A NOVEL APPROACH TO SECURE DISTRIBUTED DATA STORAGE SCHEME WITH IDENTIFY BASED MECHANISM

Shaik Noorjahan & B.Srikanth

RollNO: 15JF1D5816, Pursuing M.Tech – CSE, Gandhiji Institute of Science & Technology,
Gattu Bhimavaram.
Email: noor.aankhein@gmail.com

Associate Professor, Dept of CSE, Gandhiji Institute of Science & Technology,
Gattu Bhimavaram.
Email: srikanthjf358@gmail.com

1. ABSTRACT:

Secure distributed data storage can shift the burden of maintaining a large number of files from the owner to proxy servers. Proxy servers can convert encrypted files for the owner to encrypted files for the receiver without the necessity of knowing the content of the original files. In practice, the original files will be removed by the owner for the sake of space efficiency. Hence, the issues on confidentiality and integrity of the outsourced data must be addressed carefully. In this paper, we propose two identity-based secure distributed data storage (IBSDDS) schemes. Our schemes can capture the following properties: (1) The file owner can decide the access permission independently without the help of the private key generator (PKG); (2) For one query, a receiver can only access one file, instead of all files of the owner; (3) Our schemes are secure against the collusion attacks, namely even if the receiver can compromise the proxy servers, he cannot obtain the owner's secret key. Although the first scheme is only secure

Against the chosen plaintext attacks (CPA), the second scheme is secure against the chosen cipher text attacks (CCA). To the best of our knowledge, it is the first IBSDDS schemes where access permissions is made by the owner for an exact file and collusion attacks can be protected in the standard model.

1.1 Scope:

Access permission (re-encryption key) is bound not only to the identity of the receiver but also the file. The access permission can be decided by the owner, instead of the trusted party (PKG). Furthermore, our schemes are secure against the collusion attacks.

1.2 Problem Statement:

Users are especially concerned on the confidentiality, integrity and query of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by an untrusted third pa

2. EXISTING SYSTEM:

- Cloud computing provides users with a convenient mechanism to manage their personal files with the notion called database-as-a-service (DAS).
- In DAS schemes, a user can outsource his encrypted files to untrusted proxy servers.
- Proxy servers can perform some functions on the outsourced cipher texts without knowing anything about the original files. Unfortunately, this technique has not been employed extensively.
- The main reason lies in that users are especially concerned on the confidentiality, integrity and query of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by an untrusted third party.
- After outsourcing the files to proxy servers, the user will remove them from his local machine.
- Therefore, how to guarantee the outsourced files are not accessed by the unauthorized users and not modified by proxy servers is an important problem that has been considered in the data storage research community.
- Furthermore, how to guarantee that an authorized user can query the outsourced files from proxy servers is another concern as the proxy server only maintains the outsourced cipher texts. Consequently, research around these topics grows significantly.

2.1 DISADVANTAGES OF EXISTING SYSTEM:

- Users are especially concerned on the confidentiality, integrity and query of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by an untrusted third party.
- The outsourced files are not accessed by the unauthorized users and not modified by proxy servers is an important problem that has been considered in the data storage research community.

3. PROPOSED SYSTEM:

In this paper, we propose two identity-based secure distributed data storage (IBSDDS) schemes in standard model where, for one query, the receiver can only access one of the owner's files, instead of all files. In other words, access permission (re-encryption key) is bound not only to the identity of the receiver but also the file. The access permission can be decided by the owner, instead of the trusted party (PKG). Furthermore, our schemes are secure against the collusion attacks.

3.1 ADVANTAGES OF PROPOSED SYSTEM:

- It has two schemes of security, the first scheme is CPA secure, and the second scheme achieves CCA security.

- To the best of our knowledge, it is the first IBSDDS schemes where access permission is made by the owner for an exact file and collusion attacks can be protected in the standard model.
- To achieve a stronger security and implement file based access control, the owner must be online to authenticate requesters and also to generate access permissions for them. Therefore, the owner in our schemes needs do more computations than that in PRE schemes. Although PRE schemes can provide the similar functionalities of our schemes when the owner only has one file, these are not flexible and practical.

4. SYSTEM MODULES:

1. Owner
2. Proxy server
3. Receiver
4. Storage scheme modules

4.1 TORAGE SCHEME MODULES:

क्र Data Storage Systems
अ Networked File Systems (NFS)
अ Storage-Based Intrusion Detection Systems (SBIDS)
अ Cryptographic File Systems (CFS).
क्र Identity-based Proxy Re-encryption
क्र Identity-based Secure Distributed Data Storage

Data storage systems:

Data storage systems enable users to store their data to external proxy servers to enhance the access and availability, and reduce the maintenance cost. It is classified them into three kinds based on their security services:

अ Networked File Systems (NFS)
अ Storage-Based Intrusion Detection Systems (SBIDS)
अ Cryptographic File Systems (CFS).

Networked File Systems:

Proxy servers are assumed to be trusted. They authenticate receivers and validate access permissions. The interactions between the proxy servers and receivers are executed in a secure channel. Therefore, these systems cannot provide an end-to-end data security, namely they cannot ensure the confidentiality of the data stored at the proxy server. In these schemes, a receiver authenticates himself to the proxy server using his password. Then, the proxy server passes the authentication result to the file owner. The owner will make access permission according to the received information.

Storage-Based Intrusion Detection Systems:

An intrusion detection scheme is embedded in proxy servers or the file owner to detect the intruder's behaviors, such as adding backdoors, inserting Trojan horses and tampering with audit logs. These schemes can be classified into two types:

अ Host-based system
अ Network-based system.

Cryptographic File Systems:

An end-to- end security is provided by cryptographic protocols which are executed by the file owner to prevent proxy servers and unauthorized users from modifying and accessing the sensitive files.

Identity-based proxy Re-encryption:

Semi-trusted proxy server can transfer a cipher text for the original decryptor to a cipher text for the designated decryptor without knowing the plaintext. Identity-based cryptosystem introduced by Shamir is a system where the public key can be any arbitrary string and the secret key is issued by a trusted party called the private key generator (PKG). Being different from public key infrastructure (PKI), two parties can communicate directly without verifying their public key certificates in identity-based systems.

Identity-based secure distributed data storage:

A user's identity can be an arbitrary string and two parties can communicate with each other without checking the public key certificates. At first, the file owner encrypts his files under his identity prior to outsourcing them to proxy servers. Then, he sends the cipher texts to the proxy servers. Consequently, the proxy servers can transfer a cipher text encrypted under the identity of the owner to a cipher text encrypted under the identity of the receiver after they has obtained an access permission (re-encryption key) from the owner

5. HARDWARE&SOFTWARE REQUIREMENTS

5.1 HARDWARE REQUIREMENTS:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Ram : 512 MB.

5.2 SOFTWARE REQUIREMENTS:

- Operating system: Windows 7 .
- Coding Language : C# .Net
- Front End Tool :Visual Studio 2008

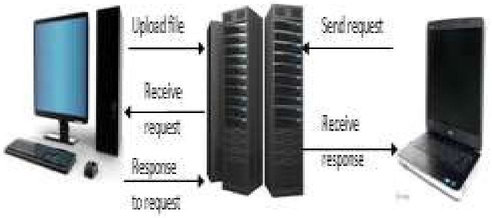
6. SYSTEM DESIGN

6.1 Design Overview

Design involves identification of classes, their relationships as well as their collaboration. In objectory, classes were divided into Entity classes, interface classes and the control classes. The Computer Aided Software Engineering tools that are available commercially do not provide any assistance in this transition. Even research CASE tools take advantage of Meta modeling are helpful only after the construction of class diagram is completed. In the Fusion method ,it used some object-orientedClass-Responsibility and Collaborator(CRC) and Objectory, used the term Agents to represent some of the hardware and software systems .In Fusion method, there was no requirement phase ,where in a user will supply the initial requirement document. Any software project is worked out by both analyst and designer. The analyst creates the Use case diagram.

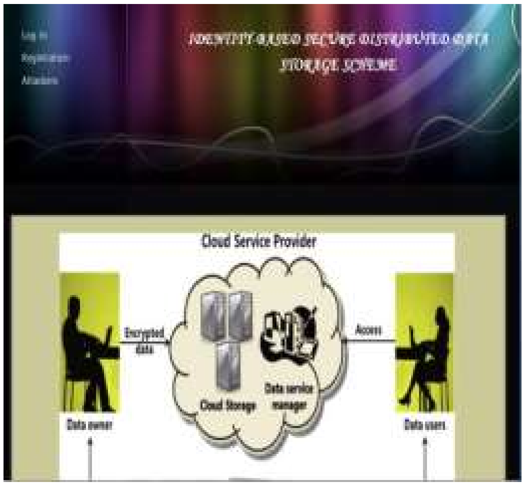
The designer creates the Class diagram. But the designer can do this only after the analyst has created the Use case diagram. Once the design is over it is need to decide which software is suitable for the application

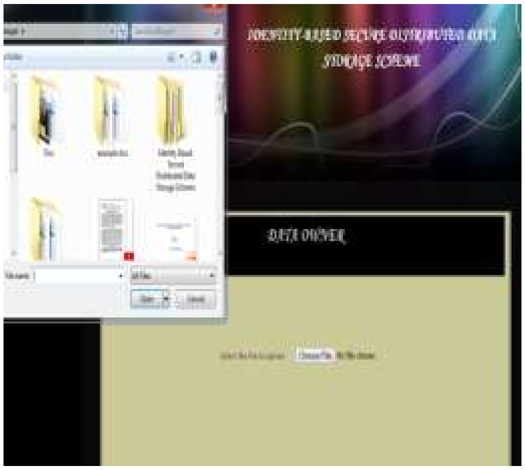
6.2. Architecture diagram



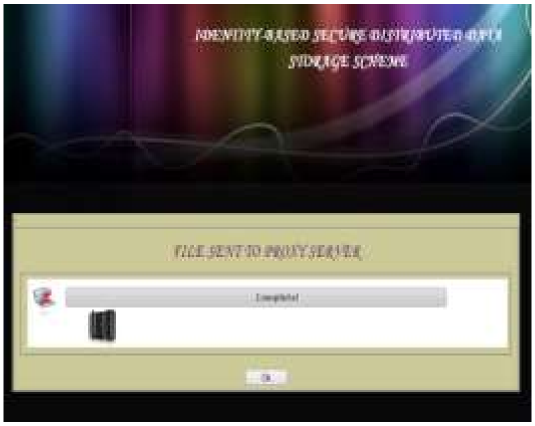
Owner Proxy Server Receiver

7. RESULTS:

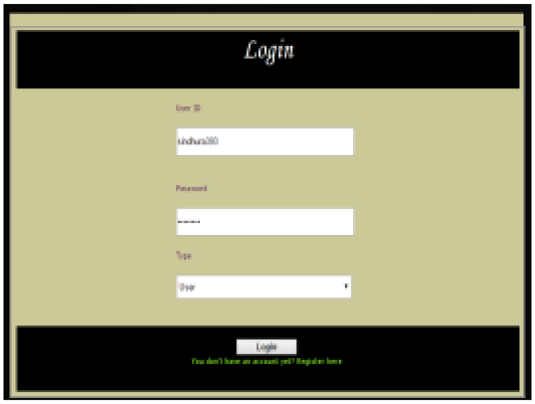




Screen shot: Choosing a file from system


IDENTITY BASED SECURE DISTRIBUTED DATA STORAGE SCHEME
FILE SENT TO PROXY SERVER
Completed
OK

Screen shot: Uploading file



User ID

sindhura200

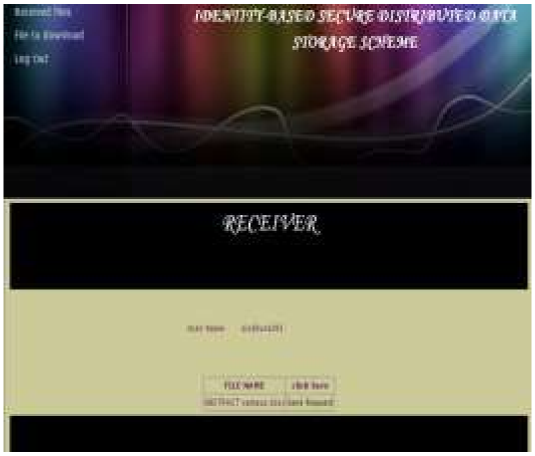
Password

Type

User

You don't have an account yet? Register here

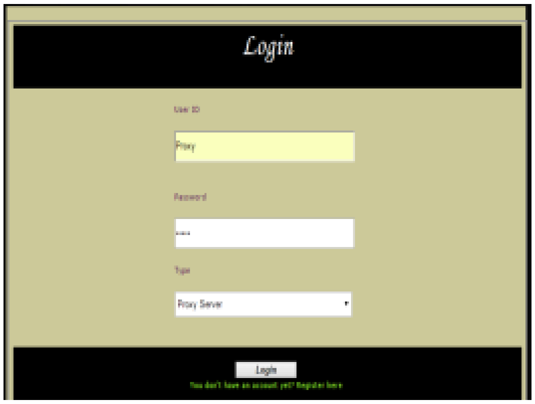
Screen shot: login page for user



IDENTITY-BASED SECURE DISTRIBUTED DATA STORAGE SCHEME

RECEIVER

Screenshot: User sending request for file



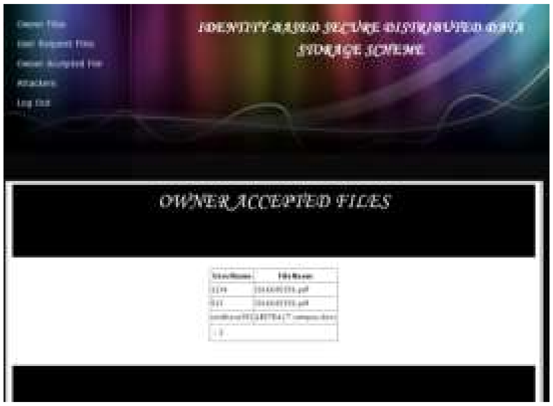
Login

User ID: Proxy

Password: ****

Type: Proxy Server

Screen shot: Proxy login page



IDENTITY-BASED SECURE DISTRIBUTED DATA STORAGE SCHEME

OWNER ACCEPTED FILES

Screen shot: Details saved by Proxy server.

Hackers Detected in Proxy Server

8. CONCLUSION

Distributed data storage schemes provide the users with convenience to outsource their files to untrusted proxy servers. Identity-based secure distributed data storage (IBSDDS) schemes are a special kind of distributed data storage schemes where users are identified by their identities and can communicate without the need of verifying the public key certificates. In this paper, we proposed two new IBSDDS schemes in standard model where, for one query, the receiver can only access one file, instead of all files. Furthermore, the access permission can be made by the owner, instead of the trusted party. Notably, our schemes are secure against the collusion attacks. The first scheme is CPA secure, while the second one is CCA secure.

9. FUTURE ENHANCEMENTS

Our future enhancements for identity-based secure distributed data storage (IBSDDS) are to allow user to upload PDF files and excel sheets. Future research will include advancements like uploading the pictures, images, videos in encrypted format for user convenience.

10. BIBLIOGRAPHY

1. H. Hacig¨ um¨ us, B. R. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in Proceedings: SIGMOD Conference - SIGMOD'02 (M. J. Franklin, B. Moon, and A. Ailamaki, eds.), vol. 2002, (Madison, Wisconsin, USA), pp. 216–227, ACM, Jun. 2002. [2]

2. L. Bouganim and P. Pucheral, "Chip-secured data access: Confi- dential data on untrusted servers," in Proc. International Conference on Very Large Data Bases - VLDB'02, (Hong Kong, China), pp. 131–142, Morgan Kaufmann, Aug. 2002.

3. U. Maheshwari, R. Vingralek, and W. Shapiro, "How to build a trusted database system on untrusted storage," in Proc. Symposium on Operating System Design and Implementation - OSDI'00, (San Diego, California, USA), pp. 135–150, USENIX, Oct. 2000.

4. A. Ivan and Y. Dodis, "Proxy cryptography revisited," in Proc. Network and Distributed System Security Symposium - NDSS'03, (San Diego, California, USA), pp. 1–20, The Internet Society, Feb. 2003.

A. Shamir, "Identity-based cryptosystems and signature scheme," in Proc. Advances in Cryptology - CRYPTO'84 (G. R. Blakley and D. Chaum, eds.), vol. 196 of Lecture Notes in Computer Science, (Santa Barbara, California, USA), pp. 47–53, Springer, Aug. 1984. 5. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Proc. Advances in Cryptology - CRYPTO'01 (J. Kil- ian, ed.), vol. 2139 of Lecture Notes in Computer Science, (Santa Barbara, California, USA), pp. 213–229, Springer, Aug. 2001.

6. M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. Applied Cryptography and Network Security - ACNS'07 (J. Katz and M. Yung, eds.), vol. 4521 of Lecture Notes in Computer Science, (Zhuhai, China), pp. 288–306, Springer, Jun. 2007.