ISSN No. 0976-5697

Volume 8, No. 3, March April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Reliable certificate less general verification for CPSS against malevolent auditors

B.Mamatha*, Neha George**, Neha Chawhan** and Mrunal Shasthri**
Asst. Prof.*, Student**
Department of CSE, Guru Nanak Institutions, Ibrahimpatnam
Hyderabad, India

Abstract: Cloud computing has many security menaces, among this Trust Management is considered as one of the biggest menaces. Privacy is a major concern in cloud computing because of the flexible and elastic nature of cloud . Maintaining the secured privacy of data stored by the consumer is a difficult task to be performed .Storing data in the cloud is advantageous the cloud does not offer any of the data integrity and trusted management issues and guarantee. Here, in this paper we discuss about the implementation of Cloud Armour. Cloud Armour can be defined as a trust management frame work .Trust as a Service (TaaS) is one of the feature provided by cloud armour. The TaaS has 1.To provide privacy and trust quality the TaaS has a unique protocol. 2. It has a quality model to determine the quality feedback to protect the cloud service from malicious users 3.Redistributed implementation of the trusted management service is made available with the help of a handy model

Keywords: Data storage, privacy-preserving, Trust Management, Cloud Armour

I. INTRODUCTION

Cloud storage helps us in remote data storage and allows us to enjoy the services provided by high quality application and services from bunch of computing resources with out the problem of storage and maintenance. CPSS lets individual to store and share information collected from personal devices[1]. This data collected by CPSS is important to read peoples life . Owner thinks storing the data in a cloud is a good way of data management . But users do not have physical way of data, this makes it difficult to maintain the integrity of data in cloud computing . User should be able to use the cloud storage with out worrying about the integrity of the cloud .So enabling public auditability of cloud storage is important so that the user can resort the Third Party Auditor (TPA) to check the accuracy and consistency of data .[2] In this paper we propose public verification of cloud based cyber physical social- system against malevolent auditors. It allows TPA to audit multiple users simultaneously and efficiently . This security feature makes the system highly secure and efficient.

Cloud computing has a long list of advantages in IT industry ,it is considered as the next generation of internet .The cloud allows the users to easily access the data that is stored in it from any part of the world. The cloud provides us with world wide network access ,resource pooling irrespective of location, self service , elasticity of resources that is the degree to which the cloud is able to adopt to changes by allocating and de-allocating of resources , the pricing is done on the basis if usage of cloud . All these features provided by the cloud makes the storage of data in the cloud very beneficial and easy .One of the main advantage of cloud computing is the data is stored and managed in a efficient manner .

Cloud computing has many appealing advantages but there are high chances of increase in security threats . One of the major security threat is trust management . The cloud is highly dynamic , distributed and non transparent in nature which leads to many security threats like privacy , security , handiness . Protecting the privacy of the consumers by preventing unauthorized users from accessing the data is a difficult task. Though storing data in cloud is attractive for long term data storage the cloud doesn't offer any data integrity. To ensure integrity ,accuracy , consistency of the data in cloud we should enable public verification against malicious audit.[3]

II. EXISTING SYSTEM

Cloud auditing is used by the service providers to make their performance an services available to authentic users . in existing system private auditing is used for re generating the code[4] . In the existing system it also requires the owner of the data to stay online through out the auditing process .A large amount of data is out sourced so if it requires the owner to stay online through the period of auditing its impractical [5]. The existing system is highly expensive

III. PROPOSED SYSTEM

To ensure the integrity of data stored on an untrusted server, this project is proposed for proof of irretrievability (POR) technique. we here design a certificate less general verification scheme against malevolent auditors for CPSS. Our approach can possess lower communication cost compared with the Fortress ,it provides a complete outsourcing solution of data not only the data itself ,but total security of data

A. *Proposed System Advantages*

- Absence of data owner is possible
- Regeneration problem of authenticators is solved

IV. SYSTEM ARCHITECTURE

Here in system architecture we have 3 main entities namely cloud user that is admin ,who can authority to handle the client forms ..the admin has also login account ,he has to login and then take the client information and client requests and then after all the information if he finds the client valid and authorized he then sends the private key to the client then can change password too□the second entity is client ,who has lots of data to store in cloud .He has to get registered and then fill the details asked for and then with the details provided has to login the page then after he can view the file, download the file, upload the file, edit the file, and can also change the verification key if needed in case...the other most important entity is the third party ,one is cloud service provider who provides plenty of services for the client such that it can use the services till the extend. when the client requests the TPA gets the key verification and then after verification it goes to cloud server.

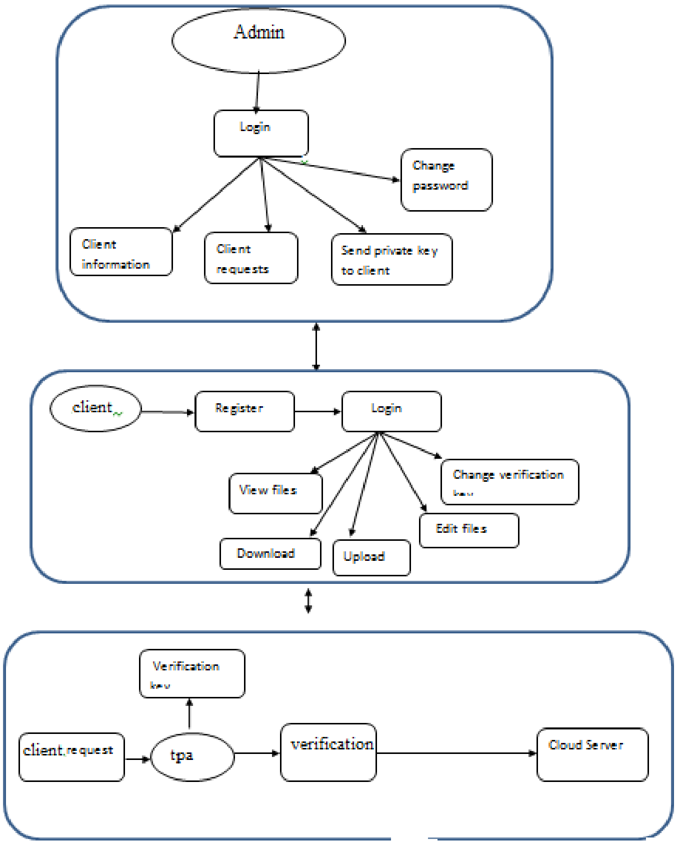

Fig.1. System Architecture

V. MODULES

1. User Interface
2. Admin Auditing
3. Third Party Verification
4. Cloud-User Interactions

A . Methods Description

1. User Interface:

User connects to server where one must provide username and password after that they can able to connect the server.And If the user already exits then he can directly login into the server else user must register their details such as username, password e.t.c., into the server. Server will create the account for the user

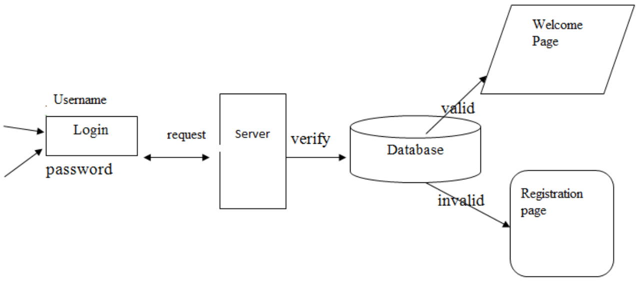

Fig. 2 . User Interface

2. Admin Auditing:

This is the second method of our project. Here admin generates private key for the authorized user, which is needed for the users to log in to the application. Admin have the right to audit the user details and to know who are using the application. client get private key from admin only after registration. If the client is not registered properly then he can□t get any key from the admin ,without having key he is not able to login

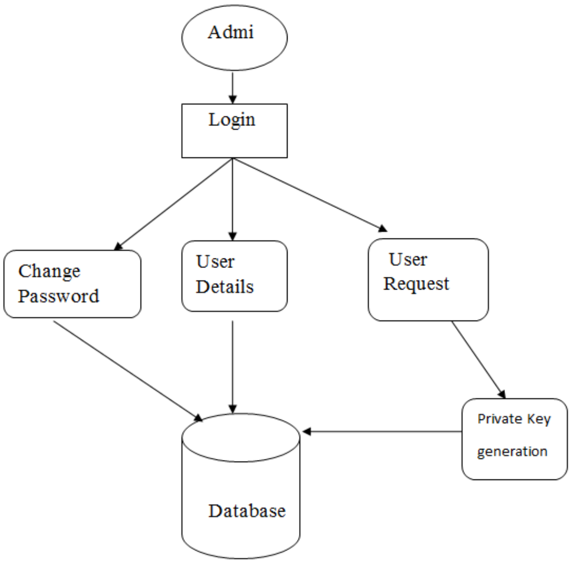

Fig.3 Admin Audit

3. Third Party Verification:

This is the third method of our project. In this the third parties play a important role ,they are responsible for providing security and maintaining the cloud servers. Before giving any access to the user the third party checks the user authentication with the help of verification key provided by them .

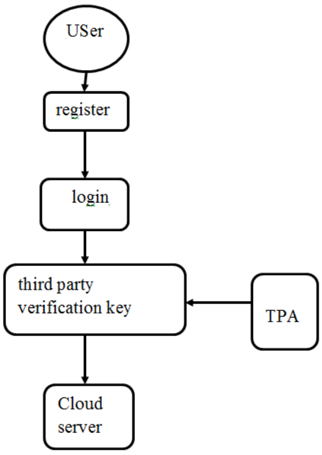

Fig. 4 Third Party Verification

4. Cloud-User Interactions:

This is the fourth method of project. The user interacts with the cloud servers through the third party. The users can use the services provided by the cloud providers such as upload files ,edit files ,download files e.t.c., .For the purpose of security and best sevices ,the third party verifies the authorization of the user before providing any service.

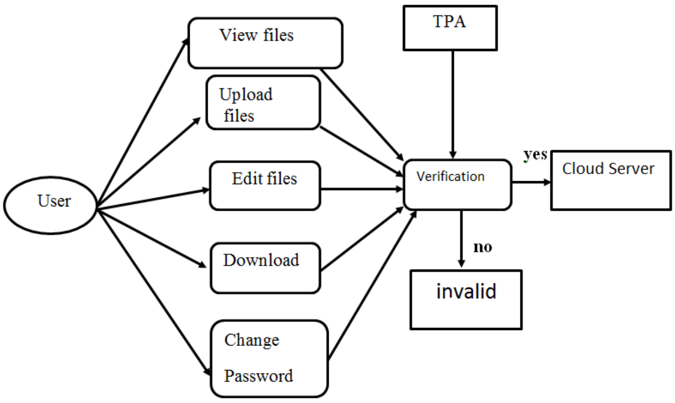

Fig.5 Cloud-User Interaction

VI. FUTURE ENHANCMENT

By using multi cloud or multi server this protocol can be put into effect and is geniune. Implementation of cloud excludes the requirement of encoding the cloud and ensure that the newly stored data after each cycle of repair has fault tolerance.

VII. CONCLUSION

In this, we first point out the vulnerability of the Certificateless verification for cloud.Then, we propose the first reliable certificateless general verification for cloud storage in CPSS with full proofs of security against malevolent auditors and arbitrary adversaries in the security model. With this an auditor does not need to manage certificates. Meanwhile, a malevolent auditor/CPSS user cannot impact the security of our scheme. A formal security proof proves the security. Performance analysis demonstrates that our security is efficient and practical.

VIII. ACKNOWLEDGMENT

We felt great pleasure in submitting this paper on SCLPV: Secure Certificate less Public Verification for Cloud-Based Cyber-Physical-Social Systems against Malicious Auditors .First and for most we express our deep sense of gratitude ,sincere thanks to Asst .prof .B. Mamatha for best support ,opinion ,view and thoughts have been really helpful.

IX. REFERENCES

[1] R. R. Raj, I. Lee, L. Sha, and J. Stankovic, □Cyber -physical systems: The next computing revolution,□ in *Proc. Des. Autom. Conf.*, 2010, pp. 731□736.

[2] C.Wang, S. S. Chow, Q.Wang, K. Ren, andW. Lou, □Privacy-preserving public auditing for secure cloud storage,□ *IEEE Trans. Comput.*, vol. 62,no. 2, pp. 362□375, Feb. 2013.

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, □Enabling public verifiabilityand data dynamics for storage security in cloud computing,□ in *Proc. Eur. Symp. Res. Comput. Sec.*, 2009, pp. 355□370.

.[4] C.Wang, Q.Wang, K. Ren, andW. Lou,□Privacy -preserving public auditing for data storage security in cloud computing,□ in *Proc. IEEE Conf.Comput. Commun.*, 2010, pp. 1□9. 2015, to be published. doi: 10.1109/TDSC.2015.2406704 .

[5] R. K. Ganti, Y. Tsai, and T. F. Abdelzaher, □Senseworld: Towards cyberphysical social networks,□ in *Proc. Int. Conf. Inf. Process. Sensor Netw.*,2008, pp. 563□564.