**A**

**SEMINAR REPORT**

**ON**

Anonymous and Traceable Group Data Sharing in Cloud Computing

**SUBMITTED BY**

**Name: Indrajeet Devale**

**University Exam No.: T150384249**

**UNDER GUIDANCE OF**

**PROF. Bharati Ainapure**

**COMPUTER ENGINEERING DEPARTMENT,**

**MAEER’S MIT COLLEGE OF ENGINEERING, PUNE.**

**\* 2018-2019 \***

****

MAHARASHTRA ACADEMY OF ENGINEERING AND EDUCATIONAL

RESEARCH’S

MIT COLLEGE OF ENGINEERING,

## PUNE

DEPARTMENT OF COMPUTER ENGINEERING

# CERTIFICATE

This is to certify that Mr./Ms. Indrajeet Devale of TE Computer, Roll No. 3162028, has successfully completed seminar on

**Anonymous and Traceable Group Data Sharing in Cloud Computing**

to my satisfaction and submitted the same during the academic year 2018-2019 towards the partial fulfillment of degree of Bachelor of Engineering under Savatribai Phule Pune University, under the Department of Computer Engineering, MIT College of Engineering., Pune.

Prof. Bharati Ainapure Prof. Bharati Dixit

Seminar Guide Head Computer Department

**Acknowledgement**

Seminar report on “Anonymous and Traceable Group Data Sharing in Cloud Computing” is an outcome of guidance and moral support on me throughout the work. For this I acknowledge and express my profound sense of gratitude and thanks to everybody who have been a source of inspiration during the seminar presentation. I am highly obliged to my guide Prof. Bharati Ainapure for her valuable instructions, guidance, corrections and providing help whenever needed in my T. E. seminar and its presentation.

Date:

Place: Pune

Indrajeet Devale

Roll Number: 3162028

TE-Computer

**Index**

**1. Introduction**………………………………….…………………….……..7

1.1 What is Cloud Computing?.............................................................7

1.2 Types of Data Sharing…………………………………………….8

**2. Literature Survey**……………………………………………………….11

**3. Security in Cloud Computing**………………………………………….**.**13

**4. Real life example for Group Sharing**…………………………………..14

**5. Objectives and Goals**……………………………………………….……16

* 1. Arbitrary Number of Users and Dynamic Changes………………16
  2. Confidentiality of Outsourced Data……………………………....16
  3. Traceability in an anonymous environment……………………....16
  4. Authentication Services and Fault Tolerant property…………..…16

**6. Algorithms and Tools used**……………………………………………....17

* 1. Cryptographic Bilinear Maps…………………………………..….17
  2. Group Signature……………………………………………….…..17
  3. Block Design and (v, k+1,1)-design………………………………18

1. **System Model**………………………………………………………....19
   1. Components of System Model…………………………..……….…19
   2. Functions of System Model………..…………………………….….19
2. **Threat Model**…………………………………………………………**.**21
3. **Design Goals**……………………………………………….…………..23
   1. Dynamic Change……………………………………………….........23
   2. Data Confidentiality…………………………………………………23
   3. Anonymity…………………………………………………...………23
   4. Traceability………………………………………..………………....23
   5. Fault Tolerant Property………………………………………………23
4. **Proposed Scheme**……………………………………………………...24
   1. Initialization………………………….………………………24
   2. Key Generation…………………….…………..….…………25
   3. Fault Detection……………………….……...……………….28
5. **Conclusion and Future Scope**………………………………………...29
6. **References**…………………………………………………...…………30

**Abstract**

Cloud Computing is one of the most upcoming and exciting technologies which is introduced in all the sectors of military, medicine, business, and many other fields. Group data sharing in Cloud Computing is also an exciting prospect as not only does it guarantee efficiency in data sharing, but it also means various users, entities, parties can come together to share data with each other and thus contribute to their topic.

However, with this, there are many challenges in Cloud Computing. Security of the data on the cloud is of utmost importance. In addition, how to achieve both anonymity and traceability is also a challenge in the cloud for data sharing. The research paper discussed in this report focuses on having an efficient data sharing model for a group connected internally and then with the cloud with high security and efﬁciency in an anonymous manner. Using the concept of key agreement and group signature, the research paper referred in this report proposes a unique solution to this problem by having an anonymous cloud group data sharing system which also has the feature of traceability in public clouds.

**Index Terms -** Group data sharing, anonymous, traceability, key agreement, symmetric balanced incomplete block design (SBIBD).

**Chapter 1 – Introduction**

* 1. **What is Cloud Computing?**

Cloud computing is a data sharing model where every device is linked to a common storage resource and/or other devices. This interconnection leads to easier data sharing among devices as they all store and edit contents of the same resource.[1] This resource centre can be thought of as an amorphous cloud which acts as a virtual server for all the devices and users connected to it. Hence, the name, Cloud Computing. Cloud computing is used to minimize costs in the IT sector as it follows a “pay-as-you-use” model [23]. It also requires less hands-on maintenance and hence companies prefer to use the cloud system as less maintenance leads to lesser instances of downtime since there is less issue of management, costs, allocation of resources, and hence the applications can be deployed faster and consistently.

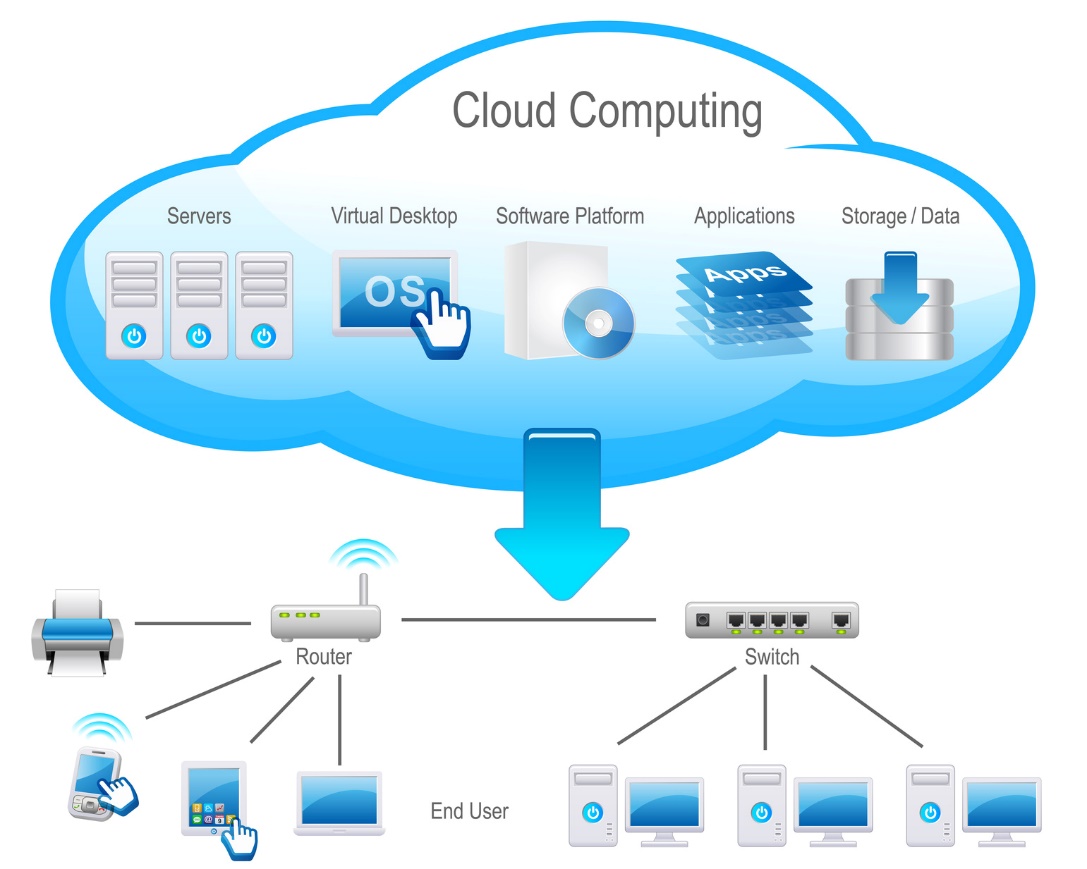


Figure 1.1 Basic Model of Cloud Computing

The above model (figure 1.1) shows how the cloud system works. The end user is connected to the cloud through hubs or switches. Devices are also connected through a router directly to the cloud. Through these networking devices, the user is able to access the servers on the cloud, deploy computer applications on the cloud and also use it as a storage resource.

Thus, reduction of cost, high capacity networks and virtualization of storage space is the reason Cloud Computing is the preferred network model.

Compared to traditional methods of data sharing, Cloud Computing has certainly attracted the interest of researchers as not only is it more efficient and has various data sharing capabilities, but it also has low energy consumption. Cloud Computing provides users with limitless computing resources and provide users with limitless storage resources which is necessary in the current computing world. [1]-[3].

Storage in cloud computing is one of the most important features as it is how electronic devices connect with each other which enables free flow of data. However, ever since the inception of Cloud Computing not much attention has been given to group data sharing using cloud in which users with common interests come together to share data with each other on topics of common interest directly for co-operative and research purposes. [4], [5].

**1.2 Types of Data Sharing**

The various applications of group data sharing are electronic health networks [6], wireless body area networks [7], and electronic literature in libraries. There are two ways to share data in a cloud storage:

1. One-to-Many pattern

This refers to the scenario where one client authorizes access to his/her data

for many clients [8].

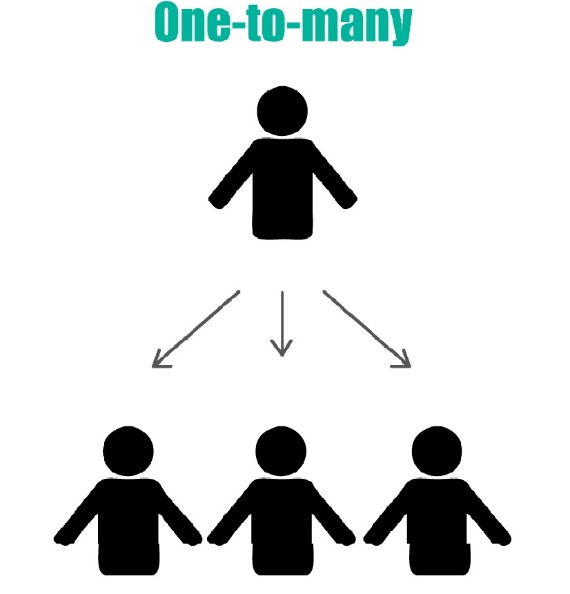


Figure 1.2 One-To-Many model

In figure 1.2, you can see that the one entity, which is the admin in this scenario is connected to all the other members or entities. However, the other members are not interconnected with each other. Hence, this is known as the one-to-many model as the one entity is connected to many entities.

1. Many-to-Many pattern

The Many-to-Many pattern refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time

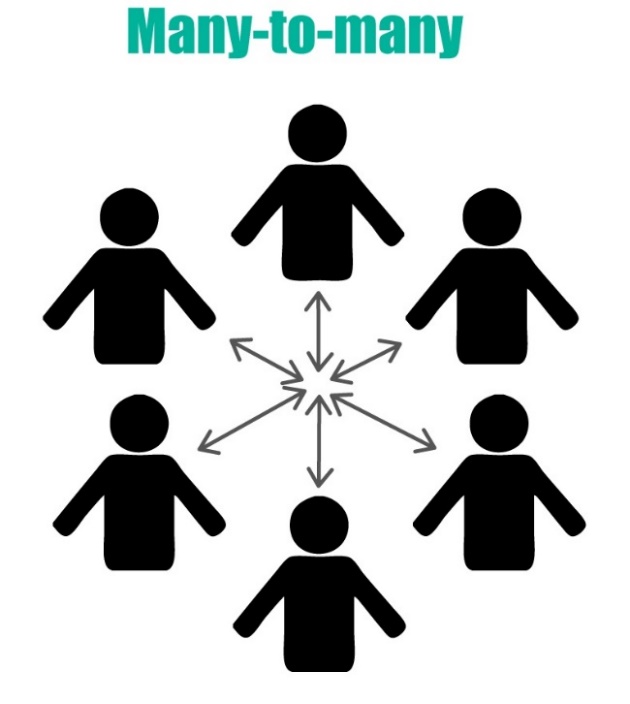


Figure 1.3 Many-to-Many Model

In the figure1.3, we can see how all the members are interconnected to each other. In the many-to-many model, there is no one central admin to which all the members are connected. Hence, since all the members are connected to each other, this is known as the Many-to-Many model.

In the system presented by the original authors of the research paper, the many-to-many model is used.

**Chapter 2. - Literature Survey**

**2.1 Proxy Re-encryption Scheme**

Ateniese [13] proposed a proxy re-encryption scheme to manage distributed ﬁle systems that attempt to achieve secure data storage in the semi-trusted party. Based on bilinear maps, the security of the system was certainly strengthened. It provided stronger security than [14], however it was still susceptible under collusion attacks and revoked malicious users.

**2.2 Access Control in Cloud Computing using KA-ABE technique**

In order to overcome the vulnerabilities in the above-mentioned systems, an effective access control for cloud computing was proposed by Yu [11]. This system attempts to protect the user from outsourced data attacks and revoked malicious users. It provides effective access control as the user chooses a random key to encrypt each data file with which is then encrypted by key policy attribute-based encryption (KA-ABE) technique. Authorized users are provided with the access structure and secret key by the group manager which can be used to decrypt the outsourced data. The problem with this system is that it is designed only for a One-to-Many system. Hence, it cannot be applied to many real-life scenarios.

**2.3 Anonymous and Traceable data sharing model**

A number of studies have been proposed to protect users’ privacy [15]. A traceable privacy preserving communication scheme was proposed for vehicle to-grid networks in smart grids. [16]. This system is not vulnerable however it can be applied to only one-to-one data sharing model and does not consider a group data sharing cloud system.

A secure scheme was proposed by Liu [17] to support anonymous data sharing in cloud computing. Both anonymity and traceability are well supported by employing the group signature technique. Since there is dynamic broadcast encryption, real-time changes can be made to the user profile or user data. However, this system is again susceptible to collusion attacks by the cloud server and the threat from malicious revoked users.

**2.4 Centralized data sharing model**

In [18], the key management system falls into two categories: The ﬁrst is key distribution, in which the generation and distribution of the key is completely accomplished by a centralized controller. The second is key agreement, where all the members in the group fairly contribute, negotiate and determine a common conference key together. However, having centralized control can be a huge disadvantage to security since it is vulnerable and will be a target for various malicious attacks and might prove to be the bottleneck. It will also cause a huge load for the centralized control.

In the paper published by the original authors, they focus on constructing an efﬁcient and secure data sharing scheme that can support anonymous and traceable group data sharing in cloud computing. Collusion attack is also considered and addressed, while the problem of revoked user is considered. Many-to-many group data sharing is also supported in the proposed scheme.

The research paper Anonymous and Traceable Group Data Sharing in Cloud Computing written by **Jian Shen**, **Tianqi Zhou**, **Xiaofeng Chen**, **Jin Li**, and **Willy Susilo** talks about how they have used various methods and tools to ensure anonymous sharing of data in a group which uses Cloud Computing while also providing traceability.

**Chapter 3 - Security in Cloud Computing**

Security of one’s stored data is one of the main challenges facing Cloud Computing.

- In cloud computing, the data is stored by the users with the help of a third-party vendor.

- It needs to be ensured that only entities with authority have the ability to access this data.

- Not only does the data storing have to be efficient, it also needs to provide proper security and accessibility but only to identified users. For this User Identification system can be used.

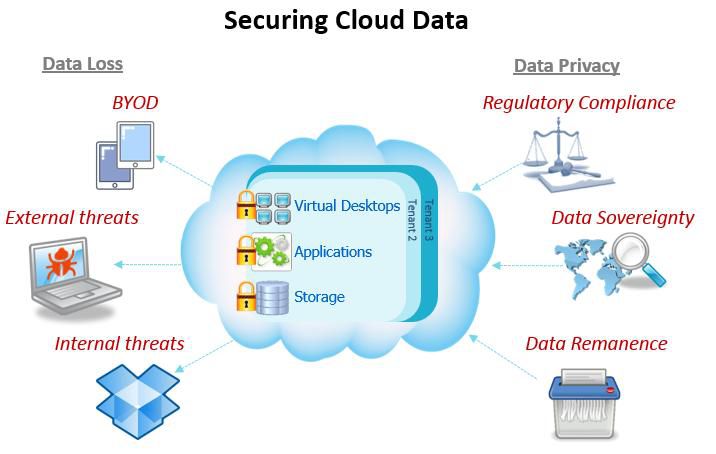


Figure 3.1 Security Threats in Cloud Computing

In figure 3.1, we see the various external security threats to the cloud. They are classified into Data Loss and Data Privacy.

1. Data Loss – Sensitive information can be lost due to leakage, or disappearance/damage from the cloud [25]. This can cause a massive loss to a company or organisation.
2. Data Privacy – Data Privacy is basically maintaining the confidentiality of personal information on the cloud. Information stored on the cloud can be sensitive and hence this is a serious challenge in cloud computing.

Some of the Security Threats to Cloud Computing are:

1. BYOD: BYOD stands for Bring Your Own Device. When an employee who is working for an organisation attaches personal smartphone or tablet to an organizational network or machine, malware could migrate from the phone or tablet of the user to the organisational network or machine. Sensitive data can also somehow make its way to the user’s personal device which is a huge security lapse.[26]
2. External Threats: There can be various external threats to the cloud from various third person entities which might be listening or interfering in your network and eventually gain access to your data.
3. Internal Threats: Malicious or revoked users can be a big threat as not only they might have access to the data due to the access key not being changed but they also might modify the contents of the cloud with a malicious intent.
4. Regulatory Compliance: Cloud works on the “honest but curious” policy. This means that although cloud service provider won’t modify the contents of the data, it does have access to your data. This is a legal grey area as there is no way of ensuring that your data is not being given access to by cloud service providers to third party vendors.
5. Data Sovereignty: Different countries have different compliance laws on data regulation. Some countries might define their laws such that the cloud service providers have to give access to the concerned authorities on demand.
6. Data Remanence: Sometimes, even though data has been deleted off the cloud by the user, some data may remain. This remnant data can be sensitive. To counter this, wiping off entire data and replacing it with garbage value is a very common solution.

**Chapter 4 - Real Life Example for Group Sharing**

To explain the goals of the research paper, the following real- life scenario is considered [23]:

Consider a group of scientists at a research institution who want to share their data or results only and only with each other. Some scientists would like to share their data anonymously. In this case, due to unreliability of security in cloud and relatively low control over the cloud data as compared to traditional forms of data storage the authors of the research paper wanted to achieve an anonymous method of sharing data while also upholding security and efficiency. Since scientists might leave or join the institution anytime, the authors had to ensure that their solution works for an arbitrary and variable number of entities. To ensure this, the data and key should be updated dynamically as soon as changes in the number of entities or the authority of an entity takes place, in an efficient manner.

The second challenge is the confidentiality of the data in the cloud. In this example, the data uploaded by the scientists can/will be of utmost importance and sensitive. No entity would agree to participate in this group of cloud computing if the system cannot guarantee the security of data.

A significant challenge in Cloud Computing is also that it should follow a many-to-many model instead of having a group manager with the highest authority. This will ensure efficient sharing of data and the user or entity will have greater control over the data.

In simple words, the authors needed to put forth a solution wherein a particular user or entity can choose who can view his published data and he can also update or delete it as per his own choice rather than waiting for a group manager to approve of his decision. However, with such freedom given to the user, there is another challenge which can arise due to this which is talked about in the next paragraph.

Since this is a many-to-many group sharing pattern, there is a need for authentication services to prevent the misuse of the data or to prevent misbehaviour by any user or entity. There can also be a different key attack in which the hash values of two secure conference keys can be the same. To prevent this from happening a fault tolerant method should be used. This will ensure that malicious attacks on the cloud won’t have any effect on the data and security won’t be compromised.

**Chapter 5 - Objectives and Goals**

Basically, the goal is to achieve anonymous data sharing in a group cloud having high security and high efficiency. They have also felt the need to address all the challenges presented in the Example section and also provide optimal solutions to all of them.

Following are the solutions to counter the challenges presented [9]-[12]:

* 1. **Arbitrary Number of Users and Dynamic Changes support**

1. The concept of volunteer is introduced to satisfy the Symmetric Balanced Incomplete Block Design (SBIBD). This ensures that the number of users can be arbitrary instead of a prime number *k.* [24]
2. Users get the freedom to join or leave freely.
3. This scheme can support dynamic changes of users and many to many data sharing pattern.
   1. **Confidentiality of Outsourced Data**
4. Encryption of outsourced data takes place using a common conference key before it is uploaded.
5. For this, the security is dependent on the Elliptic Curve Cryptography (ECC) and the Bilinear Difﬁe-Hellman (BDH) assumption.
6. As a result of this, users can exchange data with others safely in the semi-secure cloud.
   1. **Traceability in an anonymous environment**
7. Since this is a many-to-many model, users in the cloud can freely share data with each other directly.
8. Users can share data anonymously in the cloud without their identity getting revealed.
9. However, as a safety or security measure, in case of any dispute, group manager or group admin can choose to reveal identity of data owner based on the group signature bound with the data.
   1. **Authentication Services and Fault Tolerant property**
10. Each member exchanges messages along with the group signature to declare that their identity is valid.
11. All uploaded data files are bound with group signature. Due to this, the cloud can verify the validity of the file.

**Chapter 6 - Algorithms and Tools used**

Thus, the above-mentioned schemes aim to address all the challenges for group data sharing in cloud computing elegantly. This paper also presents some preliminaries in cryptographic and combinatorial mathematics. The various security algorithms are also explained like Cryptographic Bilinear Maps, Group Signature, Block Design and various other security assumptions.

* 1. **Cryptographic Bilinear Maps**
* Let G1 be an additive cyclic group of order Q and G2 be a cyclic multiplicative group of order Q, then it has the following properties [23]:
  + - * 1. Bilinear: For any P,Q ∈ G1 and a,b ∈ Z, we haveˆ e(aP,bQ)=ˆ e(P,Q)ab
        2. Non-degenerate: If P is a generator of G1, then ˆ e(P,P) ∈ F∗ p2 is a generator of G2. In other words, ˆ e(P,P)=1.
        3. Computable: Given P,Q ∈ G1, an efﬁcient algorithm exists to compute ˆ e(P,Q).
  1. **Group Signature**
* This technique allows the group members to anonymously sign messages in the name of the group.

Concept of group signatures was first introduced by David Chaum and Eugene van Hyst in 1991.[22].

For this technique, the Group Manager is an essential part of the process. He is responsible for managing the entry and exit of group members.

Furthermore, in case of a dispute, he is responsible for revealing the true identity of the participating group members, if necessary.

The group should in general be anonymous, traceable and unforgeable for it to secure.

The authors of this research paper have applied a variant of the short group signature scheme to achieve anonymous data sharing with efﬁcient access control and traceability.

* 1. **Block Design and (v, k+1,1)-design**
* A block design is basically a set in a family of subsets whose members are chosen to satisfy some set of properties that are deemed to be useful for a particular application.[21]
* The following are the properties of a Balanced Incomplete Block Design:
* b blocks have the same number k of plots each
* Each treatment is replicated r times in the design.
* Parameters k and v of V satisfy the condition of k <v such that no block contains all the elements of the set V.
* Parameters b and v of V satisfy the condition of b ≥v.

The case of equality is called a symmetric design.

Here, v is the number of elements of V, b denotes the number of blocks, and k indicates the number of elements in each block. If the condition of k = r and b = v holds, then it is a symmetric balanced incomplete block design (SBIBD).

**Chapter 7 - System Model**

The main aim of Cloud Computing is that user’s having common interests sharing their research or findings or topics of common interest. The 3 main entities of the system model are shown in figure 7.1:

1. Cloud
2. Group Manager
3. Members or Users

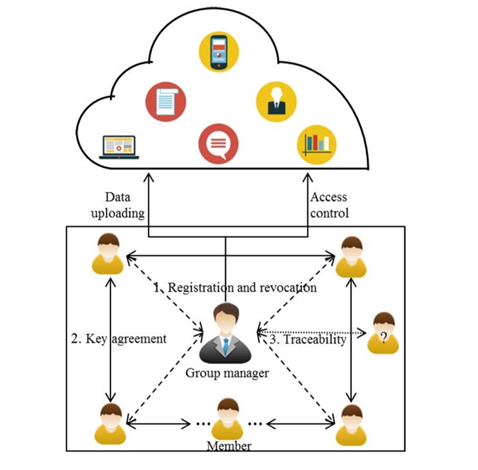


Figure 7.1 System Model [23]

**7.1 Components of the System Model**

1) Cloud

* Along with providing users with unlimited data storage, Cloud also provides data sharing between users.
* One of the main characteristics of Cloud is that it follows the “honest but curious” [20],[19] policy.
* This means that the Cloud would not modify, add or delete data from the cloud deliberately, but it will be curious to know the contents of the data uploaded along with other details as well as the user’s identity.
* Hence, in the scheme suggested by the authors, the Cloud is a semi-trustable party.

2) Group Manager

* The Group Manager is an important role in the system suggested by the authors.
* Its task is to be responsible for generating system parameters, managing group members and for the fault tolerance detection.
* In the presented system, the Group Manager has to be a third-party entity trusted by both the users and the Cloud.

3) Members

* Members are basically the series of users according to the SBIBD model.
* In the scheme used by the authors, the members or users are people with similar interests coming together to share or receive or store relevant data in the Cloud.

As stated previously, the biggest challenge in having shared data on the same cloud is the security and confidentiality of the data. To counter this, in the system introduced by the authors, users of the same group conduct a key agreement based on the SBIBD structure. Moreover, a common conference key is used to encrypt the data that will be uploaded to the cloud to ensure the conﬁdentiality of the outsourced data. Due to this, any malicious external entity cannot modify or access contents of the cloud without having the common conference key which is dynamic and issued to each verified user by the system.

Anonymity of sharing data in the cloud group is also one of the main concerns of a user. To solve this problem, a technique called group signatures is used, which allows users in the same group to anonymously share data in the cloud. This ensures that even though the data is traceable to the original user, it still remains confidential as the user identity is in the encrypted form.

In the system model shown in figure 7.1, all the users with common interests register themselves with the group manager to take part in the cloud group system. Also, all members of the cloud agree on a common conference key which allows them to take part and have access in the cloud group system. This is also used to decrypt or encrypt the outsourced data. Finally, when a dispute occurs, the group manager is able to reveal the real identity of the group member.

**7.2 Functions of the System Model**

The 3 main functions of a System Model are:

1. Registration of the User: Whenever a new user joins the group, he/she has to register with the group manager. The User ID of the newly joined user and the signature is stored in the Group Manager’s registry.
2. Key Agreement: Using a dynamically changing common conference key, the users can modify the contents of the cloud. The identity of the user is protected because the user ID is encrypted.
3. Traceability: Traceability is a very important feature of the proposed system as in case of any dispute, the contents uploaded by a particular user can be traced back to him/her even though the user ID is encrypted. If it is a malicious user, the group manager can choose to reveal the identity of the malicious user.

**Chapter 8 – Threat Model**

As discussed in Chapter 3, security is the main challenge of a cloud system. Following are some attacks which threaten the security of the Cloud System:

1. An attacker outside the system tries to reveal the common conference key and tries to decrypt the outsourced data present on the cloud.
2. A revoked user may hold the common conference key to the cloud and hence attempt to modify or access the contents of the cloud. The conference key is updated periodically and conveyed to the current users through a secure network.
3. Some malicious user, active on the cloud, might generate different sub keys and transmit different messages to the different users. This makes it difficult for the Group Manager to trace back data to the malicious user.
4. A proficient external attacker might duplicate the valid signature of a current user and might try to modify data posing as the member or even reveal the original user’s identity.

Since, the cloud works on a “honest but curious” model, in our system the cloud will not modify or delete data from the cloud. However, the cloud will be interested and check the contents from time to time.

**Chapter 9 - Design Goals**

**9.1 Dynamic Change**

* One of the main problems when having a dynamic group is ensuring the security and confidentiality of the data.
* The system should also ensure that all current members should be authenticated when accessing data and all the revoked members should have no access to the data in the cloud.

**9.2 Data Confidentiality**

* The cloud server and external entities should have no access to data on the cloud.
* In the presented system, a common conference key is used by all the users to encrypt the data before uploading it on the cloud.
* With respect to the SBIBD, the communication and computation complexities for generating the common conference key are relatively small.
  1. **Anonymity**
* Confidentiality should be guaranteed in the cloud group system.
* Otherwise, only a few users would be willing to share their data.
  1. **Traceability**
* In case of disputes, the group manager should be able to trace the uploaded data back to the original user who has uploaded the data.
* The system does provide the ability to trace the content back to the user in our model.
  1. **Fault-Tolerant Property**
* This property guarantees that even in the case of a malicious member being present, the remaining authenticated members should still be able to have their own common conference key.

**Chapter 10 - The Proposed Scheme**

They propose the scheme, which is based on low communication and computation complexities. Our scheme can be divided into 5 parts:

* 1. **Initialization**
* Initialization is performed by the group manager.
* It includes parameter initialization, user registration, and SBIBD construction.
  1. Parameter Initialization
  + In this a parameter l is selected as input of BDH parameter generator.
  + Using this, a bilinear map group system is returned.
  + The parameter is kept private till the end as a master key.
  1. User Registration
     + Each group member registers with the group manager with his/her identity ID.
     + The secret key for a member is then added to the group user list of the group manager.
  2. SBIBD Construction
* Since the communication model is based on the SBIBD structure, it reduces the communication complexity and computational complexity for generating a common conference key.
* The SBIBD also supports efficient key updating.
* Hence, the structure of SBIBD should be prepared first.
* The group manager is responsible for the preparation of structure of SBIBD according to the number of group users.

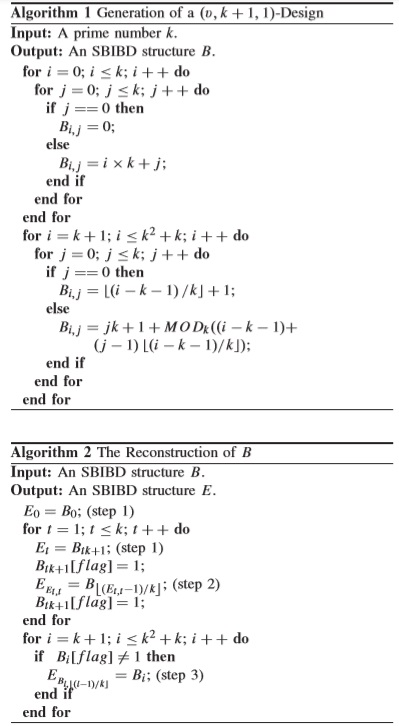


Figure 10.1 Algorithm to generate SBIBD structure

Algorithm 1(figure 10.1) creates the structure B of a (*v*, *k* + 1,1) design. However, the key agreement protocol requires that in the structure of the SBIBD, each block B*i* contains element *i*. Therefore, Algorithm 2 is designed to transform B to E to satisfy this requirement. The group manager checks whether *kn* = (−1 +√ 4*n*−1)/2 is a prime number, where n is the number of registered members. If not, the smallest prime number *kp*, which is larger than   
*kn*, should be found. The reconstructed E is be used as the communication model for key agreement. Using this model, the common conference key is derived for *v* members.

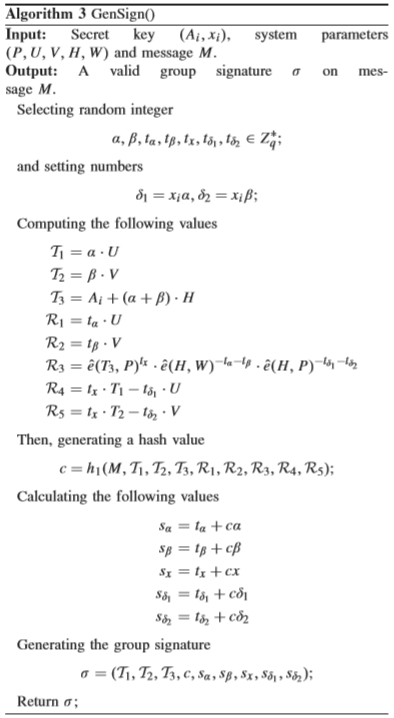
* 1. **Key Generation**
* In this step, 2 rounds are required to generate common conference key for all the team members.
* The way messages are generated is based on the (v, k + 1,1)-design.
* If the number of members cannot meet the structure of SBIBD, many messages will be missing in key generation.
* Therefore, some volunteers will be introduced to support data sharing with an arbitrary number of group members in the cloud, and a common conference key will be generated among them.
* These volunteer members will be selected by the Group Manager based on how active and trustable the members are.
* Hence, members with a good reputation can be volunteer blocks to complete the SBIBD.
* All the members need to submit their ID to the Group Manager to register themselves and receive the secret key.
* After the process of selecting and registering volunteers is done, the system needs two rounds to generate a common conference key for everyone.
* 

Figure 10.2 Algorithm for Generating Signature

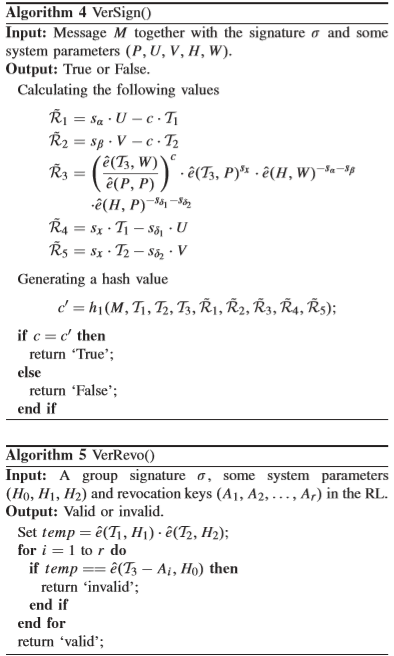


Figure 10.3 Algorithm to verify signature

* GenSign ()
* This algorithm is used to generate the signature key for every member in the cloud group. (figure 10.2)
* VerSign ()
* When a user tries to access the data, his identity is authorized by authroizing the signature key the user holds. (figure 10.3)
* VerRevo ()
* When a user’s signature key and the key present in the group manager’s registry do not match, system denies access to the user. (figure 10.3)

In short, volunteer is a virtual member in a conference who helps the real members complete some calculations and transfer information.

**10.3 Fault Detection**

* In the system, it cannot be guaranteed that there will be no users with malicious intent.
* These members can destroy the conference by generating different sub keys with the same group.
* Consequently, group members may generate different conference keys.
* The group manager is needed to ensure that each member generates a different conference key so that the conference will not be destroyed or delayed by any malicious users.

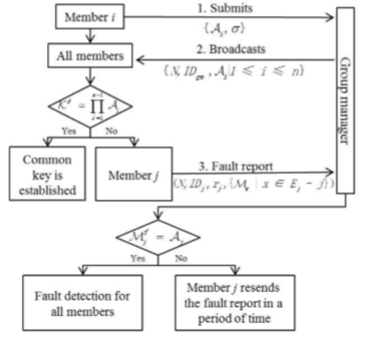
****

Figure 10.4 Block Design for Fault Detection

As shown in figure 10.4, during initialization, each member *i* needs to submit *Ai = Mf i* together with the group signature *σi* to the group manager. The group manager then broadcasts his identity key and the signature key of the respective member to him/her. Every member then checks the authenticity of the key broadcasted to it. If the equation is true for all members, then a common conference key K is established among all members. Otherwise, fault detection is performed to resist the different key attack. A fault report is sent to the group manager. The malicious member will then be restricted by the group manager. After the fault detection phase, an authenticated common conference key is derived among all the honest members. honest member will not be removed from the conference, while a malicious member will be detected and removed from the conference. The position of malicious members is filled in by volunteer. Therefore, the proposed scheme can not only resist the different key attack from malicious members but also provide the property of fault tolerance.

* 1. **Traceability**

When an argument is generated for a data file, the group manager receives the signature of the user on the file. In case of any dispute, or if any malicious activity takes place, the group manager can trace back the data back to the malicious user. The group manager can then reveal the identity of the malicious user if necessary. This is possible because the group manager has the User ID of all the users in his registry.

**Chapter 11 - Conclusion and Future Scope**

In the referenced paper, the authors have presented a secure, anonymous and fault-tolerant key agreement for group data sharing in a cloud storage scheme. The security of the outsourced data and the support to the cloud system for secure data sharing is possible only because of the SBIBD and group signature technique. Authentication services and efﬁcient access control are achieved with respect to the group signature technique. The system can also support the feature of traceability due to which any malicious content uploaded by a malicious user can be traced back to him/her. The group manager can also choose to reveal the identity of the malicious user in case of any dispute. Due to the key agreement and efﬁcient access control, the computational complexity and communication complexity for updating the common conference key and the encrypted data are relatively low.

There is a very wide scope for Cloud Computing in a group in the future. Various fields such as medicine, research, and military can benefit from the use of cloud computing as it will guarantee them unlimited storage and less complicated storage systems. The various challenges which Cloud Computing faces as of now will lead to more research in the field giving rise to solutions to those challenges which in turn will strengthen the security and stability of Cloud Computing. Data can be more freely shared among multiple users while having a moderator administer the exchange of data. Hence, in the future we will see a huge boom in the field of Cloud Computing being integrated in various systems thus leading to greater interconnectivity across various software and interfaces.

**13. References**

[1] J. Yu, K. Ren, C. Wang, and V. Varadharajan, “Enabling cloud storage auditing with key-exposure resistance,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.

[2] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly veriﬁable databases with efﬁcient updates,” IEEE Trans. Depend. Sec. Comput., vol. 12, no. 5, pp. 546–556, Sep. 2015.

[3] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New algorithms for secure outsourcing of modular exponentiations,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.

[4] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based data sharing for resource-limited users in cloud computing,” Comput. Secur., vol. 72, pp. 1–12, Jan. 2018, doi: 10.1016/j.cose.2017.08.007.

[5] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, “Block design-based key agreement for group data sharing in cloud computing,” IEEE Trans. Depend. Sec. Comput., to be published, doi: 10.1109/TDSC.2017.2725953.

[6] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, “FRR: Fair remote retrieval of outsourced private medical records in electronic health networks,” J. Biomed. Inform., vol. 50, pp. 226–233, Aug. 2014.

[7] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, “A lightweight multi-layer authentication protocol for wireless body area networks,” Future Generat. Comput. Syst., vol. 78, pp. 956–963, Jan. 2016, doi: 10.1016/j.future.2016.11.033.

[8] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.

[9] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, “Veriﬁable computation over large database with incremental updates,” IEEE Trans. Comput., vol. 65, no. 10, pp. 3184–3195, Oct. 2016. [10] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, “An efﬁcient public auditing protocol with novel dynamic structure for cloud data,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and ﬁne-grained data access control in cloud computing,” in Proc. Conf. Inf. Commun., 2010, pp. 1–9.

[12] X. Yi, “Identity-based fault-tolerant conference key agreement,” IEEE Trans. Depend. Sec. Comput., vol. 1, no. 3, pp. 170–178, Jul. 2004.

[13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.

[14] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” Eurocrypt, vol. 1403, pp. 127–144, May 1998.

[15] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, “Privacypreserving outsourced classiﬁcation in cloud computing,” in Cluster Computing, 2017, doi: 10.1007/s10586-017-0849-9.

[16] H. Wang, B. Qin, Q. Wu, and L. Xu, “TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2340–2351, Nov. 2015.

[17] X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: Secure multi-owner data sharing for dynamic groups in the cloud,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[18] J. Shen, S. Moh, and I. Chung, “Identity-based key agreement protocol employing a symmetric balanced incomplete block design,” J. Commun. Netw., vol. 14, no. 6, pp. 682–691, Dec. 2012.

[19] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure provenance: The essential of bread and butter of data forensics in cloud computing,” in Proc. ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS), Beijing, China, Apr. 2010, pp. 282–292.

[20] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and ﬁne-grained data access control in cloud computing,” in Proc. Conf. Inf. Commun., 2010, pp. 1–9.

[21] R. A. Brualdi, Introductory Combinatorics. Upper Saddle River, NJ, USA: Pearson Prentice-Hall, 2010

[22] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc. Annu. Int. Cryptol. Conf., 2004, pp. 41–55.

[23] Jian Shen , Member, Tianqi Zhou, Xiaofeng Chen, Jin Li and Willy Susilo, “Anonymous and Traceable Group Data Sharing in Cloud Computing”, IEEE Transactions on Information Forensics and Security, Vol. 13, No. 4, April 2018

[24] Bose, R. C. “A Note on Fisher's Inequality for Balanced Incomplete Block Designs.” [Ann. Math. Statist.](https://projecteuclid.org/euclid.aoms), Volume 20, Number 4

[25] Simon Liu, Rick Kuhn “Data Loss Prevention” [IT Professional](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6294) ( Volume: 12 , [Issue: 2](https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=5439500) , March-April 2010 ), pp 10-13

[26] Miller, K. W., Voas, J., & Hurlburt, G “BYOD: Security and Privacy Considerations” [IT Professional](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6294) ( Volume: 14 , [Issue: 5](https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6320581) , Sept.-Oct. 2012 ), pp 53-55