trans Internet Inf Syst 9:2703–2718. https://doi.org/10.3837/tiis.2015.07.021.

[85] Wei G, Lu R, Shao J (2014) EFADS: Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re-encryption. J Comput Syst Sci 80:1549–1562. https://doi.org/10.1016/j.jcss.2014.04.021.

[86] Wang C, Ren K, Wang J (2011) Secure and practical outsourcing of linear programming in cloud computing. In: 2011 Proceedings IEEE INFOCOM. IEEE, pp 820–828 https://doi.org/10.1109/INFCOM.2011.5935305.

[87] Liang K, Chu C-K, Tan X, et al (2014) Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. Theor Comput Sci 539:87–105. https://doi.org/10.1016/j.tcs.2014.04.027.

[88] Liu W, Denizci Guillet B, Xiao Q, Law R (2014) Globalization or localization of consumer preferences: The case of hotel room booking. Tour Manag 41:148–157. https://doi.org/10.1016/j.tourman.2013.09.004.

[89] Qin Z, Wu S, Xiong H (2015) Strongly Secure and Cost-Effective Certificateless Proxy Re-encryption Scheme for Data Sharing in Cloud Computing. In: First International Conference. pp 205–216 https://doi.org/10.1007/978-3-319-22047-5_17.

[90] Dharani R, Narmatha M (2014) Secured Data Sharing With Traceability In Cloud Environment. Int J Invent Comput Sci Eng 1:1–9.

[91] Diffie W, Hellman M (1976) new directions in cryptography. IEEE Trans Inf Theory 22:644–654. https://doi.org/10.1109/TIT.1976.1055638.

[92] Song W, Zou H, Liu H, Chen J (2016) A practical group key management algorithm for cloud data sharing with dynamic group. China Commun 13:205–216. https://doi.org/10.1109/CC.2016.7513215.
[93] Lee S, Kim Y, Kim K, Ryu D-H (2003) An Efficient Tree-Based Group Key Agreement Using Bilinear Map. Springer-Verlag Berlin Heidelberg https://doi.org/10.1007/978-3-540-45203-4_28.
[94] Liu X, Zhang Y, Wang B, Yan J (2013) Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud. IEEE Trans Parallel Distrib Syst 24:1182–1191. https://doi.org/10.1109/TPDS.2012.331.
[95] Boneh D, Boyen X, Goh E-J (2005) Hierarchical Identity Based Encryption with Constant Size Ciphertext. In: An extended abstract of this paper appears in R. Cramer, editor, Advances in Cryptology—EURO. Springer, pp 440–456 https://doi.org/10.1007/11426639_26.
[96] Gadge S V. (2014) Analysis and Security based on Attribute based Encryption for data sharing. Int J Emerg Res Manag &Technolog 3:74– 78
[97] Adusumilli P, Zou X, Ramamurthy B (2005) DGKD: Distributed Group Key Distribution with Authentication Capability. In: Workshop on Information Assurance and Securit. IEEE, West Point, NY https://doi.org/10.1109/IAW.2005.1495965.
[98] Kim Y, Perrig A, Tsudik G (2000) Simple and fault-tolerant key agreement for dynamic collaborative groups. In: Proceedings of the 7th ACM conference on Computer and communications security - CCS '00. ACM Press, New York, New York, USA, pp 235–244 https://doi.org/10.1145/352600.352638.
[99] Thakare VR, Singh KJ (2016) Ternary tree based TGDH protocol for dynamic secure group data sharing in healthcare cloud. In: 2016 International Conference on Inventive Computation Technologies (ICICT). IEEE, pp 1–7 https://doi.org/10.1109/INVENTIVE.2016.7823294.
[100] Arockiam L, Parthasarathy G, Monikandan S (2012) Privacy in Cloud Computing : A Survey. In: Computer Science & Information Technology (CS & IT). Academy & Industry Research Collaboration Center (AIRCC), pp 321–330 https://doi.org/10.5121/csit.2012.2331.
[101] Dharavath R, Bhima K (2011) Distributed Group Key Management with Cluster based Communication for Dynamic Peer Groups. Int J Adv Comput Sci Appl 2:82–89 https://doi.org/10.14569/IJACSA.2011.020214.
[102] Kim DH, Song S, Shin SJ, Park N (2011) an extended cloud computing architecture for immediate sharing of avionic contents. In: Communications in Computer and Information Science. pp 439–446 https://doi.org/10.1007/978-3-642-23312-8_55.
[103] Wang G, Liu Q, Wu J, Guo M (2011) Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Comput Secur 30:320–331. https://doi.org/10.1016/j.cose.2011.05.006.
[104] Madhavi K V., Tamilkodi R, Sudha KJ (2012) Cloud Computing: Security threats and Counter Measures. Int J Res Comput Commun Technol IJRCCT 1:125–128.
[105] Kumar S, Goudar RH (2012) Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. Int J Futur Comput Commun 1:356–360 https://doi.org/10.7763/IJFCC.2012.V1.95.
[106] Jamil D, Zaki H (2011) Security issues in cloud computing and countermeasures. Int J Eng Sci Technol 3:2672–2676.
[107] Xue K, Hong P (2014) A dynamic secure group sharing framework in public cloud computing. IEEE Trans Cloud Comput 2:459–470. https://doi.org/10.1109/TCC.2014.2366152.
[108] Wang LL, Chen KF, Mao XP, Wang YT (2014) Efficient and provably-secure certificateless proxy re-encryption scheme for secure cloud data sharing. J Shanghai Jiaotong Univ 19:398–405. https://doi.org/10.1007/s12204-014-1514-6.
[109] Gellman R (2013) Privacy in the clouds: risks to privacy and confidentiality from cloud computing. In: World Priv. Forum. file://192.168.1.201/Guidance/Documents/HMD/%2316HMD035/%2316HMD035_Working Doc/27.04.2017/Reference BP/20141210031010501.pdf. Accessed 27 Apr 2017.
[110] Pearson S (2009) Taking account of privacy when designing cloud computing services. In: 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. IEEE, pp 44–52 https://doi.org/10.1109/CLOUD.2009.5071532.
[111] Zhou M, Zhang R, Xie W, et al (2010) Security and Privacy in Cloud Computing: A Survey. In: 2010 Sixth International Conference on Semantics, Knowledge and Grids. IEEE, pp 105–112 https://doi.org/10.1109/SKG.2010.19.
[112] Mallaiah K, Ramachandram S, Gandhi RK (2015) Multi user searchable encryption schemes using Trusted Proxy for cloud based Relational Databases. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, pp 1554–1559 https://doi.org/10.1109/ICGCIoT.2015.7380714.
[113] Tu SS, Niu SZ, Li H, et al (2012) Fine-grained access control and revocation for sharing data on clouds. In: Proceedings of the 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops, IPDPSW 2012. IEEE, Shanghai, pp 2146–2155 https://doi.org/10.1109/IPDPSW.2012.265.
[114] Yuan K, Liu Z, Jia C, et al (2013) Multi-user Public Key Timed-Release Searchable Encryption. In: 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies. IEEE, pp 363–370 https://doi.org/10.1109/EIDWT.2013.69.
[115] Dong X, Yu J, Luo Y, et al (2014) achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. Comput Secur 42:151–164. https://doi.org/10.1016/j.cose.2013.12.002.
[116] Wang Q, Zhu Y, Luo X (2014) Multi-user Searchable Encryption with Coarser-Grained Access Control without Key Sharing. In: 2014 International Conference on Cloud Computing and Big Data. IEEE, pp 119–125 https://doi.org/10.1109/CCBD.2014.29.
[117] Jin S, Peng J (2009) Key Graphs and Secret Sharing Be Used in Network Multicast Security. In: 2009 International Symposium on Computer Network and Multimedia Technology. IEEE, pp 1–5 https://doi.org/10.1109/CNMT.2009.5374682.
[118] Cheng-Kang Chu, Chow SSM, Wen-Guey Tzeng, et al (2014) Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage. IEEE Trans Parallel Distrib Syst 25:468–477. https://doi.org/10.1109/TPDS.2013.112.
[119] Lin HY, Hsieh MY, Li KC (2015) Secured map reduce computing based on virtual machine using threshold secret sharing and group signature mechanisms in cloud computing environments. Telecommun Syst 60:303–313. https://doi.org/10.1007/s11235-015-0031-8.
[120] Ruan Z, Liang W, Luo H, Yan H (2015) A Novel Data Sharing Mechanism via Cloud-Based Dynamic Audit for Social Internet of Vehicles. In: Second International Conference. Chengdu, China, pp 78–88 https://doi.org/10.1007/978-3-319-27293-1_8.
[121] Dhanshri A, Raut S. (2015) Review of Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation. Int J Adv Res Comput Sci Softw Eng 5:693 –697
[122] Vinupriya R, Kayalvizhi C, Malarvizhi S (2015) A Secure Data sharing for groups dynamically in Public Cloud. Int J Innov Res Comput Commun Eng 3:10867–10872
[123] Cui B, Liu Z, Wang L (2015) Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage. IEEE Trans Comput 1–1. https://doi.org/10.1109/TC.2015.2389959.
[124] Shahina KM (2016) A Secure Group Sharing Framework Using TGDH Scheme. Int J Sci Res 5:668–673.
[125] Chaudhary A, Thakur R, Mann M (2014) Security in Cloud Computing By Using Homomorphic Encryption Scheme with Diffie-Hellman Algorithm. Int J Adv Comput Eng Netw 2:42–46.
[126] Harn L, Lin C (2010) Authenticated Group Key Transfer Protocol Based on Secret Sharing. IEEE Trans Comput 59:842–846 https://doi.org/10.1109/TC.2010.40.
[127] Abdalla M, Pointcheval D (2006) A Scalable Password-based Group Key Exchange Protocol in the Standard Model. In: Advances in Cryptology – Proceedings. Shanghai, China, pp 332–347 https://doi.org/10.1007/11935230_22.
[128] Pandranki V lakshmi, Krishna N (2012) Secure Group Key Transfer Protocol Based on Secret Sharing. Int J Comput Sci Inf Technol 3:4712 – 4717.
[129] Xu L, Wu X, Zhang X (2012) CL-PRE: a certificateless proxy re-encryption scheme for secure data sharing with public cloud. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security - ASIACCS '12. ACM Press, New York, New York, USA, p 87 https://doi.org/10.1145/2414456.2414507.
[130] Ma H, Zhang R (2015) Secure Cloud Storage for Dynamic Group: How to Achieve Identity Privacy-Preserving and Privilege Control. 254–267. https://doi.org/10.1007/978-3-319-25645-0.
[131] Swarna A, Maryam SA (2016) Increasing Security Level in Data Sharing Using Ring Signature in Cloud Environment. J Eng Res Appl w 6:1–6.