ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Secured Cloud Storage with Third Party Audit

Punam A. Patil, Nilesh S.Vani

Research Scholar, ME Computer, Godavari College of Engineering, Jalgaon, Maharashtra, India

Assistant Professor, Dept. of Computer, Godavari College of Engineering, Jalgaon, Maharashtra, India

ABSTRACT: In Trusted Computing Platform – secure storage is one of the important functionality. And the fasted growing fields in computer science – Cloud Computing.Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. To address this problem, here, propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, cloud computing system is combined with trusted computing .In this model, some important security services - Authentication ,Authorization ,Encryption are provided .The authentication and authorization should be prioritized in the area of computer security for protection.. To strengthen user's control, also provide distributed auditing mechanisms. Also provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.

KEYWORDS: Trusted Computing Platform, Cloud Computing, Authentication, Authorization, Encryption.

I. INTRODUCTION

In our lives, the internet is an important part, spreading over every corner .Every day scientists seek to improve the services offered through the internet. The trusted computing is a term that refers to technologies for resolving computer security problems. Trusted computing is an active research in the field of information security. Cloud computing is a collection of computers and servers that are publically accessible via Internet. Fortunately, the secure storage technology has been widely recognized and used in trusted computing field. The trusted computer group (TCG) proposed a set of hardware and software technologies to enable the construction of trusted platforms .Trusted computing platform will be used in authentication, confidentiality and integrity in cloud computer environment. Cloud computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable and often virtualized resources as a service over the Internet. To date, there are a number of notable commercial and individual cloud computing services, including Amazon, Google, Microsoft, Yahoo, and Sales force. Details of the services provided are abstracted from the users who no longer need to be experts of technology infrastructure. Moreover, users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services.

In this paper, design and implementation of enhanced authentication and authorization for trusted cloud computing are described. In section I introduce the system to be developed. Section II discusses the existing system and analysis with their drawback and objective. Section III describes the proposed system methodology .Section IV describes the implementation details. Section V describes the results and related discussions. Finally, in Section VI, gives the concluding remark and future research work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. According to the introduction, the privacy part of the key pair and the corresponding authorization data is secret stored in key object node as a whole by encrypting them using parent key.

In the analysis done in [1], Song Cheng etc., In order to effectively solve the key synchronization problem in TCP key management mechanism; they proposed a security-enhanced trusted key authorization management mechanism. The main idea is that a data item (child key information) is added in the parent key object node. Improved key hierarchy authorization management.

In [2],Kailash Patidar etc., to propose a model system in which cloud computing system is combined with trusted computing platform with trusted platform module. In that model, some important security services including authentication, confidentiality and integrity are provided in cloud computing system.

In the analysis done in [3], Xuefeng Liu etc., design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation.

In [4], it investigates the access control mechanism in the cloud. That work has focused on the existing control access mechanism in cloud computing environments. Finally, they conclude that security features provided by service providers in a cloud computing is not totally trustful.

III. PROPOSED WORK

Main Modules:-

A. Client Module:

In this module, the client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the clients name and its password for security process. If it is satisfied then received the queries from the client and search the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative Path to those intruders.

B. System Module:

Representative network architecture for cloud data storage is illustrated in Figure 1. Three different network entities can be identified as follows:

• User:

Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

• Cloud Service Provider (CSP):

A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems,

• Third Party Auditor (TPA):

An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

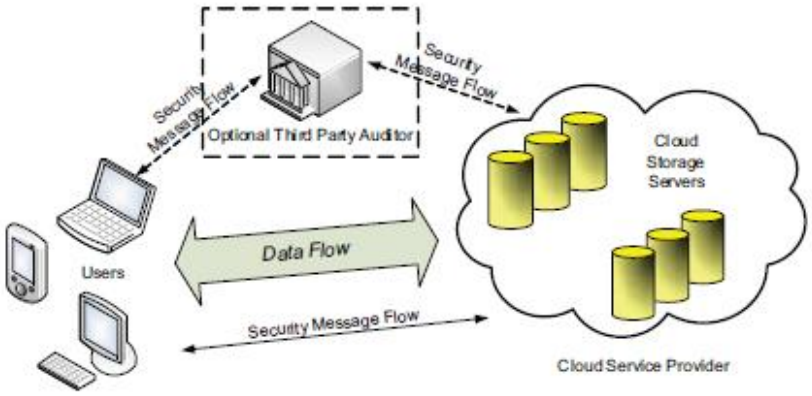

Figure.1 System Architecture

C. Cloud data storage Module:

Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. Users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case that users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In this model, assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

D. Cloud Authentication Server:

The Authentication Server (AS) functions as any AS would with a few additional behaviours added to the typical client-authentication protocol. The first addition is the sending of the client authentication information to the masquerading router. The AS in this model also functions as a ticketing authority, controlling permissions on the application network. The other optional function that should be supported by the AS is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request.

E. Unauthorized data modification and corruption module:

One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

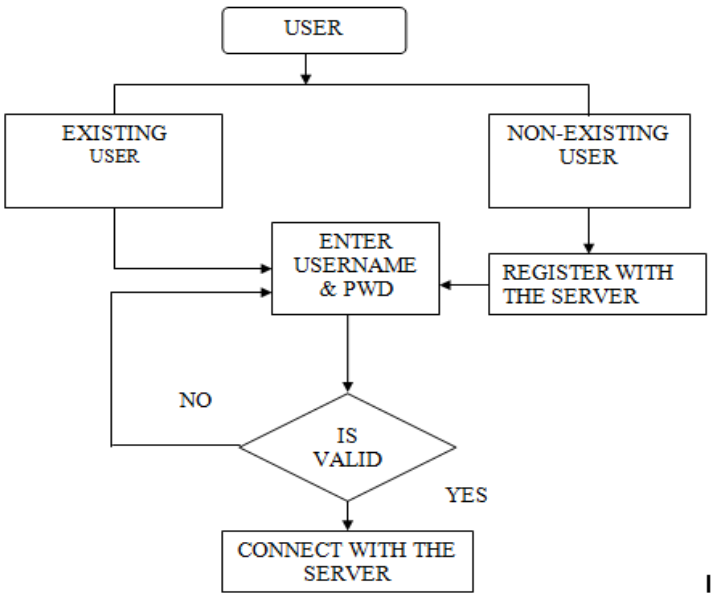

Figure.2.Flow Diagram of Client

IV. IMPLEMENTATIONS

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Our Protocol Works in Four Phases:

A. **Initialization**

- To secure hash function H : 0; 1!Z*qs the two servers S1 and S2 jointly decide a cyclic group G of large prime order q with a generator g1 which maps a message of random length into an l-bit integer, where l=log2q.
- Next, S1 chooses an integer s1 from Z*q randomly, and S2 chooses an integer s2 from Z*q randomly, and S1 and S2 exchange g1s1 and g1s2.
- After that, S1 and S2 together publish public system parameters G, q, g1, g2, H where g2 = g1s1s2.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

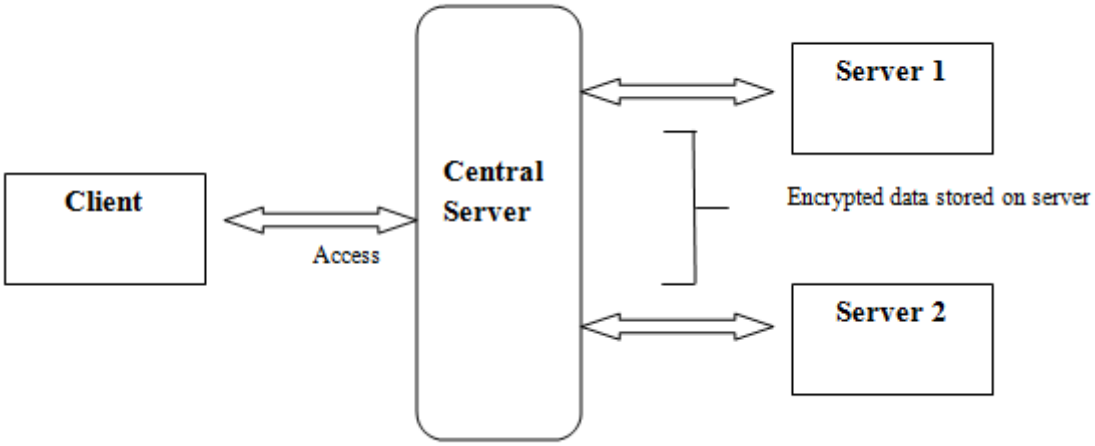

Figure.3.Implementation Diagram of system

B. **Registration**

For authentication, each client C is need to register both server S1 and S2 through unlike secure channels.

- Firstly, the client C generates encryption and decryption key pairs (xi; yi) using the public parameters published by the two servers where yi = g1xi for the server Si (i =1).
- Then, client C selects a password pwC and encrypts that password by using the encryption key yi, i.e., (g2pwc; yi) = (Ai; Bi) = (g1ai; g2pwcyiai) (i=1, 2) where ai is chosen randomly from Z _ q, according to encryption.
- Next, the client C chooses b1 randomly from Z*q and lets b2 = H(pwC) b1, where stands for two l-bit blocks exclusive OR Finally, client C sends the password authentication information to S1 through a secure channel, i.e. Auth(1) = x1; a1; b1; (g2pwc; y2) and the password authentication information to S2 through another secure channel i.e. Auth(2) = x2; a2; b2; (g2pwd;y1):
- Next, client C remembers the only password pwC.

C. **Client Registration Module**

- In this module client is registering as an authentic user by entering username, password, personal mobile number and other necessary information. The entered data will be directed towards web server using SOAP protocol for further processing.

D. **Server Modules (Two Servers)**

- This module will store the password coming from web server and will be retrieved only at the time of authentication to maintain the securities in the system.

V. RESULTS AND DISCUSSIONS

In our scheme, provide enhanced authentication and authorization for security purpose. Authentication provides a way of identifying a user. The process of authentication is based on each user having a unique set of criteria for gaining access. If the credentials are at variance, authentication fails and network access is denied. Following authentication, a user must gain authorization for doing certain tasks. Usually, authorization occurs within the context of authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Code security protects the normal, day-to-day operations of an app, tool, or daemon. But what happens when your code is under siege? It is often essential to know not only what the user is doing but also who the user is and whether the user is allowed to do that. This is where authentication and authorization come into play. Also, even if an attacker owns a discarded secret key and knows the equivalent key, he will not be able to authorize to use that key. Our scheme is feasible in hardware and software aspects. This scheme is feasible in hardware and software aspects.

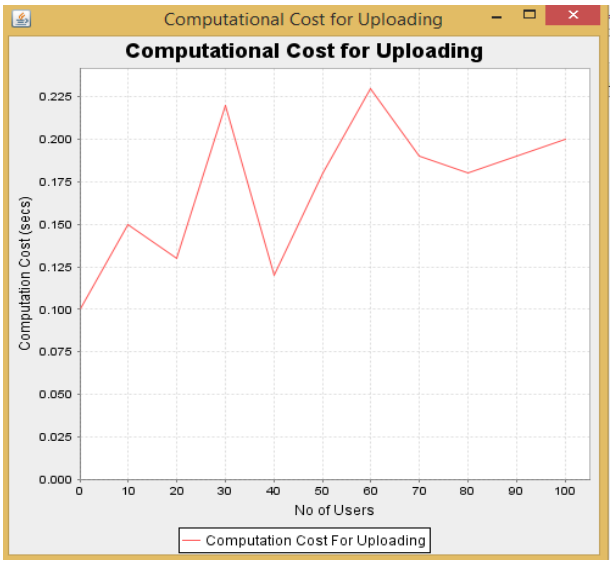

Figure.4 Computation Cost for Uploading

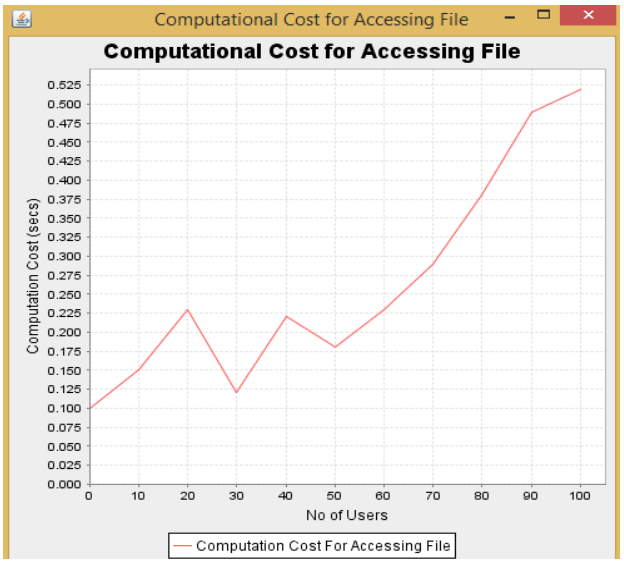

Figure.5 Computation Accessing File

The concept of Uploading File is, to transfer or copy a file or files from own computer to another computer. For instance, might transfer a file from home PC to the Yahoo server that stores Web Hosting files. As shown in Figure.4, X- axis represent the no. of Users and Y-axis represent the Computational Cost (secs) that indicates computational cost for uploading file per secs by no. of users.

The concept of Accessing File is, to transfer or copy a file from another computer to your own. You might download a file from your Web Hosting account to your home PC. As shown in Figure.5, X- axis represent the no. of Users and Y-axis represent the Computational Cost (secs) that indicates computational cost for accessing file per secs by no. of users.

Thus, Simulation results are showing our scheme is more efficient and secure than existing system.

VI. CONCLUSION AND FUTURE WORK

In this paper, proposed innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. Our approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge. In future, would also like to study over the impact of more security in this proposed model.

ACKNOWLEGMENT

Authors would like to thank Godavari College of Engineering and Technology which provided all the necessary facilities.

REFERENCES

[1] Song Cheng, Li Jing, Peng Weiping and Tian Xinji, "A Security Enhance Key Authorization Management Scheme for Trusted Computing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Platform," IEEE, pp. 1573– 76, 2012.

[2] Kailas Patidar, Ravindra Gupta, Gajendra Singh, Megha Jain, Priyanka Shrivastava "Integrating the Trusted Computing Platform into the Security of Cloud Computing System" volume 2, Issue 2,February 2012.s

[3] Xueteng Liu, Yuqing Zhang, MemberIEEE, Boyang Wang and Jingbo Yan Yan, "Mona: Secure Multi – Owner Data Sharing for Dynamic Groups in the Cloud IEEE Transactions on Parallel and Distributed Systems volume l. 24, No. 6 ,pp.1182-1191,June 2013.

[4] Mauro José A. de Melo and Zair Abdelouahab, "A Study of Access Control in Cloud Computing", Journal of Computers and Technology Volume 3 No. 3,pp.453-457, Nov-Dec, 2012.

[5] Rajan Sameer, Jairath Apurva, "Cloud Computing The Fifth generation of Computing", International Conference on Communicati n Systems and Network Technologies, pp.25-36,2011