International Journal of Research in Advent Technology, Vol.2, No.3, March 2014

E-ISSN: 2321-9637

Decentralization of Cloud Computing Security

Aaliya peerzada[1], Zaid Khan[2], Prof. Supriya Madane[3],
Department of Information technology[1,2,3]
Trinity College Of Engineering and Research [1,2,3],Pune, India.
Email: aaliya_peerzada@hotmail.com[1], zaid.khan91@gmail.com[2], sups9.madane@gmail.com[3]

Abstract- Organisations store client's data in their internal storage memory and protect these confidential files using firewall, so that it is protected against intruders. They also form policies to avoid disclosure of client's data by organisational employees. Cloud computing systems store client's data in the storage space provided by the organisations which are responsible for providing the services of cloud. Service providers must use strong measures to protect their clients' data, especially to avoid disclosure of user data by unauthorized employees or insiders. The most common method of privacy is storing the data in encrypted form. If the cloud system is carrying out both the processes, that is, the encryption of client's data and storage of it, then the system administrators responsible for this process acquire the encrypted data and the keys required for decryption. Thus they can access confidential information without authorization and this poses a risk of information disclosure which is unsuitable from the point of view of cloud system security. This study proposes a security model for cloud computing using two clouds, one responsible for the encryption and decryption of client's data only and the other responsible for storage of this encrypted data. This can be achieved by integrating the concept of Trusted Computing Platform (TCP). The cloud responsible for the data storage must not store data in plaintext or original form but must store it in encrypted format only, and the cloud responsible for data encryption and decryption (i.e TCP cloud) must delete all data upon the completion of encryption or decryption process and must store only the decryption keys. Both the clouds work in accordance with each other without having any interaction between them. Hence the client's data is secure from the administrative point of view also.

Index Terms- Cloud Computing; Trusted Computing Platform (TCP); Encryption and Decryption cloud.

[1] INTRODUCTION

A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Shared resources, software and information are provided to computers and other devices on demand. It allows people to do things they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology. Through cloud computing, clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic. The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud. All of this is available through a simple internet connection using a standard browser. Since cloud computing share distributed resources via the network in an open environment, it makes it important for us to develop the security solutions for cloud computing applications.

We proposed a method to build a security model for cloud computing system by integrating the trusted computing platform(TCP) [1] into cloud computing system. By this we'll be separating the encryption and decryption process from the storage of user data. TCP is a chip (combination of hardware and software) providing various security services. Thus with this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing environment. Furthermore, the cloud responsible for the data storage must not store data in original or plaintext form, and the cloud responsible for data encryption and decryption must delete all data upon completion of encryption or decryption.

[2] BACKGROUND STUDY

Trusted Computing Platform (TCP), which is based on Trusted Platform Module (TPM), can be integrated into the cloud computing system for providing security. The TCP is a chip which provides authentication, confidentiality and integrity in the cloud computing environment. TCP functionality consists of two basic services, authenticated boot and encryption, which work together. An authenticated boot service finds out which operating system is booted on the machine which in turn will help in providing security. It provides the TCP functionality which is authentication boot service, encryption

/decryption of data and storing of its respective private key. But TCP is a hardware that is a chip which is fitted on the motherboard of all the cloud servers which has a very high costing so it is not very much affordable. Hence not all cloud computing organisations can use this technology. To make it available for all we have decided to develop a software version of it, which constitutes our TCP cloud.

Separating the encryption/decryption service from storage service [2] would help provide better security to the cloud computing system. It involves a separate encryption/decryption cloud service to the business model, wherein two service providers split responsibility of data encryption/decryption and data storage. This to a certain extent provides security from the administrative point of view but still hold a few drawbacks. The separation of services still exists in the same cloud under the same cloud administrator. Hence it still poses the risks of data leakage or misuse by the administrator. Thus we have come up with this new concept where there will be two different clouds, one responsible for data storage only and the other cloud responsible for encryption/decryption only. This cloud includes the TCP functioning also. The two clouds have no interaction at all and work independently. Thus by integrating all the above ideas and working out on the drawbacks we have come up with this new concept of decentralization of cloud computing security.

[3] PROBLEM DEFINITION

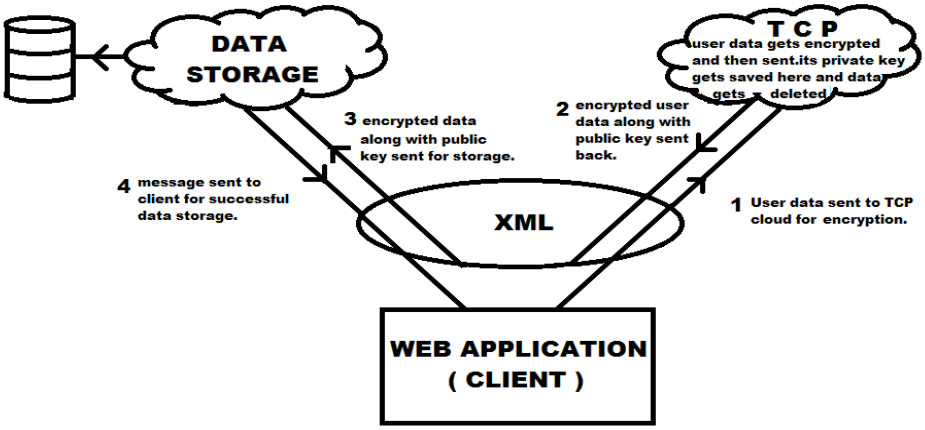
In a cloud computing environment, the necessary resources required by client's are leased by the organization providing these services and the client's confidential data gets stored on the cloud. This setup can help a company save on the software, hardware and infrastructure costs however storing the company's confidential data on the cloud creates a risk of disclosure of important and confidential business information, which can prove harmful for the progress of a company.

The main aim of are project is to provide high end security to the cloud computing environment by separating the data storage from the encryption/decryption of user data. The core concept of this study is to separate the encryption /decryption process from the storage process so as to prevent wrongful disclosure of important data from the administrative point of view. We have proposed a method to build a security model for cloud computing system by integrating the idea of trusted computing platform (TCP) into cloud computing system. TCP is a chip (combination of hardware and software) providing various security services. For cloud computing technology to spread, the service providers must use such policies which build up a high trust factor among its clients. This study proposes a security model for cloud computing based on a separate encryption and decryption service cloud and separate storage cloud, emphasizing that the encryption/decryption process and the storage of encrypted data will be vested within two different clouds altogether. This will provide higher security to the client's data as the encrypted data would be stored in the storage cloud and its respective private key would be stored altogether in another cloud that is our TCP cloud. The two clouds will not have any sort of interaction with each other thus providing high end security to the users. Both the clouds will be working independently. The storage cloud will only be responsible for storing the encrypted client's data and the TCP cloud will only be responsible for storing its respective private key. Furthermore, the TCP cloud will not be allowed to store the client's data, once it has been encrypted and sent back by it, all the data from the TCP cloud should be deleted and only its respective private key should be stored. The storage cloud will only be storing the encrypted client's data but it won't be having its private key to decrypt. Hence there will be no risks or threats of improper disclosure of data even from the administrative point of view. The TCP cloud will also perform Digital signatures thus ensuring data integrity of the client's data. We can also include the authentication boot service in the TCP cloud that will help the cloud system know the configuration settings (Operating system) of the client's machine. In this manner we can provide a secure way of storing the client's data on the cloud by decentralizing the cloud computing security, hence providing high end security to the user data in cloud**.**

[4] SYSTEM DESIGN

The working of storing and retrieving of data in cloud, through our concept.

4.1. For data storage :



Step 1: For a new user, the user will first create a new account. The user details will be stored at the storage cloud. After the user logs in to the cloud and has got authenticated, it might send a request to upload data or might use some resources which may require to store the data, so firstly using the diffie-hellman key exchange algorithm the user and the TCP cloud will share a secret key which will be used for encrypting and decrypting the data along their path. Once the secret key has been computed the user will encrypt the desired data using this secret key and send this encrypted data to the TCP cloud in a secure manner.

Step 2: At the TCP cloud, this user data gets decrypted using the shared secret key formed by diffie- hellman key exchange algorithm. Then user data again gets encrypted using the RSA algorithm, developing public and private key. After encryption, SHA-1 algorithm is performed for verification purposes. Then this encrypted data along with the public key and user ID is sent back to the cloud application. After encrypting the data and sending it back, the user data gets deleted from the TCP cloud and its private key along with the public key, the hash and user ID gets saved at the TCP cloud. So the TCP cloud only has the private key stored but no data at its side.

Step 3: Meanwhile from the cloud application this encrypted data along with public key and user ID is sent to the storage cloud, where it is securely stored.

Step 4: The client then gets a message from the storage cloud stating that the data was successfully stored. If any errors occur in storing the data, then it is made known to the client through a failure message.

4.2. For data retrieval:

Step 1: When the user wants to access/download their stored data, the system first verifies its authentication. After successfully verifying the user, a request for data retrieval is sent to the storage cloud having the user ID and public key.

Step 2: The storage cloud searches for the requested data by matching the public keys and user ID. After the data has been found it is sent back to the client side.

Step 3: This encrypted data is then sent to the TCP cloud where it gets decrypted using the private key. System uses the received user ID and public key to index the user's private key (decryption key), which is then used for decryption of received data. It is important to use the correct decryption key to bring back the data to its correct original form. After the data is decrypted, using the SHA-1 algorithm (hash) it is verified whether the data is the same as how it was stored or there are any modifications made.

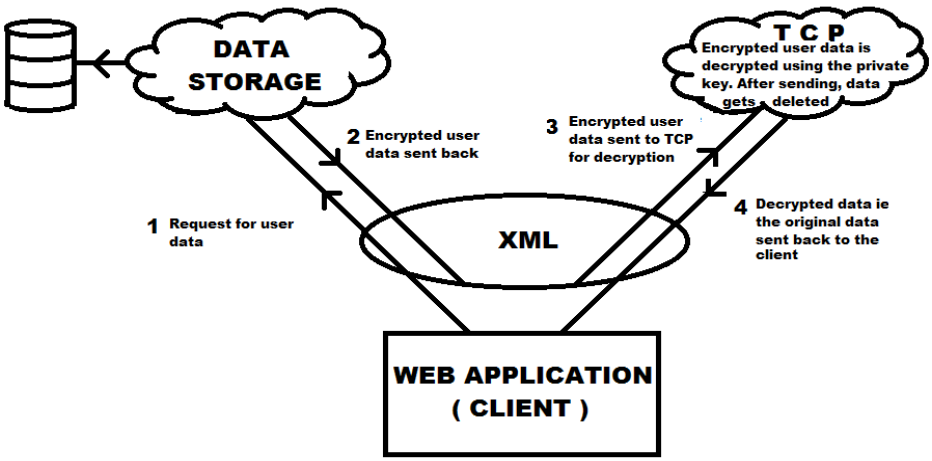


Fig 2: The conceptual diagram showing data retrieval process in cloud computing environment.

Step 4: After verification the decrypted data(original data) is sent back to the client in an encrypted manner using the diffie- hellman key exchange algorithm. After the client's data is sent, the TCP cloud is not allowed to retain the data and so any client's data in encrypted or original form is deleted thus preventing storage of data and key in the same system. This is the most important criteria for ensuring the privacy of user data.

5. CONCLUSION

This study proposes a concept for Cloud Computing based on decentralizing the security working of cloud by separating encryption and decryption service cloud that is our TCP cloud from the storage cloud, which implies that the storage and encryption/decryption of user data must be allotted to two different service providers which are present in two different clouds altogether. The functionality of Storage Cloud includes storing user data which has already been encrypted through a TCP Cloud. The functionality of TCP cloud include encrypting/decrypting, providing digital signatures to the user data and sending it back, after which the data gets deleted from the TCP cloud and only its respective private key gets stored at the cloud. These clouds do not interact with each other in any manner and work independently. Thus the TCP cloud only consists of the private key (decryption key) but has no user data stored in it and the Storage cloud consists of only the encrypted data but does not have its respective decryption key. As both these clouds have no interaction with each other the data remains stored safely in an encrypted manner even from the administrative point of view. In this manner we decentralize the working of data storage process thus providing immense security to the cloud computing environment.

[5] ACKNOWLEDGEMENTS

Our sincere thanks to our project guide Prof.Supriya Madane, Prof.Sarita.S.Gaikwad the head of department and Prof. Prakash Dabir, the Principle of Trinity college of engg and research(TCOER), for their valuable guidance and constant encouragement.

[6] REFERENCES

[1] The Security of Cloud Computing System enabled by Trusted Computing Technology. Published by: Zhidong Shen, Qiang Tong.

[2] A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service. Published by: Jing-Jang Hwang and Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu.

[3] Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing.

[4] 3-Dimensional Security in Cloud Computing.

[5] Multi-dimensional password generation technique for accessing cloud services.