TRANSLUCENCE PROTOTYPE MODEL FOR DATA SECURITY IN CLOUD PLATFORM USING DOUBLE ENCRYPTION TECHNIQUE

Sagarika Behera[1], Jhansi Rani P[2]

[1]Research Scholar, Dept. of CSE , CMR Institute of Technology, VTU ,Bengaluru
[2]Professor, Dept. of CSE, CMR Institute of Technology, VTU ,Bengaluru

E-mail: sagarika.b@cmrit.ac.in[1], jhansirani.p@cmrit.ac.in[2]

Received: April 2020 Revised and Accepted: June 2020

ABSTRACT: Distributed computations are emerging advancements in the computer world at the present moment and information security along with confidentiality is an important problem. In this situation, cloud computing emerged as a viable solution for industries, businesses, organizations with pay-per-use service. These cloud service providers (CSP) maintain meta-information in private indexing where some of the time it led to confidential and information assurance controversy. If meta-information is undermined, at that point unapproved access to customer information is conceivable. For the insurance of customer information, we present a translucence prototype (TP) in this research paper. TP gives a component location where the cloud supplier designs the administration on the cloud by giving the administration data around the distributed repository gadgets contain the information. It is the accountability of the Transparency Service Model (TSM) to store information in concern and the cloud suppliers can't access directly to information stockpiling on different gadgets.

KEYWORDS: Translucence Prototype (TP), Cloud Service Provider (CSP), Key Provider, Crypto Provider.

I. INTRODUCTION

The cloud providers keep user's meta-information in databases which are located on their sites where now and again it is vulnerable to security and information assurance issue. On the off chance that meta-information is undermined than unapproved access to customer information is conceivable. For the assurance of customer information, we present a prototype known as a translucence prototype (TP) for the Transparency Service Model in this paper. TSM gives a system for the cloud supplier to arrange the administration on the cloud by providing the administration data about the distributed storage gadgets which contain the information. One of the fundamental issues in distributed computing is information security and protection. At the point when a customer stores information on the cloud he/she has no physical access to the establishment taking care of the data or information. This is an imperative concern since most business and customers hate their information to be vulnerable against any information security and insurance issues.

II. RELATED WORKS

Salman Ashraf, et.al [1] presented a transparency service model (TSM) in their paper.

B. Muthulakshmi, et.al [2] proposed a double encryption and decryption method. They have analyzed some existing methods KNN, hybrid cryptography, etc. and the disadvantages of those methods. Timothy Oladunni, et.al [3] analyzed the existing homomorphic encryption algorithms and the real-time application of the homomorphic encryption method. Cong Wang, et.al [4] claimed that if there exists a malicious server in a distributed storage system then their scheme can achieve the integration of storage correctness and data error localization by using homomorphic token. This plan accomplishes the reconciliation of capacity accuracy protection and information mistake limitation, i.e., the recognizable proof of making trouble server(s).

In the paper [6] Danilo Ardagna, et.al had talked about Quality-of-Service (QoS) management which is one of the difficulties presented by cloud applications. QOS problem includes allocating resources to different cloud applications to make sure good service to the customers. This can be considered with different dimensions such as performance, reliability, and availability. Masrat Yousuf Pandith [5] talked about data security and protection worries in distributed computing.

Yunchuan Sun, Junsheng Zhang, Yongping Xiong and Guangyu Zhu [7] discussed the data security and protection worries in distributed computing. Information security has reliably been a significant issue in data innovation. S. Subashini and V. Kavitha [8] analyzed the security issues existing in all three service models of cloud computing. Gurpreet Kaur, et. al [9] analyzed the existing different cryptographic algorithms and compared the local mean time and speed up the ratio of different algorithms for various input sizes. Moussa Ouedraogo, Severine Mignon, Herve Cholez, Steven Furnell and Eric Dubois [10] proposed a transparency service model to provide better security transparency between the cloud service provider (CSP) and cloud service customer (CSC). Umar Mukhtar Ismail, et. al [11] presented a framework for security transparency in the cloud system. They have analyzed it from three different levels such as conceptual level, technical level, and organizational level.

III. PROPOSED METHODOLOGY

Figure 1 shows the proposed method for Transparency Service Model (TSM). The main aim of this service model is to give a transparency service to the customer where they can store their data in a transparent manner. Cloud providers will not have direct access to those devices where customer's data are stored. TSM will take care of storing user's data on those devices. Users will not directly interact with the cloud infrastructure. Whenever a user wants to store and retrieve data from the cloud storage, he/she will interact with TSM. In turn, TSM will interact with cloud storage.

The interaction steps between different modules of translucence prototype are explained below with reference to Figure 2.

1. The user requests a key from the key provider.
2. The Key Provider sends a key to the user.
3. After getting the key it sends the data and key to the cryptography provider to encrypt the data.
4. The Cryptography Provider encrypts the data and sends back the encrypted data to the user.
5. User sends the encrypted data to the TSM applications to store it in the cloud.
6. TSM interacts with the cloud service to store the user's encrypted data. Since the entire cloud service providers encrypt the customer's data before storing it into the cloud, it again encrypts the encrypted data. So here user's data double encrypted before going to the cloud service.
7. TSM sends a message to the user after successfully storing the data in the cloud storage.
8. It also interacts with the TSM and TSM interacts with the cloud service system when the user needs to access the data from the cloud storage.

The various operations which can be done in different modules are given below.

3.1 Account Operations

Record activities module provides the following functionalities to the end clients of our system.

- Register another customer account
- Log in to a current record
- Logout from the meeting
- Edit the current Profile

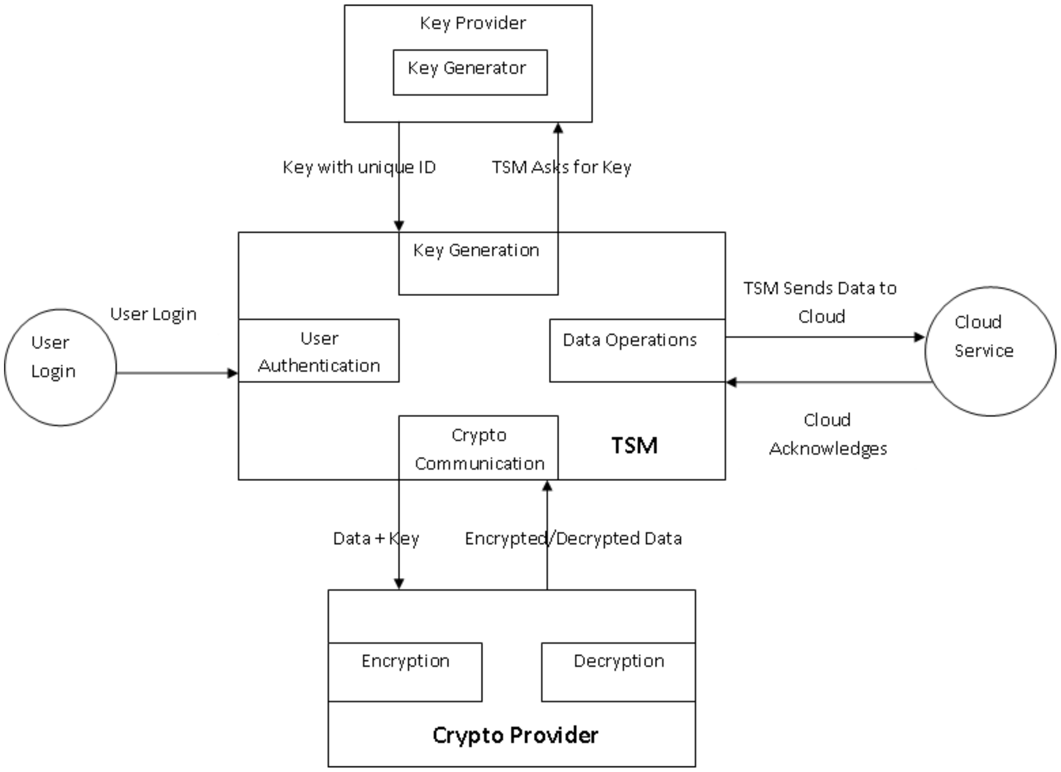

Figure 1. Proposed translucence prototype for double encryption of data in cloud platform

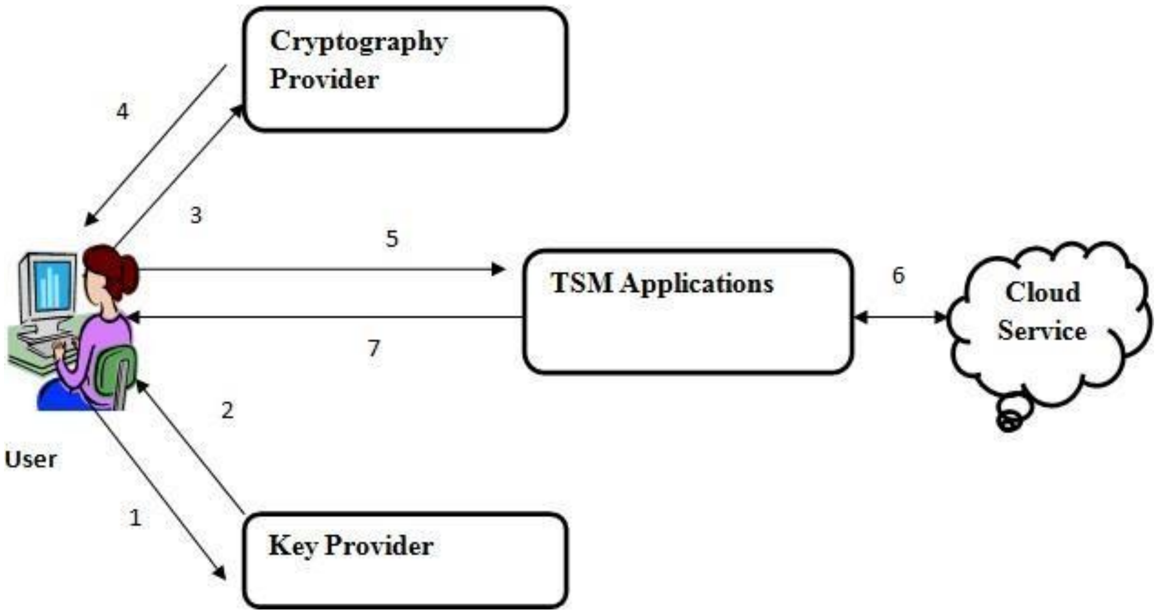

Figure 2. Interaction between different Modules of TP

- Change Password for security issues
- Forgot Password and get the present secret word over an email
- Delete a current Account

3.2 Key Provider

This module enables the end-user to perform a couple of operations with reference to the encryption keys

- *Key Generation Operation*

This component provides the user with a feature where they can generate a new key of the required length. This is used while writing new data to the cloud. Here we have used AES-256(Advanced Encryption Standard-256) for encryption. So the length of the key is 256 bits.

3.3 Cryptography Provider

This module enables the user to perform cryptographic operations on the input data. The users can perform the below two operations using this module.

- *Encryption Operations*

This component provides the user with a feature where they can perform encryption of the given input data. Before invoking this component, the user must have already generated the unique key for encryption using the Key Provider component described earlier. In this paper, we are proposing a double encryption method to provide more security and privacy to the user data. Before the user's data will move to the cloud, it has been encrypted using the AES-256 encryption algorithm and moved to TSM applications.

- *Decryption Operations*

This component provides the user with a feature where they can perform the decryption of the given input data. Before invoking this component, the user must have already generated the unique key for encryption using the Key Provider component we described earlier.

3.4 Transparency Service Model

This module is the one which the end-users will have direct access to and we will be providing a user interface (UI) for the user. This portal will have multiple sub- components as described below.

- *User Account Operations*

This segment checks the authenticity of the client to get into our system. It validates the client by checking it's login information.

- *Key Provider configuration*

This module enables the final user to specify the endpoint where the key provider has been deployed. It sets the URL and port number of the key provider.

- *Cryptography Provider configuration*

This module enables the final user to specify the endpoint where the cryptography provider has been deployed. It sets the URL and port number of the cryptography provider.

- *Data Write Operation*

This segment enables the final user to perform the data write process to the cloud storage space. The structured data will be persisted in the MySQL an instance of the cloud application deployed in any of the cloud service providers; whereas the unstructured data uploaded using a browse button will be persisted on the cloud storage file system. The customer first will have to select the data model indicating the type of data to be written on to the cloud. After selecting the data model, the user will be asked to provide the key-value pairs for the data models for encryption. The data written by the user will be encrypted using the AES-256 cryptography.

- *Data Read Operation*

Here the final user will be able to see the list of all the data they had written on to the cloud storage space in the previous section. The list of all the data will be retrieved from the MySQL instance and also from the cloud storage file system of the cloud storage space and then it will display on the HTML interface. The user can then perform the data decryption of the data using the Advanced Encryption Standard (AES) cryptography.

- *Data Share Operation*

Here the users will be able to share his/her data with other registered users, and also can access the data shared with him/her from other registered users. While sharing the data, the owner must specify the level of access to be granted to the shared user. The access level will either be read-only access or read-write access. The data owners will have the privilege of changing the access levels on the shared data at any point of time.

IV. RESULTS

4.1 Key Provider

This portal allows the end user to generate the key.

- **Key Generation**

This component gives the user a feature that allows them to generate a new key K_{new}, of the required length L_1. Here we have generated an encryption key K_{new} of 256 bit (32bytes) and an initialization vector V_1 of 16 bytes for CBC (Cipher Blocker Chaining) mode. This V_1 is used with the secret key for data encryption and it prevents repetition of data encryption which makes it difficult for the hacker to perform dictionary attack to break the cipher. The 32 bytes key and 16 bytes initialization vector generated in our system is as below.

K_{new}=E8B6C00C9ADC5E75BB656ECD429CB1643A25B111FCD22C6622D53E07 22439993

V_1 =E486BB61EB213ED88CC3CFB938CD58D7

This 32 bytes key will be stored in the form of 4X8 matrix. Here each column is a word which consists of 4 bytes. The words are denoted as W_0 to W_7.

W_0=E8B6C00C, W_1=9ADC5E75, W_2=BB656ECD, W_3=429CB164, W_4=3A25B111, W_5= FCD22C66, W_6=22D53E07, W_7=22439993

K_{new} is represented in the form of 4X8 matrix:

$$\begin{bmatrix} E8 & 9A & BB & 42 & 3A & FC & 22 & 22 \\ B6 & DC & 65 & 9C & 25 & D2 & D5 & 43 \\ C0 & 5E & 6E & B1 & B1 & 2C & 3E & 99 \\ 0C & 75 & CD & 64 & 11 & 66 & 07 & 93 \end{bmatrix}$$

After generating the key K_{new}, it sends back to the user.

4.2 Cryptography Provider

This portal allows the user to perform the cryptographic operations on the data being input. With reference to this portal the users can perform the two operations below.

- **Encryption operation**

AES algorithm encrypts a plain text block P of 128 bits into a cipher text block C of size 128 bits using encryption key K_{new}. Here each block is represented by 4 words and encryption key K_{new} is represented by 8

words and number of rounds N_{round} required is
14. If the block size is not a multiple of 16 bytes, then padding will be done to make it multiple of 16 bytes.

After getting the key from the key provider user sends the input plain text file with the key to the cryptography provider to do the encryption of input text file. Here a plain text file named as “TEST.txt” given as input file with the encryption key K_{new} generated in the previous step.

cipher_text = aes_encryption (“TEST.txt”, K_{new})

Table1 shows the plain text which is present in the input file and the cipher text which we got after performing the encryption.

Plain Text	Cipher Text
hi everyone this is a nice experience to work on this project. I had learnt so many things.	U2FsdGVkX18BnzgbbaSt/AULM8PUX6h5i8N93 FN3U+U9YS0gD5qxuBXxIHH5jO9f kvsWZjwxCo+JoUK4tDUqwXsRY2iEmufFQn12e oMdBFToIwafJuFtxf2V9jPzzhRw COY46XTzFwlx2fn3VxZkLQ==

Table1. Plain text and corresponding cipher text after performing encryption

After performing AES-256 CBC (Cipher Blocker Chaining) mode operation on the plain text, cipher text is generated and stored in a file ”OUT.txt”.

- **Decryption operation**

This component provides the user with a functionality in which they can decrypt the data given as input.

plain_text = aes_decryption (“OUT.txt”, K_{new})

Here “OUT.txt” file which contains the cipher text is given as input with the encryption Key$K_{new}$and after decryption the output is stored in another file”OUT1.txt”. The OUT1.txt file contains the same plain text which the original input file TEST.txt contains. Table 2 shows the cipher text and the corresponding plain text after decryption.

Cipher Text	Plain Text
U2FsdGVkX18BnzgbbaSt/AULM8PUX6h5i8N 93FN3U+U9YS0gD5qxuBXxIHH5jO9f kvsWZjwxCo+JoUK4tDUqwXsRY2iEmufFQn 12eoMdBFToIwafJuFtxf2V9jPzzhRw COY46XTzFwlx2fn3VxZkLQ==	hi everyone this is a nice experience to work on this project. I had learnt so many things.

Table2. Cipher text and corresponding plain text after decryption

These encryption and decryption process executed on Intel(R) core i7-4770 CPU 3.40 GHZ, 8 GB RAM, X64-based processor. We found that on average it takes 2.57 ms for encryption and 1.16 ms for decryption.

V. SECURITY ANALYSIS OF PROPOSED TRANSLUCENCE PROTOTYPE

In this section we will conduct informal security review by heuristic method of our proposed translucence prototype. In Table 3 we have shown some cloud security threats and the majors which we have taken in our proposed system for those threats.

Sl. No.	Security Threats	Majors
1	Malicious Insiders	TSM selects cloud resources randomly to save users' data. Nobody knows in which drive users' data is residing. So it is difficult for the insiders to access it. Since data encryption is achieved using AES standard encryption techniques, decryption will take years.
2	Malicious Outsiders	TSM uses password to restrict all outsiders' access to data. Authentication tops the original protection for the cloud platform. If a certain outsider has to hack the data, first they have to break the security in the cloud and then somehow compromise security offered by TSM.
3	Denial of Service (DOS)	In this proposed scheme TSM verifies the authenticity of the user. User login to use the TSM applications and it has no direct access to the cloud system. So this scheme is robust enough against DOS attack.
4	Nefarious use of Cloud System	In this system users are unable to directly access the cloud system. TSM acts as a cloud- based user interface. But malicious users are not permitted to misuse the cloud services.
5	Data Leakage	Data leakage is avoided since double encryption is performed on user data before moving to the cloud storage system.
6	Unauthorized Access	To authenticate the user to sign in to the TSM, a multifactor authentication that uses the user's email id as user name and password is used. Unauthorized access is limited in this way.

Table3. Cloud related security threats and majors provided by translucence prototype

V. CONCLUSION

Here we have proposed a model for dealing with the issue of information security and protection in distributed computing by disguising data from cloud service providers and their employees. The main reason for the model is to take control of the duty to save and recover information from the cloud so that the model knows where certain customer's information lives. We have utilized key of AES algorithm for encryption and decoding of information as it is broadly utilized for security in numerous USA government organizations and it has had not very many assaults against it. We have facilitated the proposed method on remote virtual machine; along these lines in any case who registers with the model can utilize the administrations of the cloud.

VI. REFERENCES

[1]. Salman Ashraf, Muqaddas Gull, Tanzila Kehkashan and Saira Moin u Din "Transparency Service Model For Data Security In Cloud Computing", International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2018 .

[2]. B. Muthulakshmi, M.Venkatesulu, " Privacy and Security Aware Cloud Storage using Double Cryptography Method", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4S2, December 2019

[3]. Timothy Oladunni, Sharad Sharma, "Homomorphic Encryption and Data Security in the Cloud", EPiC Series in Computing, Volume 64, 2019, Pages 129–138

[4]. Cong Wang, Qian Wang, and KuiRen "Ensuring Data Storage Security in Cloud Computing", 978-1-4244-3876-1/09/$25.00 ©2009 IEEE .

[5]. MasratYousuf Pandith "Data security and privacy concerns in cloud computing", Internet of Things and Cloud Computing Journal 2014; 2(2):6-11.

[6]. DaniloArdagna, GiulianoCasale, Michele Ciavotta, Juan F Pérez and Weikun Wang "Quality-of-service in cloud computing: modeling techniques and their applications" Ardagna et al. Journal of Internet

Services and Applications 2014,5:11.

[7]. Yunchuan Sun, Junsheng Zhang, YongpingXiong, and Guangyu Zhu "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks Volume2014.

[8]. S. Subashini and V. Kavitha, "Review: A survey on security issues in service delivery models of cloud computing, "Int. Journal of Network and Computer Applications, pp. 1–11, January2011.

[9]. GurpreetKaur, Manish Mahajan Gurpreetkaur "Analyzing Data Security for cloud

[10]. computing using cryptographic Algorithms" etal.Int Journal of Engineering Research and Applications. ISSN: 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013,pp.782-786

[11]. Moussa Ouedraogo, Severine Mignon, HerveCholez, Steven Furnell and Eric Dubois, "Security transparency: the next frontier for security research in the cloud", Journal of Cloud Computing: Advances, Systems and Applications (2015) 4:12

[12]. Umar Mukhtar Ismail, Shareeful Islam , MoussaOuedraogo and Edgar Weippl," A Framework for Security Transparency in Cloud Computing", Future Internet 2016, 8, 5; doi:10.3390/fi8010005