International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

File Data Sharing in Multiple Blocks in Cloud using TTP

Bethala Shirisha & Bethala Pravallika
[1]Assistant Professor, MTech, Department of CSE, CMRIT,JNTUH
[2]Assistant Professor, MTech, Department of IT, IARE, JNTUH
E-mail: [1]shirishasai34@gmail.com, [2]pravallika03@gmail.com

ABSTRACT *Cloud computing is an Internet-based computing. Computing services, such as data, storage, software, computing, and application, are delivered to local devices through Internet. The major security issue of cloud computing is that the cloud provider must ensure that their infrastructure is secure, and that prevent illegal data accesses from outsiders, other clients, Or even the unauthorized cloud employees. In this paper, we deal with cloud security services including key agreement and authentication. By using Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing, we design the secure cloud computing (SCC). Two types of SCC are proposed. One requires a trusted third party (TTP), and the other does not need a TTP. Also, our SCC can be extended to multi-server SCC (MSCC) to fit an environment, where each multi-server system contains multiple servers to collaborate for serving applications. Due to the strong security and operation efficiency, the proposed SCC and MSCC are extremely suitable for use in cloud computing.*

Keywords: Elliptic Curve Diffie-Hellman (ECDH), multi-server SCC (MSCC), secure cloud computing (SCC), Trusted third party (TTP)

1. INTRODUCTION

Cloud computing is a type of Internet-based computing, and it is one of the foundations of the next generation of computing. Computing services, such as data, storage, software, computing, and application, are delivered to local devices through Internet . In cloud computing, the service is fully served by the provider and the client needs nothing but a personal device and Internet access. The cloud computing can either be hosted on-site by the company or off-site such as Microsoft's SkyDrive, Google Drive, Samsung's S-Cloud service, Apple's iCloud, Amazon's Cloud Drive. Recent applications, e.g., multimedia streaming, virtual reality, and robotics , have used cloud computing provide the services. Also, platforms like Google Apps (e.g., Gmail, Google Groups, Google Calendar, ...), YouTube, Vimeo, Flickr, Slideshare and Skype adopt the cloud computing technology. As cloud computing becomes more and more popular, how to secure cloud computing and protect data security deserves studying. Some issues in cloud computing security are surveyed and studied.

For providing cloud services, the sensitive data for all clients should be stored in the cloud host. At this time, the data security and the personal privacy should be assured. The cloud provider should guarantee these data and personal information in host database against all accesses of the unauthorized insiders or the malicious outsiders.

Accordingly, some secure cloud computing schemes based on secret sharing approach were proposed. For example, the PASS (data Privacy by Authentication and Secret Sharing) in prevents client's data privacy from the unauthorized access. The PASS adopts public key cryptosystem to encrypt its share, and this increases the transmission cost. PASS chooses not to store the secret key (shared between the client and the cloud server) anywhere in the cloud because of the secret isolation guideline.

However, the client needs to store the secret key because the cloud server does not send its share to the client. So, if the client's device is compromised (for example the local computer or the smart card is cracked) then the secret key will leak out.

In this paper, we deal with cloud security services including key agreement and authentication described in, and solve the above weaknesses of PASS. By using symmetric bivariate polynomial based secret sharing, we design the secure cloud computing (SCC). Two types of SCC are proposed. One requires a trusted third party (TTP) in the cloud like the scheme in , and the other does not need a TTP. Also, our SCC provides mutual authentication to avoid connecting the fake server. The proposed SCC can be extended to multi-server SCC (MSCC) to fit an environment, where each multi-server system contains multiple servers to collaborate for serving applications. Due to the strong security and operation efficiency, the proposed SCC and MSCC are extremely suitable for use in cloud computing.

The paper is organized as follows. Section II gives some preliminaries. Two types of SCC are introduced in Section III, and the MSCC (the extension of SCC) is proposed in Section IV. Performance evaluation and security analysis are shown in Section V, and Section VI is conclusion.

2. PRELIMINARIES

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

- Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
- It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
- When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1) Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2) Select methods for presenting information.
3) Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

Multi cloud storage

Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computer's processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks . the cloud user upload the data into multi cloud. cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a *multi-Cloud* .A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

Cooperative PDP

Cooperative PDP (CPDP) schemes adopting zero-knowledge property and three-layered index hierarchy, respectively. In particular efficient method for selecting the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers. cooperative PDP (CPDP) scheme without compromising data privacy based on modern cryptographic techniques

Data Integrity

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Third Party Auditor

Trusted Third Party (TTP) whois trusted to store verification parameters and offerpublic query services for these parameters. In our system the Trusted Third Party, view the user data blocks and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data blocks. If any odification tried by cloud owner a alert is send to the Trused Third Party.

Cloud User

The Cloud Userwho have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data.the User's Data is converted into data blocks . the data blocks is uploaded to

the cloud. The TPA view the data blocks and Uploaded in multi cloud. The user can update the uploaded data. If the user wants to download their files, the data's in multi cloud is integrated and downloaded.

3. TYPES OF SCC

In this paper, we propose two types of secure cloud computing: one is SCC and the other is MSCC. Also, the key sharing in both SCC and MSCC can be implemented with using TTP and without using TTP, respectively. Here, we show two scenarios where our schemes can be applied:

(i) single server or multi server (SCC or MSCC)

(ii) using TTP or not using TTP (with TTP or w/o TTP) for key sharing.

i) SCC or MSCC:

In SCC, a cloud server can provide services to customers alone. For some applications, the services need to be accomplished through different servers. In MSCC, a service provider may organize resources and builds appropriate multiserver systems to provide various services to customers. Each multi-server system contains multiple servers, which can be devoted to serve one type of service requests and applications.

However, more servers increase authentication cost when using SCC approach. Our MSCC is based on SCC, and uses the same approach through summation homomorphism. Therefore, when customers submit service requests to a service provider, the service provider determines adopting SCC (single server) or MSCC (multiple servers) for providing services.

As we know, everything on one server (singleserver environment) is easy for setting up an application quickly. However, it offers little in the way of scalability and component isolation. Suppose that application and database contend for the same server resources. This case may cause poor performance. To prevent this problem, a multiple-server environment is the most common application scenario. For example, we may install Microsoft Internet Information Services (IIS) and Microsoft SQL Server on different computers. On the other hand, cloud computing is a large-scale distributed computing paradigm where computing resources are available to users. Therefore, a multi-server environment has the good scalability.

Here, we use an example of integrating multi servers to improve the performance in cloud computing to demonstrate our advantage. For example, we can adopt the approach of using load balancers to implement the server setups in cloud computing. Via distributing the workload across multiple servers, we can enhance not only the performance but also the reliability. When one of the servers fails, other servers will handle the traffic until it recovers from a server failure.

ii) With TTP or w/o TTP:

When using TTP to implement the key sharing phase, we need a secure channel, e.g., VPN, and this enhances the transmission cost. Also, we need a third party in SCC/MSCC. If we use ECDH in key sharing phase, we do not need TTP. However, Diffie Hellman-like protocol will be compromised by the so-called clogging attack, in which an opponent sends a public Diffie Hellman key to the AS. The AS then computes the secret key. Repeated messages of this type can clog AS with useless work. As a result, AS spends considerable computing resources for doing useless computation.

4. Performance and Security Analysis

Next, we discuss the following issues to compare the proposed SCC, and the proposed MSCC in detail

Shares sent from server and client:

our SCC and MSCC can share an intermediate key between the client and the cloud servers. The client can use the symmetric encryption (e.g., AES) to send his share to the cloud server. Also, the cloud server can send data to the client. our scheme only uses symmetric encryption to transmit share between AS and the client. Finally, we save the encryption/decryption cost.

Homomorphism property in MSCC:

In the present cloud environment, some applications may need different collaborated severs. When directly applying SCC for multi-server environment, the authentication should be repeated M times for a multi-server system including M servers. Via the homomorphism property, our MSCC can authenticate M servers simultaneously in one operation. For key recovery, if using SCC for multi-server environment, we need M secret keys for these M servers. In MSCC, the homomorphism property lets the client share one common secret key with these M servers.

Security Analysis

Our SCC has two types: one is with TTP and the other is without TTP. It is reasonable that TTP is assumed to be honest and is trusted by the client and the cloud server. For the SCC without TTP, we adopt ECDH to securely share the bivariate polynomial. Both types assure of securely sharing bivariate polynomial between the client and the cloud server. The main objective of the proposed SCC/MSCC is to prevent malicious insiders in cloud server and outsiders to login the authorized account and determine the secret key.

We first define the scope of the security issues that our SCC and MSCC discuss:

(i) outsider attack,

(ii) insider attack.

(iii) server side attack, and

(iv) client side attack.

Here, we use outsider and insider to represent the attacker who is unauthorized and authorized to the cloud server. For example, a hacker in the Internet is an outsider, while a malicious cloud employee is an insider.

The difference between the protocols with TTP and without TTP is only the generation of bivariate polynomial. So, we only give security analysis for SCC and MSCC for each security issue.

Outsider Attack:

An attacker from outside the perimeter is not authorized to access the cloud database. He can only intercept the information from the public channel, i.e., can only collect x-coordinates of the shares for the client and the cloud server.

5. Literature survey

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

6. CONCLUSION

In this paper, we propose two types of SCC: one is with TTP and the other is without TTP. The main objective of our schemes is to protect the data privacy and security in the Cloud server. We add the symmetric property in secret

sharing to successfully reduce the cost to share the shares between the client and the server. Also, by the homomorphism property of secret sharing, we extend SSC to MSCC fitting the multi-server environment. When compared with the previous PASS, our schemes have the better security and performance.

7. REFERENCES

[1] National Institute of Standards and Technology, "The NIST definition of cloud computing," Information Technology Laboratory, 2009.

[2] K. Stanoevska-Slabeva, T. Wozniak, and S. Ristol "Grid and cloud computing- a business perspective on technology and applications," Springer-Verlag, Berlin, Heidelberg, 2009.

[3] Z. Huang, C. Mei, L. Li, and T. Woo, "CloudStream: delivering highquality streaming videos through a cloud-based SVC proxy," Proc. Of 2011 IEEE Infocom, USA, 2011.

[4] C. Robertson, B. MacIntyre, B. Walker, "An evaluation of graphical context as a means for ameliorating the effects of registration error,"IEEE Transactions on Visualization and Computer Graphics, vol. 15, pp.179-192, 2009.

[5] Y. Chen, Z. Du, M. Garcia-Acosta, "Robot as a Service in Cloud Computing," Proc. of 2010 Fifth IEEE International Symposium on Service Oriented System Engineering, USA, 2010.

[6] T.K. Mendhe, P.A. Kamble, and A.K. Thakre, "Survey on security, storage, and networking of cloud computing, International Journal on Computer Science and Engineering, vol. 4, pp. 1780-1785, 2012.

[7] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 3, pp. 583-592, 2012.

[8] M.D. Ryan, "Cloud computing security: the scientific challenge, and a survey of solutions," The Journal of Systems and Software, (doi: http://dx.doi.org/10.1016/j.jss.2012.12.025), 2012.

[9] S.A. Almulla, and C.Y. Yeun, "New secure storage architecture for cloud computing," Communications in Computer and Information Science, vol. 184, pp. 75-84, 2011.

[10] D.J. Huang, Z.B. Zhou, L. Xu, T.T. Xing, and Y.J. Zhong, "Secure data processing framework for mobile cloud computing," Proc. Of 2011 IEEE Conference on Computer Communications, pp.614-618, 2011.

[11] J.S. Lin, "Cloud data storage with group collaboration supports," Communications in Computer and Information Science, vol. 136, pp. 423-431, 2011.

[12] G.W. Xu, C.L. Chen, H.Y. Wang, Z.P. Zang, M.G. Pang, and P. Jiang, "Two-level verification of data integrity for data storage in cloud computing," Communications in Computer and Information Science, vol. 143, pp. 439-445, 2011.

[13] L. Zhou, V. Varadharajan, and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud," The Computer Journal, vol. 54, pp. 1675-1687, 2011.

[14] J.H. Yeh, "A PASS scheme in cloud computing - protecting data privacy by authentication and secret sharing," Proc. of International Conference on Security and Management, 2011.

[15] R. D'Souza, D. Jao, I. Mironov, and O. Pandey, "Publicly verifiable secret sharing for cloud-based key management," Proc. of 2011 Indocrypt, pp. 290-309, 2011.