SECURE STORAGE AND ACCESS OF DATA IN CLOUD COMPUTING

Vaishnavi
PG Scholar, Department of Computer Science and Engineering
Pandian Saraswathi Yadav Engineering College, Sivagangai, Tamil Nadu

Abstract
Cloud computing is the most demanded advanced technology throughout the world. It is one of the most significant topic whose application is being researched in today's time. One of the prominent services offered in cloud computing is the cloud storage. With the cloud storage, data is stored on multiple third party servers, rather than on the dedicated server used in traditional networked data storage. All data stored on multiple third party servers is not cared by the user and no one knows where exactly data saved. It is cared by the cloud storage provider that claims that they can protect the data but no one believes them. Data stored over cloud and flow through network in the plain text format is security threat. This paper proposes a method that allows user to store and access the data securely from the cloud storage. It also guarantees that no one except the authenticated user can access the data neither the cloud storage provider. This method ensures the security and privacy of data stored on cloud. A further advantage of this method is that if there is security breach at the cloud provider, the user's data will continue to be secure since all data is encrypted. Users also need not to worry about cloud providers gaining access to their data illegally.

Keywords: *Cloud Computing Security, Cloud Security, Cloud Storage Security*.

Introduction

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, and processing and band width. But where does security fit into all this? Security analysts and practitioners generally say proceed, but proceed with caution. All the risks to sensitive corporate data associated with outsourcing apply to cloud computing, and then some. Enforcing security policy and meeting compliance requirements are tough enough when you deal with third parties and their known or unknown subcontractors, especially on a global scale.

We propose a method to build a trusted computing environment for cloud computing system by providing the method that encrypts the data at client side using secret key before sending to cloud storage and decrypts the data using same secret key after receiving from cloud storage. These both operations is done at client side making use of secret key in this way secret key never leaves the client computer and user is assured about security of data stored in cloud. The rest of this paper is organized as follows. We first provide the basic concept of cloud storage in section 2. Then, section 3 describes preliminaries. Section 4, 5, 6 discussed the proposed method and section 7 describes the conclusion and future work ideas.

Basic Concept of Cloud Storage

Cloud storage is one of the primary use of cloud computing. With the cloud storage, data is stored on multiple third party servers, rather than on the dedicated servers used in traditional networked data storage. When storing data, the user sees a virtual server that is, it appears as if the data is stored in a particular place with specific name. But that place does not exist in reality. It is just a pseudonym used to reference virtual space carved out of the cloud. In reality, the user's data could be stored on any one or more of computers used to create the cloud [3].

The actual storage location may even differ from day to day or even minute to minute, as the cloud dynamically manages available storage space. But even though the location is virtual, user sees a static location for his data and can actually manage his storage space as if it were connected to his own pc. Typical cloud storage system architecture includes a master control server and several storage servers, as shown in figure 1.At its most basic level, a cloud storage system needs just one data server connected to the internet. A client sends copies of files over internet to the data server, which then records the information.

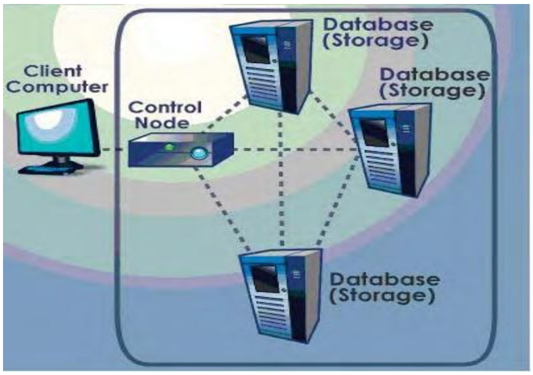

Figure 1 Typical cloud storage system architecture

When client wishes to retrieve the information, he or she accesses the data server through a web based interface. The server then either sends the files back to the client or allows the client to access and manipulate the files on the server itself.

Priliminaries

In1985, Neal Koblitz and Victor Miller independently suggested the use of elliptic curves in public key cryptography [1,4]. Supporters of elliptic curve cryptography (ECC) claim that ECC requires much smaller keys than those used inconventional public key cryptosystems, while maintaining an equal level of security. The use of elliptic curves therefore allows faster encryption and decryption. We now describe the elliptic curve cryptography Diffie-Hellman Algorithm [1,2]. For Alice and Bob to communicate securely over an insecure network they can exchange a private key over this network in the following way:

- A particular rational base point P is published in a public domain for use with a particular elliptic curve E (Fq) also published in a public domain.
- Alice and Bob choose random integers k_A and k_B respectively, which they use as private keys.

- Alice computes k_A *P, Bob computes k_B *P and they exchange these values over an insecure network.
- Using the information they received from each other and their private keys, both Alice and Bob compute $(k_A * k_B)*P = k_A *(k_B *P)=k_B*(k_A*P)$.This value is then the shared secret that only Alice and Bob possess. Note that the difficulty of the ECDLP ensures that the private keys k_A and k_B and the shared secret $(k_A * k_B)*P$ are difficult to compute given k_A *P and k_B *P. Thus, Alice and Bob do not compromise their private keys or their shared secret in the exchange.

Now that Alice and Bob share this secret that is almost impossible for a third party to discover, they can use this shared secret in a classical crypto systems to communicate securely over the network.

ECC Encryption / Decryption

Several approaches to encryption/ decryption using elliptic curves have been analyzed. This paper describes one of them. The first task in this system is to encode the plain text message to be sent as an x-y point Pm. It is the point Pm that will be encrypted as a cipher text and subsequently decrypted. Note that we cannot simply encode the message as theory coordinate of a point, because not all such coordinates are in Ep (a,b). There are approaches to encoding. We developed a scheme that will be reported elsewhere. As with the key exchange system, an encryption/decryption system requires a point G and an elliptic group Ep (a, b) as parameters. Each user A selects a private key n_A and generates a public key

$$P_A= n_A \text{ x } G. \qquad (1)$$

To encrypt and send a message Pm to B, A chooses a random positive integer x and produces the cipher text Cm consisting to the pair of points [2].

$$Cm= \{xG, Pm+xP_B\} \qquad (2)$$

Note that A has used B’s public key P_B. To decrypt the cipher text, B multiplies the first point in the pair by B’s secret key and subtracts the result from the second point:

$$P_m+xP_B– nB(xG)=P_m+x(nBG)– nB(xG)=P_m \qquad (3)$$

A has masked the message Pm by adding x P_B to it. Nobody but A knows the value of x, so even though PB is a public key, nobody can remove them ask x P_B. However, A also includes a “clue,” which is enough to remove the mask if one knows the private key n_B. For an attacker to recover the message, the attacker would have to compute x given G and xG, which is hard.

Proposed Method

In order to achieve secure, storage and access on outsource data in the cloud we exploit the technique of elliptic curve cryptography encryption to protect data files and proposed model has two part in the cloud storage server, Private data section and Shared data section. These two part of the cloud storage server makes the sharing of data easy and secure. User use the private data section to store his private data that is accessible to particular user only, whereas shared data section is used to store the data that needs to be shared among trusted users. This section is accessible to the particular user and his trusted users only.

Data stored over cloud and flow through network in plaintext format is a security threat. So, in our proposed model all the data stored in both section (Private data section, Shared data section) will been crypted by using the elliptic curve cryptography approach. As this method is based on secret key cryptography, the data stored on the private data section is encrypted by ECC private key and the data stored on the shared data section is encrypted by ECC public key.

The goal to use elliptic curve cryptography (ECC) is that it fits well for an efficient and secure encryption scheme. It is more efficient than the ubiquitous RSA based schemes because ECC utilizes smaller key sizes for equivalent security.

Authentication

User must be authenticated to access the service from cloud. The commonly used security mechanism for data access is user name and password pair. User provides the user name and password pair to cloud service provider and then cloud service provider checks the authenticity of the user. If user is authorized, cloud service provider will load cryptographic model (E-Module) to the client end that is responsible for cryptographic operation.

Operation

Cryptographic module asks for pin number to generate the secret key.

Encryption

The data that has to stored in a cloud cannot be stored in plain text format due to security reason so it must be transformed into an encrypted format. Cryptographic modules use the secret key to encrypt the user’s data that needs to store on cloud.

Decryption

This method deals with the decrypting the data after downloading from cloud. On user requests to download data stored on cloud, server will send the data in encrypted format. After arrival of data at client end Cryptographic module will decrypt it and original file is available to client.

Private Data Section

This section is only to store the user’s private data and ensures the security and privacy of private data section only. It uses all the above four operation to store and access the data from cloud storage. The architecture model of this section is shown in Figure-2, letter shown in arrow of the model is the above operation number. When user want to store private data it should be stored in the private section of the respective user that is accessible to particular user only. All the data stored in the private data section will be encrypted by secret key that is generated by E-module using ECC private key.

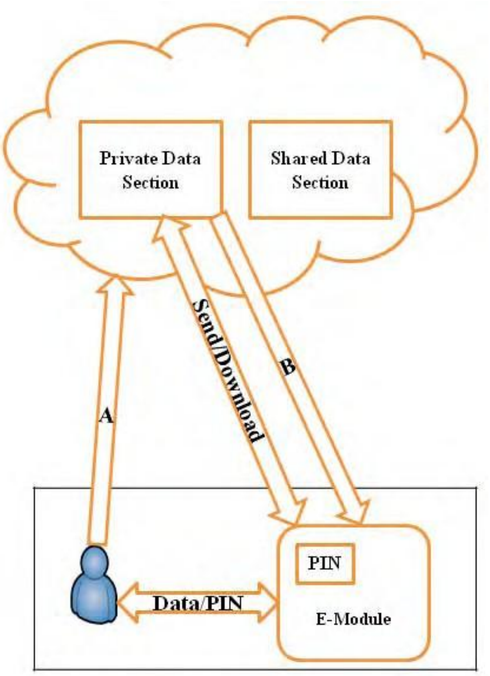

Figure 2 E-module for private data section

Shared Data Section

This section store the data that needs to share among trusted users, it can be implemented as shown in the figure 3, and letter shown in arrow of the model is the above operation number. This model also uses all the four operations discussed above to store and access the data from cloud storage. When user wants to store data that he wants to make it publically available or share among trusted users then he will store data in shared data section. Data stored in the shared data section will be encrypted by secret key that is generated by E-module using ECC public key.

To make accessible data in shared data section among trusted users, user can create the group and data stored in group section can be accessible to all members of the group. To access the shared data group users A and B have to exchange the pin number which will be helpful for cryptographic operations. Elliptic Curve Diffie-Hellman key exchange algorithm is used to exchange the pin number. After exchanging the pin number users, A and B can use that to store and access data on the shared data section.

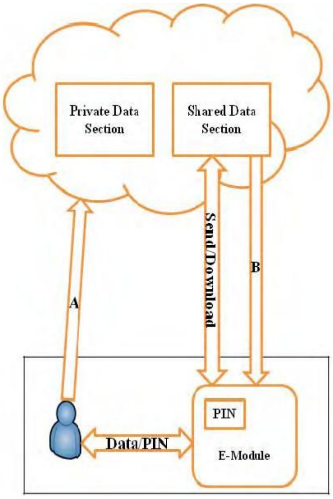

Figure 3 E-module for shared data section

All the encryption and decryption is performed at client side only by making use of secret key that is generated by E-module using ECC private key. Cloud server does not have any idea of secret key and the pin number used for encryption. So, even the data stored in the encrypted format and the algorithm used to encrypt is available to cloud, it is very difficult to decrypt the data.

Conclusion

The main goal is to securely store and access data in cloud that is not controlled by the owner of the data. We exploit the technique of elliptic curve cryptography encryption to protect data files in the cloud. Two part of the cloud server improved the performance during storage and accessing of data. The ECC Encryption algorithm used for encryption is another advantage to improve the performance during encryption and decryption process. We assume that this way of storing and accessing data is much secure and have high performance. Our efforts are going on to solve the problem of group sharing of data in the shared data section as in this scheme only member of group can access the data shared data section. One to many, many to one, many to many communication is not possible

References

1. V. Miller. “Uses of Elliptic Curves in cryptography”. CRYPT’85, LNCS218, pp 417-426, 1986.
2. W. Stallings. Cryptography and Network Security: Principles and Practice. (3rded.). Prentice Hall, Upper Saddle River, New Jersey, 2003
3. Wassim Itani Ayman Kayssi Ali Chehab ,“Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures”, Eighth IEEE International Conference on Dependable, 2009
4. N. Koblitz, “Elliptic Curve Cryptosystems ”, Mathematics of Computation, vol. 48, pp.203 -209, January1987.