International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10577-10583
© Research India Publications. http://www.ripublication.com

Secure Data Retrieval Scheme in Cloud Computing Using Homomorphic Cryptographic Approach

N. Madhusudhana Reddy[1]
*[1]Research Scholar, Department of Computer Science and Engineering,
Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh, India.
Associate Professor, Department of Computer Science and Engineering,
Rajeev Gandhi Memorial college of Engineering and Technology, Nandyal, Andhra Pradesh, India.*

Dr. C. Nagaraju[2]
[2]Associate Professor, YSR Engineering College, Yogi Vemana University, Proddatur, Andhra Pradesh, India.

Dr. A. Ananda Rao[3]
*[3]Professor of C and Director of Academic and Planning, Jawaharlal Nehru Technological University, Ananatapur,
Andhra Pradesh, India.*

Abstract

Homomorphic encryption technology can settle a dispute of data privacy security in cloud environment, but there are many problems in the process of access the data which is encrypted by a homomorphic algorithm in the cloud. In this paper, on the premise of attribute encryption, we propose a fully homomorphic encrypt scheme which based on attribute encryption with LSSS matrix. This scheme supports fine-grained cum flexible access control along with "Query-Response" mechanism to enable users to efficiently retrieve desired data from cloud servers. In addition, the scheme should support considerable flexibility to revoke system privileges from users without updating the key client, it reduces the pressure of the client greatly. Finally, security analysis illustrates that the scheme can resist collusion attack. A comparison of the performance from existing CP-ABE scheme, indicates that our scheme reduces the computation cost greatly for users.

Keywords: Homomorphic encryption; access control; attribute revocation; ciphertext retrieval;

INTRODUCTION

Cloud computing has almost unlimited computing power and storage space as distributed computing technology. However, due to the cloud data out of the user's control, the use of these data in the process must be to ensure data privacy and effective access control. In order to solve the problem of data privacy and carry out effective operation, we can perform data by fully homomorphic encryption. Fully homomorphic encryption satisfied f(Enc(μ))=Enc(f(μ)). This property is consistent with the needs of cloud computing model such as cloud computing security, ciphertext retrieval etc. Therefore, it has great theoretical significance and application value to study the homomorphic encryption.

In recent years, fully homomorphic technology has developed rapidly. The implementation of access control strategy requires a trusted entity method in traditional access control, but cloud service providers no longer trusted, so the Data Owner (DO) needs to encrypt data before upload it. In order to realize access control effectively of encrypted data, we can use CP-ABE. The scheme construct a policy based multi user homomorphic encryption scheme[21] which satisfies the homomorphic operation and the demand of data sharing among the users. However, in the revocation, the data owner must encrypt the relevant documents in time and update the key to the users involved to ensure that the revocation of the authority of the user cannot decrypt the relevant documents the data that give users a large amount of calculation. In the Scheme [2] an access control scheme is proposed to support the outsourcing and decryption which makes the DO doesn't need to be encrypted in real time during the process of revocation[1][7]. There is no need to re-encrypt the ciphertext, and the attribute revocation will not affect the other users who have not been revoked.

Although the classic CP -ABE scheme can achieve fine-grained access, it does not support the ciphertext retrieval service, and the full homomorphic encryption scheme can achieve ciphertext retrieval. However, it is vulnerable to chosen plaintext attack. Based on the advantages of the two, we construct a ciphertext policy access scheme which supports ciphertext retrieval scheme with the revocation attribute in the Cloud Service Provider(CSP)[23]. This scheme based on strategy using fully homomorphic encryption witch support for multi-user computing and sharing of ciphertext, fine grained access control, and realize the DO does not need to stay online during the key revocation, it reduces the impact on related users' legal decryption, finally we given a ciphertext retrieval scheme in accordance with the encryption algorithm.

RELATED WORK

A. Fully Homomorphic Encryption

Beginning in 2009, homomorphic encryption scheme has been proposed. In the literature [3-7], by compressing the decryption circuit to reduce the depth of the circuit and use homomorphic decryption to reduce the noise so that fully homomorphic encryption finally accomplishes. But the construction method of these schemes complexity is high. The literature [4] constructs a homomorphic encryption scheme based on LWE (Learning with Error) . This scheme is more efficient, but the public key size is still too large[15]. The data recipient of the above program is a single user, and the user's data sharing and data access control problem do not be considered.Fig.1 shows the model of encryption and decryption of data which is stored and retrieved from cloud.

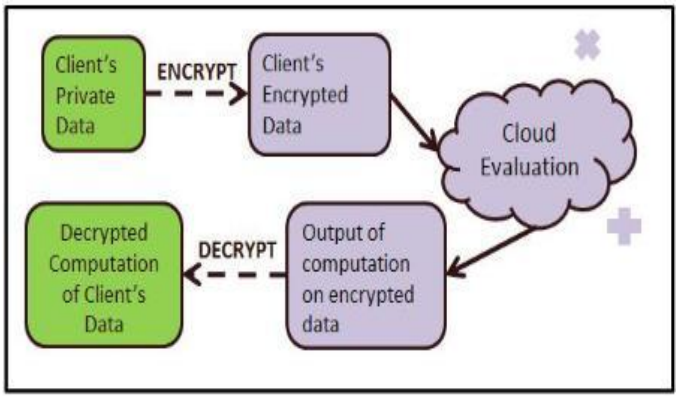

Client's Private Data
ENCRYPT
Client's Encrypted Data
Cloud Evaluation
Decrypted Computation of Client's Data
DECRYPT
Output of computation on encrypted data

Figure 1: Encryption and decryption model

B. Attribute Encryption

Attribute encryption achieves fine-grained access control of data [5]. The core of access control scheme based on the attribute is how to split the secret into several sub secrets, and map each sub secret to different access control attribute sets. Sahai and Waters et al [6] do pioneering work in the attribute code, its theoretical basis is derived from (n, t) threshold secret sharing. The combining of Threshold secret sharing and access strategy through two basic forms in general, one is the secret sharing tree based on Lagrange interpolation method; another is the sharing of matrix [8] based on the linear secret sharing schemes (LSSS). LSSS converting access strategy and secret into a matrix which attribute associated with party. Compared with the Lagrange interpolation method, LSSS efficiency is improved greatly in calculate the value of secret sharing. That reduces the amount of calculation of the amount of the secret recovery by matrix operation. Recently, it has been widely applied [9].The process of performing encryption using attributes is clearly illustrated in Fig.2.

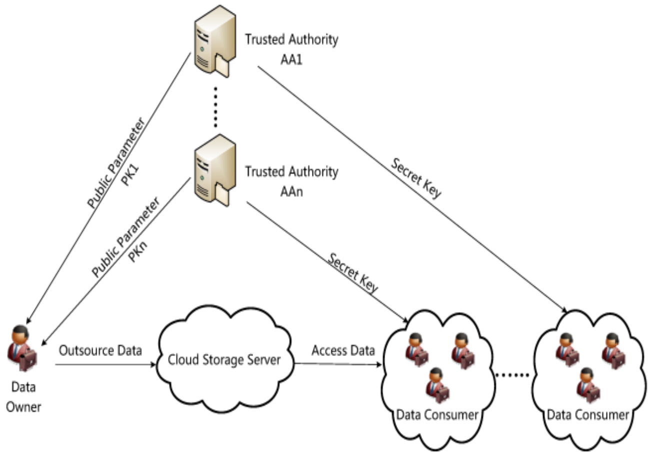


Figure 2: Attribute Based Encryption

CLOUD DATABASE

“Pay as you go“ is a trend followed in today's cloud computing environment. It means users just have to pay only for the services used. Nowadays cloud database services are emerging as one of the most important services among cloud computing [12]. When large distance has to be covered and data has to be transferred per terabyte, it costs much. That is why cloud database become popular as it provides numerous advantages.

Cloud Database provides low and cheap cost availability to customers. Because of cloud computing characteristic features, for new applications cloud computing provides best and economical way to set up and help many small scale business to come up which were previously not able to come up due to financial problem in old traditional method [29]

Cloud Database as a Service

Database Management System is an application which provides the creation, management of the database. Professionals can enter new records, update, modify and delete data whenever required. Users can handle all tasks related to data, also insertion and modification. Reports, query, and tables are all parts of database handling software called database management software[16][28].The concept of cloud computing in olden times was being composed of five characteristics, four deployment models and three service models but in today's scenario, it is being extended and more categories have been added like Storage-as-a-Service, Security-as-a-Service and Database-as-a-Service [30]. In recent times, an important part of the cloud is a scalable database which comprises updating of work and decision system.

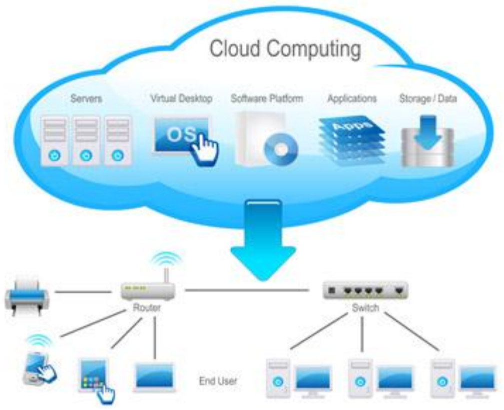


Figure 3: Cloud service architecture

The way the data was being saved and retrieved is being changed with the emergence of cloud database. Given a cost price, servers and applications like database are provided as cloud services. In changing trend, many technical advantages like no need to spend money in physical setup of database offices and handling tasks because resources are available as services online.Fig.3 describes the levels of cloud architecture in which a user can store the data securely and it can be retrieved safely. Now the requirement of having data centers is finished as cloud database provide service easily. Users may also make own applications which are possible because of resources being provided by PaaS model to cloud databases.

Requirements of cloud database management in cloud

Whether an organization has been taken, a research center, or any education center it remains the primary needs to process data fast and in an efficient manner. For this purpose, institutes plan and manage database processing tasks so as to handle work of database such as installing, maintaining tasks[6]. Database related tedious tasks are very much difficult to manage and a small problem left will turn out complicated , rather than buying hardware and products related to database ,connecting the networks along with employing experienced persons it will be better to make use of cloud database services because of inexpensiveness and easier and effective management of database related tasks .

Financial investment tends not to change as different hardware, software and networks costs may decrease but costs of people managing such complicated tasks continue to increase. It may happen that professionals costs will dominate over the solution to database handling costs [31]. For having an arrangement of data, the database needs to be restructured, makeup with some alterations, restored, take a backup, to make adjustments for spacing. There is not much development in the area when there no impact on the accessibility of database solution, and still movement from one database to next becomes possible [32]. Because moving up from one database to next makes some components unavailable to use.

Locations where computers and related components are being housed or data centers more precisely, are using database management systems. But much earlier it was up to the developers to select the type of database for the cloud and perform the installing and managing tasks. They also need to deal with the complicated administration tasks on their own [33]. Positive aspects are full control is provided as a selection of own database and its dealing can be done. PaaS Service dealers now provide up with database services on a cloud in order to reduce the workload of cloud customers and the work is taken over by cloud provider who takes care of controlling everything starting from the handling of logs to recovering and backing up of all records. The developer needs to deal up to table and query maintenance. Sometimes there is an organization which takes up tasks of database services[9][18].

For the creation, storage and management of database tasks there are many database service providers. Rather than using organization computing infrastructure, customers can access data using hardware and software by the service provider. Now positive aspects are many, like it may happen that at database service providers side there may be a changing in software, hardware or networking side or there may be a failure but the customers will have no effect on the problem because it will be dealt with database service providers side[3][10]. Generally, the organization just takes into use system for database services whose administration is done by service providers. Now there is no need for buying, modifying, updating and performing such tasks related to the database by cloud customers.

Whether it is financial, business, or any internet related work, database is needed everywhere for some or the other purpose. The old method, which is known as a traditional database system[8] which was much in use. Several disadvantages of this database systems are –

1) Difficult maintenance works

2) Scalability and configuration problems

3) Complication in choosing from the available systems

4) Cost price of some systems much more than expected

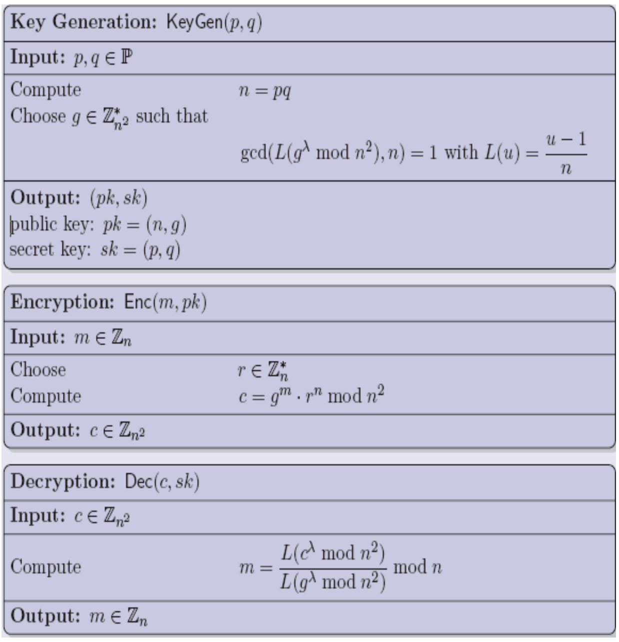
So these disadvantages are tackled up by the cloud-based Database as a service. In today's scenario, any DBaaS features cannot find out that is able to cope up with all the disadvantages. So there will be next boom of an evolution of database [34].

Fully Homomorphic Encryption scheme

C. Gentry proposed Fully Homomorphic Encryption scheme [11]. In this scheme, there is no need for decryption in order to do any processing of any function on encrypted data, so this method allows computation over data which is in encrypted form. Before data is stored at the server, using Fully Homomorphic Encryption, data is encrypted. Whenever there is a need for query execution, an equivalent query is developed over encrypted data. So processing work is now performed over encrypted data as any valid SQL query which is being sent to a server and processed and returns result (encrypted) to a client. Here it is decrypted back to get an answer.

This is a good approach but processing work may be slow [12]. Another kind of method which can be used is to make the client as encrypted data storage. Data gets stored at the server but before that, it is encrypted by a client. So for query processing work, the needed database part is converted to decrypted form and shifted on the client machine. Now database which was previously encrypted is now converted to plain text database on which query can be processed upon to get output. This is useful technology but because of shifting of the needed relations in databases, there is a huge load on working as traffic gets increased. So issues related to performance are generated. Maintaining of own databases servers at client side becomes necessary here but it hides the DAAS model benefits.

There are big industries and companies where lakhs of people work and lakhs of people are associated with customers for services. There is a large amount of information related to this, which is critically necessary for the execution of all works. But leakage of this data is also possible, for this maintaining security[35] becomes an everyday necessity. As query execution at server successfully along with maintaining privacy is becoming the real requirement. This gave a direction to our work.Some related techniques related to cloud databases taking the above requirement can be classified into software based and hardware based techniques.



Key Generation: $\mathsf{KeyGen}(p, q)$

Input: $p, q \in \mathbb{P}$

Compute $n = pq$

Choose $g \in \mathbb{Z}^*_{n^2}$ such that

$$\gcd(L(g^\lambda \bmod n^2), n) = 1 \text{ with } L(u) = \frac{u-1}{n}$$

Output: (pk, sk)

public key: $pk = (n, g)$

secret key: $sk = (p, q)$

Encryption: $\mathsf{Enc}(m, pk)$

Input: $m \in \mathbb{Z}_n$

Choose $r \in \mathbb{Z}^*_n$

Compute $c = g^m \cdot r^n \bmod n^2$

Output: $c \in \mathbb{Z}_{n^2}$

Decryption: $\mathsf{Dec}(c, sk)$

Input: $c \in \mathbb{Z}_{n^2}$

Compute $m = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$

Output: $m \in \mathbb{Z}_n$

The proposed algorithm is used for key generation in which the key is used only by the user who want to retrieve data from the cloud so that the data is securely transferred to the customer and then the user have to decrypt it for making use of the data.

CryptDB

It is the software based approach. Here encryption of each attribute is performed in separation. Schemes used are as follows:

1) RND – This is randomized scheme for encryption which not includes ciphertext operation
2) DET – This is a deterministic scheme for encryption which works as equality predicates.
3) OPE – This is a type of encryption scheme which maintains order preserving technique.
4) JOIN – This encryption scheme gives support to equijoins on cipher text.
5) SEARCH – Word search technique is used by this search scheme.

The main theme on which this Crypt DB was built is “onions". Like an onion is made up of a number of layers similarly here for a single data value many layers of encryption scheme are made. But this approach suffers from performance issues. As there are many layers of encryption for security but for each and every query all the layers of encryption have to be worked upon. So the execution becomes slower. Especially when it is the first time of execution, the layer of encryption has to be removed so it takes much longer time. The next execution takes less time but first time takes the most time and reduces performance.

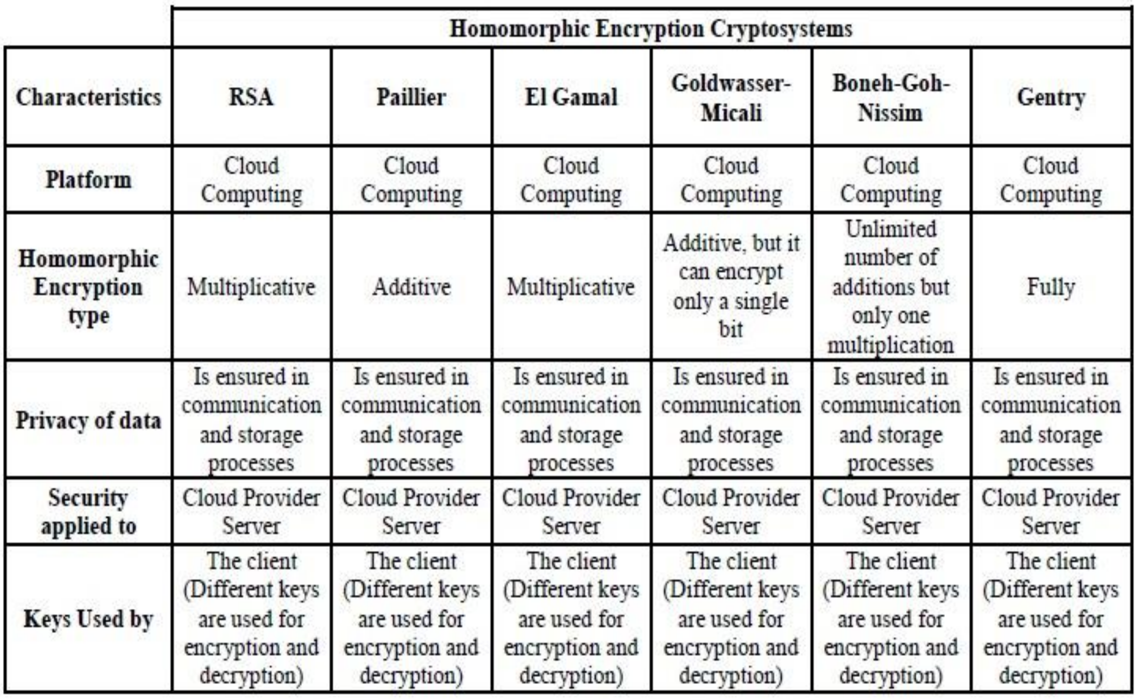
Though there is no need to maintain databases at client side in CryptDB but it supports very limited SQL constructs. For the practical usage in big industries there is a need for a cloud database model which can maintain privacy for many records and with very limited SQL constructs it is not possible, so it is not much in use.

RESULTS & DISCUSSIONS

In the table beneath we contrast distinctive Homomorphic Encryption cryptosystems concurring with the accompanying qualities:

- Homomorphic Encryption sort.
- The regard for protection of touchy information.
- If security is connected at the supplier of cloud or on client.
- Who utilize the encryption and unscrambling keys?

Table 4.1: Properties of Cryptosystems



	Homomorphic Encryption Cryptosystems					
Characteristics	**RSA**	**Paillier**	**El Gamal**	**Goldwasser-Micali**	**Boneh-Goh-Nissim**	**Gentry**
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Homomorphic Encryption type	Multiplicative	Additive	Multiplicative	Additive, but it can encrypt only a single bit	Unlimited number of additions but only one multiplication	Fully
Privacy of data	Is ensured in communication and storage processes	Is ensured in communication and storage processes	Is ensured in communication and storage processes	Is ensured in communication and storage processes	Is ensured in communication and storage processes	Is ensured in communication and storage processes
Security applied to	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server
Keys Used by	The client (Different keys are used for encryption and decryption)	The client (Different keys are used for encryption and decryption)	The client (Different keys are used for encryption and decryption)	The client (Different keys are used for encryption and decryption)	The client (Different keys are used for encryption and decryption)	The client (Different keys are used for encryption and decryption)

In 2009 Craig Gentry of IBM has proposed the primary encryption framework "completely homomorphic" that assesses a discretionary number of increases and duplications and along these lines figure any kind of capacity on encoded information. The cryptosystem of perceives a constraint comes from a blunder term that increments with every operation. Once the mistake resilience is surpassed, the outcome can't be unscrambled.

The proposed mechanisms is compared with the existing methodologies and the throughput is observed as low when compared to other schemes. The below figure illustrates the throughput time of the proposed and various existing encryption mechanisms.

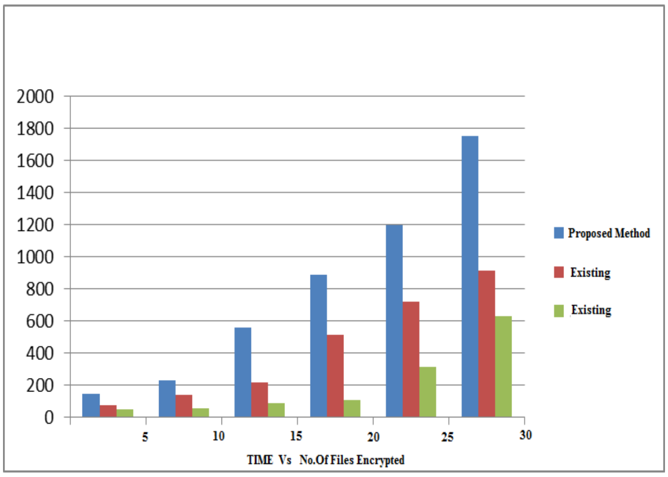


Figure 4: Throughput of the proposed method.

Performance Results of the proposed scheme

In MANETs the hubs are dependably progressing and there might be situations where the dynamic way may never again be dynamic and accordingly, the beneficiary may not get every one of the parcels sent by the sender. Fig 5 delineates the achievement rate of the systems with n dynamic ways and g bunches settled by arbitrarily executing the hubs. The hubs in the systems are collapsed haphazardly by utilizing Exponential appropriation gave by the capacity of hubs. From Fig 5 unmistakably the achievement rate increments by decreasing the quantity of gatherings in the system. This is on account of by lessening the quantity of gatherings in the system we would expand the quantity of dynamic ways in each gathering. Only one fractional message from each gathering is sufficient to recuperate the whole message. This is on the grounds that by expanding the quantity of ways in each gathering, the likelihood of one way in each gathering staying dynamic is high and with it the likelihood of recuperation of the message at the beneficiary is additionally high. The achievement rate step by step diminishes with the progressive increment in the quantity of gatherings in the system. Along these lines to get the achievement rate as 100% in the system it is smarter to diminish the quantity of gatherings, accordingly expanding the quantity of dynamic ways in each gathering.

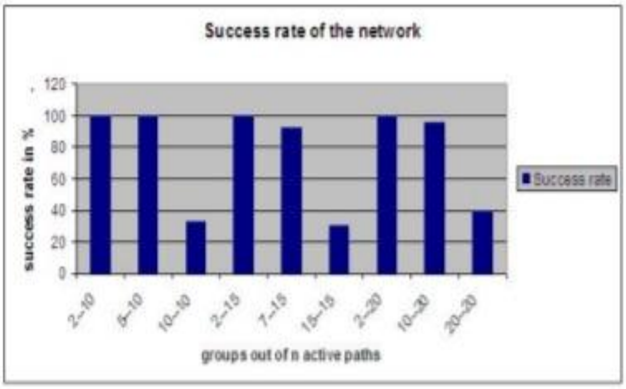


Figure 5: Rate of Success of established network

CONCLUSIONS

In this paper, we combine the advantages of CP-ABE and homomorphic encryption to construct a fully homomorphic encryption scheme with a fine-grained access control. The secret sharing matrix shared secret value which can represent arbitrary access structure, part of the implementation decryption of decryption by CSP and process of decryption with the high efficiency. In this paper, the secure sharing and ciphertext retrieval of multi-user in cloud environment are realized. Because the number of rows and the number of attributes are the same when the Boolean circuit is transformed into the corresponding LSSS matrix, when the set of attributes is large, the number of lines and the size of the ciphertext is relatively large, which affects the speed of encryption and decryption. The next step is to consider as much as possible the small Boolean access policy to the LSSS transformation scheme instead of the transformation in this paper to reduce communication costs.

REFERENCES

[1] Rajesh et. Al, International Journal of Advanced Research in Computer Science and Software Engineering 2(9),September -2012,pp. 115-120

[2] Gonzalez et al. Journal of Cloud Computing :Advances, Systems and Applications , 2012,1:11

[3] Shankland S, HP's Hurd dings cloud computing, 2009,IBM, CNET News.

[4] Catteddu D, Hogben G,Benefits, risks and recommendations for information security. Tech. rep., European Network and Information Security Agency, 2009,enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment

[5] CSA, Security Guidance for Critical Areas of Focus in Cloud Computing, Tech. rep., Cloud Security Alliance,2009

[6] Mather T, Kumaraswamy S,Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance,2009,1st edition. O'Reilly Media

[7] Chen Y, Paxson V, Katz RH,What's New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

[8] Mell P, Grance T,The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology, 2009,www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[9] Ibrahim AS, Hamlyn-Harris J, Grundy J, Emerging Security Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC,2010,Cloud Workshop, APSEC'10

[10] Catteddu D, Hogben G,Benefits, risks and recommendations for information security. Tech. rep., European Network and Information Security Agency, 2009,enisa.europa.eu/act/rm/files/deliverables/cloudcomputing- risk-assessment

[11] Tompkins D,Security for Cloud-based Enterprise Applications,2009. http://blog.dt.org/index.php/2009/02/security-for-cloud-basedenterprise- applications/

[12] Jensen M, Schwenk J, Gruschka N, Iacono LL,On Technical Security Issues in Cloud Computing,2009, In: IEEE Internation Conference on Cloud Computing. pp 109–116

[13] Hubbard D, Jr LJH, Sutton M, Top Threats to Cloud Computing. Tech. rep., Cloud Security Alliance,2010, cloudsecurityalliance.org/research/projects/top-threats-to-cloud-computing/

[14] TrendMicro, Cloud Computing Security - Making Virtual MachinesCloud-Ready. Trend Micro White Paper,2010

[15] Genovese S, Akamai Introduces Cloud-Based Firewall, 2009, http://cloudcomputing.sys-con.com/node/1219023

[16] Hulme GV, Cloud Passage aims to ease cloud server security management, 2011, http://www.csoonline.com/article/658121/cloudpassageaims-to-ease-cloud-server-security-management

[17] Oleshchuk VA, Køien GM, Security and Privacy in the Cloud – A Long-Term View. In: 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless Vitae), Wireless Vitae,2011, pp 1–5, http://dx.doi.org/10.1109/Wireless Vitae.2011.5940876

[18] Google,2011, Google App Engine. code.google.com/appengine/

[19] Google, Google Query Language (GQL), 2011. code.google.com/intl/en/appengine/docs/python/overview.html

[20] StackOverflow , 2011 , Does using non-SQL databases obviate the need for guarding against SQL injection?stackoverflow.com/questions/1823536/does-using-non-sql-databasesobviate-the-need-for-guarding-against-sql-injection

[21] Rose J, 2011 ,Cloudy with a chance of zero day. www.owasp.org/images/1/12/Cloudy with a chance of 0 day Jon Rose-Tom Leavey.pdf

[22] Balkan A ,2011, Why Google App Engine is broken and what Googlemust do to fix it. aralbalkan.com/1504

[23] Balkan A , 2011,Why Google App Engine is broken and what Google must do to fix it. aralbalkan.com/1504

[24] Salesforce, 2011, Salesforce Security Statement. salesforce.com/ company/privacy/security.jsp

[25] Espiner T,2007,Salesforce tight-lipped after phishing attack.zdnet.co.uk/news/security-threats/2007/11/07/salesforce-tight-lipped-after-phishing-attack-39290616/

[26] Yee A, 2007 ,Implications of Salesforce Phishing Incident.ebizq.net/blogs/securityinsider/2007/11/-implications of salesforce phi.php

[27] Salesforce , 2011 , Security Implementation Guide.login.salesforce.com /help /doc/en/salesforce security impl guide.pdf

[28] Li H, Dai Y, Tian L, Yang H ,Identity-Based Authentication for Cloud Computing. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom , 2009.

[29] Amazon ,Elastic Compute Cloud (EC2), 2011. aws.amazon.com/ec2/

[30] Kaufman C, Venkatapathy R, 2010,Windows Azure Security Overview. go.microsoft.com/?linkid=9740388

[31] McMillan R ,2010,Google Attack Part of Widespread Spying Effort. PCWorld

[32] Mills E ,2010, Behind the China attacks on Google. CNET News

[33] Arrington M ,2010,Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations. TechCrunch

[34] Bosch J, 2009,Google Accounts Attacked by Phishing Scam. BrickHouse Security Blog

[35] Telegraph T, 2009 , Facebook Users Targeted By Phishing Attack. The Telegraph.