Efficient and Secured Data Sharing Schemes on Cloud for Access Control and Storage

S.P. Marke Y.M. Kurwade V ilas M. Thakare

Abstract- **With the rapid development of cloud computing, cloud storage has become a cost effective solution for many users with the demand of data storage. However there are two major concerns like whether it is secured to store private data in cloud and security issues in data sharing with other users. There are five techniques discussed here in this paper Encrypted data sharing scheme, Collaborative key management protocol in CP-ABE, Time Domain attribute based access protocol (TAAC), Revisited attribute based data sharing scheme, Broadcast group key management (BGKM) and its secure construction called ACV-BGKM etc. But some problems exist in these methods. So to overcome these problems that are given in analysis and discussion a new improved method is proposed.**

Keywords: Cloud computing, access control, security, privacy, data sharing, encryption, storage.

1. INTRODUCTION

Cloud computing has become a research hot-spot due to its distinguished long-list advantages. One of the most promising applications is on-line data sharing[1]. A data owner is usually willing to store large amounts of data in cloud. But without any data protection, cloud service provider(CSP) can gain access to all the data which brings out a potential security risk to the user[2]. Also any unauthorized user or intruder will be able to gain access to the data. This brings out the need for access control. Various data sharing schemes are present which can be used to increase the security and efficiency for the users in cloud computing[3,4,5]. There are five different techniques discussed in this paper which are Encrypted data sharing scheme, Collaborative key management protocol in CP-ABE, Time Domain attribute based access protocol (TAAC), Revisited attribute based data sharing scheme, Broadcast group key management(BGKM) and its secure construction called ACV-BGKM. These schemes provide security to the user data along with the access control policy ,privacy and efficiency to the users in cloud computing. But these methods have some limitations and so to overcome these problems an improved new scheme in cloud for access control and storage has been suggested which is "Advanced Attribute-Based Content sharing in Cloud" which guarantees sharing of both the data and multimedia contents.

2. BACKGROUND

Many studies on different schemes have been done to develop new schemes for secured and efficient data sharing in cloud. Different authors have proposed these schemes which have been in practice for the past years. Such schemes are : Encrypted data sharing scheme for secure cloud storage is proposed to achieve broadcast data sharing by taking advantage of broadcast encryption. This enables to directly share the encrypted data to the target users without the intervention of data owner while keeping data privacy which enables to achieve better performance in data sharing [1]. Collaborative key management protocol in CP-ABE (Ciphertext Policy Attribute Based Encryption) for cloud data sharing is proposed. to issue and store private keys without adding any extra hardware. This scheme solves the keyescrow problem and key exposure and reduces the client decryption overhead [2]. Time Domain attribute based access protocol (TAAC) is proposed for secure sharing of cloud based video content. A time domain attribute based encryption scheme is used to control the users of who can decrypt the video contents. This scheme is probably more secure in generic group model and efficient in practice [3]. Revisited attribute based data sharing scheme is proposed to solve the key-escrow issue and improve the expressiveness of the attribute so as to make the scheme more friendly in cloud computing applications. The complexity for access control is reduced and both the storage cost and encryption is reduced [4]. Broadcast Group Key management scheme and its secure construction called as ACV-BGKM is proposed to give some secrets to users based on the identity and then later allow them to derive actual symmetric keys based on their secrets. This schemes provide an efficient approach for access control for documents in an untrusted cloud file storage [5].

This paper introduces five different schemes for data sharing in cloud. These are Encrypted data sharing scheme, Collaborative key management protocol in CP-ABE, Time domain attribute based access protocol (TAAC), Revisited Attribute based data sharing scheme, Broadcast Group key management and its secure construction called as ACVBGKM.

These are organized as follows.

Section I Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on mobility models. **Section VI** proposed method and VII outcome result possible. Finally **section VIII** Conclude this review paper

3. PREVIOUS WORK DONE

In research literature, various schemes have been studied for efficient and secure data sharing in cloud and improve the performance in terms of security, privacy and access control. Linmei Jiang et al.(2014) [1] has proposed an encrypted data sharing scheme for secure cloud storage. This achieves the broadcast data sharing with the help of broadcast encryption and this schemes is proven to provide data privacy, improve the sharing performance and efficient to be used by the users. Guofeng Lin et al.(2017) [2] has presented the collaborative key management protocol in ciphertext policy attribute based encryption (CP-ABE) for cloud data sharing. Theses schemes solves the key-escrow problem and gives better performance in terms of cloud based data sharing on mobile devices. Kan Yang et al(2016). [3] has proposed the time domain attribute based access control for the secure sharing of video contents. The time domain attribute based encryption scheme to allow only specified users to decrypt the video contents. This scheme is provably more secure in generic group model and is efficient in practice. Shulan Wang et al.(2016) [4] has presented the revisited attribute based data sharing scheme not only to solve the key-escrow issue but also to improve the expressiveness of the computing applications. This scheme reduces both the storage cost and encryption complexity and also able to achieve efficient and secure data sharing in cloud computing. Mohamed Nabeel et al.(2013) [5] has proposed a new key management scheme called broadcast group key management (BGKM) and then gave its secure construction of a BGKM scheme called ACV-BGKM. The idea here is to give some secrets to the user and later allow them to derive symmetric keys based on their secrets and other public information. This scheme provides an efficient approach for encryption based access control for documents in an untrusted cloud file storage.

4. EXISTING METHODOLOGIES

There are several different schemes implemented for data sharing in cloud for past several decades which are used by a large number of users in cloud computing applications. The different schemes discussed here are : Encrypted data sharing scheme, Collaborative key management protocol in CP-ABE, Time domain attribute based access protocol (TAAC), Revisited attribute based data sharing scheme, Broadcast group key management (BGKM) and its secure construction ACV-BGKM.

4.1 Encrypted Data Sharing scheme :

Encrypted data sharing scheme is used where data is shared among different users and security is of great concern. This scheme achieves broadcast data sharing with the use of broadcast data encryption technique. The broadcast data encryption technique is a cryptographic access control technology where the data is transferred from one to many such as TV, video conference, etc. Broadcast encryption is of two types one is symmetric and other is asymmetric. This encrypted data sharing scheme works for the dynamically changing size of the users. This scheme is analysed for its security and storage costs. Hence it is more suitable for data sharing in cloud storage environment [1].

4.2 Collaborative key management protocol in CP-ABE:

Ciphertext policy attribute-based encryption (CP-ABE) is a promising cryptographic technique for fine-grained access control of outsourced data in the cloud. However there are some drawbacks present which hinder the popularity of the application. So a new improved scheme is proposed which is a collaborative key management protocol in CP-ABE. It allows for the storage of private keys without adding any extra hardware. This scheme not only solves the key escrow problem but also the key exposure and it also reduces the client decryption overhead. It shows better performance in terms of cloud-based outsourced data sharing on mobile devices [2].

4.3 Time Domain Attribute-Based Access Control :

With the ever-increasing demands on multimedia, cloud computing due to its convenient and resources has become a natural platform to process, store and share video contents. Time domain attribute-based access control scheme is proposed to allow the secure sharing of video contents. This scheme works by embedding the time into both the ciphertexts and keys and only the users who have sufficient attributes can decrypt the video contents. It allows to achieve dynamic change of user's attributes. TAAC scheme is provably more secure and efficient in practice [3].

4.4 Revisited Attribute-Based Data Sharing scheme :

Ciphertext policy attribute-based encryption (CP-ABE) is a very promising encryption technique for secure data sharing in cloud computing. The data owner is fully control the access policy associated with the data which is to be shared. However, CP-ABE is limited to have potential risk that is known as keyescrow problem. So, this data sharing scheme is revisited to solve the key-escrow problem so as to make the resulting scheme more friendly in cloud computing applications. This revisited scheme lightens the complexity of access policy and both the storage cost and encryption complexity are relieved. This proposed scheme achieves efficient and secure data sharing in cloud computing [4].

4.5 Broadcast Group Key Management :

While sharing data in public clouds an important security concern comes when sharing documents and control the access policies. One approach is to encrypt documents but this approach has several weaknesses. So based on this idea, a new key management scheme called broadcast group key management (BGKM) and then give a secure construction of BGKM scheme called ACV-BGKM. The idea used here is used to give some secrets to the users based on the identity attributes and later allow them to derive actual symmetric keys based on their secrets and some public information. In this scheme adding users and updating apps can be done performed efficiently. This scheme provides an efficient approach for fine-grained encryption-based access control for documents in an untrusted cloud file storage [5].

5. ANALYSIS AND DISCUSSION

The Encrypted data sharing scheme which is based on conditional proxy broadcast re-encryption scheme is analysed for the security and shown it is secured against the semitrusted CSP. It allows dynamically to add the users and remove from the cloud [1]. Collaborative key management protocol in CP ABE when compared with the traditional attribute-based encryption algorithm is proven to enhance security and efficiency in cloud data sharing [2]. Time Domain Attribute Based Access control is analysed for secure sharing of video contents in cloud computing environment. This scheme is analysed under the metrics of storage overhead, computation and communication cost and provides better performance in terms of security and efficiency [3]. Revisited Attribute-Based Data Sharing scheme is given to solve the key-escrow issue and fully control the access policies associated with the data to be shared. It enhances data confidentiality and privacy in cloud system [4]. Broadcast group key management (BGKM) scheme enables the users to selectively share documents in an untrusted cloud environment. It provides an efficient approach and guarantees enhanced security along with access control policies while sharing the documents [5].

Mobility scheme	Advantages	Disadvantages
Encrypted Data Sharing scheme	This scheme provides the security and decreases the storage costs. It supports the dynamically changing size of users thereby giving better performance of data sharing in cloud environment.	The efficiency of this scheme is little slower .
Collaborative key management protocol in CPABE	This proposed methodology solves not only the key escrow problem but also key exposure. It provides better performance in terms of outsourced data sharing on mobile devices.	The drawback of this method is its increases ciphertext size, increased encryption and decryption costs.
Time Domain Attribute-Based Access control	This scheme enables to securely share video contents in cloud environment. This method is secure and efficient in practice.	This method is not well suited for real cloud based multimedia systems.
Revisited Attribute Based Data sharing scheme	This scheme solves the key escrow problem and is more friendly in cloud applications. It enhances data confidentiality and privacy in cloud systems.	Larger attribute sized which is employed in the scheme can increase the complexity
Broadcast Group key management	This scheme and its secure construction ACV-BGKM provides securely sharing documents in an untrusted cloud environment. It can support large number of users.	This method does not support traitor tracing and privacy preserving querying capabilities.

TABLE 1: Comparisons between different mobility schemes

6. PROPOSED METHODOLOGY

Different data sharing schemes are available for sharing data in cloud environment. With its cost effectiveness and large scale networks, data sharing in cloud has increased on a large scale. But with this benefit comes up with a lot of issues which are needed to be addressed effectively. For ex. data sharing in cloud should preserve the privacy of the users, provide security, less complexity, less space used and decreased costs. Different methods discussed here address different problems based on different parameters. To address the various problems associated with data sharing we propose an efficient and secure data sharing schemes on cloud which is “Advanced Attribute- Based Content Sharing in Cloud” . This proposed scheme provides the access control and storage policies in cloud. For ex. consider a client in cloud wants to share documents and multimedia contents to another user then this scheme will work as follows : When the multimedia contents are transferred, a time domain attribute encryption scheme embed the time so that only authorized users can access the contents. The attribute updating method supports the dynamic change of users. The two party issuing protocol guarantees the authority of the users key. Also the BGKM scheme is used here to effectively share the documents in an untrusted cloud environment. This proposed scheme provides both the access control and storage function in cloud computing applications. The algorithm which is given below defines the flow of the method.

Basic steps of algorithm:

Step1: The client sends a multimedia content message in the cloud environment to the other user.

Step2: Then the contents are encrypted using the time domain attribute based access control scheme for secure sharing of multimedia contents. This will enable us to limit the contents only to authorized users.

Step3: Then the update method and BGKM is applied to support the dynamic number of users in cloud and thereby assuring the security and privacy of both the sending and receiving users.

Step4: Thus the contents encrypted by using this proposed scheme is sent over the network to the receiver.

Step5: The receiving user thus receives the desired content which are sent by the sending client. Diagrammatic representation of proposed method is shown as follows:

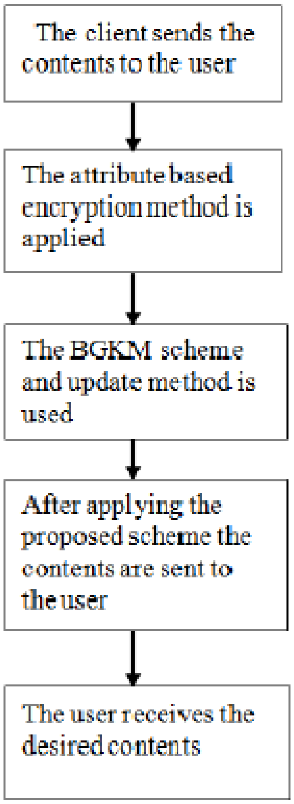
The client sends the contents to the user
The attribute based encryption method is applied
The BGKM scheme and update method is used
After applying the proposed scheme the contents are sent to the user
The user receives the desired contents

Fig 1: Flow of the Algorithm showing the proposed scheme

7. OUTCOME AND POSSIBLE RESULTS

In this way the proposed method can be used to effectively share not only data but also the multimedia contents and documents in a secure manner. This scheme guarantees both the access control and storage functionalities for content sharing. It also supports the dynamic changing of the users so that large number of users can be supported.

8. CONCLUSION

This paper focused on the study of various data sharing schemes i.e. Encrypted Data Sharing scheme, Collaborative key management protocol in CP-ABE, Revisited Attribute-Based Data Sharing scheme, Time Domain Attribute-Based Access Control scheme, Broadcast Group Key management and its secure construction called ACV-BGKM. But these schemes have some drawbacks in each of it. So to overcome this we have proposed "Advanced Attribute-Based Content Sharing in Cloud" . This scheme provides for both the data and multimedia content sharing in cloud. .

9. FUTURE SCOPE

From observations of the proposed method, in our future work we will implement this scheme for simultaneous sharing of contents by different users to other users in many-to-many manner.

.

ACKNOWLEDGEMENT

This technical paper is supported by all the teaching and nonteaching staff of our department. I am also grateful to Y.M. Kurwade for his assistance who moderated this paper and improved the manuscript significantly. I also express my immense gratitude to V.M. Thakare for sharing his pearls of wisdom and giving the suggestions which helped to make this paper.

REFERENCES

[1] Mohammad Tahooni, Amir Darehshoorzadeh, AzzedineBoukerche, "Mobility-based Opportunistic Routing for MobileAd-Hoc Networks", *ACM,* 10.1145/2653481.2653485, September 2014.

[2] Guofeng Lin, Hanshu Hong, Zhixin Sun, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute- Based Encryption for Cloud Data Sharing", *IEEE ACCESS,*Vol. 5, June 2017

[3] Kan Yeng, Zhen Liu, Xiaohua Jia, Sherman Shen, "Time- Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach" *IEEE TRANSACTIONS ON MULTIMEDIA,*Vol. 18, No. 5, May 2016.

[4]Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, Weixin Xie, "Attribute-BasedData Sharing Scheme Revisited in Cloud Computing", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,*Vol. 11, No. 8, August 2016.

[5]Mohamed Nabeel, Ning Shang, Elisa Bertino, "Privacy Preserving Policy-Based content Sharing in Public Clouds", *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING,*Vol. 25, No. 11, November 2013.