INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND APPLICATIONS
VOLUME XII, ISSUE VIII, AUGUST 2018, WWW.IJCEA.COM, ISSN 2321-3469

A SEGMENT BASED SCHEME FOR SECURE DATA SHARINGIN CLOUD

Abu Salim and Rajesh Kumar Tiwari

Department of Computer Science and Engineering, Glocal School of Technology and Computer Science. Glocal University, Saharanpur, U.P.

ABSTRACT:

Cloud computing makes it possible to share data, which brings a plethora of advantages to the consumers of the platform. These advantages include extensive access to networks, resource polling, rapid elasticity, and measurable services. The security risk is increased when the data are relocated to an outside place on a CSP (cloud service provider) server. The key security risks associated can be classified in terms of confidentiality, integrity, and availability. Depends on the type of consumers that make use of cloud storage, data is divided into the various groups. In our plan, we separated the data into three categories: the first kind, in which the data is used by only one person, which is the owner; the second type, in which the data is accessed by a small number of consumers; and the third type, in which the data is utilized by a significant number of users. In order to accommodate these three categories of data, the storage capacity available in the cloud will be divided into three groups: S1, S2, and S3. S1 will be used only by the owner, whereas S2 and S3 will be used by a restricted and a big number of users respectively. The usage of a symmetric and asymmetric cryptographic technique in conjunction with proxy re-encryption has been implemented in order to provide secure access and protection for these three categories of data.

Keywords: Segmentation, cloud storage, symmetric key cryptography, asymmetric key cryptography, and proxy re-encryption**.**

[1] INTRODUCTION

As part of cloud-based data sharing, user data is transferred from personal storage to distant storage that is kept up by a third party known as the cloud service provider. In a multitenant setting, CSP offers users scalable, on-demand services that are paid based on their usage. By

eliminating the need for users to operate their own data centers, the cloud reduces the expense of hardware software installation and management.
The three parties which participate in the cloud computing are.

- Data owner: The individual who hired a third party to store his data in the cloud.
- Users: The individuals to whom Permission is granted by the data owner to obtain the data in accordance with the access control policy.
- A cloud service provider (CSP) is a business that provides users with hardware and software services. The cloud provider provides, Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Physical and logical security of data must be ensured when it migrates to the cloud. Physical security refers to restricting unauthorized entry to the location and whatever inside it. Logical security relates to access controls within the operating system or access rule at network layer like firewall, router, and switches. Both of these threats are protected by the CSP.
The following privacy and security standards must be met in order to share data in the cloud.

[1] Data Confidentiality: No one, not even the cloud service provider, should be able to access the data without authorization. Data security can be abused both in transit and at rest. Therefore, it is important to protect data during transmission and storage.

[2] User Revocation: When a user's access privileges have been suspended, they should no longer allow them to access any data. However, this should not affect any other individuals.

[3] Scalable and Efficient: Cloud storage needs to be extensible and effective, allowing for the easy addition of new users and the removal of existing users' access privileges.
[4] Entity collusion: Even when specific users collaborate, they shouldn't have access to shared data without the consent of the data owner.

Researchers have devised a variety of schemes [1-6] to address the issues described above, but to the best of our knowledge, none of these schemes fully addresses all of the issues raised. According to the variety of users, our system splits the data into three categories and secures each of these groups. Data and the calculated Message Authentication Code (MAC) will be protected with a symmetric key cryptography technique before storage. We want to employ the Advanced Encryption Standard (AES)[7] as it provides higher security on smaller key size[8]. The data will be kept in the proper portion of the cloud storage, and CSP keeps an authentication register on the cloud storage which contains a list of authorized consumers, a re-encryption key (for S3), and a tag Values (TV). The Segment a user is permitted access to is identified by the tag

values (TV). Data requests for Segments 2 and 3 will be authenticated against the register for each request.

Segment S2 is protected using asymmetric key encryption and S3 with Proxy Re-Encryption. symmetric key will be distributed securely to the authorized users.

[2] RELATED WORKS

Researchers have conducted various studies aimed at improving the security of shared data in cloud environments. In order to safeguard data stored in the cloud, a cryptographic system may be used. In the following part, we have examined some strategies proposed by researchers to safeguard data.

Data breaches represent a significant security concern that needs attention within the realm of cloud infrastructure. The vulnerability of the whole cloud environment to a high-value assault arises due to the storage of substantial quantities of data from diverse users inside the cloud, which may be accessed by a hostile user [9].

In [10] author propose a cloud security system that utilizes the AB-HKU and AB-SIGN schemes to protect data stored in the cloud. This protocol employs the modes of read, write, delegation, and revocation to provide the user with the permissions of reading, writing, delegating, and revoking access. In the realm of data management, it is possible to access and modify data in both read and write modes. On the other hand, the processes of delegation and revocation are used to grant and withdraw access permissions, respectively.

In [11] authors proposed a technique that offers both integrity and privacy for cloud data. The use of AES and RSA-based partial homomorphic encryption (PHE) by the author serves the purpose of ensuring both integrity and privacy for cloud data.

In [12] The authors proposed a technique that offers security for both data and computation. The data is partitioned into m distinct segments and then authenticated by a trustworthy third party. The encrypted data and signature, which have been encrypted using a session key, are sent to a cloud storage system. Upon receipt, the cloud server proceeds to decode the data. If the validation process is successful, the decrypted data is then saved on the cloud storage system.

In their work [13], authors. introduced a cloud storage system known as Depot. This system offers both security and liveliness for stored data, eliminating the need for users to place faith in the accuracy of the depot server.

In [14] the authors have put up a proposal that leverages the usage of Key-Policy Attribute-Based Encryption (KP-ABE), proxy re-encryption, and lazy encryption techniques. In this proposed framework, the majority of computational tasks are offloaded to the cloud server while ensuring the non-disclosure of any sensitive data. However, it is important to note that in this scheme, there exists a possibility for the cloud server to get knowledge of user attributes and a portion of the secret key.

[3] PURPOSE WORK

In our plan, we intended to divide the space available for cloud storage into three sections labelled S1, S2, and S3, respectively. The data that are used by the owner are stored in Segment S1, while the data that will be used by a limited number of users will be stored in Segment S2, and the data that are heavily used by a large group of users will be stored in Segment S3. We make use of a tag known as the Tag Value (TV), that will determine the Segment in which the data will be saved. Tv will be assigned by the actual owner of the data.

A TV value of 1 indicates that the data will be kept in the Segment S1 and that the data owner will be the only one to utilize it. The TV value 2 indicates that the data will be kept in Segment S2 and that only a restricted number of users will be able to access it. The information that the TV value 3 denotes that it will be saved in Segment S3, where it will be accessed by a many users.

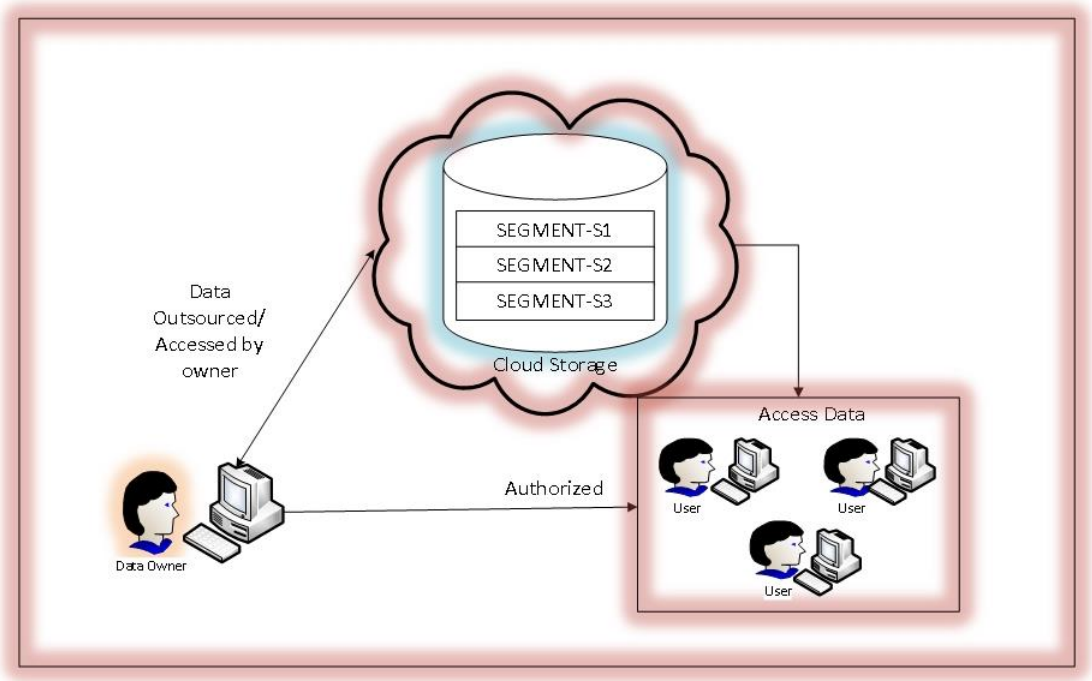

Figure: 1. System Diagram

Our scheme work in two phases, the first phase deals with the processing and storage of the data, while the second phase is concerned with providing access to the stored data. During the phase of processing files, the message authentication code (MAC) will be computed on the data and then encrypted along with the data. The MAC value, data and the TV value will be kept at cloud storage. TV value is used to indicate the Segment in which the data will be saved,

We encrypt data in segment S1 using symmetric key cryptography like AES since the Segment S1 will only be accessed by its owner. This kind of cryptography requires less computing overhead as opposed to public key cryptography. There is no requirement for exchanging the key since the data will only be utilized by the owner itself. Additionally, the accuracy of the saved data may be checked by the owner of the data by making use of the MAC value.

The data in Segment S2 have a restricted number of users, and has the data encrypted using symmetric key and can only be viewed by a select group of users. The symmetric key will be sent to the authorized users utilizing public key cryptography methods such as RSA. The user first asks for data from CSP, who then checks the authorization list and the segment that is assigned to him. In the scenario of Segment S2, if the authorization is valid, CSP will send the user's requested data. Next, the user demands a symmetric key from the data owner, who then encrypts the key using his public key and sends it to him. The user then decrypts the key with his private key and obtains the session key.

for the Segment S3, Proxy-Encryption and the CP-ABE scheme will be used. The data before storage are encrypted with a symmetric key called k, and then the owner chooses second random number called k1, and encrypt with access policy that is associated with the user. on the receiving data access request from the user, Data owner will compute $k_2 = k \oplus k_1$. CSP uses authorization list to verify validity of request. if valid CSP will re-encrypt k2 with the use of a re-encryption key, this may be decoded with the use of his private key in order to get k2. By using his ABE key, he is able to get k1, which can then be used to compute $k = k_1 \oplus k_2$ in order to acquire k, which is the symmetric key and allows data to be decrypted.

Processing by the data owner

1. The data owner encrypts the data using symmetric key, which is k.
   $C_a = E_k(d)$

2. The access policy that is connected with the user is used to encrypt integer called k1.
   $C_b = A.enc_{PK}(A_{pol}, K_1)$

3. Perform the computations $k_2 = k \oplus k_1$ for k2 and save to the storage.
   $k_2 = k \oplus k_1$

Authorization of users by the data owner

1. CSP calculate $A.sk_b = A.keygen(SK_m, I)$ and deliver in a secure manner to the user, where I refer to the collection of attributes, secure key of the user is $A.sk_b$, and the master key is SK_m.

2.The data owner's private key $sk_a = a$ and the user's public key $pk_b = g^b$ are both used in the generation of the re-encryption key$rk_{a\to b} = g^{b/a}$. Each user will have their own unique user ID and re-encryption key $(pk_B, g^{b/a})$, both of which will be saved on the cloud storage system.

Data Access by user from Segment S3

1. The user sends the message to the CSP; the CSP checks the authorized list, if the message is legitimate, re-encryption key and k2 will be retrieved and re-encrypted k2 using the re-encryption key in the following manner:

$$C_c = (Z^r.k_2, g^{ra})$$

$$C_c = (Z^r.k_2, e(g^{ra}, rk_{A\longrightarrow B}))$$

$$C_c = (Z^r.k_2, e(g^{ra}, g^{b/a}))$$

$$C_c = (Z^r.k_2, Z^{rb})$$

Now CSP send $\{C_a, C_{b,} C_c\}$ to the user.

2. The user obtains k1 by using his key $A.sk_b$, the user is able to recover k2 using his key sk_b .User calculates $k = k_1 \oplus k_2$ and decrypt the C_a to retrieve the data

User Account Termination

In the event of data kept in segment S1, where the only data owner is the user, user cancellation is not required. However, in the case of data stored in segments S2 and S3, records associated to the user will be deleted from the authorization list. Afterwards, any request from the user for data access from the section S2 and S3 will not be fulfilled by the CSP.

Removal of Data

In each of these scenarios, the Cloud Storage Provider (CSP) will remove the related file from the cloud storage upon receiving a request to do so from the data owner.

[6] SECURITY ANALYSIS AND DISCUSSION

The data owner is going to keep data in the segment S1 that is used exclusively by him. as the data owner moves his personal data to cloud storage, the owner is relieved of the responsibility of maintaining expensive hardware and software resources. In addition, the data storage space can be modified according to the user's needs, and the data owner will only be charged for the amount of space that the user actually occupies.

In the instance of segment S2, which only allows a limited number of users, both the data owner and the user needed just two data encryption and decryption processes. This is because the data is encrypted using a symmetric key, and the symmetric key is passed to the user using public key cryptography such as RSA. The data owner is obligated to encrypt the data using a symmetric key, and since this symmetric key must also be encrypted using the users' public key, there must be two separate processes for encrypting and decrypting the data.

In the scenario of segment S3, which is accessible by a high number of users, exchanging symmetric keys with each individual user would be challenging. In our plan, to alleviate the pressure on the data owner to distribute keys to each individual user, we made use of proxy encryption, in which the data owner is not participating in the data access process. However, in this scenario, the user is needed to produce a re-encryption key for each authorized user, the CSP is required to re-encrypt K2 with the re-encryption key, and the user is required to execute three decryption processes, two in order to get the symmetric key, and one in order to obtain the data.

Because the data stay encrypted during the whole of the sharing process, the confidentiality, privacy, and integrity of the data are maintained throughout all three segments. Neither the CSP nor any other user who is not authorized to view the data is able to do so. To validate data message authentication code (MAC) value is used.

In any of the three scenarios, it is not necessary to provide the secret key in advance. Because the data is exclusively utilized by the data owner, there is no need to swap keys in the case of S1. In the case of S2, symmetric keys are traded using the public keys of the respective users. In the case of S3, the re-encryption key $(g^b)^{1/a}$ is kept on the CSP. This key is generated by the owner of the data, and all that is needed from the user is their public key. Under the assumption of the inverse exponent, it is unidirectional since the proxy cannot calculate $g^{a/b}$ from $g^{b/a}$, and the CSP cannot collude with the data owner to extract users' private keys because the private key of user b cannot be constructed from. $g^{b/a}$.

[6] CONCLUSION

In our method of data sharing, the number of users who are sharing the data determines the Segment, in our scheme cloud storage space id to be divided into three separate segments. Since the number of users who are sharing the data determines the Segment, the process of sharing data inside each segment needed a different number of encryption and decryption steps. In the first scenario, only one encryption and decryption process are required, and the data is encrypted with a symmetric key. In the second scenario, however, only two encryption and decryption processes are required. Because the number of users in this scenario is limited, encrypting symmetric key with user public key will not be a problem for the data owner. In this scenario, the data owner must be involved in key distribution. In contrast, the data owner of Segment 3, which is accessible by a significant number of users, must produce a re-encryption key that will be saved on the server in the authentication list of users. In this scenario, the data owner does not need to be online to distribute the key, but there are several steps involved in encrypting and decrypting the data before it can be shared.

REFERENCES

[1] Khan, M. A. (2016). A survey of security issues for cloud computing. Journal of network and computer applications, 71, 11-29.

[2] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. International Journal of Engineering Research and Applications, 7(6), 31-38.

[3] An, Y. Z., Zaaba, Z. F., & Samsudin, N. F. (2016, November). Reviews on security issues and challenges in cloud computing. In IOP Conference Series: Materials Science and Engineering (Vol. 160, No. 1, p. 012106). IOP Publishing.

[4] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. International Journal of Engineering Research and Applications, 7(6), 31-38.

[5] D. Xin, Y. Jiadi, L. Yuan et al. "Achieving an effective, scalable and privacy preserving datasharing service in cloud computing". Computers and Security 42, 151–164, 2014.

[6] KS Bharath, E. Yousef, H. Gerry, KM Sanjay. "A secure data sharing and query processing framework via federation of cloud computing". Inf. Syst. J. 48,196–212, 2015

[7] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Accessed on 15.08.2017

[8] https://www.certicom.com/index.php/the-next-generation-of-cryptography, Accessed on 19.08.17

[9] Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128-135.

[10] Zarandioon S, Yao D, Ganaphthy V, "K2C: cryptography cloud storage with lazy revocationand anonymous access", Securecomm, 2011.

[11] Mohammed Faez Al-Jaberi, Anazida Zainal, "Data Integrity and Privacy Model in Cloud Computing", International Symposium on Biometrics and Security Technologies (ISBAST), IEEE. 2014

[12] Lifei Weia, Haojin Zhua, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, Athanasios V. Vasilakos, "Security and privacy for storage and computation in cloud computing",Information Sciences, 2014, Volume 258, 371-386.

[13] P. Mahajan, S. Setty, S. Lee et al., "Depot: cloud storage with minimaltrust,"ACMTransactions on Computer Systems, vol. 29, no. 4, article 12, 2011.

[14] S. Yu, C. Wang, K. Ren, W. Lou, "Achieving secure, scalable, and fine-grained data accesscontrol in cloud computing", in: Proc. of IEEE INFOCOM, San Diego, CA, March 2010.