Data Sharing using BFID Encryption for Privacy Preseration of Data in Cloud

Mr. Swapnil P. Deshmukh
ME Student
Department of Computer Science
S. S. G. B. College of Engineering
Bhusawal, India
swarup3369@gmail.com

Prof. Yogesh S. Patil
Assistant Professor
Department of Computer Science
S. S. G. B. College of Engineering
Bhusawal, India
yogeshe146@gmail.com

Prof. Dinesh D. Patil
Head of Department
Department of Computer Science
S. S. G. B. College of Engineering
Bhusawal, India
dineshonly@gmail.com

***Abstract*—**The most important functionality in cloud storage is data sharing. With the advent of cloud computing [1], data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy and integrity, sensitive data have to be encrypted before outsourcing, which causes the need of traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance.Typically cloud computing is a combination of computing recourses accessible via internet. Historically the client or organizations store data in data centers with firewall and various security techniques used to protect data against intrudes to access the data. Since the data was contained to data centers in limits of organisation, the control over the data was more and well defined procedures could be used for accessing its own data. Howeverin cloud computing, since the data is stored anywhere across the world, the client organizations have less control over the stored data.Identity-Based Encryption (IBE) which is used to simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. **Identity-based encryption (IBE**) is an important aspect of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is provides unique information about the identity of the user (e.g. a user's Identification). This can use the text-value of the name or domain name as a key or the physical IP address it translates to.

Keywords *- Computing, identity, storage, data, cloud*

*****

I. INTRODUCTION

In networking technology sectors and an increase in the need for computing resources have encourage many organizations to outsource their storage and computing needs. [2][3]This new economic and computing model is commonly called to as cloud computing and includes various types of services such as: infrastructure as a service (IaaS), where a customer makes use of a service provider's computing, networking or storage infrastructure; platform as a service (PaaS), where a customer leverages the provider's resources to run custom applications; and finally software as a service (SaaS), where customers use various software that are run on the providers infrastructure.Cloud computing is a way of computing in which dynamically scalable and commonly virtualized resources are provided as a service over the Internet. In recent years, more and more users store their sensitive data in cloud. To ensure the security of the remotely stored data, users need to encrypt important data. Cloud systems can be used to enable data sharing capabilities and this can provide a huge benefit to the user. According to a survey by Information Week, nearly all organisations shared their data somehow with 74 % sharing their data with customers and 64 % sharing with suppliers.

Key Properties to Cloud Computing:

- **User centric: -** once user connected with cloud, user can access images data messages applications, whatever- becomes authorized to the user access.
- **Task centric: -** instead of focusing on the application,here the focus is on what one needs to be done and the application customized for us.
- **Powerful: -** connecting hundreds of thousands of computers together in a cloud creates a wealth of computing power which is impossible for single desktop pc.
- **Accessible: -** because data is stored in cloud user can retrieve more information from multiple repositories.
- **Intelligent: -** with all the data stored in computers of cloud, data mining and analysis are necessary to access that information in an intelligent manner.
- **Programmable: -** many of the tasks necessary with the cloud must be automated. foreg. data to protect the integrity of data information stored on single computer must be replicable on other computers in cloud. If one computer goes offline cloud's programming automatically redistributes the data to other computers.

II. RELATED WORKS

Proposed by Mambo and Okamoto[4], a proxy cryptosystem is a systemwhere a user can delegate his/her decryption right to a designated decrypter.Subsequently, Blaze, Bleumer and Strauss14 extended this notion by introducing the concept of proxy re-encryption (PRE). In this new cryptographicprimitive, a proxy server can transfer a ciphetext designated for one user toanother ciphertext designated for another user without the need to have theknowledge on the plaintext.

Introduced by Shamir[5], identity-based encryption (IBE) is an efficientcryptographic system where the public key can be any arbitrary string andthe secret key is extracted from a trusted party called private key generator(PKG).

Boneh and Franklin[6] proposed the first practical IBE scheme basedon the bilinear group. Since its seminal introduction, IBE schemeshavebeen discussed extensively as in this new cryptographic notion, the need forpublic key infrastructure (PKI) has been eliminated efficiently.

Ivan and Dodis[7] proposed two identity-based proxy encryption schemeswhere the master secret key held by the PKG is split into two parts. One is forthe user and the other is for the proxy server. Then, the user can cooperatewith the proxy server to decrypt a ciphertext. Unfortunately, these schemesare not secure against the collusion attacksas the user and the proxy servercan collaborate to compute the master secret key.

Green and Ateniese[8] introduced the concept of identity-based proxy re encryption (IBPRE). In an IBPRE scheme, a proxy server can transfer aciphertext encrypted under one identity to a ciphertext encrypted under another identity without learning the contents of the plaintext.

Subsequently, Matsuo[9] proposed two IBPRE schemes. In the first scheme, a ciphertext encrypted under traditional PKI can be transferred to a cipher text encrypted under an identity in IBE schemes. Meanwhile, the secondscheme is proposed to transfer a ciphetext encrypted under the identity ofthe original decyprter to a ciphertext encrypted under the identity of the designated decrypter.

Boyang Wang, Baochun Li and HuiLi[10] introduces Knox is a privacy preserving mechanism for data stored in the cloud and shared among a large number of users in a group. In know,group signature is used to construct homomorphic authenticators, so that a third party auditor (TPA)is able to verify the integrity of the shared data for users without retrieving the entire data .In it the identity of the signer on each block in shared data is kept private from TPA. Knox exploits homomorphic MACs to reduce the space used to store verification information.

III. PROPOSED SYSTEM

Identity-based encryption (IBE)[12][13][14] is a type of public-key encryption in which the public-key of a user can be set as an identity-string of the user (e.g.an email address). There is a trusted party called Third party auditor (TPA) in IBE which holds a master-secret key and issues a secret key to each user with respect to the user identity. The encryptor can take the public parameter and a user identity to encrypt a message. The requester can decrypt this cipher text by his secret key.

1. Data Owner Module:

In this module, the client sends the query to the server. Based on the query the server sends the corresponding file to the client.

2. System Module:

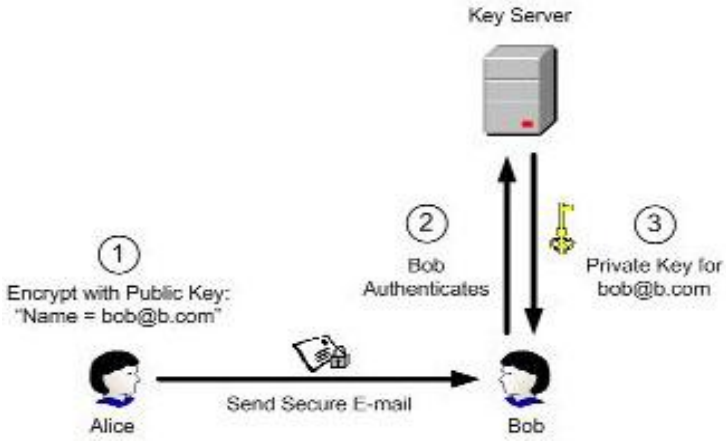
IDE: - In this module server encrypts the data and send to the client.

Privacy Preservation: -In this module server verified the encrypted data and responsible for maintaining the integrity of a encrypted data.

TPA: -In this module server will check the authorized person that by verifying the ID generated by the client.

Key – generation: -In this module the server generate the public key based on client Id for decryption of the data.

3. End User: In this module, the client first make a request for file after permission given by the owner client can access file.



 ISSN: 2321-8169
133 – 136

IV. FLOW OF SYSTEM

The flow of proposed system is as shown in below.

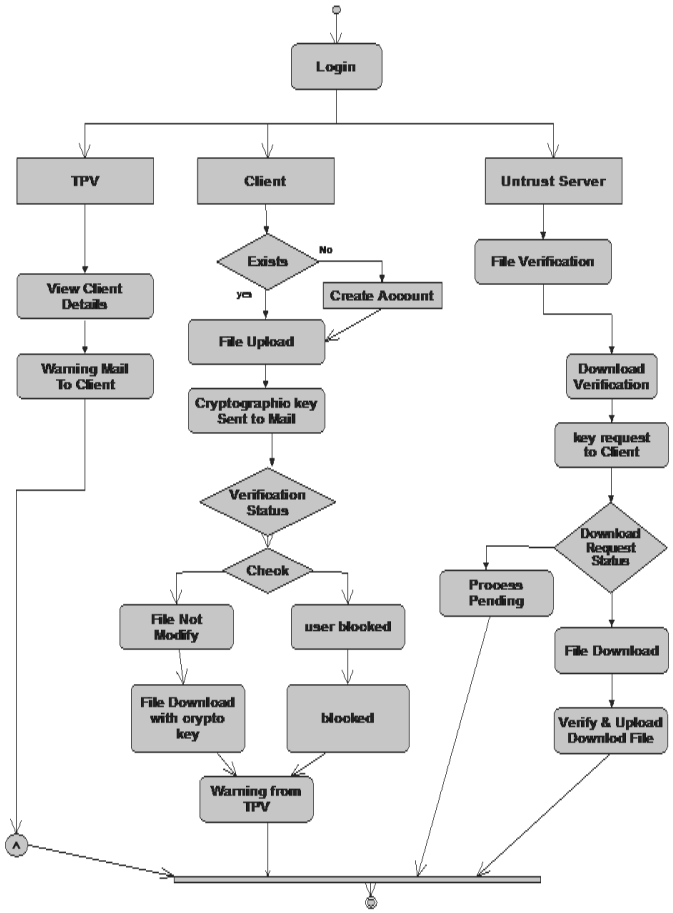


Figure 1: Flow of Proposed System

User needs first register and login into system. After that he uploads his file onto the system. Then user provides the secret key for encryption of original data. As well as this system support dual encryption methodology like data is encrypted using secret key and secret key is also encrypted which provide better security mechanism. The two random keys are generated called parent key and child key. The parent key is used by TPA to verify the originality of the data share by the user and child key used by the requester to decrypt the file. The file is used by requester if that file is verified by the TPA. If the requester try to download the without verification then file alert message is generate at the TPA login and the request is blocked by the TPA

V. IMPLEMENTATION

There are four entities in an identity-based data storage scheme: the private key generator (PKG), the data owner, the proxy server (PS) and the requester. The PKG validates the users' identities and issues secret keys to them. The data owner encrypts his files and outsources them to the proxy server. He validates the requesters and issues access permissions to the proxy server. The proxy server stores the ciphertexts and can transfer the two ciphertexts for the requester when he obtains corresponding re-encryption keys from the owner. The requester can decrypt the re-encrypted ciphertext. Identity-based data storage scheme supporting intra-domain and inter domain queries consists of the following algorithms:

An IBE scheme consists of 4 algorithms:

Setup Takes a security parameter ℓ and outputs system Parameters params and master-key.

Encrypt Takes as inputs params, id ∈ {0, 1}* and message m and outputs a ciphertext C.

ExtractPrivateKey Takes as inputs params, master-key and id ∈ {0, 1}* and outputs a private decryption key did.

Decrypt Takes as inputs params, private key did and message C and outputs a message m.

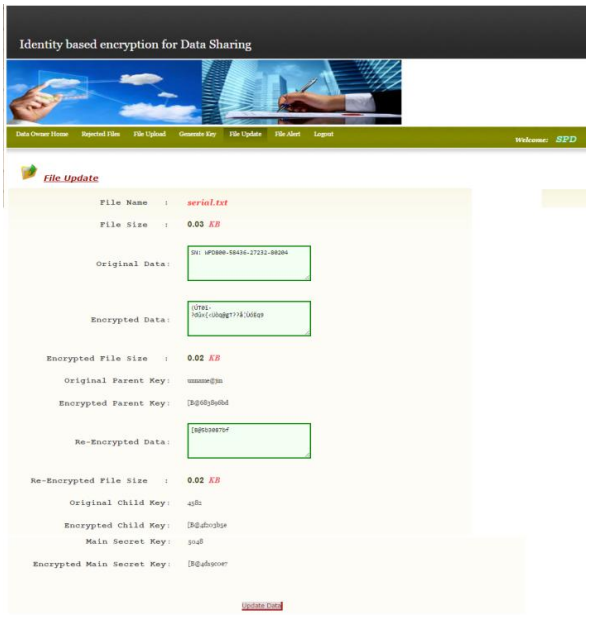


Figure 2: - Key Generation and File encryption usingIdentity.

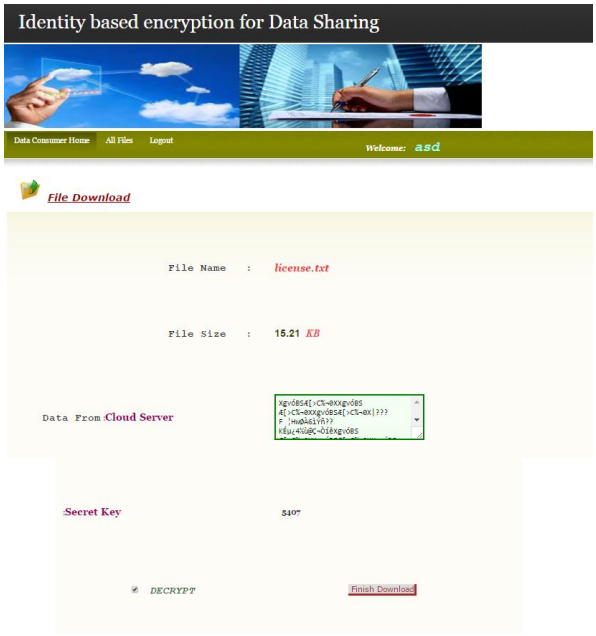


Figure 3: - File Decryption by the requester

VI. PERFORMANCE EVALUATION

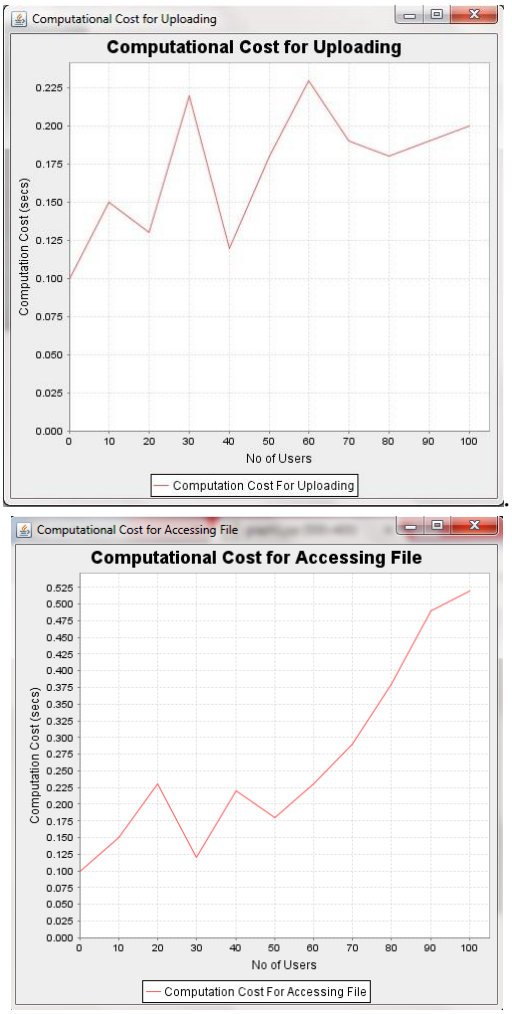


Figure 4: i) Computational cost achieved at uploading ii) Computational cost accessing file.

CONCLUSION

Identity-based data storage scheme which is suitable to the cloud computingscenario as it supports both intra-domain and inter-domain queries. In this scheme, the access key is bound to not only the requester's identity but alsothe requested ciphertext, and can be computed by the owner independentlywithout the help of the PKG. For one query, the requester can only accessone file of the owner, instead of all files. Furthermore, our scheme is secureagainst the collusion attacks.This technique is based on Identity based cryptography it reduces the problem of storage space required for aggregation and identifier of the data called as class.

REFERENCES

[1] Ning Cao, Cong Wang, Ming Li "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data",IEEE Transactions on Parallel and Distributed Systems Volume: 25, 222 – 233, Issue: 1, Jan. 2014 .

[2] Xiao Z, Xiao Y "Security and privacy in cloud computing", IEEE Commun Surveys Tutorials: 1–17, 99

[3] Chen D, Zhao, "Data security and privacy protection issues in cloud computing", International conference on computer science and electronics engineering, pp. 647–651.

[4] Mambo M, Okamoto E. "Proxy cryptosystems: Delegation of the power to decrypt ciphertexts", IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences 54-63 1997; E80A(1).

[5] Shamir A. "Identity-based cryptosystems and signature scheme". In: Blakley GR, Chaum D, eds. Proceedings: "Advances in Cryptology - CRYPTO 1984"; vol. 196 of Lecture Notes in Computer Science. Santa Barbara, California, USA: Springer-Verlag 47-53 1984.

[6] Ivan A, Dodis Y. "Proxy cryptography revisited". In: Proceedings: "Net- work and Distributed System Security Symposium" - NDSS 2003. San Diego, California, USA: The Internet Society; 1-20: 2003.

[7] Green M, Ateniese G. "Identity-based proxy re-encryption". In: Katz J, Yung M, eds. Proceedings: "Applied Cryptography and Network Security" - ACNS 2007; vol. 4521 of Lecture Notes in Computer Science. Zhuhai, China: Springer-Verlag 288-306:2007.

[8] Matsuo T. "Proxy re-encryption systems for identity-based encryption". In: Takagi T, Okamoto T, Okamoto E, Okamoto T, eds. Proceedings: "Pairing-Based Cryptography" - Pairing 2007; vol. 4575 of Lecture Notes in Computer Science. Tokyo, Japan: Springer-Verlag; 247-267: 2007.

[9] Wang L, Wang L, Mambo M, Okamoto E. "New identity-based proxy re-encryption schemes to prevent collusion attacks". In: Joye M, Miyaji A, Otsuka A, eds. Proceedings: "Pairing-Based Cryptography" – Pairing 2010 ; vol. 6487 of Lecture Notes in Computer Science. Yamanaka Hot Spring, Japan: Springer-Verlag; 327-346:2010.

[10] Boyang Wang, Baochun Li and Hui Li, "ACNS'12 Proceedings of the 10th international conference on Applied Cryptography and Network Security", Pages 507-525.

[11] Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng,"Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", *IEEE Transactions On Parallel And Distributed System*, Vol 25, No. 2 February 2014.

[12] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139, pp. 213–229, Springer 2001.

[13] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Proceedings of Advances in Cryptology - EUROCRYPT '05, ser. LNCS, vol. 3494.pp. 457–473, Springer, 2005.

[14] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," in ACM Conference on Computer and Communications Security, pp. 152–161 2010.