ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 6, pp. 17321-17324, June, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

SECURE FILE TRANSMISSION USING KEY ENCRYPTION

Satish Kumar T*., Ravi Shekhar., Sagar Kar Choudhury., Rosh Kumar and Rishabh K

Department of Computer Science Engineering, Global Academy of Technology, Bengaluru, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0806.0330

ARTICLE INFO

Article History:

Received 16th March, 2017
Received in revised form 25th April, 2017
Accepted 23rd May, 2017
Published online 28th June, 2017

Key Words:

Cloud Computing, Cloud Security, IT, Encryption

ABSTRACT

To get reliable, customized and quality of service guarantee, a computing paradigm like cloud computing should be used in Computation environments. It not only provide over whelming storage capacity for data but also faster computing to business customers over the internet. As a result of virtualization, global duplication and migration, the lack of data in the cloud, the stored data in the cloud and the computed results may not be properly managed and completely trusted by the cloud tenants. A lot of preceding work on the cloud security focuses on computation security rather than taking the security with respect to storage into consideration. In this paper, a proposal is made to secure file uploaded by individual. The detailed analysis of the method through the algorithm is discussed in the paper. Additional experiments demonstrate the effectiveness and performance of the used 128-bit encryption algorithm.

INTRODUCTION

Cloud services play a vital role in storage of data in the current times. Cloud storage services provide users and enterprises with various options to store and process their data in third-party data centers. Cloud computing also focuses on maximizing the effectiveness of shared resources.

The cloud providers provide service as Platform as a service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) [1]. There are four models which are deployed in the cloud which are, private cloud, public cloud, hybrid cloud and community cloud [2].

As cloud computing is becoming popular more information such as emails, health records and governments related documents are uploaded into cloud [3]. Majority of the companies prefer to store their data into cloud so that they can reduce storage and management costs [4]. Owing to the cloud's nature as a shared resource, access control and privacy are of concern. One of the main concern with respect to cloud is that all the heterogeneous data has to be stored in the file, while ensuring that the data of all the clients is secure [5].

Some major threats with respect to SaaS are application security, multi-tenancy, data security and accessibility [6]. Some of the key challenges in PaaS are hidden complexity of the platform, multi-tenant environment and updates of the environment [7].

The sharing of components of the cloud to reduce the cost of the tenant is called as multi-tenancy [8]. The main challenge with respect to data security is privacy, the user who uploads data to the cloud has no knowledge of the cloud infrastructure [9].

With many corporations using cloud storage, it is important for the cloud service provider to ensure that the data stored in their cloud is private. The data in the cloud may be critical and hence, it is essential for the clients to be confident that their data in the cloud is secure from other users as well as from the cloud service provider.

The cloud computing model has three components which are cloud service provider, client (owner) or user [10]. The cloud service provider provides the space for storage of client's data. The client (individual or organization) can upload the data into a cloud. The user can view the data stored in the cloud.

A major security challenge in cloud computing is that the owner may not be able to control the flow of data [11]. To preserve the security of data, encryption of data must be done [11]. Some of the attacks that could be done on the cloud are divide and conquer attack and poison attack [12] or denial of service attack [9].

Corresponding author:* **Satish Kumar T
Department of Computer Science Engineering, Global Academy of Technology, Bengaluru, India

Related Works

Some of the traditional security models include Chinese wall, homomorphic encryption, and etc. The Chinese wall is a traditional security model which has data in hierarchy where first level has individual items called objects, the second level has group of objects called as dataset and third level has groups of companies [13]. The homomorphic encryption is done when we do some computations on encrypted data to get encrypted result. The decrypted result will have the same encryption computations done on the raw data [4].

One main service provided by the cloud is storage (Simple Storage Services-Amazon S3) [14]. Since data stored in the cloud can be critical it must be encrypted so that it is not accessible by other users (without privilege).

Encryption is a common practice to ensure the privacy of data. There are basically 3 types of encryption algorithms which are asymmetric key algorithms in which the private key will be hidden from the other users, symmetric key algorithms in which the same key is used in encryption as well as decryption and hashing [15]. Another cryptographic technique is the hash function which converts the plain text into some random characters equivalent to the number of characters of the original text [16].

In Broadcast encryption (BE) method, the user sends the message in encrypted format and the intended users with be able to decrypt the message [17]. In [18], the project incorporates Attribute Based Encryption (ABE) which is another model for encryption. Another model called proxy re encryption (PRE) is also used for the securing of data [19]. Another model used, stores the data as images rather than raw data as an encryption [20].

System Design

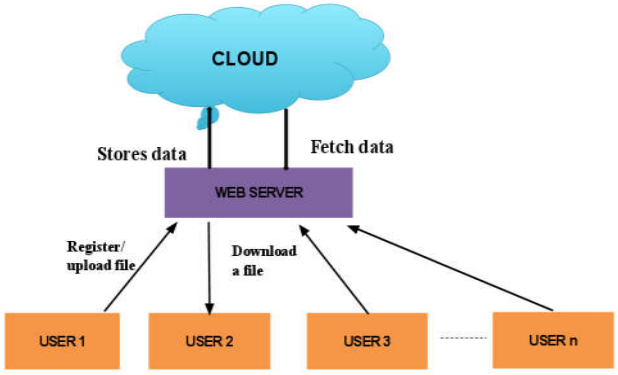

Figure 1 Proposed model for secure file transmission

The model aims to encrypt the data stored in the cloud so that the cloud service provider or any user other than the file owner cannot see the data. The proposed model is shown in the Figure 1. The Figure 1 shows how the transmission of data is secure. This model uses a 128 bit key encryption method so that the data is private. In this model, the client who creates the file is known as file owner. The file owner can delete his/her own file or modify the data in the file. If client other than the file owner wants to access the file, he will have to request for key from the file owner. The file owner may choose to share the key or not based on his choice. The file owner can do any modification on his file. If another client does any modification to the file, it will be informed to the file owner. Only if the modification is allowed by the file owner, it will hold valid, otherwise, it will be nullified. The file owner can delete his own file. No other user can delete the file of any other user.

Algorithm

1. Start
2. If client(!REG)
3. Register
4. Else
5. Client(LOGIN)
6. If login(SUCCESS)
7. If file(UPLOAD)
8. Upload
9. Else if file(VIEW)
10. If Client(FILE OWNER)
11. View
12. Else
13. Ask for key from owner
14. Else if file(MODIFY)
15. If Client(FILE OWNER)
16. Modify
17. Else
18. Modify the file and ask for confirmation
19. Else if(DELETE)
20. If Client(FILE OWNER)
21. Delete
22. Else
23. Return to home page
24. Stop

The algorithm aforementioned implements the following actions. The client has to register to do any operation with the file. The registered client can upload his own file into the cloud. The file owner has the privilege to view, modify or delete his own file. Any registered client other than the file owner has to submit the key in order to view the file uploaded. The registered client can do modifications on the file, but only if the owner acknowledges it, then the modification will be reflected. The registered client cannot delete the file which has not been uploaded by him.

Sequence Diagram

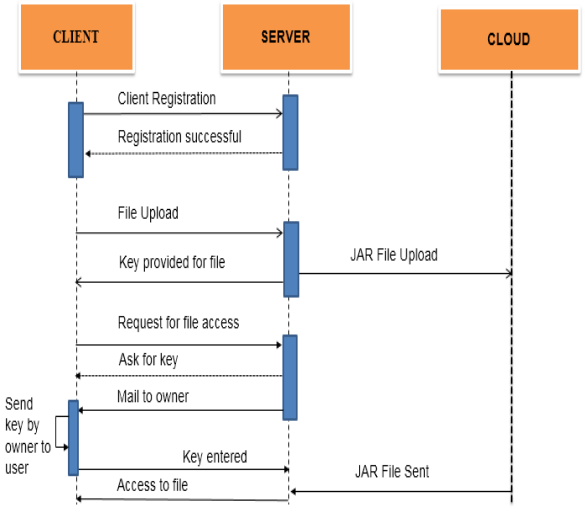

Figure 2 Sequence diagram of the working of model

The Figure 2 shows the sequence of actions that happen in the suggested model. The client has to register in order to perform any operation in the cloud. The client can upload the file, if uploaded successfully, he/she will get a key for the file and the file will be saved as a jar file into the cloud. If any other client wants to use the file, he will have to request the owner for the key. If done so, a mail will be sent to the file owner saying that a user wants to access his/her file. If the owner shares the key with the client, the client enters the key, the JAR file is decrypted to its original equivalent and then sent to the client.

CONCLUSION AND FUTURE WORK

The data that is uploaded into the cloud is now secure since it is protected with a 6 digit security code. The file when stored into the cloud is converted into a jar file, so even if the owner downloads it and breaks it, he/she will get a machine language code which is not readable. Hence, it can be said that the data fed into the cloud is now secure.

Rather than using the 128 bit data encryption algorithm as in this model, an even more sophisticated 256 bit data encryption algorithm can be used so that the data is more secure.

And a new key can be generated each time the file is opened to confirm safety and stop data propagation. This ensures that the file cannot be opened by different users even though the user shares the key with another user.

References

1. Bacon, Jean, David Eyers, Thomas FJ-M. Pasquier, Jatinder Singh, Ioannis Papagiannis, and Peter Pietzuch. "Information flow control for secure cloud computing." IEEE Transactions on Network and Service Management 11, no. 1 (2014): 76-89.
2. Park, Jun-Hak, Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, Chul-Woo Lee, and Hyoung-Chun Kim. "A Study on Cloud Forensics and Challenges in SaaS Application Environment." In High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on, pp. 734-740. IEEE, 2016.
3. Rudy and C. Cassandra, "Study of Cloud Computing intention of use for learning improvement in Higher Education (case study: Private higher education institution in Jakarta)," 2016 International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 2016, pp. 84-88.
4. El Makkaoui, Khalid, Abderrahim Beni-Hssane, and Abdellah Ezzati. "Can hybrid Homomorphic Encryption schemes be practical?." In Multimedia Computing and Systems (ICMCS), 2016 5th International Conference on, pp. 294-298. IEEE, 2016.
5. Wang, Cong, Ning Cao, Kui Ren, and Wenjing Lou. "Enabling secure and efficient ranked keyword search over outsourced cloud data." IEEE Transactions on parallel and distributed systems 23, no. 8 (2012): 1467-1479.
6. Basu, Srijita, Anirban Sengupta, and Chandan Mazumdar. "Implementing Chinese Wall security model for cloud-based services." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1083-1089. IEEE, 2015.
7. Gesvindr, David, Barbora Buhnova, and Ondrej Gasior. "Quality Evaluation of PaaS Cloud Application Design Using Generated Prototypes." In Software Architecture (ICSA), 2017 IEEE International Conference on, pp. 31-40. IEEE, 2017.
8. Ochei, Laud Charles, Andrei Petrovski, and Julian M. Bass. "Optimizing the deployment of cloud-hosted application components for guaranteeing multitenancy isolation." In Information Society (i-Society), 2016 International Conference on, pp. 77-83. IEEE, 2016.
9. Hitaswi, N., and K. Chandrasekaran. "A bio-inspired model to provide data security in cloud storage." In Information Technology (InCITe)-The Next Generation IT Summit on the Theme-Internet of Things: Connect your Worlds, International Conference on, pp. 203-208. IEEE, 2016.
10. Sood, Sandeep K. "A combined approach to ensure data security in cloud computing." Journal of Network and Computer Applications 35, no. 6 (2012): 1831-1838.
11. Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).
12. Xu, Jia, Ee-Chien Chang, and Jianying Zhou. "Weak leakage-resilient client-side deduplication of encrypted data in cloud storage." In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, pp. 195-206. ACM, 2013.
13. Brewer, David FC, and Michael J. Nash. "The chinese wall security policy." In Security and Privacy, 1989. Proceedings., 1989 IEEE Symposium on, pp. 206-214. IEEE, 1989. aws.amazon.com/s3
14. Choudhury, Tanupriya, and Praveen Kumar. "Proposal and implementation of cloud security algorithm to enhance the security of the layers." In System Modeling & Advancement in Research Trends (SMART), International Conference, pp. 316-321. IEEE, 2016.
15. Arfan, M. "Mobile cloud computing security using cryptographic hash function algorithm." In Information Technology, Computer, and Electrical Engineering (ICITACEE), 2016 3rd International Conference on, pp. 1-5. IEEE, 2016.
16. Rabaninejad, Reyhaneh, Mohammad Hassan Ameri, Mahshid Delavar, and Javad Mohajeri. "On the security of yrl, an anonymous broadcast encryption scheme." In Telecommunications (IST), 2016 8th International Symposium on, pp. 752-755. IEEE, 2016.
17. Wang, Dan, Zhenfu Cao, and Xiaolei Dong. "Outsourcing attribute-based encryption with multi-keywords and similarity ranking search." In Computer and Communications (ICCC), 2016 2nd IEEE International Conference on, pp. 28-32. IEEE, 2016.

18. Hu, Xing, Chunming Tang, and Duncan S. Wong. "Highly Efficient Proxy Re-encryption Schemes for User-End Encrypted Cloud Data Sharing." In Parallel and Distributed Computing (ISPDC), 2016 15th International Symposium on, pp. 261-268. IEEE, 2016.
19. Sarkar, Mrinal Kanti, and Sanjay Kumar. "Ensuring data storage security in cloud computing based on hybrid encryption schemes." In Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on, pp. 320-325. IEEE, 2016.

How to cite this article:

Satish Kumar T *et al*.2017, Secure File Transmission Using Key Encryption. *Int J Recent Sci Res.* 8(6), pp. 17321-17324. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0806.0330

****