EFFICIENT, SECURE REMOTE DATA ACCESS IN CLOUD USING DYNAMIC DATA AND INDIRECT MUTUAL TRUST

Sujata Yankanchi[1], Rashmi K H[2]

[1]*Department of Computer Science and Engineering, Godutai Engineering College for Women, Kalburagi*
[2]*Assistant Professor, Department of Computer Science and Engineering, Godutai Engineering College for Women, Kalburagi*

Abstract

Currently, the storage of the large data on a local server is problematic and costly. Storage-as-a-service provides the pay as you go pricing model. The sensitive data produced by organizations is outpacing having problem with their storage ability. The maintenance huge amount of data is expensive and it is having high price. Cloud service provider which is a paid facility of the organizations. Saas makes the reduction in cost of the maintenance and distributes the burden of the large huge local data and a data owner is having higher desired level of security. In this cloud based storage we propose the following: 1. It makes the owner to outsource data, and performs the dynamic operations such as insert, delete, update. 2. Provides the recently updated outsourced data to the registered user. 3. Guarantees the mutual trust between the owner and the CSP 4. Revokes or grants the access of the outsourced data.

***Keywords** - Mutual Trust, Dynamic Data, Access Control, Confidentiality*

---***---

1. INTRODUCTION

All computer users have access to the internet; many users are using some of applications, such as social networking, Gmail, Google docs and so on. Not only are authorized users switching to cloud services. Cloud computing has several advantages for its users. E.g. maintenance cost, elastic and access to the data. Cloud computing will be much more effective in the future. Many users not knowing that where their data is stored and how it is Kept confidential. Cloud computing refers to a high risk of maintaining a personal data on its users. and the applications, and it has direct connection to a server. Cloud computing emerged as recent technology and it has several advantages like cost effectiveness, less communication overhead, low cost and flexibility and immediate access of wide range of applications, mobility. Cloud computing is probably to the most cost efficient to use, manage and update. Storing information in the cloud gives the almost unlimited storage capacity.

In the current era, many organizations require the large storage capacity which is a problematic and costly. Storing the information such as information, personal information etc.. Cloud computing is a term or metaphor based on utility and the consumption of the computer resources. It involves the deploying groups of the remote server and the software networks that allow different types of data sources can be uploaded for real time processing to get the computing results without storing of the needed data. The critical infrastructure [2] such as power plants, industrial sensor networks etc.There are some concerns related to the security, intactness of the data and access permission of the data.

2. RELATED WORK

The literature survey is related to reading, analysis, evaluating and summarizing scholarly materials about a specific topic. Literature review is the basic step in development process. Developing the tool it is necessary to determine which operating system and language can be used for the developing the tool. The clients start building the tool the programmer need lot of external support. Literature survey spare the details of research carried out on the available frame works. This research gave me overview of the security of the data and various ways of securing the information.

Literature survey is the most important step in development process. Before development it is required to find the time, financial fitness and company strength. Once these things are sufficient, then next steps are to be finding which operating system and language can be used for developing the instrument. Once a programmer start constructing the tool the programmers need outside support. This reinforce can be obtained from experienced programmers, from google or from websites.

G.Atenies et.al [1] in “Provable Data Possession (PDP) at Untrusted Stores”, in proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2007, pp.598-609.

A client has stored data at servers which are not safe to store the data, to check that the server has the real data without accessing it. This style produces probabilistic proofs. In this we have the PDP schemes those are more well organized than the previous, compared with schemes that provides lower security. Communication at the server is low. disk IO is covered by the PDP performance. Verifying the originality of data has become a critical problem to store data at untrusted servers. It is associated with the peer-peer systems. Storage in records requires the secure about the authenticity of data on storage, namely that storage servers posses data. It is effective to find that data have been altered or deleted while accessing the data. Network storage represents an unique performance demands. The model is different in that it make servers to get small portions of the file. We providing framework for the PDP scheme. It verifies that an outsourced storage site keeps the m files, and it is a collection of m blocks. The client processes the data an gives a part of data which is stored at local machine. PDP protocol is the basic to construct underlying record searching systems which are necessary for developing for the long term of the data. The client may alter the file which is stored at the server. The client may increase the file or it may contain the some of the additional metadata stored at the server. The programmer remove the data before the execution, but server has to verify that the file has stored successfully. The client may encrypt the file. verifying the untrusted server stores the client's data. PDP scheme which minimizes the file blocks access.

F.Sebe et.al [2] in "Remote data possession checking in critical information infrastructure", "IEEE Trans. on Knowl. and Data Eng., vol.20, no. 8, 2008.

Remote data possession checking protocol is the checking a remote server may access uncorrupted file. In this we have data possession checking protocols which takes as in the following:

i. It enables an infinity number integrity verification.
ii. Its running time is maximum and which can select at the set up time.

It in used in intrusion-detection systems.

G.Ateniese et.al [3] in "scalable and efficient provable data possession", 4th international Conference on security and privacy in communication Networks, 2008, pp. 1-10.

Outsourcing of a storage is a growing technology which provides a lot issues in security, most of the problems are identified. Main problem is providing how it is accessed frequently,efficiently and securely to check that a storage server is assured for storing its clients data. The server storage is imagined to be untrusted in terms of both confidentiality and flexibility. where we are not using bulk encryption. a third party provider stores data owner data. The third party provider should be trusted to store the data .the data should be available when user and owner is required. identifies any mistakes from the client. It supports cryptography in symmetric key and is well suited for third party verification.

3. EXISTING SYSTEM

The current existing system has the traditional access control method considering that the data owner and the storage servers are in the same assured range. But this not working when the data falls out of the range. It should takes management of the outsourced data. It is available to data owner in outside of the trust domain. Existing researches are close to our work in field such as cryptographic file system, access control and confidentiality, integrity of the outsourced data.

3.1 Disadvantage of the Existing System

The existing system is not secure because cloud provider may alter or modify the information.

3.2 Proposed System

In our proposed work we propose a scheme that related to important theme related to the outsourcing the storage of data, such mutual trust, integrity, confidentiality and access permission .the data stored at remote server not only retrieved by the user but they also update the data and can perform the dynamic operations such as add, remove , append. Etc..The authorized user can have access to the latest version of the data. From this we can identify that the accessed data is stale. We are providing the indirect trust between the data owner and cloud service provider. An external factor is used to find the misbehaviour from entity and responsible entiity also being identified. Finally we have the access permission for the authorized users and revoke the unauthorized user.

3.3. Advantages of the proposed systems.

They are as follows

1. Here we are generating key for files, so without key we cannot download the file. Using encryption and decryption techniques.
2. Authorized user will have the latest version of the outsourced data.
3. Access permission for the outsourced data to only the authorized users.
4. It revokes the access for the any unauthorized user.

3.4 System Components and Relations

Based on this paper that contains some important problems related to outsourcing data, known as data dynamic, newness, mutual assurance and access permission. The storage of the cloud computing contains the four main components as shown in fig.4. The components such as data owner, authorized user, CSP and TTP. Data owner generates the sensitive data for the outsourcing and makes the data accessible for only the authorized user. Authorized users are the owner's client and they can access the data. Cloud Service Provider (CSP) controls the servers and gives paid storage space on its infrastructure. The owner's data is stored in CSP. Accessible for the authorized users as and when needed. The last component we introducing is TTP is an entity assured by the all other entities. It checks and finds any misbehaviour or mistakes which occurs and finds the party who is held responsible for this. In fig.4 it shows the relations between the system components. The relation between the system entities are denoted by the two different lines, solid line and dotted line. Solid line indicates the direct trust between the entities. Direct trust relation exists between the data owner and the authorized user. Moreover CSP trust the TTP. On the other side there is a mutual distrust relation between data owner, authorized user and CSP. Since we introduced the TTP it guarantees the indirect trust between these three components. Direct trust relation between the data owner and the authorized users.

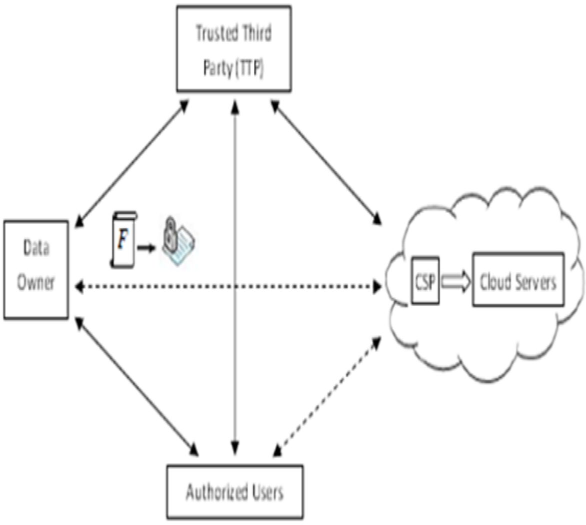


Fig.3 System Components and Relations

3.5 Security Requirements

There are some security requirements such as authenicity, intactness, access pemission and the newness.

Confidentiality: the sensitive data must be private and it is to be guaranteed from the TTP, the CSP and the Users .

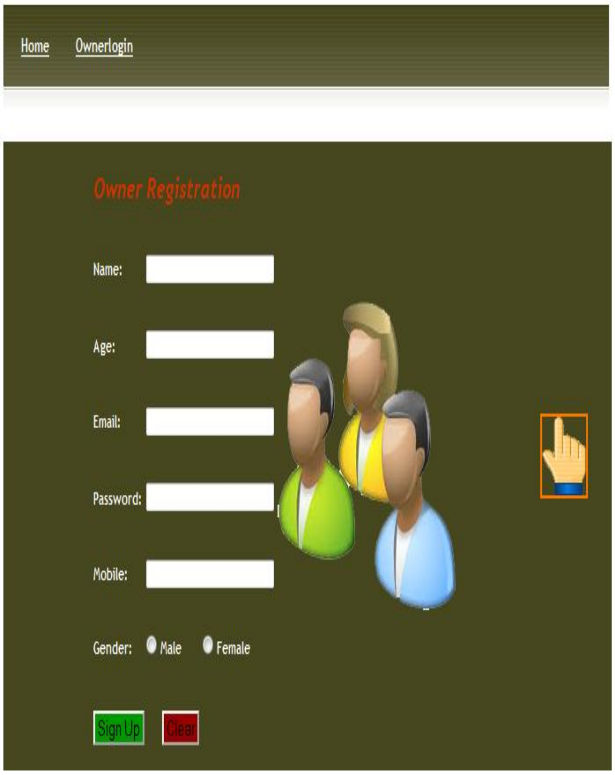
Integrity: it maintains the originality of the data.

Newness: the users will get the most recent and updated version of the data.

Access control: grants or revokes the data. Only the registered users can get the sensitive data. The unauthorized users can read old data, and they are not able to read most recent data.

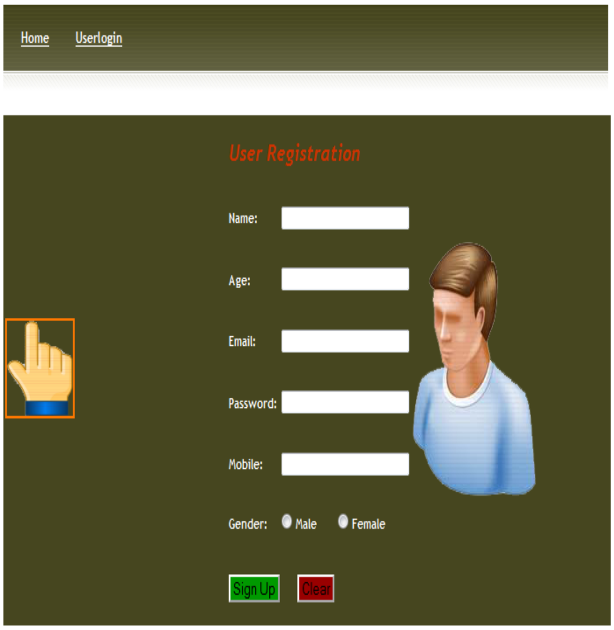
4. RESULTS AND DISCUSSIONS.

4.1 Data Owner Registration



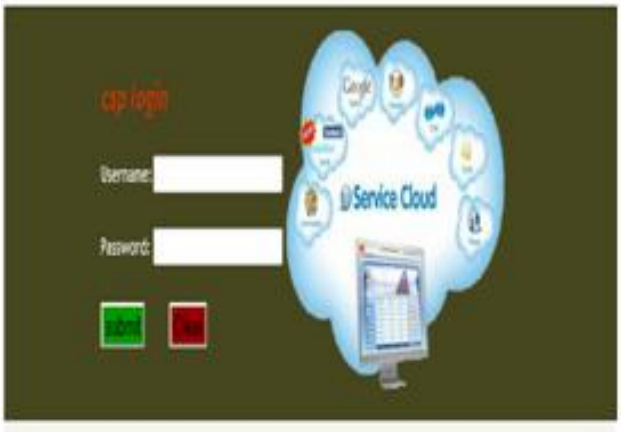
Owner after successful registration can login and performs the insertion, deletion, update some block level operation on data. Before sending data it has to be encrypted with the certain security and key algorithms.

4.2 Data User Registration



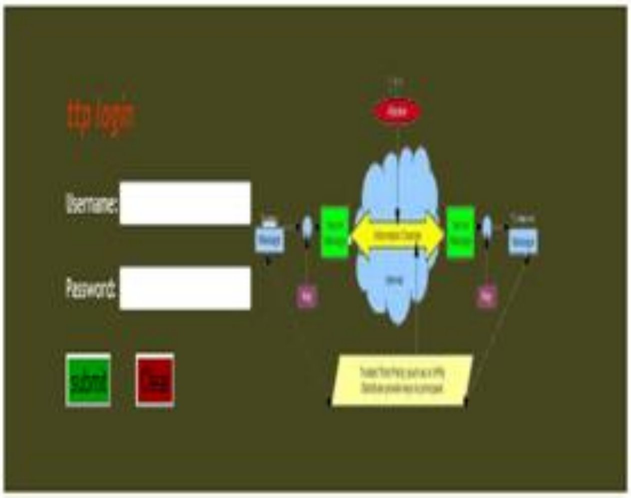
User can login and if they are authorized user they are having the decryption key can access the data. They can view the data and download the data

4.3 Cloud Service Provider



Cloud server provider maintains the storage of the data. Gives access to the data. Files are stored on the cloud storage

4.4 Trusted Third Party Registration



Trusted third party finds disputes occurred. It keeps tracks of the each file and the records.

5. CONCLUSION

In this storage scheme it uses the concept of the OTP and as well as the secret key. Owner has the rights to give access to the outsourced data. it is flexible to the users to view the data. in case a Of any dispute regarding data intactness, TTP enhances the mistaken party. We storing the files in the bock level.

ACKNOWLDGEMENTS

Hence, we declare that the above mentioned work is done by ourselves and it is not implemented in any of the current system and we have provided the security and encryption of the data.

REFERENCES

[1] G.Atenies, R.Burns, R.Curtmola in “Provable Data Possession (PDP) at Untrusted Stores”, in proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2007, pp.598-609.

[2] F.Sebe, J.Domingo-Ferrer, A.Martinez-Balleste in “Efficient Remote data possession checking in critical information infrastructure”, “IEEE Trans. on Knowl. and Data Eng., vol.20, no. 8, 2008.

[3] G.Ateniese et.al [3] in “scalable and efficient provable data possession”, 4th international Conference on security and privacy in communication Networks, 2008, pp. 1-10.

[4] C.Erway, A.K upc and R.tamassia, “Dynamis provable data Possession”, in proceedings of the 16th ACM Conference on computer and communication security. 2009, pp. 213-222.

[5] Q.Wang, C.Wang, J.Li, K.Ren and W.Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing “, in proceedings of the 14th European Conference on research in computer security, 2009,pp.355-370.

[6] A.F.Barsoum and M.A.Hassan,” Provable data possession and replication of data over cloud servers”, centre for applied cryptographic research, report 2020/32, https://www.cacr.math.uwaterloo.ca/techreports/2010/32/cacr2010-32.pdf.

[7] R.Curtmola, O.Khan, R.Burns and G.Atenies, “MR-PDP:multiple-replica provable data possession”, in 28th IEEE ICDCS,2008,PP.411-420.

[8] A.F. Barsoum and M.A.Hassan, “ On verifying dynamic multiple data copies over cloud server”, Cryptology ePrint Archive, Report 2011/447, 2011,2011, http://eprint.iacr.org/.

[9] K.D.Bowers, A.Jules and A.Opera, “HAIL: a high availability and integrity layer for cloud storage”, in CCS’09:Proceedings of the 16th ACM conference on Computer and Communication Security. New York, NY,USA: ACM,2009,PP.187-198.

[10] Y.Dodis, S.Vadhan and D.Wichs, “Proofs of retrievability via hardness amplification”,in proceedings of the 6th theory cryptographic conference on 2009.