IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. II (Nov – Dec. 2015), PP 34-39
www.iosrjournals.org

"SL-SKE (Signature Less-Secret Key Encryption) For Data-Sharing in Clouds"

[1]V. Trivikramaraja, [2]Mr. R Sathiya Raj
[1]*PG Student, Department Of Computer Science & Engineering Madanapalle Institute of Technology & Science Madanapalle, India*
[2]*Asst.Professor, Department Of Computer Science & Engineering Madanapalle Institute of Technology & Science Madanapalle, India*

Abstract: *Cloud computing is typically defined as a type of computing that relies on sharing computing resources. The Infrastructure as a Service in cloud offers the data-center services to store and manage information, the private information can be shared among the business-company employees or the member's of a community. Preserving data privacy requires it to be encrypted before uploading into the cloud server. The authorized users' are only intended to download and decrypt using a secret-key. The presently existing cryptographic models use key management protocols to address key revocation problems and some other uses reliable security controller for issuing the signatures and attach secret-keys to the users. This leads to a lot of overhead. In our proposed model, we introduce a novel secure data sharing algorithm SL-SKE (Signature Less-Secret Key Encryption) does not require a digital-signature and also no additioal reliable security controller is required. The complete algorithm runs among the cloud server, data owner and the trusted-users. The newly generated keys are fully based on the user's profile. It will be intimated to the user through an email. Finally the results shows that it minimizes the overheads and the additional requirements like a trusted third party.*

Keywords*: Cloudcomputing, certificate less cryptography, confidentiality, access control.*

I. Introduction

The cloud computing is used as a figure to "the Internet", cloud computing is nothing but "a type of Internet-based computing," where various services such as servers, storage and applications are delivered to an organization's computers and devices via the Internet. Due to the benefits of public cloud storage, organizations have been adopting public cloud services such as Microsoft Skydrive and Dropbox to manage their data. Services models explain the type of service that the service provider is offering. That is, shared sensitive data must be strongly secured from unauthorized accesses. The confidentiality of sensitive data stored in public clouds, a commonly adopted approach is to encrypt the data before uploading it to the cloud.

The cloud does not know the keys to encrypt the data; confidentiality of the data from the cloud is assured. However, as many organizations are required to enforce fine-grained access control to the data, the encryption mechanism should able to support FGEB access control. This typical approach helps to support FGEB access control which encrypts the set of data with same Access Control.

II. Related Work

Key management systems minimize re-keying overheads, but it is a complex process.Reliable Security Controller (RSC) that generates new keys or rekeys for every authorized user and that itself a heavy weight approach. The Attribute Based Encryption is difficult to manage when the user having the key is left the group.

A. Disadvantages

1. Re-keying complexity
2. Cost of key-management is high
3. Need a trusted third party to manage the keysorSignatures.
4. Performance degradations

III. Proposed Work

Secure data sharing algorithm SL-SKE (Signature Less-Secret Key Encryption) not requires to have a digital-signature, not even a reliable security controller is required.The cloud server, data-owner and the trusted-users are only involved in privacy control. The cloud server creates a new secret key of the user based on the user's profile with the help of security privileges; the owner encrypts and submits the confidential information to the cloud server.The newly generated keys and that will be informed to the user through an email.On request from an authorized user the server executes level-1 decryption and at user side level-2 completely decrypts the cipher text

A. Advantages of Proposed System

1. No Re-keying complexity
2. Highly trusted
3. No need for trusted third party
4. Security improvements at less computation cost.

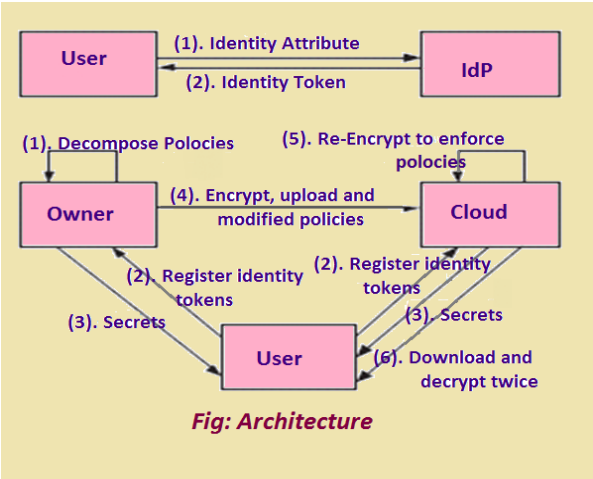


Figure: System Architecture

1. Profile verification authority
2. User signup
3. Data uploading and encryption
4. Data downloading and decryption
5. Encryption evolution management

A. Profile Verification Authority

Identity Provider is an authority of ID and are highly trusted third parties are that grants the identity tokens to the Users which is based on their profile attributes. It must be noted as Identity Providers no needs to be online after they will issues the identity tokens.

B User Signup

The Users can sign up with their token to get the credentials in order to the decrypts the data and then they are allowed to the accessibility. The Users register with their credentials are interrelated to the attribute conditions in ACC with the Owner and the rest of the identity credentials that are interrelated to the attribute conditions in ACB/ACC with the Cloud. When the Users registers with the Owner then the Owner grants two sets of secrets for the attribute conditions in ACC those are also present in the sub Access control policies in ACPB Cloud. The Owner keeps one set and gives the other set to the Cloud. Two different pairs are used in order to avoid the Cloud from decrypting the Owner encrypted data.

C. Data Uploading And Encryption

The Owner first encrypts the data based on the Owner's sub Access Control Policies in order to hide the content from the Cloud and then uploads them along with the public information. Owner updates the

security policy with the access rule i.e., user, data item, action to the remaining sub Access Control Policies to the Cloud. The Cloud in turn encrypts the data based on the keys generated using its own Attribute Based-General Key Management::KeyGen algorithm. Note that the Attribute Based-General Key Management::KeyGen at the Cloud takes the security provided to the Users and the sub Access Control Policies given by the Owner into consideration to generate credentials.

D.D**ata Downloading And Decryption**

The Users downloads the encrypted data from the Cloud and decrypts twice to access the data. First the Cloud generated public information tuples were used to derive the Object Linking And Embedding key and then the Owner generated public information tuples is used to derive the ILE key using the Attribute Based-General Key Management::KeyDecr algorithm. These credentials are allows a User to decrypts a data item only if the User satisfies the actual ACP implements to the data item.

E. Encryption Evolution Management

Either Access Control Policies or the user credentials may change. Further, already the encrypted data may goes through common updates. In such a situation data already encrypted and it must be the re-encrypted with a new credential. As the Cloud performs the access control enforcing encryption, it is an as usual re-encrypts the expensive data without the involvement of the Owner.

Keygeneration Algorithm

The main use of the key generation algorithm is sending keys to the user, the main key provided by the owner through email and cloud can provide the key through mail. once the data user can enter both the keys automatically he can see the owner the data.

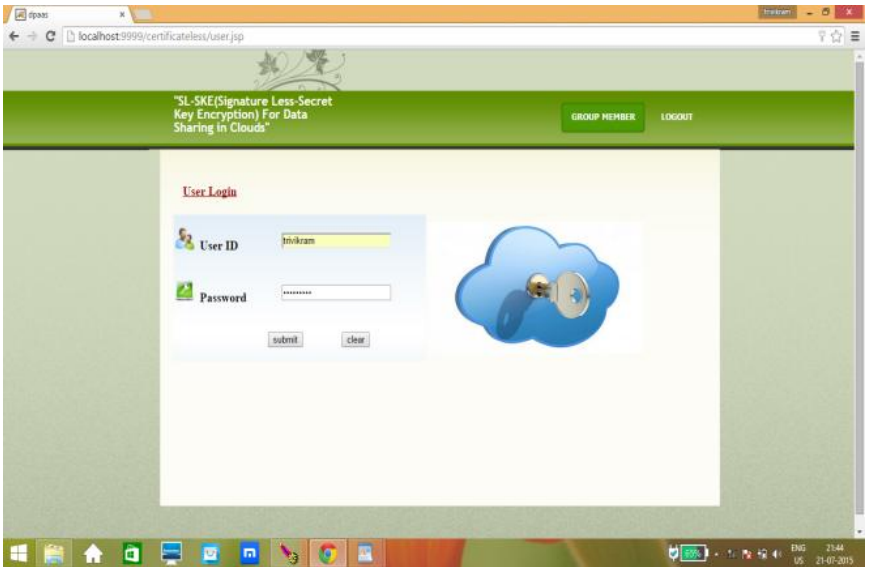
Inputs

Gmem->group member
GP->group manager
CS->cloud server
K->key
SK->send key
RK->request key

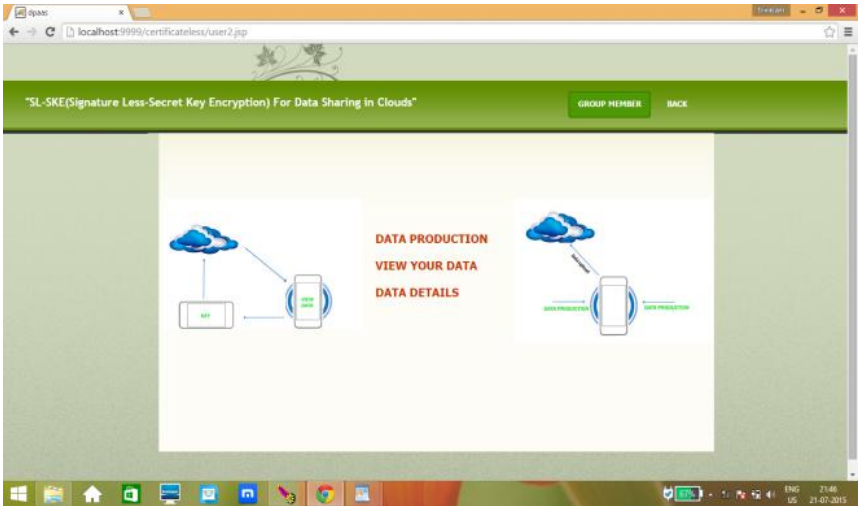
Output

Result-> R

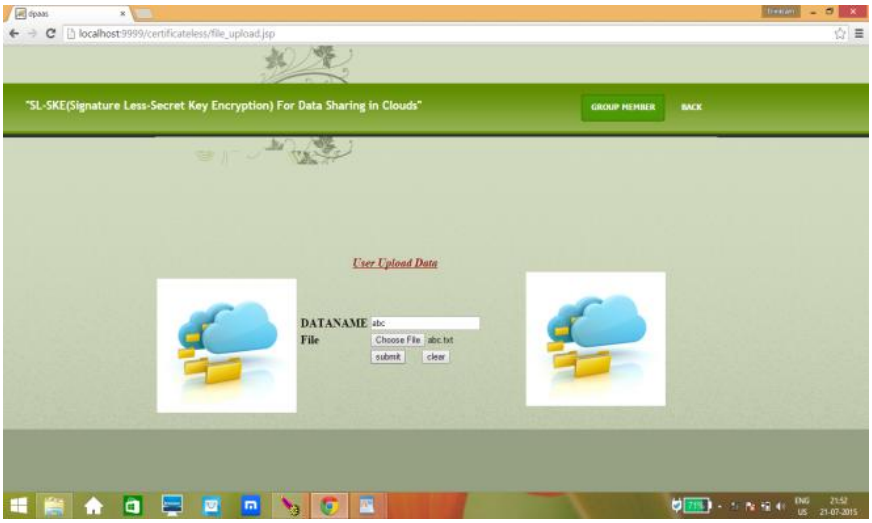
1.BEGIN
2.**Gmem** register
3.**Gmem** login
4.upload **F's**
5.**Gmem** request **GMkey**
6.**GM** generates key to **Gmem**
7.**Gmem** request **SK** from **CS**
8.**CS** sends **SK** to **Gmem**
9.**Gmem** access userfiles
10.display **R**
11.END



A:login page for the registered users

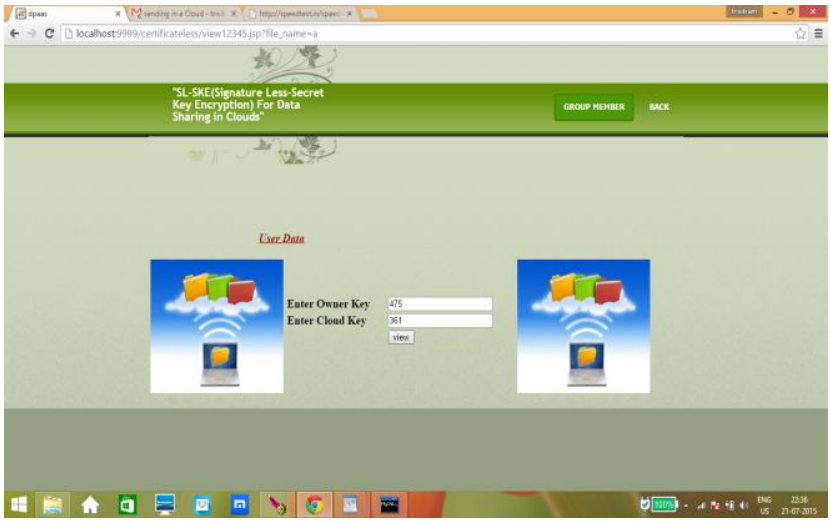


B: user operations.



C: File Uploaded by user

D:Owner views the requested user files



E:Data view of the user using cloud and owner keys

IV. Conclusion

In this paper we have proposed the first Signature Less Secret Key Encryption scheme without pairing operations and provided its formal security. Our SL-SKE solves the key escrow problem and revocation problem. Using the SL-SKE scheme as a key building block, we proposed an improved approach to securely share sensitive data in public clouds through an email concept by using the both owner and cloud keys which are based on the user's profile verification authority. Our approach supports immediate revocation and assures the confidentiality of the data stored in an untrusted public cloud while enforcing the access control policies of the data owner. Our experimental results shows the efficiency of basic SL-SKE scheme and improved approach for the public cloud. Further, for multiple users satisfying the same access control policies, our improved approach performs only a single encryption of each data item and reduces the overall overhead at the data owner.

Future Enhancement

For future enhancement, we have to improve the performances of an encrypting data. I can provide the AES algorithm for both uploading data and encrypts the data.

References

[1]. Certificateless Public Key Cryptography Sattam S . Al-Riyami and Kenneth G. Paterson Information Security Group, Royal Holloway, University of London, Egham, Surrey, TW20
[2]. Relations Among Notions of Security for Public- Key Encryption Scheme Bellare A. Desai D. Pointchevaly P. Rogawayz Februa 1999.
[3]. Attribute-Based Encryption for Fine- Grained Access Control of Encrypted Data Vipul Goyal Omkant Pandeyy Amit Sahaiz Brent.
[4]. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of ACM SIGMOD Conference, 2004.
[5]. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," ACM Computer Survey, vol.45, no. 6,pp. 965–981, 1998.