International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.2, No.3, June 2013, pp. 184~193
ISSN: 2089-3337

SSAP: Augmentation based Secure Storage Authentication and Privacy System in Cloud Environment

T. Prasath*, N. Aravindhu, D. Rampriya***
*M.Tech Final Year, Departement of Computer Science and Engineering, Christ College of Engineering & Technology, Pondicherry University, Puducherry.
** Assistant Professor, Departement of Computer Science and Engineering, Christ College of Engineering & Technology, Puducherry.

Article Info

Article history:

Received Mar 12th, 2013
Revised Apr 15th, 2013
Accepted May 10th, 2013

Keyword:

Cloud storage
Cloud Suite
Persistence server
TUV server
Key server
Security

ABSTRACT

In a cloud storage system storing of data in a third party cloud system that causes serious concern about data confidentiality and in protecting the data via encryption schemes though it provides protection mechanism the functionality of storage system are limited and supports some malicious operations over encrypted data. Developing a cloud based business solution suite for an organization that well equipped with resourceful environment. This suite follows Trusted user verification server that checks for the user authentication to grab the data from the persistence server and some improved schemes such as ISID is facilitated. In this paper we enhance a SSAP (Secure storage authentication and privacy) system that proposes a re-encryption scheme that formulates the secure distributed storage system which is named as erasure code-based cloud storage system. The main contribution is the proxy re-encryption scheme which encodes the messages and forwarding operation over encrypted data. There are certain parameters for a number of copies of a message dispatched to storage servers queried by key servers. By using SUV (Straight unsigned verification) scheme the improved secrecy ID (ISID) scheme is addressed at the receiving end. These parameters allow more flexible adjustment between the storage servers and authentication between the two mediators which an ISID scheme that provides efficiency and provable secure system.

Corresponding Author:

T. Prasath,
M.Tech Final Year, Department of computer Science and Engineering,
Christ College of Engineering & Technology,
Pondicherry University, Puducherry.
Email: prasath.27101987@gmail.com

1. INTRODUCTION

In general cloud computing is an service provider via internet and perform a computational task according to the users need, but the user does not know what computation is performed at the back end and how the storage management was done. Storage-as-service is one of facility provided by cloud computing among various services. The need of this service was increasing rapidly because this service provide the cloud user a needed storage space and reduces the maintenance cost, many organization moves their data to the cloud storage and extending the storage capacity later according to their needs. In common robustness of the data was maintained by storing the copy of same data in different storage servers this replication method was done by an alternative encoding process by codeword symbol generation. If any storage server gets fault data retrieval was done based on the codeword symbol used. Storing of data in the providers storage system may cause a serious anxiety on data privacy. For this disadvantage a cryptographic method are used to store the data in cloud storage before the codeword symbol generation. This paper aims to develop a cloud based

business solution to enrich the surface of wealthier organization. There are many business suites which was not fulfilled with the exact needs of the business people to cope up with the day today security issues. Normally the business perspective some issues related to data consistency, maintenance, robustness and confidentiality are focused. So as to fulfill the needs of a business here the cloud based solution suite is developed for facilitating the robustness and privacy to confidentially maintain the persistent data. Here five major parts are decomposed as data transformer, persistence server, secure key server, trusted user verification server, data grabber. Data transformer are the users involved in forwarding the data to the receiver using their public and receiver private key. On considering the cloud persistence and secure key server, a system consists of various storage server and key server to maintain the robustness of data. Storing the cryptographic key in a single system or an local disk is risky, so to provide security in cloud server a cryptographic functions are used by key server behalf of user. A distributed persistence servers in the cloud environment follows an threshold proxy re-encryption scheme and erasure code method to maintain the data robustness and integrity. Encoding operation over encrypted data and forwarding operation over encrypted and encoded data was supported by these schemes which was applied in the persistence server, each individual persistence server performs proxy re-encryption and encoding process without depending on other server and partial decryption was carried out by a key server. In a SSAP system the persistence server allocation was done based on the message blocks and the key server was allocated based on the persistence server used, key server was less than the persistence server. On considering the trusted people verification server (TPVS) it follows an improved secrecy ID (ISID) scheme, which is developed from the Straight unsigned verification (SUV) scheme, which provides an revocation capabilities. This scheme follows certain procedure to maintain the privacy of ID and verification of members in a group, this was done to make the system a secure one. The data grabbers are the user involved in retrieving the data which was forwarded by the data forwarder, to perform this they involve in compromising the TPVS server by proving that they are the authorized user to access the forwarded data.

2. ARCHITECTURAL VIEW OF A SSAP SYSTEM

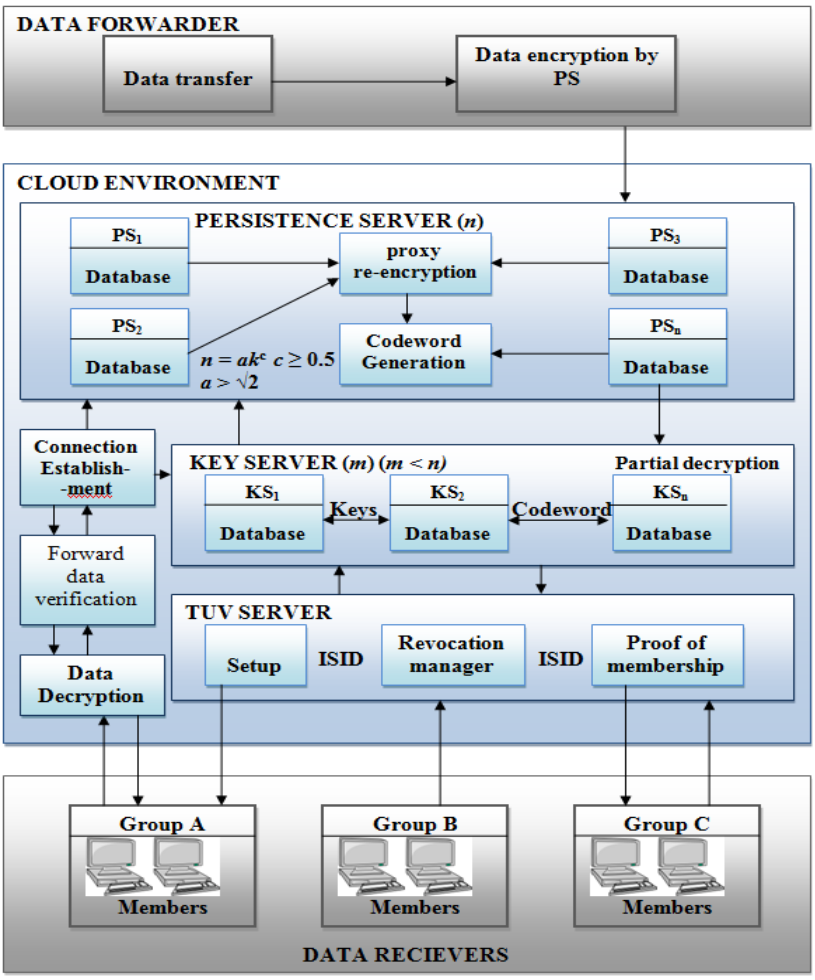

Figure 1. Architectural view of a SSAP system

The overall design of a SSAP system contains the cloud environment with effective services. There are different servers in it, which provide security, integrity, privacy services through the cloud environment. This system uses persistence server, key server and TPV server to provide the above mentioned services. In this system the allocation of the persistence servers and the key servers are done based on certain criteria, which involves in the proxy re-encryption, code generation and secure storage. The TPV server is indicated with certain schemes to maintain the privacy of user in a group and provides membership authentication for group members. The scheme followed in TUVS includes a revocation list to maintain the details of authorized and unauthorized user.

3. SSAP MAJOR PARTS:

In SSAP system major five parts involved are decomposed they are, data transfer module in with data files are encrypted before transformed, Persistence Server module deals with the proxy re-encryption, data robustness, Key server module deals with secure key maintenance, TUVS deals with verification and authorization.

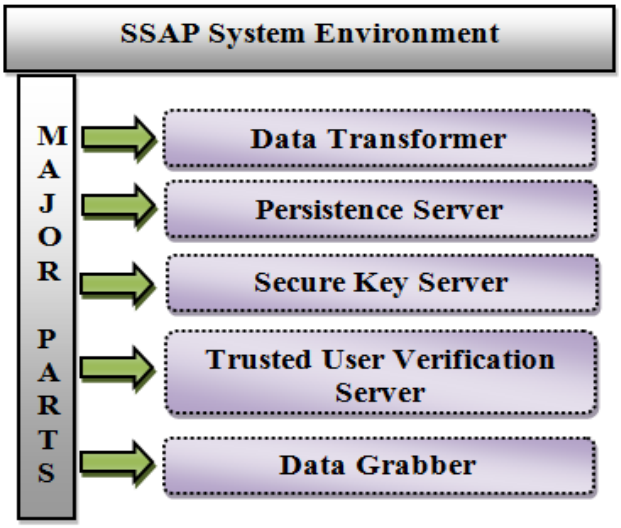

Figure 2. Major parts of SSAP system

4. DATA TRANSFORMER

Data transformer are the users uses the cloud network to perform data transformation for different users at the receiver end. To perform this action the user undergoes the join procedure to have his/here own account to access the persistence server to store the data and deliver the file to different grabbers in the other end who are considered as an authorized person to receive the file form the sender. Certain process carried by the Data transformer are account creation, file encryption via server, data forwarding.

4.1. Account Creation

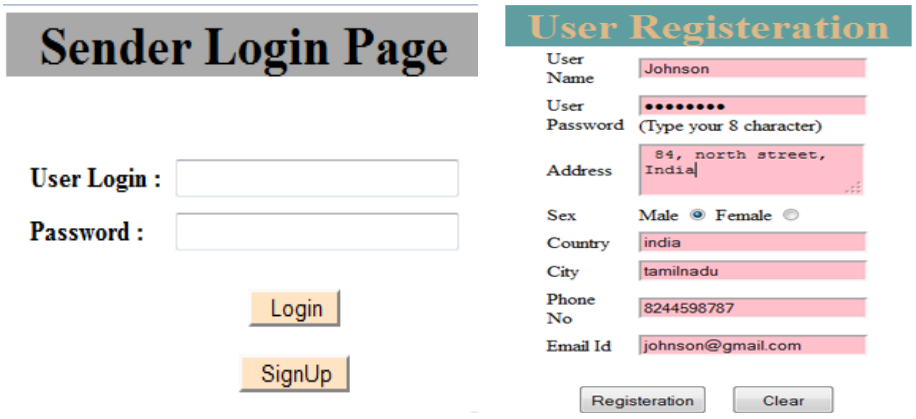

Figure 3. New account creation for data forwarder

In this phase is user A will create a new account for the data transformer. To create a new account user A undergoes registration process by providing the basic information in the registration form, here the account creator will choose his/her own private and public key. If the registration process gets successes they became an new user to access the persistence server to store the files and forward the files.

4.2. File encryption

The file that has to be stored/forwarded was encrypted for security reason. For this the persistence server access person will upload the file through an web page provided, if the uploading file process gets completed the encryption take place automatically via server because of this facility the file forwarder user A will not involve in time allocation for encryption process.

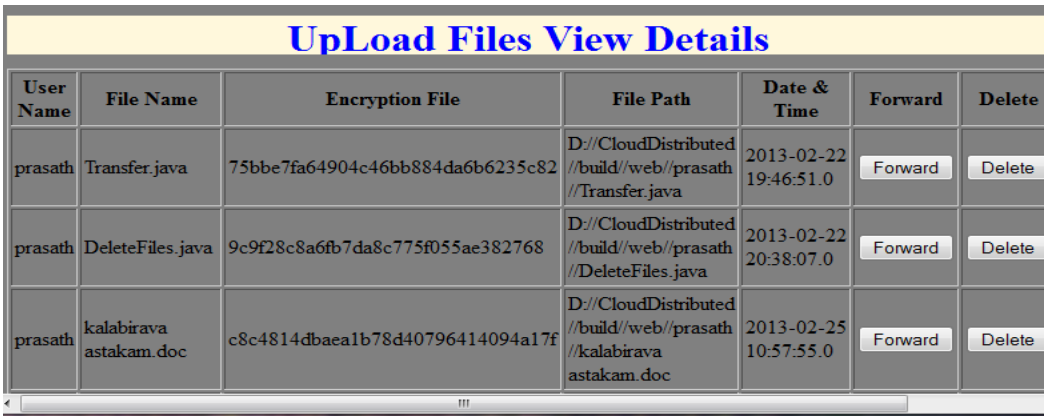

Figure 4. Overview of uploaded file encrption

4.3. Data Forwarding

Here the data/file transformer user A will use the public key of the receiver user B to forward the file. Based on the private key of user A and public key of user B provided the server will delivers the file to user B.

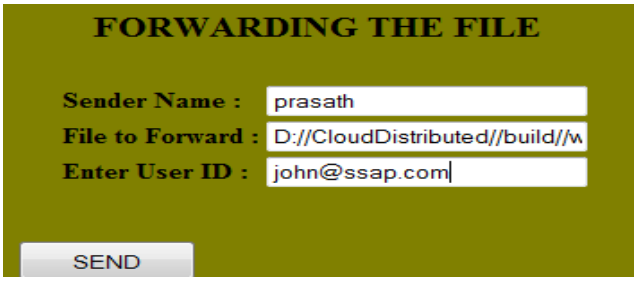

Figure 5. Sample view of file forwarding

5. PERSISTENCE SERVER (PS)

The persistence server provides storage space for the cloud account holder. This server involves in data partition, proxy re-encryption and code creation. Imagine that there are 'n' distributed storage servers in the cloud Persistence system. A message is divided into k blocks and represented as a vector of 'k' symbols [1]. To provide a secure storage system a proxy re-encryption method was done this method supports decentralized erasure codes on the encrypted messages and forwarding operations over encrypted and encoded messages[2]. The server allocation was done by considering the given formula $n=ak^c$ where $c\geq 1.5$ and $a>\sqrt{2}$ outcome allows the number of storage servers which much be greater than the number of blocks of a message k. Each storage system which was allotted for storing the block of data will holds the codeword symbol which is an encoded result. Encoded result was obtained based on the combination of encoded message. To maintain data robustness copies of messages/data are stored in different persistence servers. Some of the Phases involved in persistence server are Novel user allocation, Data Storage, Data Forwarding, Data Retrieval, and System Recovering.

Encrypt Files						
User Name	File Server1	File Size	File Server2	File Size	File Server3	File Size
raja	c3ef7e79079	12kb	3c6ab09a49df	1kb	dcbb96d63	1kb
raja	1dac1a479e5	15kb	b88aa778795e	1kb	0732cabef	18kb
raja	664364c29be	4kb	8e6c87353d9b	1kb	eedaf466d	12kb
ganesh	aa0ce151f91	1kb	10390cf0bb74	0kb	64e3d6c7c	12kb
null	23d43567531	2kb	399d0c58f473	3kb	832265eed	0kb
kannan	c432b62dd56	18kb	d3a415aa0140	0kb	d87c58dc9	3kb
null	880cfb88e3d	3kb	b5bbbb91e28b	2kb	1fe9dc2ef	1kb
null	93a7d908af3	7kb	e87aab099150	4kb	89a431b9b	15kb
prasath	75bbe7fa649	1kb	04c46bb884da	9kb	6b6235c82	3kb

Figure 6. overview of storage servers

5.1. Novel User allocation

In this phase access for new user A was provided by the cloud persistence server, after getting the basic system parameters from A. Finally user A will holds private and public key (PK_A, SK_A) then the key was transferred to key server for security reason.

5.2. Data Storage

Here the encrypted message was dispatched to the storage server then the message was divided into a ‘k’ block, each block will holds an ID. Each block messages are encrypted into an cipher text and send to the arbitrarily selected storage servers[3][4]. Consider that the storage server may holds less than ‘k’ message blocks. Assume that all the storage server already recognizes the value of ‘k’.

5.3. Data Forwarding

In this phase the encrypted message in the persistence with identifier ID was forwarded to the receiver user B. User B at the receiving end will perform decryption to retrieve the message using his secret key[7]. To do this the user A will use his secret key (SK_A) with user B’s pubic key (PK_B) with helps in re-encryption computation $RK^{ID}_{A\rightarrow B}$. The obtained computational result was send to all selected persistence servers. Then each server involves in re-encrypt the codeword symbol for the lateral retrieval by the user B. Based on the provided public key of B the re-encryption of the code word was carried out.

5.4. Data Retrieval

In this phase the user A or user B involves in retrieving the message/data from the persistence server. The data stored in the server may be stored by him or forwarder to him. The user involves in retrieving the data will send an request to the storage server via key server, an authentication process was carried out by an server with the users involved. After the process gets completed the decryption of data was done through key server to obtain an original message/data.

5.5. System Recovering

If any allotted storage server undergone failure then a new server is added in the system recovering phase. The newly available server will send a query to ‘n’ available server to retrieve the code word symbol, a linear combination was done for retrieval and stores it.

6. SECURE KEY SERVER (SKS)

Key Severs stores the private and public key of the user and decrypt it. The key provided to the user during the registration process was moved to the key server so that the user can retrieve the key if he forget it. The key server plays an important role during message/data retrieval by a users A or B. After authentication process completed with user A at the data retrieval phase, each key server KS_i needs ‘n’ arbitrarily selected persistence servers to get codeword symbols and does fractional decryption on the received codeword symbols by using the key share $SK_{A,i}$. To end with, user A combines the partly decrypted codeword symbols to obtain the unique message M.

Key Server Details

ID	UserName	Encryption Password	Decryption Password
9	suresh	¬6i	suresh12345
10	raja	k21{^XÜÎ—f□ø‹3+	raja658923
11	viji	I¾ÇÆNH3=c>âòcþ	viji43575788

Figure 7. overview of key server

7. Trusted user verification server (TUVS)

This server provides security for the user ID and for the data in the persistence server. The users involves in downloading/grabbing the data from the persistence server have to compromise this server to prove that they are the authorized users to download the file/data. TUVS follows straight unsigned verification (SUV) that is an improved secrecy ID (ISID) scheme for an cancellation capabilities. ISID involves four procedure they are setup, bond process, verification of correlation, Revocation.

7.1. Setup

In this procedure the grabber at the receiver end will get his group public key and the private key for server compromisation at later. Here the server gets the requirements from the receiving end user and process the received information from the user B to provide the private and public key here the user does not chose his own key. The server will generate and issuer will provide the private and public key to the user B/data grabber.

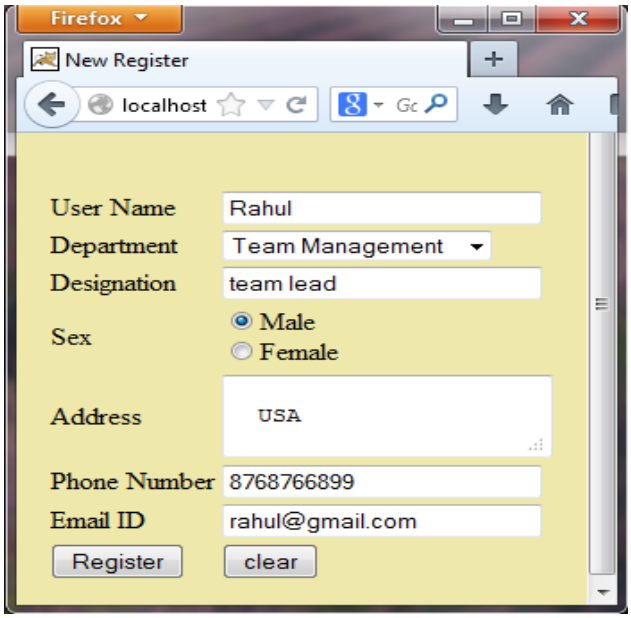

Figure 8. Account creation for receiver/data grabber

7.2. Bond process

In this procedure the bonding process that is an agreement between the issuer and the user B was processed to get an group correlation at the end of agreement processing the User B will get the group public and private key.

Figure 9. Publishing private and public key

7.3. Verification of correlation

Here a steps was followed between the prover user B and the verifier before downloading the data/file from the persistence server which was forwarded by user A[10]. The steps involved are:

- Verifier receives the request from the user B for downloading the data,
- User B receives the response from the verifier for Authentication process,
- An signature process was carried out between the user B and verifier,
- Authentication of signature was done by verifier after receiving the signature from user B,
- At last authorization was given by verifier to download the data.

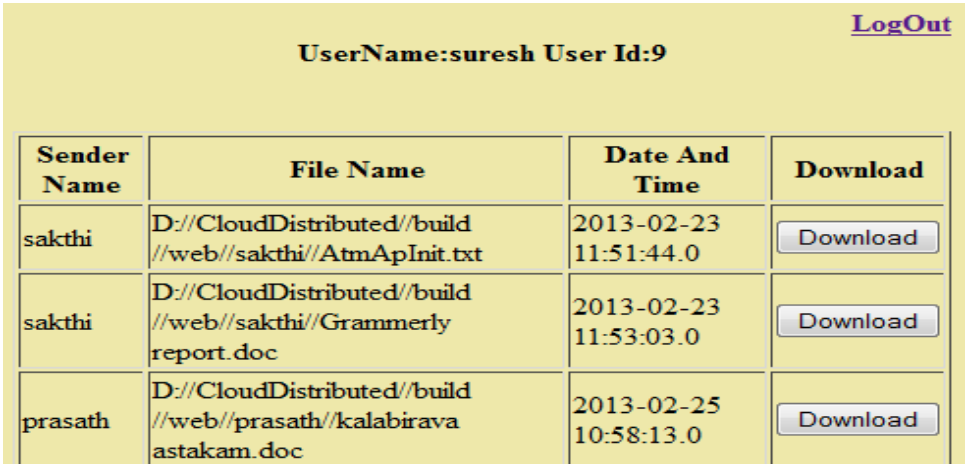

Figure 10. Alloted account for new user

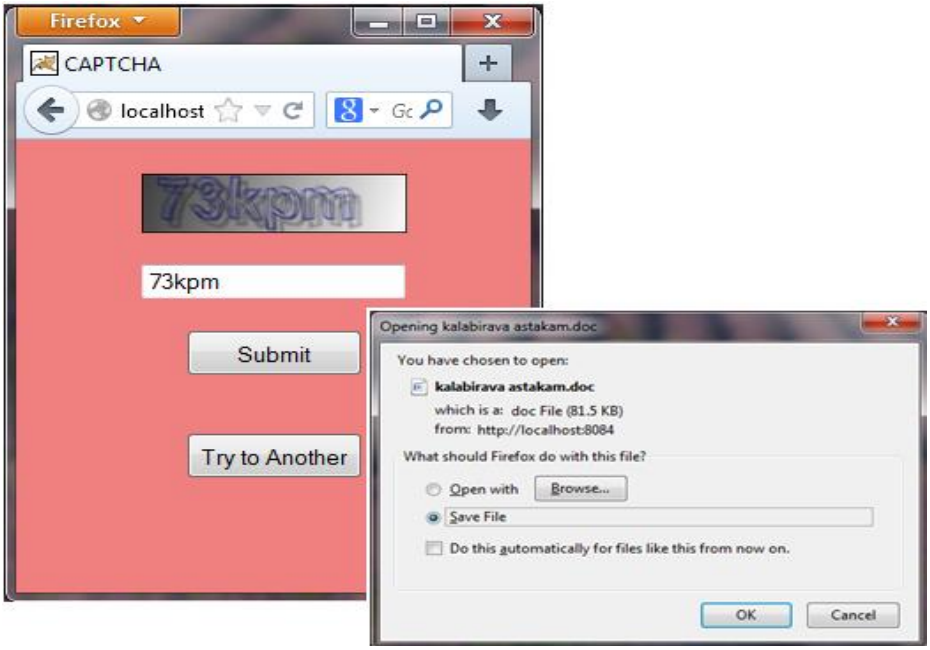

Figure 11. Secure file download

In this paper the signature verification was given in the form of security enhancement and verification. Consider that the user B uses his public and private key given by the issuer to perform login to access his cloud account to view his files which was forwarded by user A. when the download link was used, a signature process was carried out in the form of security enhancement and verification if user B is a authorized one than an download of an file started at the end of this process.

7.4. Revocation

Here revocation carried out based on the private key of the member, signature performed by the user/receiver and issuer proposal. A list was maintained in this procedure to prove security for the data and the ID of the user. Account holders information are maintained at the revocation list[8]. Here two list are maintained they are authorized user list and unauthorized user list. In the authorized list and grabbers/data receivers information who have proper access of persistence server to download file was maintained. In an unauthorized list an unauthorized person those who involves in access the persistence server without account or hackers information was maintained[9]. If any person tries to compromise the server through login page an comparison was made in the revocation list to check that the compromiser is an proper user are an third party/hacker.

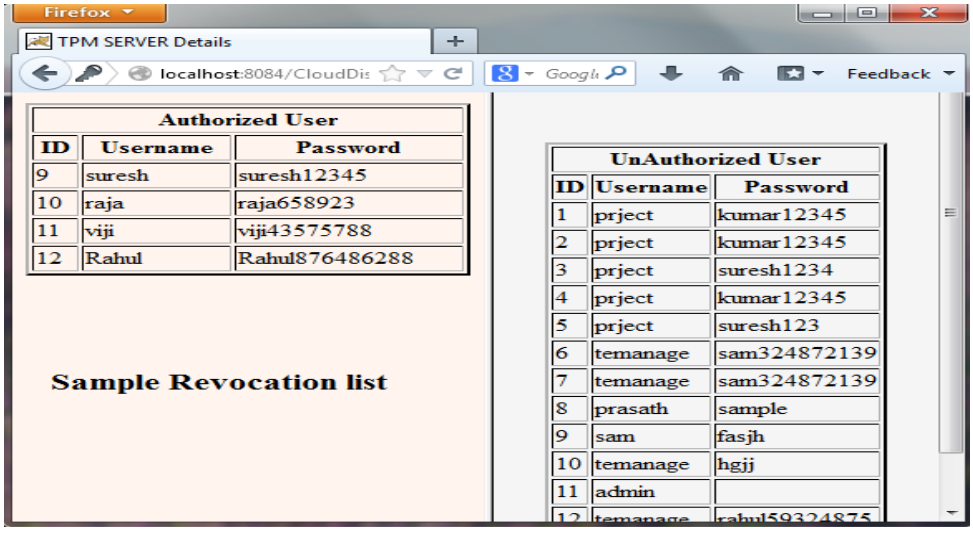

Figure 12. Sample revocation list for authorized and unauthorized user

8. DATA GRABBER

Data grabbers are the authorized user to retrieve the data/file which was forwarded to him. In this paper consider user B is a data grabber. Data grabber involves in account creation to become an authorized user to retrieve data from persistence server, forward data retrieval.

8.1 Account creation

Here the user under the role of receiving the forwarded data should have an account to access the cloud persistence server if he is member of an group. To become an member, a procedure in the form of information filling needed by the server was performed via given registration form and the success register will provide a new account to the user.

Figure 13. Login facility for grabber

8.2 Forward data retrieval

In data retrieval the user/data Grabber has to compromise the TUVS to access Key Server and persistence server. After compromising process gets completed partial decryption was done via key server and original data was obtained from the persistence server. All the above mentioned procedures in the TUVS, KS, PS servers performed for secure data retrieval.

9. CONCLUSION

On focusing security issues on cloud in this paper aims at developing a package and can be deployed on any business solution which provides the cloud enhanced environment. The package that works upon data security, confidentiality, integrity and privacy related issues to provably develop a secure storage and authentication privacy (SSAP) system in a well equipped organization. There are many supporting back end servers to access a secure data in the cloud are developed and maintained. Furthermore the proxy based schemes that are used for cloud storage system to encode and forward the ciphered data. Many schemes are used for sending and receiving the data from the storage servers which is resolved by the key server. Finally the enhancement of SSAP system is developed to provide efficiency and provable secure system. In the near future this system can be further developed as open source software on ensuing tight data security.

REFERENCES

[1] X. S. Li, *et al. Analysis and Simplification of Three-Dimensional Space Vector PWM for Three-Phase Four-Leg Inverters.* IEEE Transactions on Industrial Electronics. 2011; 58: 450-464

[2] Hsiao-Ying Lin and Wen-Guey Tzeng. *A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding.* IEEE transactions on parallel and distributed systems. 2012; 23.

[3] J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao. *Oceanstore: An Architecture for Global-Scale Persistent Storage*. Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS). 2000; 190-201.

[4] P. Druschel and A. Rowstron. *PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility.* Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII). 2001; 75-80 .

[5] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer. *Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment*. Proc. Fifth Symp. Operating System Design and Implementation (OSDI). 2002; 1-14.
[6] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran. *Ubiquitous Access to Distributed Data in Large-Scale Sensor Networks through Decentralized Erasure Codes*. Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN). 2005; 111-117.
[7] Q. Tang. *Type-Based Proxy Re-Encryption and Its Construction.* Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT). 2008; 130-144.
[8] Ernie Brickell and Jiangtao Li. *Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities*. IEEE transactions on dependable and secure computing. 2012; 9(3): 345.
[9] E. Brickell, J. Camenisch, and L. Chen. *Direct Anonymous Attestation* Proc. 11th ACM Conf. Computer and Comm. Security. 2004; 132-145.
[10] D. Boneh and H. Shacham. *Group Signatures with Verifier-Local Revocation*. Proc. 11th ACM Conf. Computer and Comm. Security. Oct. 2004; 168-177.
[11] J. Camenisch and A. Lysyanskaya. *A Signature Scheme with Efficient Protocols*. Proc. Third Conf. Security in Comm. Networks. 2002; 268-289.
[12] D. Boneh, X. Boyen, and H. Shacham. *Short Group Signatures*. Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '04). 2004; 41-55.
[13] J. Camenisch and M. Stadler. *Efficient Group Signature Schemes for Large Groups*. Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '97). 1997; 410-424.

BIOGRAPHY OF AUTHORS

Mr. T. Prasath pursuing my Post Graduation Final Year M.Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under Graduation (B.E.) at I.F.E.T College of Engineering, Gangrampalayam, Villupuram. Anna University Affiliated.

Mr. N. Aravindhu, Assistant Professor Department of Computer Science & Engineering. Completed M.Sc (Software Engineering) at Annamalai University and Completed M.Tech (Computer Science & Engineering) at Pondicherry University.

Mrs. D. Rampriya pursuing my Post Graduation Final Year M. Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under Graduation (B.E.) at A.V.C Engineering College, Mannampandal, Mayiladuthurai. Anna University Affiliated.