INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN : 2057-5688

MULTIPLE AUDIT QUALITIES BASED ON DISCOVERY OF ENCRYPTED CLOUD DATA

[1]Athukuri Amaranagalakshmi, [2]P. Venu Babu

[1]MTech Student, Dept of CSE, Malineni Lakshmaiah Women's Engineering College, Guntur,A.P, India

[2]Assistant Professor, Dept of CSE,Malineni Lakshmaiah Women's Engineering College, Guntur,A.P, India

Abstract: *Cloud computing provides flexible and welcome access to information distribution, which generates many advantages for network and private use. However, there is a natural protection for users to instantly outsource shared information to the cloud due to the fact that events often involve vital records. Although it causes many security issues, cloud service providers are not on the same level with users. To preserve the privacy of information for CSP files that are not based on them, contemporary responses enforce encryption techniques (for example, encryption techniques) and release decryption keys only to legal clients. However, the exchange of data within the cloud between authorized customer's remains challenging, especially on the subject of dynamic user companies. Most studies of dynamic institutional records trading in the cloud have been run using several algorithms, including ABE (entire feature-based cryptography) and CP-ABE to provide greater protection in dynamic cloud clusters with more than one script. But they still face challenges, both loss of performance and dependence on a reliable server, and they are not suitable for distribution with the problem of getting rid of jobs. Thus, the canceled user cannot get shared data before and after. To solve this in particular, in this paper, we present a suitable Multi-authority CP-ABKS (MABKS) device to handle such limits and reduce the computational and garage load on resource-limited devices in cloud structures. Additionally, the MABKS device has been expanded to support malicious feature authority tracking and feature update. Our rigorous protection evaluation shows that the MABKS is selectively comfortable in both matrix-selective and feature-selective models. Our experimental results using real global data sets show the performance and utility of the MABKS machine in real-world programs.*

ISSN : 2057-5688

Keywords: *Identity Based Encryption, Revocation, Revocable Attribute-Based Encryption, Fine-grained access*.

I. INTRODUCTION

Cloud computing is a model that offers large computing space and a huge memory space at low cost [1]. Allows users to get the expected support regardless of time and position on different platforms (for example, mobile devices and personal computers), thus, provides excellent convenience for cloud users. Among the many cloud computing help, cloud storage help, such as Apple iCloud , Microsoft Azure, and Amazon S3, can help provide an easy and easy way to share data over the Internet, which offers many benefits to our society. But also suffers from various security threats, which are the main concerns of cloud users. First, the outsourcing of data to the cloud server indicates that data is out of control of users. This can cause the user to delay because external data generally includes basic and sensitive data. Second, data is frequently shared in an open and obnoxious environment, and the cloud server will be the victim of attacks. More, the cloud server itself can detect user data for illegal revenue. Third, data distribution is inactive. That is, when user support ends, he / she must no longer control the prerequisites for obtaining shared data before and after. Therefore, when outsourcing data to the server in the cloud, customers must also manage access to such data so that only currently authorized users can receive data outsourcing.

One of the core services offered by CSPs is data storage. Despite the benefits of cloud storage, it faces many challenges that can hinder its rapid growth if left unresolved. Think of a practical application that allows a company to store and share data to its employees or departments through the cloud. With the cloud, the company can completely free itself from the local burden of storing and maintaining data. However, this also poses a security risk to data privacy. In particular, users do not trust CSP completely, while the data files stored in the cloud can be encrypted and encrypted. To solve this problem, the basic solution is to encrypt the data and then upload the encrypted data to the cloud. However, traditional encryption methods for data sharing in the cloud are not efficient or flexible. Easy to use advanced, advanced encryption methodology that allows maximum sharing of storage resources that allows sharing of data at a particular level. One of the most intelligent tools to control precise access and exchange

ISSN : 2057-5688

encrypted data is the use of Attribute Encryption (ABE) [2]. However, applying ABE directly to real applications is not easy due to many practical concerns.

In a multi-Authority cloud storage system, user features can be dynamically changed. The user may be entitled to some new functions or revoke some existing functions. You need to change your data access permissions accordingly. However, the current methods for canceling attributes are based on a reliable server or a lack of performance, they are not enough to solve the problem of cancellation control in controlling access to data in a multi-cloud storage system.

Dynamic user groups are very common in cloud applications, for example, due to user expiration or user membership changes and theft / compromise / misuse of user credentials. In dynamic user groups, Revoked users is a major security issue that needs to be addressed correctly. However, the problem with handling user deletions in cloud storage is that the Revoked user can still decrypt the old encrypted text that was allowed before it was revoked. To resolve this issue, you will need to update encrypted text stored in the cloud storage, such as by the ally cloud server (untrusted). In the literature, proxy encryption [3] has been suggested to replace authorized decryption of encrypted text, and this method has been included in ABE [4] to encrypt encrypted text by one third. Can be updated (for example, CSP for cancellation purposes). However, the proxy encryption policy requires that encryption / updates be released to the CSP to allow encrypted text updates. From a practical use point of view, it is highly advisable for CSPs to update a cryptographic text frequently, without the need for any context key.

II. REVIEW OF LITERATURE

Many encryption schemes, including IBE, only provide access control. It limits users' ability to select the encrypted data to a certain level. Cipher text Policy Attribute-Based Encryption (CP-ABE) Features [5] is a promising technology designed to control access to encrypted data. There are two types of CP-ABE systems: a CP-ABE authority [6] where all attributes are managed by the same authority and multiple CP-ABE authorities Features are from different domains and are managed by different authorities. CPABE is a multi-Authority system that is easier to access in the cloud storage system, where users can perform multiple options and data owners use the fine-grained access policy outlined in various authorities' attributes. And share the data. However, due to the issue of revocation, these multi-authority CP-ABE schemes cannot be implemented

ISSN : 2057-5688

directly from multiple agencies to control data access to the cloud storage system. It is proposed to rely on certain attribute Revocation schemes based on a reliable server to achieve attribution level cancellation. We know that data owners cannot rely solely on cloud servers, so methods for eliminating traditional attributes are no longer suitable for cloud storage systems.

Li Lin et.al [6] As for Lin et.al, Cloud computing is important for data privacy protection, as privacy leaks can prevent users from using cloud services. To ensure the confidentiality of the data, we recommend Priguarder, a new way to overcome access while recognizing confidentiality. This process involves three steps of the cloud service: user registration, data creation and data access. At each stage, users can choose two ways to interact with the cloud service provider, either directly or indirectly. With indirect format, a resource deployment system has been introduced to ensure user identity and confidentiality of attribute features across all three stages. In addition, new access control protocols have been proposed to streamline interaction between users and cloud service providers, taking advantage of data encryption and timestamp technologies. We describe the use of our methodology in the context of Amazon S3. A comprehensive theoretical analysis and simulation experiments were performed, which showed the effectiveness of the Priguarder.

Xiaoyu Li et.al.[7] The proposed ABE can satisfy the default access control function in the cloud storage system, especially for encrypted text policy attributes. Since user privileges can be issued by multiple authorities, a popup encryption is primitive for enforcing attribute-based access control over external data encryption in a multi-authority encrypted text policy. - However, many of the current authorities' system-based systems are not immune to the burden of cost overruns and the cancellation or depletion of costs in cost accounting. In this document, we propose a feature-based access control system for multi-authority cloud storage systems with two-factor protection. In our proposed scheme, any user can retrieve outsourcing data if and only if they have sufficient encrypted attribute keys with respect to the access policy and the permissions key in relation to the outsourcing data. In addition, the proposed scheme features fixed-size encrypted text and a small account cost. In addition to accepting attribute level cancellations, our proposed plan allows the data owner to cancel at the user level. Safety analysis, performance comparisons and experimental results show that our proposed scheme is not only safe but also practical.

ISSN : 2057-5688

Sushmita et.al [8] Precise access control is a requirement for data stored on cloud-like servers. Due to the large amount of data, decentralized key management plans are better than central schemes. Encryption and decryption are often very expensive and inefficient when users access data from a limited resource. We propose a Attribute Based Encryption (ABE) with fast encryption and external decryption. The main idea is to divide encryption into two stages, the initial processing step that is offline when the device is not in use and when the online step is when the data is encrypted with the policy. This makes encryption faster and more efficient than existing decentralized ABE schemes. For outsourcing decryption, data users must. An encrypted version of the decryption key has to be created that allows an untrusted proxy server to partially decrypt encrypted text into plain text information. Data users can decrypt partially encrypted text without an expensive pairing.

III. PROPOSED MABKS MECHANISM

In light of these issues, we call for an Attribute-Based Multi-Authority Keyword Research (MABKS) scheme for cloud systems to mitigate challenging situations due to performance bottleneck of unmatched points and high compute and garage needs (which is unrealistic for devices with limited resources).).). Figure 1. Shows the main differences between the multiple authority structure within the MABKS system and the single authority structure in the current schemes. Specifically, each AA within the MABKS device maintains the full feature set and is responsible for validating customer data. Certificates and intermediate secret keys generation for statistic clients, and the Certificate Authority (CA) generates the latest mystery keys for DU units. For example, a more practically connected branch (acting as a CA) in a large employer can generate complete secret keys for legal personnel to access important corporate business files, yet it can be confused with a large number of overheads when there is an overwhelming number of employees, Or even affected by a bottleneck in the performance of the individual worker if this branch is hacked or broken.

Algorithm1: $\boldsymbol{KU\ Nodes}$ $(\boldsymbol{BT},\boldsymbol{RL},\boldsymbol{t})$:

1. $X,Y \leftarrow \emptyset$
2. $for\ all(\eta_t,t_i)\epsilon RL\ do$
3. $\boldsymbol{if}\ t_i \leq t\ \boldsymbol{then}$

4. Add $\boldsymbol{Path}$ (η_i) to X
5. $end\ if$
6. $end\ for$
7. $\boldsymbol{for\ all}\ \theta\ \in \boldsymbol{X\ do}$
8. $if\ \theta_l\ \notin \boldsymbol{X\ then}$
9. $Add\ \theta_l\ to\ Y$
10. $\boldsymbol{end\ if}$
11. $if\ \theta_r\ \notin \boldsymbol{X\ then}$
12. $Add\ \theta_r\ to\ Y$
13. $\boldsymbol{end\ if}$
14. $\boldsymbol{end\ for}$
15. $\boldsymbol{if\ Y = \theta\ then}$
16. $Add\ the\ root\ note\ \varepsilon\ to\ Y$
17. $\boldsymbol{end\ if}$
18. $\boldsymbol{return\ Y}$

Our proposed MABKS Uses Binary Tree Structure to get proficient Revocation To explain the revocation procedure, we offer several signs first. root Specify the root node ε. Binary tree $\boldsymbol{BT}$, and set of nodes on $\boldsymbol{Path}(\eta)$. The path from ε to leaf node η (including ε and η) Without leaf node $\boldsymbol{\theta}$, we'll let it stand on the left θ_l and right child θ_r sides, respectively.

Here given time period is t and the revocation List is RL.

η_t,t_i , indicates that the node η_t and revoked time period is t_i and the algorithm provide output is Subset Y.

Total number of time periods T is comprised of the following polynomial time algorithms:

$\boldsymbol{Setup}(\mathbf{1}^{\lambda}, \boldsymbol{T}, \boldsymbol{N})$**:** Setup algorithm takes as input. Security parameter λ , bound time T and the Number of maximum system users is N, and it returns the results Public parameter PP and master secret key MSK, and it is connected with Revocation list $RL = \emptyset$ and State st.

$\boldsymbol{PKGen}(PP, MSK, ID)$**:** PP, MSK takes as an input by a private key Generator Algorithm and Identity $ID \in$ I and it produced a private key SK_{ID} for ID and updated list st.

ISSN : 2057-5688

$\boldsymbol{KeyUpdate}(PP,MSK,RL,t,st)$: this algorithm takes input as a MSK,PP and Key update time $t \leq T$, Revocation List RL, state st and the output is KU_t.

$\boldsymbol{Encrypt}(ID,t,PP,M)$: it takes input as a $identity\ ID, PP$, and time period $t \leq T\ and\ message\ M \in M$ to be encrypted. The output is $CT_{ID,t}$.

$\boldsymbol{DKGen}(SK_{ID},PP,KU_t)$: Here, this algorithm takes input as a KU_t , SK_{ID} and PP and Generates the Decryption is as a $DK_{ID,t}$ for ID with time t.

$\boldsymbol{CTUpdate}\left(CT_{ID,t},PP,t^{'}\right)$: $PP,CT_{ID,t}$ and time period are taken as a input by Cipher text algorithms and time period $t^{'} \geq t\ and\ its\ output\ updated\ ciphertext\ CT_{ID,t}$

$\boldsymbol{Revoke}(ID,RL,PP,st,t)$: this algorithm takes an identity $ID \in I\ \ to\ be\ revoked$, PP as a Input and revocation list RL and revocation time $t \leq T$, state st and its update RL to a new one

$Algorithm2$: $CTEncode$

1. $\boldsymbol{function}\ CTEncode(\boldsymbol{t},\boldsymbol{T})$
2. $t \leftarrow TEncode(t,T)$
3. $chk \leftarrow false$
4. $\boldsymbol{for}\ i \in [log_2\ T]\ \boldsymbol{do}$
5. $\boldsymbol{if}\ t[i] = 1\ and\ chk = false\ \boldsymbol{then}\ t[i] = 1$
6. $\boldsymbol{else}$
7. $\boldsymbol{chk} \leftarrow true$
8. $t[i] = 0$
9. $\boldsymbol{end\ if}$
10. $\boldsymbol{end\ for}$
11. $\boldsymbol{return}\ t$
12. $\boldsymbol{end\ function}$

Here,

$Time\ \boldsymbol{t}$

bounded system life time T are input and,

ISSN : 2057-5688

bit string t of the size $log_2 T$

The above algorithm is used to reduce the complexity of the space. Processing the Cipher text and the Cipher Text Delegation

SYSTEM ARCHITECTURE:

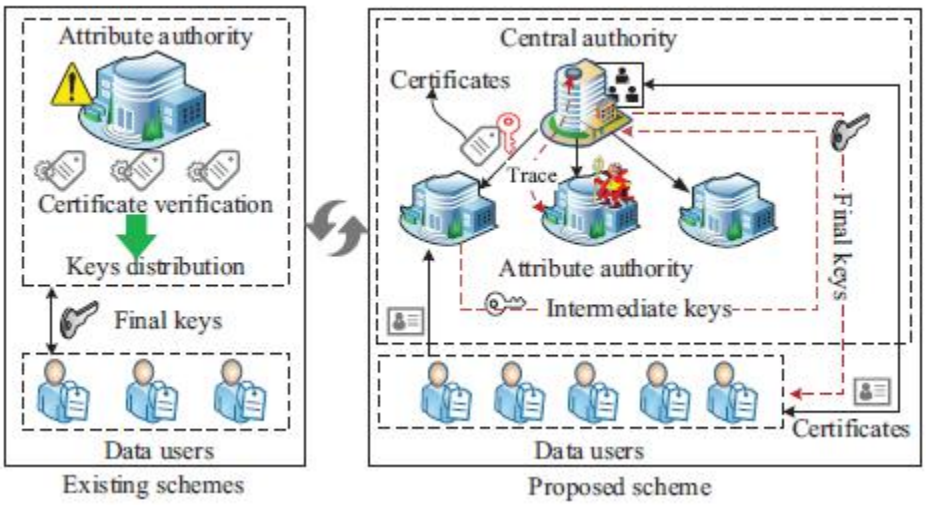

Fig.1 System model

The company can rent multiple public servers (that act as AAs) provided by other enterprises (i.e., Tencent, Amazon, Alibaba, etc.) to eliminate the fully-trusted department's computation burden (see Fig. 2) . However, these public servers may execute malicious operations and then return incorrect intermediate secret keys in order to save computation and bandwidth resources, as these servers and the fully-trusted department of this company are not in the same trusted domain. Furthermore, we cannot deploy multiple fully-trusted AAs in scheme constructions due to high communication overhead caused by building security channels. Fortunately, the CA in our MABKS system can trace the malicious AA. However, the traditional multi-authority CP-ABE schemes cannot achieve this goal, and even cannot avoid the possibility of single-point performance bottleneck that also exists in single-authority CP-ABE schemes. In summary, the main contributions of the MABKS system are shown as follows

A commercial company can employ several public servants (in their capacity as AA) provided by different companies (such as Tencent, Amazon, Alibaba and many others) to eliminate the

ISSN : 2057-5688

computational burden of the entire authorized department (see Figure 2). However, these public servers can perform malicious operations and then return invalid intermediate ambiguities, which is a good way to store bandwidth and compute assets, since these servers and a fully affiliated branch of this company are not in the same trust zone. Also, we cannot fully configure multiple supported AAs in schematic structures due to the high cost of conversation due to the creation of protection channels. Fortunately, the CA on our MABKS machine can hint at malicious AA. However, traditional multi-power CP-EBA schemes cannot achieve this intent, nor can they even avoid the chance of a single point overall performance bottleneck that also exists in CP-EBA power schemes. Not connected. In summary, the main contributions of the MABKS machine are demonstrated as follows

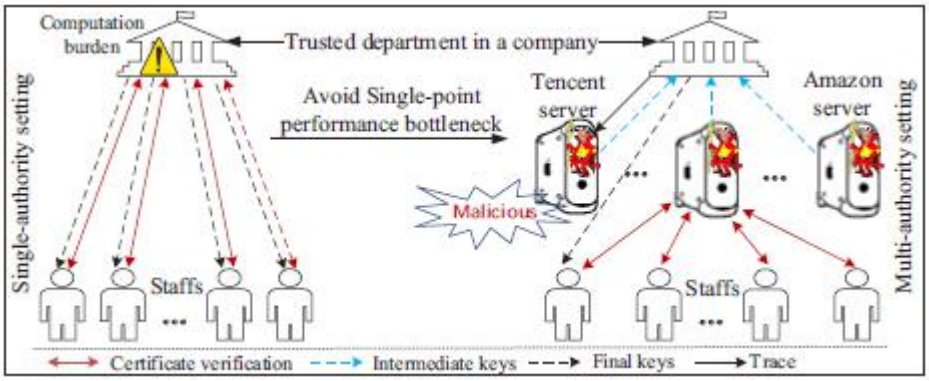

Fig.2 An example for the multi-authority scenario

RESULTS AND DISCUSSIONS

Table 1. Execution time for Encryption in ABE, CP-ABE, MABKS

File size (KB)	ABE (ms)	CP_ABE (ms)	MABKS (ms)
15	1020	940	700
17	1050	960	803
20	1110	1070	920
24	1250	1130	1120
27	1405	1380	1340
30	1650	1510	1480

ISSN : 2057-5688

Table.1 show Execution time for file Encryption in various algorithms like ABE, CP-ABE, and MABKS. The file size taken in the KB and Execution time taken in milli seconds format.

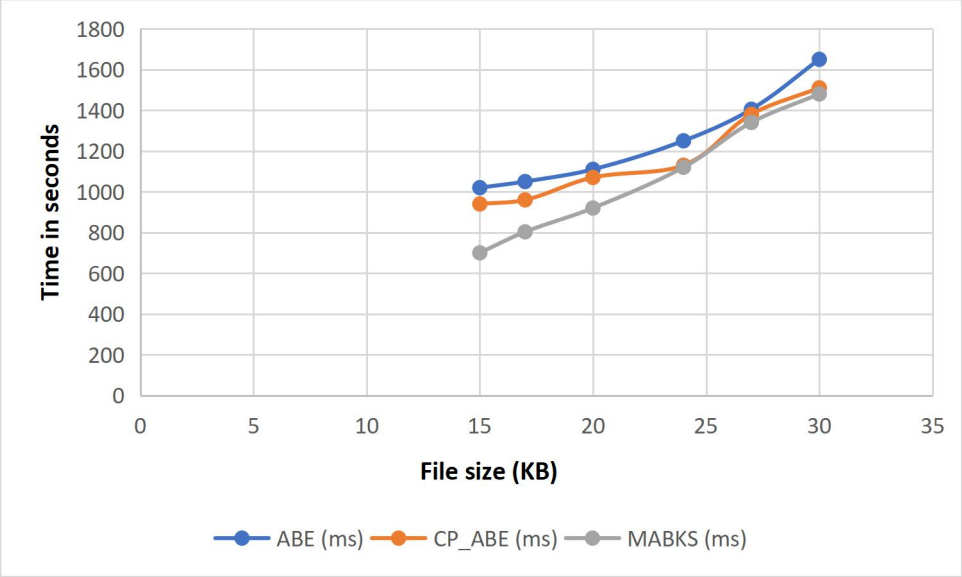

Fig.3 Execution time for Encryption Vs File size

Fig.3 shows comparison between various algorithms like, ABE, CP-ABE, and MABKS . Here x-axis indicates about File size between various algorithms and Y-axis indicates Execution time for Encryption. As shown in the chart Proposed MABKS algorithm can take less execution time for File Encryption compare with previous algorithms.

Table.2 Execution time for Decryption in Various algorithms

File size (KB)	ABE (ms)	CP_ABE (ms)	MABKS (ms)
15	820	720	510
17	890	960	700
20	910	840	675
24	1020	970	790
27	1305	1180	995

ISSN : 2057-5688

30	1560	1360	1060

The above Table shows Execution time for Decryption between ABE,CP-ABE, and MABKS.

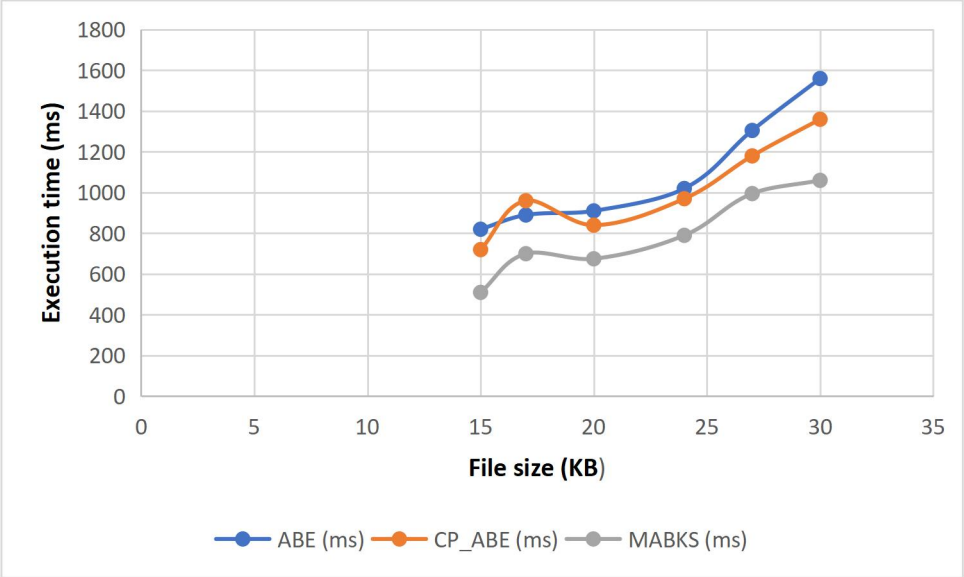

Fig.4 Execution time for Decryption and File size

Figure 4 shows the comparison between different algorithms such as ABE, CP-ABE, and MABKS. The X-axis here indicates the file size between different algorithms, and the Y-axis indicates the execution time for encryption. As suggested in the chart, the MABKS algorithm may take a shorter execution time compared to the earlier algorithm in file encryption.

IV. CONCLUSION:

In this paper, we proposed an environmentally friendly and potential MABKS device to help several authorities, so that one can avoid a performance bottleneck at a point that is unparalleled in cloud structures. Furthermore, the supplied MABKS allows us to hint at malicious AAs (eg to prevent collusion attacks) and help replace features (e.g., to prevent unauthorized access using legacy ambiguity keys). We then demonstrate the device selective integrity phase in a selective

ISSN : 2057-5688

matrix and feature selective models according to parallel q decisions BDHE and DBDH assumptions, respectively. In addition, we evaluated the system's overall performance and confirmed that garage value deductions and a full-size account were completed, unlike previous ABKS schemes. However, the main drawback is that the MABKS device cannot help with expressive search queries, including related keyword search, fuzzy search, subgroup search, etc. Future work will learn to build efficient and flexible indexing so that the MABKS system will be able to support different queries.

V. REFERENCES

[1] P. Mell and T. Grance, ‘‘The NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption,’’ in Proc. IEEE Symp. Security and privacy (S&P’07), 2007, pp. 321-334.

[3] B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,’’ in Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.

[4] V. Goyal, A. Jain,O. Pandey, andA. Sahai, ‘‘Bounded Ciphertext Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008,

pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ‘‘Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’10, 2010, pp. 62-91.

[6] Li Lin, Ting-Ting Liu, Shuang Li, Chathura M. Sarathchandra Magurawalage, Shan-Shan Tu, "PriGuarder: A Privacy-Aware Access Control Approach Based on Attribute Fuzzy Grouping in Cloud Environments", Access IEEE, vol. 6, pp. 1882-1893, 2018

ISSN : 2057-5688

[7] Xiaoyu Li, Shaohua Tang, Lingling Xu, Huaqun Wang, Jie Chen, "Two-Factor Data Access Control With Efficient Revocation for Multi-Authority Cloud Storage Systems", Access IEEE, vol. 5, pp. 393-405, 2017.

[8] Sourya Joyee De, Sushmita Ruj, "Decentralized Access Control on Data in the Cloud with Fast Encryption and Outsourced Decryption", Global Communications Conference (GLOBECOM) 2015 IEEE, pp. 1-6, 2015.