Data Storage Security Model using Homomorphic Encryption for Cloud

Banshri Modhiya[1] Dr. Chirag Thaker[2] Dr. Bhavesh Borisaniya[3]
[1]Student [2,3]Professor
[1,2,3]Department of Computer Engineering
[1,3]SSEC, Bhavnagar Gujarat, India [2]LDCE, Ahmedabad, Gujarat, India

Abstract— Cloud computing is an emerging technological paradigm providing huge infrastructure, resources, storage, and services over the Internet. The number of users are exponentially increasing day by day. Cloud computing is made up of data centers which handles large number of users. Security is the main concern in cloud computing and is major challenge for cloud users. As cloud provides multi-tenant architecture to store users' data, data security is must. To secure the data at rest on the cloud, users can encrypt the data before storing it over the cloud. However, to perform computation on encrypted data, user must have to download and decrypt the data first. To avoid this overhead from cloud user, in this paper we propose cloud data storage security model that utilize the partial homomorphic cryptography for encrypting the data over the cloud.

Key words: Data Storage Security Model, Homomorphic Encryption for Cloud

I. INTRODUCTION

The cloud computing provides ubiquitous, convenient, on demand network access to a shared pool of computing resources. The computing resources include networks, servers, storage devices, applications, and services. The shared pool of these computing resources can be released with minimal management effort or less service provider interaction using cloud computing [1].

Cloud Computing facilitates storage of applications, files and infrastructure via Internet. Cloud computing has been practiced since many years, but now a personnel avails more flexibilities in that such as buying or renting any space for performing daily operations. The savings done for cost for implementing a cloud system is quite noticeable, and the usage price can easily be scaled up or down as per the determination for the necessity.

The legitimate and the physical, both security issues are major concerns across all the different service models (i.e. software, platform, and infrastructure) of a cloud computing. It also addresses how these services are delivered, i.e. using public, private, or hybrid delivery model [2]. The cloud user and industry that access the service of cloud computing have their sensitive data over the cloud makes the security as key area of cloud computing. The importance is to have security of data and it is always vital because of the critical nature and due to huge/large complexities in data that it carries, so the requirement for security is even more determining thing. Hence data privacy and security are the concerns that are proving to be major issue to enhance the performance of cloud computing services. The user of cloud service, either an individual, organization or a firm/company should query about security issues to the cloud provider before hosting or posting/delivering their data or a set of applications on the cloud [3].

Cloud provides multi-tenant architecture to store the users' data. This may lead to data stealing and data leakage like security issues, which affects the cloud users' trust and cloud providers' reputation.

Simple way to deal with this problem is to encrypt the data before storing it over the cloud. This lead to another common issue, what if user wants to perform some simple computation over the data? It requires user to download the stored data, decrypt it, perform computation, encrypt the resultant data again, and store it back to the cloud. It is cumber some process for user and increase the overhead if user is using thin clients to access the cloud services. Hence, in this paper we propose cloud data storage security model that exploits the usage of partial holomorphic cryptography to encrypt the user data. It allows partial computation over user data.

Rest of the paper is organized as follows: Section II describes partial homomorphic encryption techniques used for cloud computing. Section III discusses the proposed cloud data storage security model followed by conclusion and references at the end.

II. PARTIALLY HOMOMORPHIC ENCRYPTION TECHNIQUES USED IN CLOUD COMPUTING

The homomorphic encryption allows computation on encrypted data. The resultant encrypted data, when decrypted matches the result obtained, if operations were performed directly on plaintext [4]. There are two types of homomorphic cryptosystems, namely partially homomorphic and fully homomorphic. Partially homomorphic cryptosystems supports only some mathematical functions (like addition and multiplication) on encrypted data, while fully homomorphic encryption supports any mathematical function. Due to major drawbacks of fully homomorphic encryption, it is not very practical. On the contrary many encryption techniques in use have partial homomorphic property.

Here we are describing some partial homomorphic techniques, which are used in cloud computing.

A. RSA

RSA is an asymmetric encryption system. It is a multiplicative homomorphic cryptosystem. If the RSA public key is (m, e) where 'm' is modulus and 'e' is exponent, then the encryption of a message x is given as [4]:

$$E(x) = x^c \bmod m$$

B. ElGamal Encryption

The ElGamal encryption system is an asymmetric encryption algorithm. It is based on Diffie-Hellman key exchange. The ElGamal encryption is based on multiplying mod p [5].

C. BGV Encryption

Most of the cryptosystem deals with integer vectors and integer polynomials [5]. The BGV encryption is an asymmetric encryption scheme which is based on the encryption of the bits.

D. Paillier cryptosystem

The Pailler cryptosystem is computationally difficult because of the computation of residue classes [4]. The scheme is an additive homomorphic cryptosystem. The additive homomorphic cryptosystem means: with the knowledge of the public-key and the encryption of messages m1 and m2, the encryption of message (m1+m2) can be computed.

E. EHC Encryption

The EHC is the new Enhanced Homomorphic Cryptosystem for homomorphic Encryption /Decryption with IND-CCA secure [5]. The scheme is a mixed (additive-multiplicative) homomorphic cryptosystem

Homomorphic Encryption Technique	Homomorphic Type	Application
RSA [4]	Multiplicative	Transaction of credit card and online banking
ElGamal [5]	Multiplicative	Used in hybrid cryptosystems
BGV [5]	Mixed	For the security of integer polynomials
Paillier [4]	Additive	E-voting system, threshold scheme
EHC [5]	Mixed	Efficient secure message transmission in mobile ad-hoc n/w

Table 1: Comparison of Various Homomorphic Encryption Techniques

Table 1 summarizes the comparison of described partial homomorphic techniques used for cloud computing. We chose ElGamal algorithm in our proposed security model because it can be used in hybrid cryptosystems.

Table 2 describes the comparison of related work found in literature. Most of the approaches failed to provide data integrity checking, message access right and computation on encrypted data, all in one solution. Our proposed approach provides all these features as shown in last line of the table.

III. PROPOSED WORK

The end hosts performs the data storage and processing using secure resources while the network simply provides transmission of these data. Thus data protection could involve privacy and security at the known end points of a data transaction. This system also includes appropriate security measures applied to protect the data in transmission. Our propose work provide strongest security of the data storage security model using ElGamal homomorphic encryption.

The main stakeholders of our model are: (i) Cloud Data Owner (CDO), who generate and own the data and possesses all rights about the operation on the data. (ii) Cloud Data User (CDU), who uses the data that are generated by the CDO based on the rights issues. The rights of one CDU can be passed to other CDU. (iii) Cloud Service Provider (CSP) is a central component for the system. It provides the facility of data warehouse for the other stakeholders.

A. Step 1: Data

Data file is hand over to this Cryptographic Primitives unit, which in turn encrypts file (C).

B. Step 2

1) Control Information

Cryptographic Primitive unit send to the Control Information and Access Rights to Cloud Access Control Mechanism unit of CSP.

2) Homomorphic encryption & Hash code

File will be encrypted using ElGamal homomorphic encryption. Encrypted file and hash value are sent to Cloud Data Storage unit of CSP.

Title	Encryption	Computation on Encrypted Data	Data Integrity Checking	Manage Access Rights
Data Storage Security Model for Cloud Computing [6]	✓	×	✓	✓
Ensuring Data Storage Security through a Novel Third Party Auditor Scheme in Cloud Computing [7]	✓	×	×	✓
Improving Security and Efficiency in Attribute-Based Data Sharing [8]	✓	×	×	✓

Cloud Storage System Enabling Secure Privacy Preserving Third Party Audit [9]	✓	×	✓	×
Data Storage Security Model using Homomorphic Encryption for Cloud (Our Approach)	✓	✓	✓	✓

Table 2: Comparison of Related Approaches

3) Computation on Encrypted Data

As data encrypted with ElGamal, CDO can perform specific computation over stored data.

C. Step 3: Data access Request

CDU makes Data Access Request to CDO and rights of the data access.

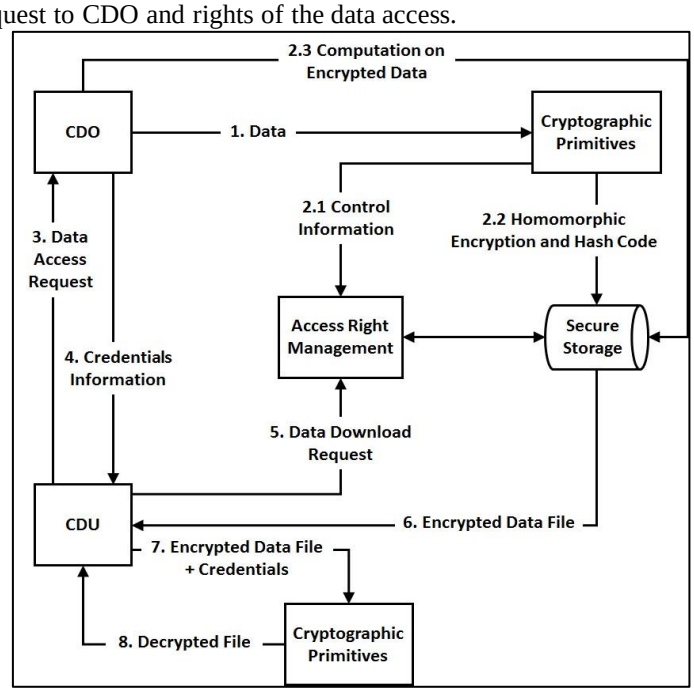

Fig. 1: Proposed Data Storage Security Model using Homomorphic Encryption for Cloud

D. Step 4: Credentials Information

CDO respond to the CDU with credential information.

E. Step 5: Data Download Request

CDU send Data Download Request to Cloud Access Control Mechanism unit of CSP.

F. Step 6: Encrypted Data File

Cloud Data Storage unit supply Encrypted Data File to CDU.

G. Step 7: Encrypted Data File and Credentials

CDU send encrypted file with credential information to the cryptographic Primitive unit.

H. Step 8: Decrypted File

Cryptographic Primitive unit does the verification of credential information of the CDU and send the decrypted data to the CDU.

Steps shows the general usage of cloud storage service- CDO encrypt the data with homomorphic encryption (ElGamal), store it over cloud, CDU makes the request to access the data, through access right management and credentials CDU can download and decrypt the data. Here, because of partial homomorphic property of ElGamal encryption CDO can also perform the computation (multiplication) over encrypted data.

IV. CONCLUSION

As cloud provides multi-tenant architecture to store users' data, data security is must. To secure the data at rest on the cloud, users can encrypt the data before storing it over the cloud. However, to perform computation on encrypted data, we must download and decrypt the data first. In order to overcome this problem we proposed data storage model for cloud that utilize the partial homomorphic cryptography for encrypting the data over the cloud.

The proposed model achieves the confidentiality by storing encrypted data over the cloud. It allows users to check the integrity of their stored data and provides functionality of minimal computation over the encrypted data stored in the cloud.

REFERENCES

[1] Peter Mell, Timothy Grance "NIST Definition of cloud computing", National Institute of Standards and Technology (NIST), 2010.
[2] Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", In Proceedings of International Conference on Emerging Intelligent Data and Web Technologies, 2011. IEEE, pp. 49-54.
[3] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. Atanu Rakshit, "Cloud security issues" In IEEE International Conference on Services Computing, 2009. IEEE, pp. 517-520.
[4] S. Ramachandram, R. Sridevi, P. Srivani "A Survey Report on Partially Homomorphic Encryption Techniques in Cloud Computing" International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 12, December 2013.
[5] Payal V. Parmar, Shraddha B. Padhar, Shafika N. Patel, Rutvij H. Jhaveri, Niyatee I. Bhatt "Survey of Various Homomorphic Encryption algorithms and Schemes" International Journal of Computer Applications, vol. 91, no. 8, April 2014.
[6] Hiren B. Patel, Dhiren R. Patel, Bhavesh Borisaniya, and Avi Patel "Data Storage Security Model for Cloud Computing" In International Conference on Advances in Communication, Network, and Computing, 2012. Springer, pp. 37-40.
[7] Shuai Han, Jianchuan "Ensuring Data Storage Security through a Novel third party Auditor scheme in Cloud Computing" In IEEE International Conference on Cloud Computing and Intelligent Systems (CCIS), 2011. IEEE, pp. 264-268.
[8] JunbeomHur "Improving Security and Efficiency in Attribute-Based Data Sharing" IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, October 2013.
[9] Prof. D. N. Rewadkar, Suchita Y. Ghatage "Cloud Storage System Enabling Secure Privacy Preserving Third Party Audit" In International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014. IEEE, pp. 695-699.