ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

A Secure Communication through Cloud Using Identity Based Proxy Re-Encryption Scheme

Ashwini R. Dhange, Associate Prof. Rashmi K. Dixit

Department of Computer Science and Engineering, Walchand Institute of Technology, Solapur, Maharashtra, India

ABSTRACT: The goal of this work is to improve the security towards remote cloud storage and improve the privacy by means of two norms such as Proxy-Reencryption Scheme and Multi-Attribute Based Encryption Logic. The modern society belong communication technologies in brutal way and performs all communications with others using global web and cloud based services; in this case security and privacy concerns for the data are growing. Attribute-based encryption (ABE) provides both access control and data security by defining users with attributes so that only those users who have matching attributes can decrypt data. In real-world applications of ABE, revocation of users or their attributes is needed so that revoked users can no longer decrypt the data. In these implementations, ABE is used in hybrid with a symmetric encryption scheme such as the Advanced Encryption Standard (AES). In this the data is encrypted with AES and the AES key is encrypted with ABE. The hybrid encryption scheme requires re-encryption of the data upon revocation to ensure that the revoked users can no longer decrypt that data. To re-encrypt the data, the data owner (DO) must download the data from the cloud, then decrypt, encrypt, and upload the data back to the cloud, resulting in both huge communication costs and computational burden on the DO depending on the size of the data to be re-encrypted. In this paper, we propose an attribute-based proxy re-encryption method in which data can be re-encrypted in the cloud without downloading any data by adopting ABE scheme. The proposed approach minimizes the communication cost between the data owners and cloud storage. For all the experimental results prove that the proposed method reduces the communication cost by as much as one quarter compared to that of the trivial solution as well as the proposed encryption schemes are more prominent to prevent any data lacks from any intruders/hackers.

KEYWORDS: Cloud Server, Deduplication, Attribute Based Encryption (ABE), Cloud Service Storage, Proxy Re-Encryption, Advanced Encryption Standard, AES.

I. INTRODUCTION

Cloud Computing, a powerful medium which allows the users to preserve the data in secured manner without any security issues. When more than one user send the same data to the cloud storage then, Deduplication is more effective. For this kind of issues a new methodology is required to preserve the data into the cloud environment without the following issues such as deduplication problems, security threats and ownership schemes. A Proxy based authentication scheme is introduced to avoid unauthorized users to enter into the server to access the data and powerful encryption scheme called Advanced Encryption Standard (AES) algorithm is useful for preventing the data from any attack more securely as well as maintain the data integrity by means of eliminating the deduplication causes. These two powerful algorithms called Proxy Authentication and AES work along with a novel server-side deduplication scheme is presented to control access to outsourced data. And by handling randomized meet encryption and secure ownership group key distribution the ownership changes dynamically.

This algorithm avoids data loss and to repeal users even though they already inherited that data, but also to legitimately-but-curious cloud storage server. The proposed scheme gives assurance of data integrity across any inconsistency attacks. So the security is increase in the proposed scheme. The efficiency analysis validates that the proposed scheme is powerful than the existing schemes, while the additional computational overhead is unimportant.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

The existing schemes providing integrity verification for different data storage systems, data dynamics has not been fully forwarded. Then how to accomplish a secure and powerful design to seamlessly integrate these two important components for data storage service residue an open challenging task in Cloud storage.

The main disadvantages spotted over the past approaches are as follows: (i) Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices and they have problem for the broad range of both internal and external threats for data integrity, (ii) Second, there is various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status, (iii) In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost besides the network. It is not a sufficient to detect the data exploitation when accessing the data, as it does not give users correctness assurance for those un-accessed data and might be too late to recover the data loss or damage and (iv) Encryption does not completely solve the problem of protecting data privacy against clouds service provider it reduces the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys.

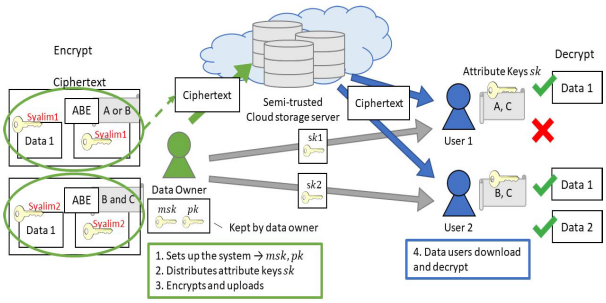


Figure 1. Cloud Server Storage – System Replication

In this paper, the proposed approach uses the convergent encryption scheme called Advanced Encryption Standard (AES) with powerful Attribute Based Encryption (ABE) Scheme, which derive keys from the hash of plaintext and Store it to server. This pointed out some security problems and presented a security model for secure data deduplication. These two protocols focus on server-side deduplication and do not consider data loss settings, against malicious users.

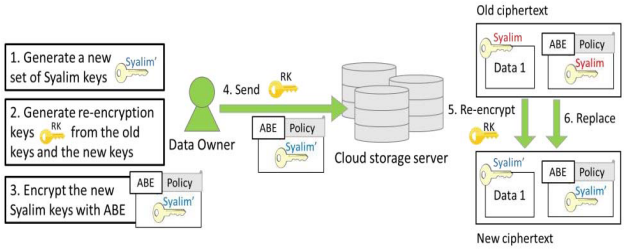


Figure 2. Proxy ReEncryption Scheme Model

A. Existing System Summary

Revocation of users or their attributes is an indispensable feature of ABE for real-world applications. In real-world situations, users and their attributes change over time within the system. For example, users may be found to be malicious, may simply leave the system, or their attributes may change. Therefore, revoking users or their attributes accordingly so that they can no longer decrypt data is important. Existing revocation methods of ABE are proposed based on the notion of using ABE to encrypt the data entirely, whereas in actual implementations, hybrid encryption of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

ABE and symmetric encryption, specifically the advanced encryption standard (AES), are used for efficiency. In hybrid encryption, data is encrypted with AES and the AES key is encrypted with ABE. Because existing revocation methods affect only ABE ciphertext, this fact introduces a problem in which users can keep the AES key prior to revocation and use it to decrypt data even after the users are revoked. Therefore, although existing revocation methods can be applied to revoke users from ABE, re-encrypting data with a new AES key is necessary so that the old AES key can no longer be used.

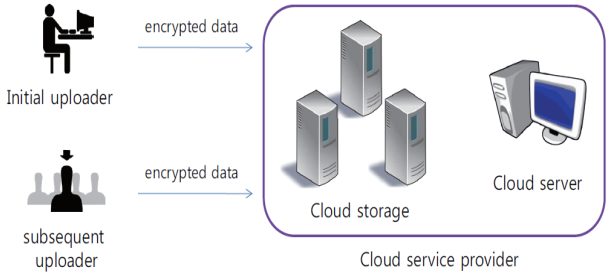


Figure 3. Traditional Data Prevention Model over Cloud Server

B. Proposed System Summary

In this proposed approach, we propose an attribute-based proxy Reencryption method for revocation in which the DO is no longer required to download any data for re-encryption. By using a symmetric encryption scheme that supports proxy Reencryption in hybrid with ABE, we can perform revocation in the cloud so that a revoked user will no longer be able to decrypt data after revocation. Specifically, we implement a symmetric encryption scheme proposed by Syalim et al. in hybrid with CP-ABE, encrypt data with Syalim's scheme, and encrypt Syalim scheme's keys with CP-ABE.

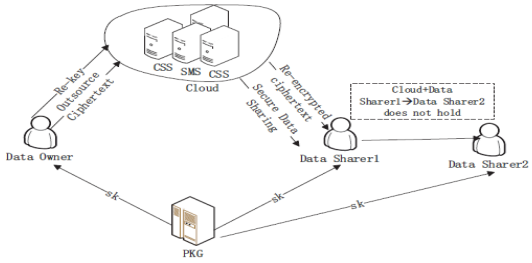


Figure 4. Proposed System Architectural Design

By using a symmetric proxy re-encryption scheme, the data can be reencrypted in the cloud without revealing any data to the cloud. In addition, the DO only has to generate a set of Reencryption keys and a new ABE ciphertext that encrypts the new Syalim scheme's keys, and then send both to the cloud for re-encryption. Therefore, in the revocation step, sending only the re-encryption keys and ABE ciphertext to the cloud is required, thus reducing the communication cost between the DO and cloud. Because the re-encrypted ciphertext is encrypted under a completely new set of keys, users cannot decrypt data even if they keep the old symmetric keys or parts of the old ciphertext.

C. User Authorization and Authentication

Proxy defines the security by means of user authorization and authentication. Proxy signature is a signature scheme, in which an original signer can delegate his/her signing capability to a proxy signer, and then the proxy signer

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

generates a signature on behalf of the original signer. From a proxy signature, a verifier can be convinced of the original signer's agreement on the signed message. Researchers have proposed 3 kinds of proxy signature algorithms: full delegation, partial delegation and partial delegation by warrant. The former two are eliminated by partial delegation with warrant which is proved to be more secure and practical, so we also use partial delegation with warrant in our protocol design.

Let A be an original signer who has an authentic key pair (PrKA and PuKA), and B be a proxy signer who has an authentic key pair (PrKB and PuKB). Let mw be A's warrant information for the delegation, which has semantic means including the original signer's identity, some information about the proxy signer (for example the identity), period of delegation validity, the qualification of messages on which the proxy signer can sign, etc. Let dA Sign PrKA; be A's signature on the warrant mw using his/her private key PrKA. A transmits dA to the proxy signer B.

D. Data Manipulation

The data manipulation module supports data owner scenario and it allows the data owner to maintain the data which is on the cloud server securely and to upload data into the cloud storage to save costs. A data owner first encrypts the data and outsources it to the cloud storage with its index information, that is, a tag. If a data owner want to uploads some data that is not already exist in the cloud storage then he is called an initial Uploader; if the data already exist in the cloud storage then it is called a subsequent uploader since it means that other data owners may have uploaded the same data previously then he is called a subsequent uploader. Hereafter, we refer to a set of data owners who share the same data in the cloud storage as an ownership group.

E. Cloud Service Provider

This is an entity that provides cloud storage services. It consists of a cloud server and cloud storage. The cloud server de-duplicates the outsourced data from users if necessary and stores the de-duplicated data in the cloud storage. The cloud server maintains data owner lists of stored data, which are composed of a tag for the stored data and the identities of its owners. The cloud server controls access to the stored data based on the ownership lists and manages (e.g., issues, revokes, and updates) group keys for each ownership group as a group key authority. The cloud server is assumed to be honest-but-curious. That is, it will honestly execute the assigned tasks in the system; however, it would like to learn as much information about the encrypted contents as possible. Thus, it should be deterred from accessing the plaintext of the encrypted data even if it is honest.

F. Data Deduplication Scheme

This data deduplication module allows the data owner to maintain the records into the server more dynamically and with full of integrity. Once the data owner uploaded the records into the database/server, which is counted and manipulated at every time while uploading the data next time into the server then If the data matches with the existing records, the system won't allow the data owner to upload the data further and blocks them to proceed.

II. LITERATURE SURVEY

In the year of 2013, the authors "D. Boneh, K. Lewi, H. Montgomery and A. Raghunathan [1]", proposed a paper titled "Key homomorphic PRFs and their applications [1]", in that they descibed such as a pseudorandom function $F:K\times X\rightarrow Y$ is said to be key homomorphic if given F(k1,x) and F(k2,x) there is an efficient algorithm to compute $F(k1 \oplus k2, x)$, where $\oplus$ denotes a group operation on k1 and k2 such as xor. Key homomorphic PRFs are natural objects to study and have a number of interesting applications: they can simplify the process of rotating encryption keys for encrypted data stored in the cloud, they give one round distributed PRFs, and they can be the basis ofa symmetric-key proxy re-encryption scheme [1].

Nowadays all known constructions for key homomorphic PRFs were only proven secure in the random oracle model. We construct the first provably secure key homomorphic PRFs in the standard model. Our main construction is based on the learning with errors (LWE) problem. We also give a construction based on the decision linear assumption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

in groups with an ℓ-linear map. We leave as an open problem the question of constructing standard model key homomorphic PRFs from more general assumptions [1][4][5].

In the year of 2016, the authors "W. C. Garrison III, A. Shull, S. Myers and A. J. Lee [2]", proposed a paper titled "On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud [2]", in that they descibed such as: It is increasingly common to outsource data storage to untrusted, third party (e.g. cloud) servers. However, in such settings, low-level online reference monitors may not be appropriate for enforcing read access, and thus cryptographic enforcement schemes (CESs) [2] may be required. Much of the research on cryptographic access control has focused on the use of specific primitives and, primarily, on how to generate appropriate keys and fails to model the access control system as a whole [2].

Recent work in the context of role-based access control has shown a gap between theoretical policy specification and computationally secure implementations of access control policies, potentially leading to insecure implementations. Without a formal model, it is hard to (i) reason about the correctness and security of a CES, and (ii) show that the security properties of a particular cryptographic primitive are sufficient to guarantee security of the CES as a whole. In this system, a rigorous definitional framework is provided for a CES that enforces read-only information flow policies (which encompass many practical forms of access control, including role-based policies) [2][7].

This framework (i) provides a tool by which instantiations of CESs can be proven correct and secure, (ii) is independent of any particular cryptographic primitives used to instantiate a CES, and (iii) helps to identify the limitations of current primitives (e.g. key assignment schemes) as components of a CES [2][8].

In the year of 2016, the authors "F. Wang, J. Mickens, N. Zeldovich and V. Vaikuntanathan [3]", proposed a paper titled "Sieve: Cryptographically enforced access control for user data in untrusted clouds [3]", in that they descibed such as: Modern web services rob users of low-level control over cloud storage—a user's single logical data set is scattered across multiple storage silos whose access controls are set by web services, not users [3][5].

The consequence is that users lack the ultimate authority to determine how their data is shared with other web services. In this system, Sieve was introduced, a new platform which selectively (and securely) exposes user data to web services. Sieve has a user-centric storage model: each user uploads encrypted data to a single cloud store, and by default, only the user knows the decryption keys. Given this storage model, Sieve defines an infrastructure to support rich, legacy web applications. Using attribute-based encryption, Sieve allows users to define intuitively understandable access policies that are cryptographically enforceable. Using key homomorphism, Sieve can reencrypt user data on storage providers in situ, revoking decryption keys from web services without revealing new keys to the storage provider [3][9]. Using secret sharing and two-factor authentication, Sieve protects cryptographic secrets against the loss of user devices like smart phones and laptops. The result is that users can enjoy rich, legacy web applications, while benefiting from cryptographically strong controls over which data a web service can access.

III. IMPLEMENTATION

Data Security Phases:

Encryption Process : C=E(P, K)
ReEncryption Process: RC=E(C,K)
Decryption Process: D=D(RC, K)
Where, P – Plaintext,
C – Ciphertext,
RC−Reencrypted Ciphertext
E – AES Encryption Algorithm
D – AES Decryption Algorithm
K – Key

Key Scramble:
SK =∑(K ⊕ MASTERKEY)
Key UnScramble:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

K=∑ (SK ⊕ MASTERKEY)
Where,
SK- Scrambled Key

Algorithm Notifications:

unm	:	User Name
DB	:	Database
emid	:	Email Id
mno	:	Mobile Number
Σ	:	Selection Operator
:=	:	Assignment Operator
⊕	:	Exclusive OR

Algorithm NewRegistration:
// Input: Username, emailID, MobileNumber, City, State, Country,Usertype
// Output: All User/DO credentials should store in DB suceessfully.

```
//Enter User/Dataowner details
unm:=Read USERNAME;
emid:=Read EMAILID;
mno:=Read MOBILE NUMBER;
city:=Read CITY;
state:=Read STATE;
country:=Read COUNTRY;
if(utype==DataOwner)
{
if(emid equals(“text_emailid”))
{“Email id already Exist”}
else
{
DBStore(unm ,emid, mno, city, state, country);
 }
}
DBStore(unm ,emid, mno, city, state, country);
}
```

Algorithm CryptoManager
//Input: Password / Original File / Encrypted File.
//Output: Hashed Password / Encrypted File / Decrypted File / Uploaded Encrypted File/
//Download Decrypted File.

1. Set crypto_algo :=AES;
   Set hash_algo :=MD5;
   master_key :=”random alphanumeric text” ;
   AES_key;
   AES_Mkey;

2. //Hash password
   Hp:=computeHash(hash_algo, password);
   return Hp;

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

3. //Create Key
   AES_key:=create_newkey(crypto_algo, doid); // Create AES key for DO
   // scramble key to store key in database
   Mkey:=scramble_key(AES_key, mastr_key);
   //map AES_Mkey to doid and store in database
   Dbstore(doid, AES_Mkey);

4. //Upload file
   Upload_file (doid, filename, file_data)
   {
   AES_Mkey:=DBFetch(doid);
   // unscramble key.
   AES_key:= unscramble_key(AES_Mkey, mastr_key);
   //encrypt file data.
   encrypted_data:=encrypt_file(file_data, Crypto_algo, AES_key) ;
   //upload encrypted file on cloud
   CloudClientInterface_uploadblock(doid, filename, encrypted_data);
   //map filename and doid in database
   DBstore(doid, filename);
   }
5. //Reencryption of data on cloud
   DBstore_file (doid, filename, encrypted_data)
   {
   AES_Mkey:=DBFetch(doid);
   // unscramble key.
   AES_key:= unscramble_key(AES_Mkey, mastr_key);
   //reencrypt file data.
   reencrypted_data:=reencrypt_file(encrypted_data, Crypto_algo, AES_key) ;
   //upload reencrypted file on cloud
   CloudClientInterface_uploadblock(doid, filename, reencrypted_data);
   //map filename and doid in database
   DBstore(doid, filename);
   }
6. //Download file
   download_file (doid, filename)
   {
   If(ifFileExist(DBFetch(doid, filename)))
   {
   //download reencrypted file from cloud
   reencrypted_data:=CloudClientInterface_download(doid, filename,);
   DBFetch(doid, AES_Mkey);
   AES_key:= unscramble_key(AES_Mkey, mastr_key); / //unscramble key.
   file:= decrypt_file(reencrypted_data, crypto_algo, AES_key) ; //decrypt file data.
   return file;
   }
   }

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

IV. EXPERIMENTAL RESULT

The following figure illustrates the home page design of the proposed system.

Figure 5. Home Page Design

The following figure illustrates the New User Registration page of the proposed system.

Figure 6. New User Registration

After successful registration cloud service provider (CSP) authenticates the user as shown in following figure by clicking on active/deactive button.

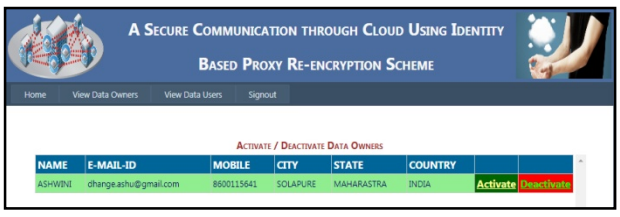


Figure 7. CSP Authentication for data Owner

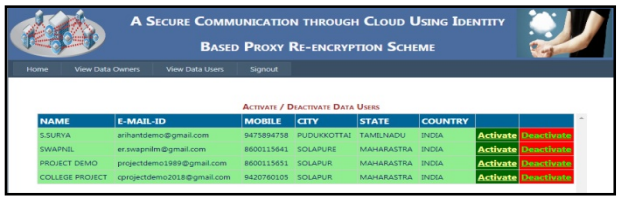


Figure 8. CSP Authentication for data user

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

The following figure shows data owner login page

Figure 9. Data owner login page

Clicking on login button it need to check identity by entering secure code which is sent on email id as shown in following figure.

Figure 10. Identity checking for Data owner

Once data owner login then following figure illustrates the Data Uploading and its Encryption nature of the proposed system.

Figure 11. Data Uploading with Encryption Strategies

The following figure shows the uploaded data.

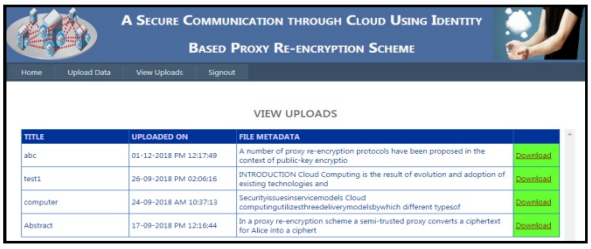


Figure 12. View Uploads for Data owner

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

When data user request particular file then the re-encryption of data done in cloud storage by proxy. To search any file data on cloud then he first login and search data by content based search as shown in following figure.

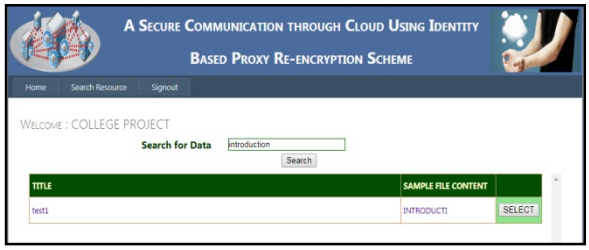


Figure 13. Data user searching data on cloud

This is the data searching process. Now for downloading file click on select button it asks security code which is sent on email id after that it shows download button clicking on that data decryption process will done then user get plaintext data as shown in following figure.

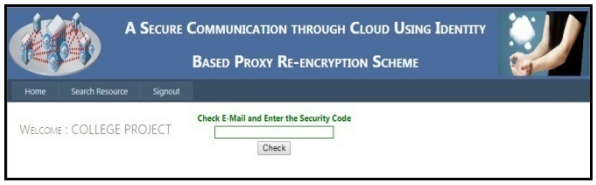
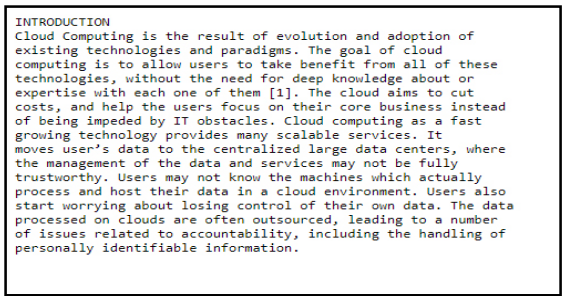


Figure 14. Security checking for download Data

Figure 15. Downloading Data



INTRODUCTION
Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them [1]. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles. Cloud computing as a fast growing technology provides many scalable services. It moves user's data to the centralized large data centers, where the management of the data and services may not be fully trustworthy. Users may not know the machines which actually process and host their data in a cloud environment. Users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information.

Figure 16. Initial Data (Decrypted Data)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

V. CONCLUSION

In this system, providing security towards remote cloud storage and improving the privacy by means of Proxy-Reencryption Scheme. In Identity based Proxy Reencryption (PRE) scheme the data owner can control sharing capability in a flexible way by using random numbers used in the encryption process. This scheme has some advantages, and can be more appropriately adapted to some applications for content sharing, such as secure cloud data sharing. The advantage of this scheme is that it consumes communication cost and time of encryption and decryption method by proposing an attribute-based proxy re-encryption method in which data can be re-encrypted in the cloud without downloading any data by adopting ABE scheme.

.

REFERENCES

[1] D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan, "Key homomorphic PRFs and their applications," Advances in Cryptology-CRYPTO 2013, LNCS, vol. 8042, pp. 410-428, 2013.
[2] W. C. Garrison III, A. Shull, S. Myers, and A. J. Lee, "On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud," 2016 IEEE Symposium on Security and Privacy (SP), pp. 819-838, 2016.
[3] F. Wang, J. Mickens, N. Zeldovich and V. Vaikuntanathan, "Sieve: Cryptographically enforced access control for user data in untrusted clouds," Proc. of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16), pp. 611-626, 2016.
[4] M. Horváth. "Attribute-Based Encryption Optimized for Cloud Computing," SOFSEM 2015: Theory and Practice of Computer Science, LNCS, vol. 8939, pp. 566-577, 2015.
[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," Proc. of the 5th ACM Symp. on Information, Computer and Communications Security, pp. 261-270, 2010.
[6] Y. Yasumura, H. Imabayashi, and H. Yamana, "Attribute-based Proxy Re-encryption Method for Revocation in Cloud Storage," Proc. of 2017 IEEE Int'l Conf. on Big Data, pp. 4476–4778, 2017.
[7] A. Sahai, and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, LNCS, vol. 3494, pp. 457-473, 2005.
[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. of the 13th ACM Conf. on Computer and Communications Security, pp. 89-98, 2006.
[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," Proc. of 2007 IEEE Symp. on Security and Privacy (SP'07), pp. 321-334, 2007.
[10] A. Syalim, T. Nishide, and K. Sakurai, "Realizing proxy reencryption in the symmetric world," Proc. of Int'l Conf. on Informatics Engineering and Information Science, CCIS, vol. 251, pp. 259-274, 2011.
[11] Y. Cheng et al., "Efficient revocation in ciphertext-policy attributebased encryption based cryptographic cloud storage," Journal of Zhejiang University SCIENCE C, vol. 14, Issue 2, pp. 85-97, 2013.
[12] S. Myers and A. Shull, "Efficient hybrid proxy re-encryption for practical revocation and key rotation," Cryptology ePrint Archive, https://eprint.iacr.org/2017/833.
[13] R. L. Rivest, "All-or-nothing encryption and the package transform," International Workshop on Fast Software Encryption, LNCS, vol. 1267, pp. 210-218, 1997.
[14] Charm: A tool for rapid cryptographic prototyping. http://www.charm-crypto.com/.
[15] Xu An Wang, Yunlong Ge, and Xiaoyuan Yang. PRE+: Dual of proxy re-encryption and its application. Cryptology ePrint Archive, Report 2013/872, 2013. http://eprint.iacr.org/2013/872.