Cloud Computing Security Management using CSP

Rasha Rokan Ismail, Taha Mohammed Hasan

Abstract: ***The cloud was defined by lots of experts, yet the NIST (National Institute of Standards and Technology) has presented the definition: "a model for*** enabling ***comfortable, on-demand network access to a shared pool of configurable computing resources The aim of this paper is a model for safe data sharing on cloud computing with intension to provide data confidentiality and access control over shared data, it also removes the burden of key management and files by users. The system also supports dynamic changes of membership and enables clients to reach the data they require even when the owner does not exist in the system. In the proposed system, a new security system is introduced, it provides a*** mechanism ***through which communication is safely achieved as well as it protects users and their hidden information from unauthorized users. The Entities in Proposed System consist of three parts: CSP, Users (owner ,clients) and TPA , in this paper the focus will be on the CSP and the users. The proposed system are provides data confidentiality, access control of share data, removes the burden of key management and file encryption/decryption byusers, support dynamically of users membership. The use of a digital signature ensures the integrity and confidentiality of sharing data sent by users so that it cannot be read by the recipient TPA as it encrypts, sends a new encrypted signature and sends it to the CSP so that it cannot read its content CSP proved to be effective in the security of cloud computing.***

Keywords: NIST, CSP, TPA

I. INTRODUCTION

The cloud was defined by lots of experts, yet the NIST (National Institute of Standards and Technology) has presented the definition: "a model for enabling comfortable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, storage, servers, services and applications) that can be provisioned and released rapidly with the smallest management effort and minimal interaction by service provider", which is the generally accepted definition. It also can be known as a modern method of computing service over the internet in which dynamically scalable and often virtualized resources are provided [1, 2].

Lately, utmost of the establishments are investigating the cloud technology in order to reduce the cost irrespective of the security level that the Cloud Service Provider (CSP) provide , nevertheless it is hard to know the profits in term of one category.[3]The security was ensured by using Cloud Service Provider(CSPs) has over the data stored by cloud clients with use of mean as firewalls and virtualization. Because of these means have some weakness , they would not offer complete data protection over the network and CSPs.

Revised Manuscript Received on July 31, 2020.

Rasha Rokan Ismail, Department of Computer Science, Diyala University, Iraq.

Taha Mohammed Hasan, Department of Computer Science, Diyala University, Iraq.

If the sensitive data is encrypted before hosting , deserve data confidentiality and privacy against CSP. A classic issue with scheme of encryption is that it is unreasonable as the huge amount communication overheads over the cloud access shapes. So, cloud wants secure means for storing and organization to reserve the confidentiality and privacy of the data [4][5]

The data stored in cloud data centers are not controlled by the cloud computing. The service of the cloud have full of governor over the data, they can accomplish any spiteful jobs like duplicate, abolishing, adapting, etc. The cloud computing guarantees definite control level over the virtual machines. As to this absence of control over the data hints in better security problems than the common cloud computing model[6]

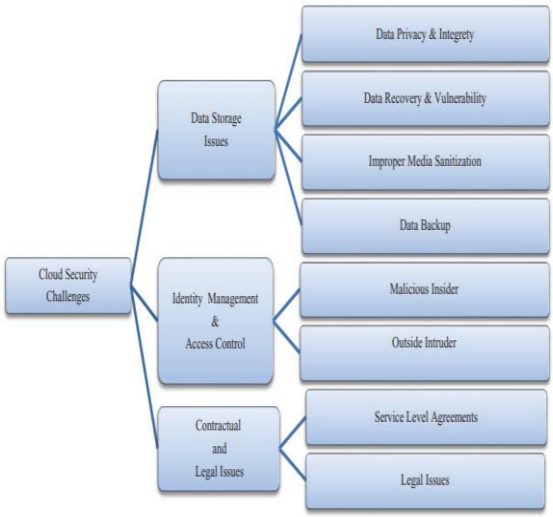

Figure 1. Cloud security Challenges

In 2018, (Ghadge and U bale) [7], proposed a secure manner for distributing keys without utilizing any protected communication channel, and the user is capable of safely getting the private keys from group administrators (managers). Only users in the gathering are able to use the cloud. A fine-grained access control and anti-collusion attack are provided by the system. Files are stored on many clouds in various groups using a hybrid cloud. A secure revocation is also supported by the system. Liu et al.[8] suggested a arrangement that has a time grounded re-encryption with algorithm of ABE to sustenance secure sharing of data between the group with admission control. This scheme guarantees that forwarded data securely extended to the users of the group and it preserves the user revocation. In this arrangement, the time age is linked with each user and by termination the revocation automatically by Cloud Service Provider (CSP).

Dhungana et al. [9] suggested a arrangement for the infrastructure of the cloud networking as framework for the identity management and it is sustained by User managed Access (UMA) protocol. Here CSP performances is as a host, whereas the authorized used acts as service owner. The authorization manager manage the service management and service requesting users also managed by authorization manager.

The aim of this paper is a model for safe data sharing on cloud computing with intension to provide data confidentiality and access control over shared data, it also removes the burden of key management and files by users. The system also supports dynamic changes of membership and enables clients to reach the data they require even when the owner does not exist in the system. In the proposed system, a new security system is introduced, it provides a mechanism through which communication is safely achieved as well as it protects users and their hidden information from unauthorized users.

II. THE ENTITIES IN PROPOSED SYSTEM

The Entities in Proposed System consist of three parts : CSP, Users (owner ,clients) and TPA , in this paper the focus will be on the CSP and the users

1) CSP: Untrusted party provider store facilities and sharing data maintain access control list (ACL) assigned by users and based on that control access of encrypted store file .This list is sent by the owner, which includes a list of all clients who want to access some files stored in csp as shown in the table (1) as well as csp will store a table containing all the information about all owners who want to access certain files in the system and as shown in the table (2) and also maintains a list of all Files uploaded by the user as shown in the table (3) .A cloud storage server (CSS) is managed by cloud service provider (CSP) through which spaces is provided to the user to store data and compute it. The CSP, who controls the management of cloud servers (CSs) and provides a paid storage space on its infrastructure to consumers. Servers are geographically distributed on vaious locations. The principle of the servers in the cloud computing is virtual servers because because the location of the required service remains unknown for users.

Table (1) Access Control List

File ID	Client ID	Access Control

Table (2) Owner Information

Owner ID	File ID

Table (3) Last Update On File

File ID	Last Update by

2) Users : Users of the system is divided in two types:

a) Owner: parson who wants to share own data to other parsons and also wants to assign access rights to persons access control list (ACL) is assigned by owner to CSP based on shared data. As shown in the table (4) that includes a list of (id) for each clients and a file that he wants to access by owner to csp .

Table (4) Access Control List (ACL)

File ID	Client ID	Access Control

Clients: significant amounts of data are owned by clients, who want to stroe them on the cloud that relies on cloud storage server for data maintenance and computation. A clients are either organizations or individual consumers. and wishes to upload file and download file it into the csp for ease of sharing or for cost saving. Can access and share data or downloaded or stored or lifted from the csp through its registration system through which owner sends a list of all clients data within the system.

III. WORKING OF PROPOSED SYSTEM

1- User enters in application through registration by getting the personal information (ID user, password, gender, age and email), the user is a member in the system will login by entering a username and password. The system activates the user and gives the specific ID. After entering the ID, a given user can login successfully, figure (2) indicates user enlistment activity

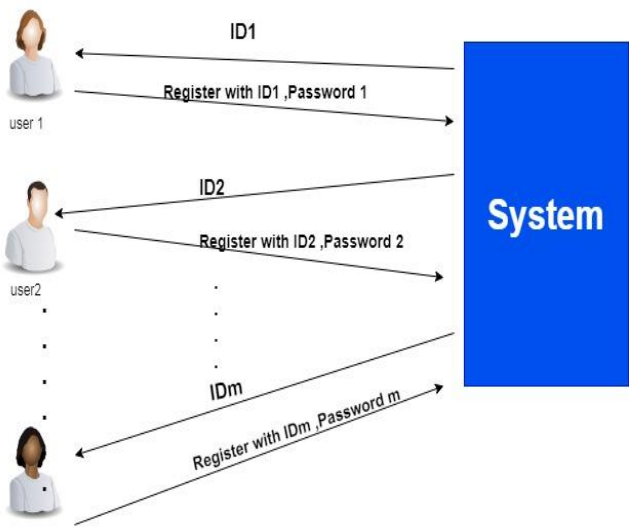

Figure (2) User Registration

The next three step is file download , upload and update as follow:

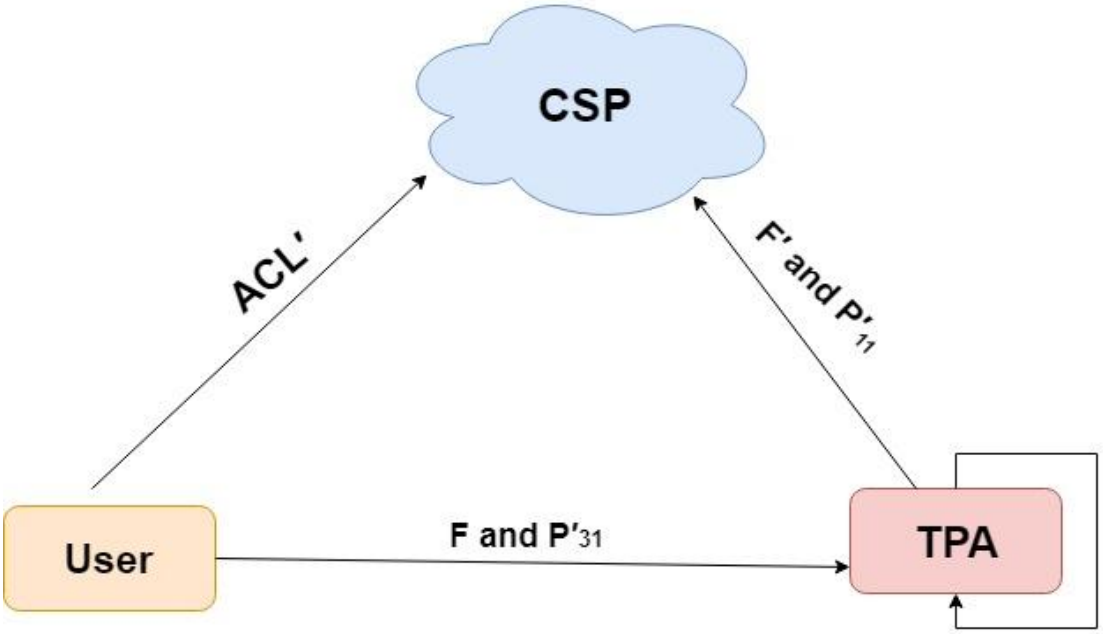

Figure (3) File Upload

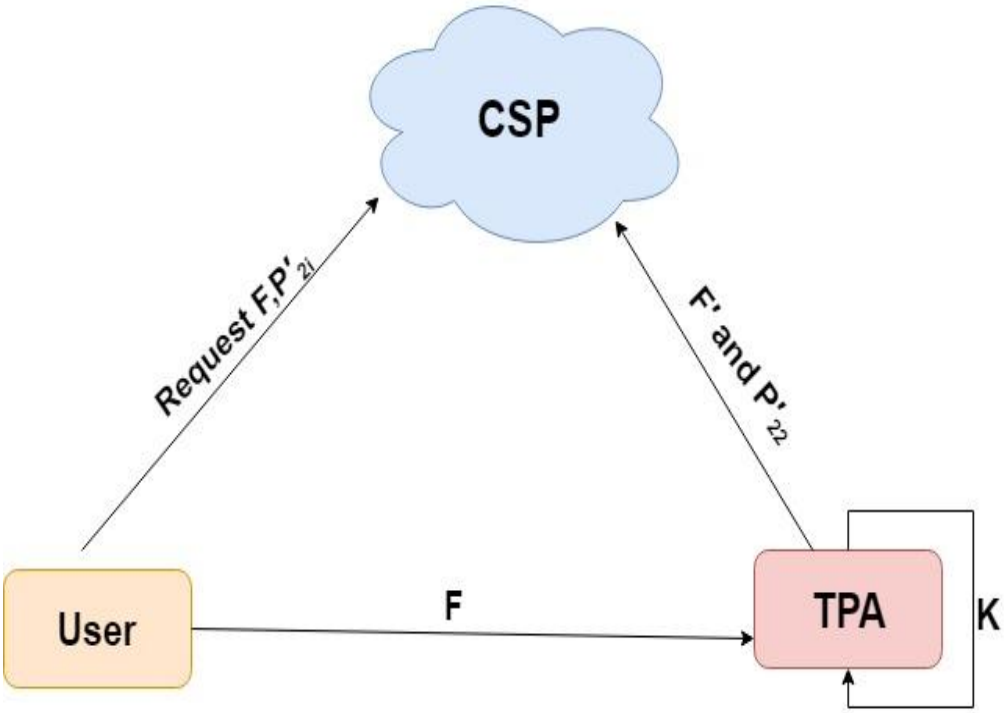

Figure (4) File Download

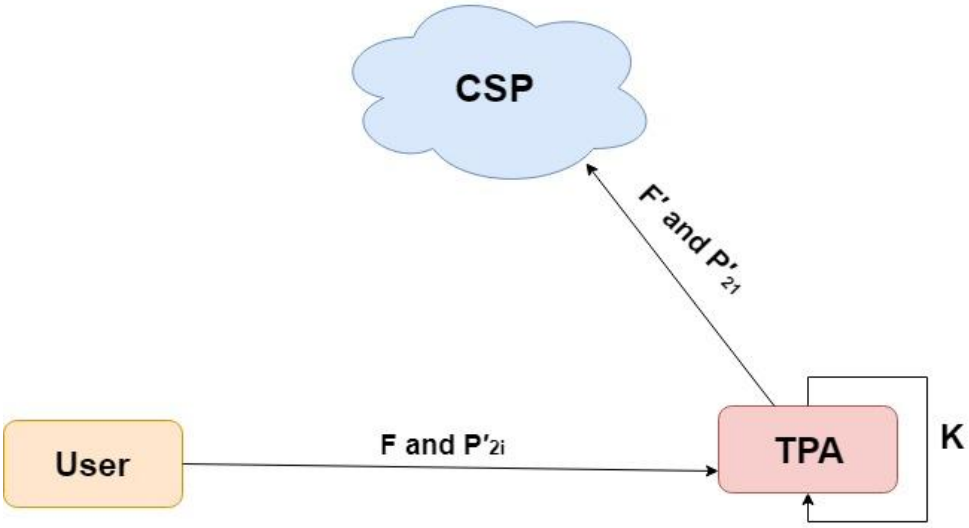

Figure (5) File Update

IV. RESULTS

CSP manages are save and manage files and information of users in the system and saves this information in tables (1), (2) and (3). The following figure (6) shows the registrant main window of the CSP, which include the CSP Id and password are entered. Figure (7) illustrates the main interface.

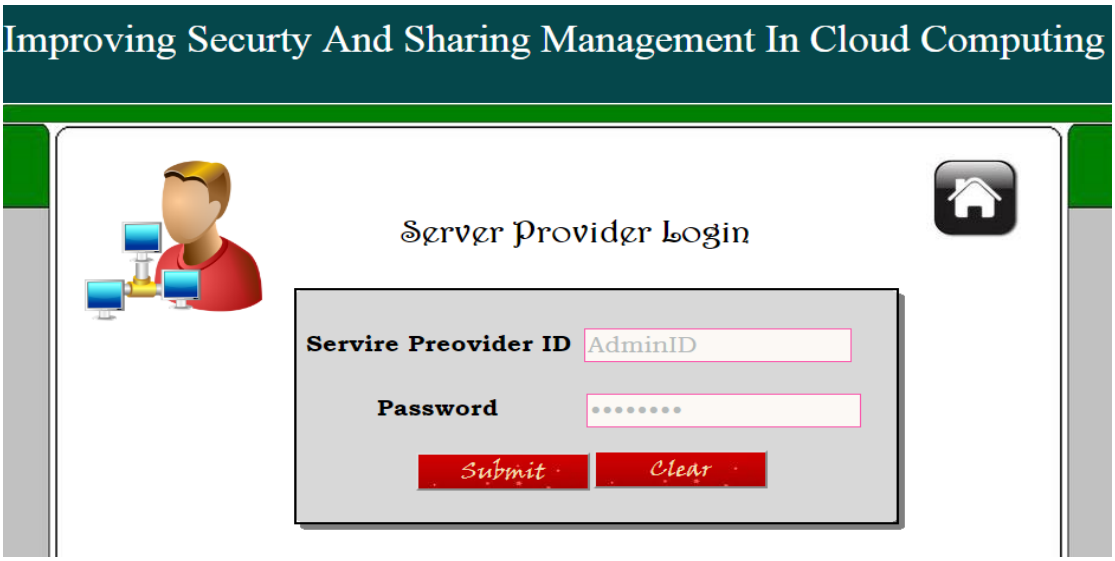

Figure (6) Login CSP Window

Figure (7) General CSP Window

CSP receives the client message (P_2) to download the specified file (F). CSP decrypts the massage signature client (d_4) and check with information access control list sent by owner in the table (1) and (2)

Figure (8) CSP Decryption Client Message (P_2)

CSP encrypts a massage by message signature using public keys (R_2). The public key is generated by the Chebyshev algorithm. CSP sends a request to the TPA containing the encrypted message ($P`_{22}$) that includes (File - id, Owner - id, Client - id) with CSP signature (R_2). The request is shown in figure (9)

Figure (9) CSP Encryption Message ($P`_{22}$)

CSP receiving the message ($P`_{22}$ )from TPA then check the contain message ( $P`_{22}$) include (file –id ,owner –id, client – id) show in the figure (10) .

Figure (11) CSP Checking Massage (P`$_{22}$)

The CSP resolves the signature of the message sender (P`$_{22}$) from TPA by using the TPA public key ($R_2$), then extracts the message ($P_{2\,2}$) and file update (F `) as shown in the figure (412).

Figure (12) CSP Decrepted Massage (P $_{22}$)

After that the CSP The updated file stores in the location of the old file in cloud show in the figure (13).

Figure (13) CSP Save Upload File in cloud

V. CONCLUSIONS

A number of conclusions were reached through the steps of system work. The following points show the basic conclusions which can be conducted from the proposed system:

1) The proposed system are provides data confidentiality, access control of share data, removes the burden of key management and file encryption/decryption byusers,support dynamically of users membership .
2) The use of a digital signature ensures the integrity and confidentiality of sharing data sent by users so that it cannot be read by the recipient TPA as it encrypts, sends a new encrypted signature and sends it to the CSP so that it cannot read its content
3) CSP proved to be effective in the security of cloud computing

REFERENCES

1. Peter, M. & Tim, G.,"The NIST definition of Cloud Computing", Information Technology Laboratory, 2009.
2. Furht B.&Escalante, A," Handbook of Cloud Computing", New York: Springer, 2010.
3. Richard Mayo, Charles Perng, “An explanation of where the ROIcomes from”, IBM, November 2009
4. P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
5. C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2)(2012) 220–232.
6. R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology (IIT), 2013, pp. 13–17.
7. M. B. Ghadge and A. S. A. Ubale, “A Survey on Block Design-based Key Agreement for Group Data Sharing in Cloud Background ”, IEEE Transactions on Dependable and Secure Computingpp, pp. 1189–1194,ISSN : 234-610 2018.
8. Y. Tang, P.P. Lee, J.C.S. Lui, R. Perlman, Secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput.9 (6) (2012) 903–916.
9. R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology (IIT), 2013, pp. 13–17.