Fastest Access of Secured Data in Cloud storage by using Attribute-based Encryption

Ramiz Shaikh
Research Scholar
Jawaharlal Institute of Technology, Borawan
M.P India

Ankit Dongre
Associate Pfrofessor
Jawaharlal Institute of Technology Borawan,
M.P. India

ABSTRACT

Cloud security is the most critical task while considering its working environment, i.e. outsourced, distributed and utility based. In such cases making the users data confidential, increases the trust over the system. Also the security procedure does not make the availability affected in any ways. The users of these kind of systems is always retained the services and securities preliminaries with respect to the data itself. As the cloud user can access its data frequently and if here some encryption is used which requires decryption and the repetitive process continues to increase the overheads. It requires some mechanism in which encryption is performed and if the user requires to perform some operations on secure file without decrypting it can be fulfilled. Thus homomorphic encryption lets the user facilitates about the performing operations on encrypted data which reduces the complexity of confidentiality operations. Also to prevent Cloud Servers from being able to learn both the data file contents and user access privilege information used to generate key along with the fastest access of secured data by using Attribute-based encryption (ABE).

Keywords

Attribute Based Encryption, Cloud Storage, Data Storage, Holomorphic.

1. INTRODUCTION

In cloud environment all the data is outsourced for services including storage and security. In such cases the users lost control over its data and the dependency is generated over the cloud provider or service provider. Thus, if the user is equipped with some controls, then the user trust is also increased and the total cloud control over the data is shifted from third party to the user. So for applying the encryption the user holds the key and not the cloud provider to increase the protection over the cloud data. But for providers view such keys are in consistence with their existing business models. These models restrict the cloud provider’s capability for information mine or otherwise exploit the users' data. If a cloud provider doesn't have access to the keys, they lose access to the information for his or her own use. Whereas a cloud supplier could comply with keep the information confidential (i.e., they will not show it to anyone else) that promise doesn't stop their own use of the information to enhance search results or deliver ads. Of course, this sort of access to the information has vast worth to some cloud suppliers and that they believe that data access in exchange for providing below-cost cloud services could be an honest trade.

Also, providing onsite cryptography at rest choices would possibly need some suppliers to considerably modify their existing software package systems that may need a considerable capital investment. That second reason is actually very important, too. A lot of cloud providers don't just store client data; they do things with that data. If the client encodes the information, it’s a murky blob to the cloud supplier - and a ton of cloud administrations would be unimaginable. Thus the problem is at both the end provider and user. To resolve these issues some third party needs to take the control over it whose primary function is to deal with such security scenarios and monitors the activities of both the user and provider. Hence the key generation is the major component which shows the importance of key and its control for enhancing the security.

1.1 Homomorphic Encryption (HE)

Homomorphic encryption schemes that allow simple computations on encrypted data have been known for a long time. It has three major components:

- **KeyGen**: This module will generate the key as per the requirement of the encryption schemes like symmetric or asymmetric algorithms. The generated key should provide effective security against any type of key based attacks. Mainly the key is default generated by the algorithmic component which is known to the provider. Thus some new mechanism needs to be developed for further improvement in security.
- **Encrypt:** This module provides the wide range of encryption solution for improved security with lesser computational loads on the servers. The practical applicability of homomorphic encryption provides the flexibility in the selection of encryption algorithms means it can be user depended or provider dependent.
- **Decrypt:** This can be considered as a major functionality of the homomorphic encryption. It differs from the traditional encryption standards where the complete data is decrypted for reading. Here the user encrypts the data by unique key and sends it to the provider. Now the provider or some other user is capable applying the mathematical operations on such homomorphically encrypted ciphertext and then revert the result in the same encrypted format to the user without reducing the confidentiality of the data.

2. LITERATURE REVIEW

In this subsection, we review some closely related works, including no interactive verifiable computation, pairing delegation and proxy reencryption. No interactive Verifiable Computation: No interactive verifiable computation [19], [20] enables a computationally weak client to outsource the computation of a function to one or more workers. The workers return the result of the function evaluation as well as a no interactive proof that the computation of the function was carried out correctly. Since these schemes [19], [20] deal with outsourcing of general computation problems and preserve the privacy of input data, they can be used to outsource decryption in ABE systems. However, the schemes proposed in [19], [20] use Gentry's fully homomorphic encryption system [21] as a building block, and thus the overhead in these schemes is currently too large to be practical . Recently, Parno et al. establish an important connection between verifiable computation and ABE. They show how to construct a verifiable computation scheme with public delegation and public verifiability from any ABE scheme and how to construct a multifunction verifiable computation scheme from the ABE scheme with outsourced decryption presented in [12]. Goldwasser et al. propose a succinct functional encryption scheme for general functions, and show that, by replacing the ABE scheme used in with their succinct functional encryption scheme, one can obtain a delegation scheme with is both publicly verifiable and secret, in the sense that the prover does not learn anything about the input or output of the function being delegated.

3. PREVIOUS ALGORITHMS USED

3.1. Paillier encryption scheme

1. Let n=p×q, where p and q are two large and different prime numbers

2.Such that gcd(n, ϕ(n))=1,

3.Calculate λ(n)=lcm(p−1, q−1) and choose g∈Z n^{2*}

4. Such that gcd (L(g λ (n)mod n 2), n)=1, where L(t)=(t-1)/n

Public key is composed of (n, g)

Private key is composed of λ(n).

For the encryption, the plaintext M is partitioned into blocks m(i) such that m(i)<n and for each plaintext m(i) we get a cipher text c(i).encryption c(i)of m(i)is given by:

c(i)= E(m(i))≡ gm(i)rin mod n2
D(c(i)) ≡L(c λ(n) mod n2)/ L(g λ(n) mod n2)Example: assume primes p and q are given as p=7, q=11, then n=p×q=77. Let g=2, r 1=5, r 2=6 and let the two messages be m1=4 and m2=5. Then, the encryption of m1 is given as:
c1≡g m1×r 1n mod n2
c1=24×577mod 77 2=3436
c 2≡ g m2×r 2n mod n2
c 2≡25×677 mod 77 2=4623.

Homomorphism: - we have c3=c1×c2≡3436×4623mod772=837.Applying the decryption algorithm over c3, which is equivalent to the addition of the two plaintexts i.e.
m3=m1+m2≡4+5 mod 77=9.
Hence Paillier supports homomorphic operation of addition modulo n2 over the plain text.

3.2. RSA cryptosystem

1. Selecting two large and different prime numbers p and q, calculating their product n=p×q and

2. Selecting an integer e, which is relatively prime to ϕ(n) and with

1<e<ϕ(n), where ϕ() is the Euler's function.

3. We need to calculate d, the inverse of e with d≡e − 1mod ϕ(n).

4.The public key is composed of the couple (e, n)

5.The private key is (d, n).

For the encryption, the plain text M is also partitioned into blocks m(i)such that m(i)<n and

for each plaintext m(i) we get a cipher text c(i):

c(i)= E(m(i))≡ $m(i)^e$ mod n

m(i)= D(c(i))≡ $c(i)^d$ mod n

Example: assume primes p and q are given as p=7, q=17, then n=p×q=119. If e=5, then gcd(ϕ(119), 5)=1 and we get d≡e – 1 modϕ(n)=77.

Let the input message be m_1=22 and m_2=19, then encryption of m_1 is given as: c_1≡22 ^{5}mod 119=99 encryption of m_2 is given as: c $_2$≡19 ^{5}mod119=66.

Homomorphism:we have $c_3=c_1×c_2$≡99×66 mod119=108.

Applying the decryption algorithm over c_3 results in 61, which is equivalent to the multiplication of the two plaintexts i.e. $m_3=m_1×m_2$≡22×19 mod 119=61.

Hence RSA supports homomorphic operation of multiplication modulo n

4. PROPOSED SYSTEM

For fast and effective encryption with lesser ciphertext size, the approach uses, partial homomorphic encryption using RSA cryptosystem. This system is capable of generating fast response with less overhead.

Improved Cryptosystem Security using User Generated Keys: Security is further increased by giving some controls to the user for generating the keys through its characteristics. This key is complex than some other methods. By using this key with RSA cryptosystem, control on data modifications and reading rights is provided to user without its information and if the providers tries to leak the data it is of no use without this user generated keys. This attributes and characteristics do not match with some other users and hence decoding the data is not possible.

It is clear that one of the most important goals of the researches about the homomorphic encryption schemes is to make them closer to practical applications. In this section, we will discuss possible ways to achieve it. The work evaluates a distributed security scheme for effective encryption of dynamic data of users.

4.1 Proposed Algorithm:

```
1: User registers to Cloud Service Provider
2: Send user details (UID, Uname) to Third Party Auditor
3: TPA Authenticates user
 4: User
5: Fetch values of Current Users Attributes (username, ID, timestamp)
 6: Generate key by Apply MD5 to Users Attributes (username, ID, timestamp)
 7: Convert the key to biginteger and make it final
public key
```

8: Apply Homomorphic (RSA) encryption to Data of message M using key
9: Send Data of message M to CSP
10: Transferring Information (UserID, UserName, FromIP, FileName, FileSize, Failed login attempts) in a Log file stored at TPA
11: Download original message by passing the Private Key

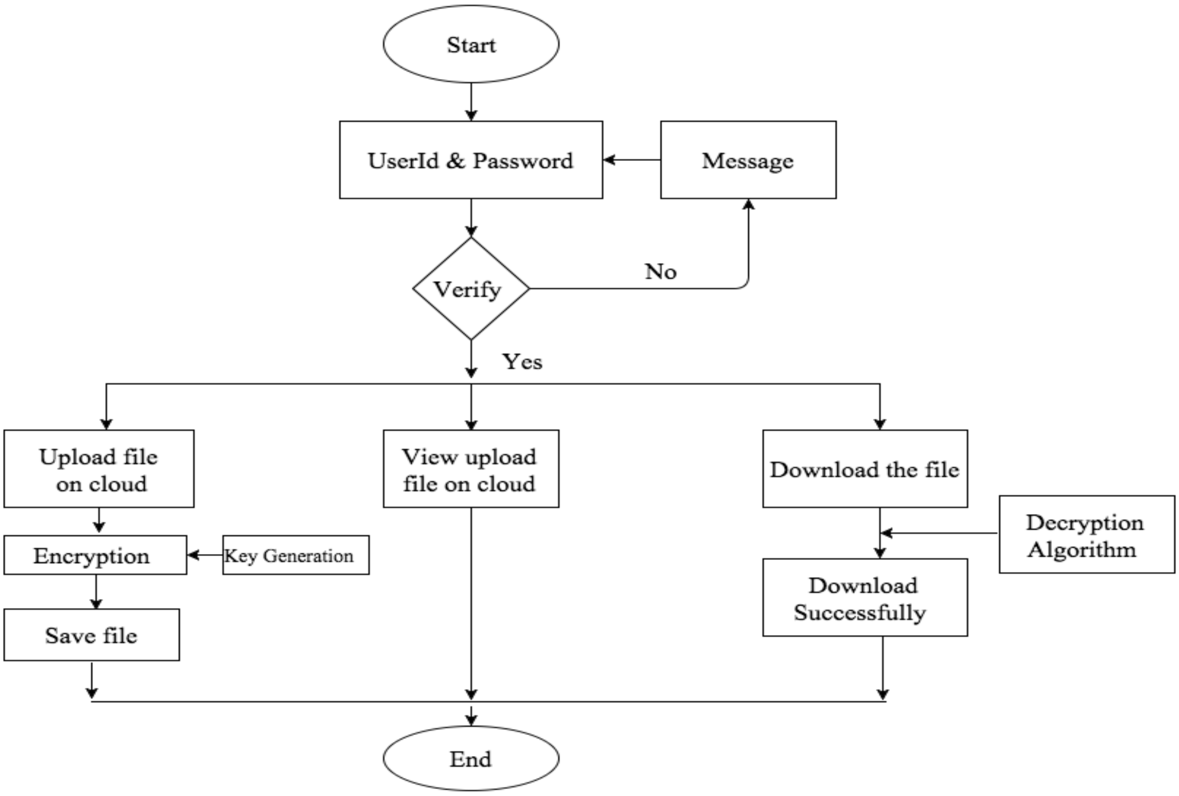

Fig.1 Proposed Algorithm

4.2 Algorithm Steps

Initially, users make its credential to login to the system. Now here this information is stored on third party and after the TPA authentication a user can log. After that, user attribute based key is generated. This element is taken as user attributes which in

combine effect generates a key based on such values. The attribute elements are, Username, Timestamp and UID of a user.

Form this composite key is generated using MD5 algorithm which gives a digests value, this value is converted to a big integer. Later on this key can be updated by the user's selection of services and this value is being verified by some third party auditors. Now to make the user data secure and reduces the load of encryption this work is using homomorphic encryption using RSA algorithms. Here the generated composite key of combined values of attributes is passed for encryption algorithms to make the data secure. Reverse process is applied for getting the data in secure channel with reduced load on servers.

Now the above process is taken in consideration and monitored from some external entity such as third party auditor which continuously watches the user's behavior. In this, the auditor traces the user's activity, its status, service details of users, this value is taken by each activity and evaluate the changes make by the approach.

The approach is proving its efficiency by its components and their integration verified by some of the modules and policies. When the load of decryption is reduced form servers the effectiveness and performance will also be raised to a certain value in terms of their processing cycles and memory. Actual values of working model are given in the next section for its evaluation.

5. CONCLUSION

Futuristic results of the technique may show the improvement in providing the security with feasible operations on cipher using partially homomorphic cryptosystems and is most suitable for outsourced cloud environment. This improved encryption is faster and less computational overhead is involved. It provides the high end reliability towards the new orientation of the system.

The third party mechanism deals with continuous monitoring of user record. This monitoring along with improved throughput and efficiency is achieved. Out of these methods an enhanced secure scenarios is generated through our proposed TPA-HE. At the initial level of our research, we get the following benefits.

- Improved security solution with less operational overheads and retains reliability on novel encryptions
- Unauthorized access is blocked using improved key generation through user characteristics.
- Continuous monitoring gives the user behavior measurements and analyzes the affection of such novel cryptosystem on other services.

6. REFERENCES

[1] Shucheng Yu, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, in Proceedings of IEEE Infocomm, ISSN: 978-1-4244-5837-0/10, 2010.

[2] Srijith“Towards Secure Cloud Bursting,Brokerage and Aggregation” 2010 Eighth IEEE European conference on web services

[3] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE,KuiRen, Member, IEEE, and Wenjing Lou, Member, IEEE “Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE-2012

[4] Cong Wang1, Qian Wang1, Kui Ren1, and Wenjing Lou2,” Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, IEEE INFOCOM 2010, San Diego, CA, March 2010

[5] Ms. Vaishnavi Moorthy1, Dr. S. Sivasubramaniam2,” Implementing Remote Data Integrity Checking Protocol for Secured Storage Services with Data Dynamics and Public Verifiability In Cloud Computing, IOSR Journal of EngineeringMar. 2012, Vol. 2(3) pp: 496-500

[6] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capability-based Cryptographic Data Access Control in Cloud Computing", in International Journal of Advanced Networking and Applications, Volume 01, Issue 01, 2011.

[7] Rosario Gennaro and Daniel Wichs, Fully Homomorphic Message Authenticators IBM Research, T.J. Watson, May 23, 2012

[8] K. Kajendran, J. Jeyaseelan, J. Joshi, “An Approach for secures Data storage using Cloud Computing” In International Journal of Computer Trends and Technology- May to June Issue 2011

[9] W. Luo, G. Bai, “Ensuring the Data Integrity In Cloud computing” In Proceedings of IEEE CCIS, 2011.

[10] S. Sanka, C. Hota, and M. Rajarajan, “Secure data access in cloud computing,” in 2010 IEEE 4th International [13] http://en.wikipedia.org/wiki

[11] H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

[12] Dianli GUO and Fengtong WEN, “A More Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment”, in Journal of Computational Information Systems, ISSN; 1553–9105, Vol. 9:No. 2, 2013, 407-413

[13] Kristin Lauter, Michael NaehrigandVinodVaikuntanathan, “Can Homomorphic Encryption be Practical”, in ACM, 2008.

[14] Craig Gentry, “Computing Arbitrary Functions of Encrypted Data”, in ACM by IBM T.J. Watson Research Center, 2008.

[15] Bharath K. Samanthula, Gerry Howser, Yousef Elmehdwi, and Sanjay Madria, “An Efficient and Secure Data Sharing Framework using Homomorphic Encryption in the Cloud”, in Cloud 1st conference by ACM, ISSN: 978-1-4503, DOI: 1596-8/12/08, 2012.

[16] Robert Griffin and SubhashSankuratripati, “Key Management Interoperability Protocol Profile Version 1.1”, in OASIS Standards Organizations at http://docs.oasis-open.org/kmip/profiles/v1.1/os/kmip-profiles-v1.1-os.doc, 2013.

[17] Web Article, “Amazon Web Services: Overview of Security Processes” by Amazon Services at http://aws.amazon.com/security,June 2013.

[18] K. Raen, C. Wang, Q. Wang, “Security Challenges for the Public Cloud”, Published by IEEE Computer Society, Jan/Feb 2012

[19] J.-P. Aumasson, L. Henzen, W. Meier, and R. Phan, “SHA-3 proposal BLAKE,” December 2010.

[20] GALS System Design: Side Channel Attack Secure Cryptographic Accelerators

[21] AES encryption and decryption http://www.iis.ee.ethz.ch/~kgf/acacia/c3.html

[22] Kamara, S., Lauter, K.: “Cryptographic cloud storage”. In: Proceedings of the 14th international conference on Financial cryptography and data security, FC'10, pp. 136-149. Springer-Verlag, Berlin, Heidelberg (2010)