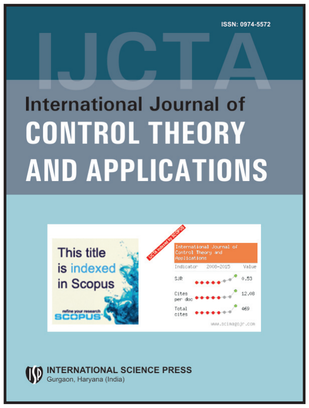

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 9 • Number 43 • 2016

Securing Cloud Data by Generating Hash Code Based Secret Key

Neethu K.P.[a], **Eldo P Elias**[b] **and Leya Elizabeth Sunny**[c]

[a]Department of Computer Science and Engineering, M.A College of Engineering, Kothamangalam, Kerala, India. Email: neethukannan911@gmail.com
[b-c]Prof. Department of Computer Science and Engineering, M.A College of Engineering, Kothamangalam, Kerala, India. Email: [b]eldope@gmail.com; [c]leyabejoy81@gmail.com

Abstract: There are various security issues that may be present in the cloud. To overcome the security issues present in the single cloud, multi-cloud concept can be used. In multi-cloud, a file uploaded by a user is divided into multiple chunks and each chunk is stored in different servers. Security can be achieved by using AES encryption algorithm. First file split is encrypted using the key provided by the user during file uploading. From second split onwards each file split is encrypted using the key which is determined from the hash code of the previous split. Thus the security can be enhanced by the dependency between each file split. Each encrypted file will be stored on different servers.

Keyword: Multi-cloud; secure hash algorithm; encryption; file splitting; load balancing.

1. INTRODUCTION

Cloud computing is a type of Internet based computing that provides shared computer processing resources and data to computers and other devices on demand [1]. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store their data. Cloud computing provides many benefits in terms of low cost and accessibility of data. The recent increase in cloud computing arises from its ability to provide software, infrastructure, platform services without requiring large investments to manage and operate them. Clouds typically involve service providers, infrastructure/resource providers and service users (or clients). They include applications delivered as services, as well as the hardware and software systems providing these services.

Cloud service providers (CSPs) offer cloud platform for their customer's high speed broadband to access the internet. Cloud computing enables convenient, on demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications. Security within cloud computing is an especially worrisome issue because of the fact that the devices used to provide services do not belong to the users themselves. The users have no control of, nor any knowledge of what could happen to their data [1].

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment [2]. There are various security challenges present in the cloud such as data integrity, data intrusion, service availability etc [3]. Single cloud environment is affected with service unavailability, malicious system administrator and data integrity challenges which can be solved by the use of multiple clouds. The proposed system used the concept of multi-cloud in which file is splitted into multiple chunks and each chunk is stored in different servers. Security is provided using AES encryption algorithm. The key used for encryption is dependent on hash value of each file split. Hash value can be determined using Secure Hashing Algorithm (SHA). Thus security can be further increased by file dependency feature.

2. RELATED WORK

Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure. A cloud provider offers many services that can benefit its customers, such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities. Reliability and availability are other benefits of the public cloud, in addition to low cost. However, there are also concerning issues for public cloud computing, most notably, issues surrounding data integrity and data confidentiality. Any customer will be worried about the security of sensitive information such as medical records or financial information.

Mohammed A. Alzain et. al., in [4] described multi-cloud model as a combination of various cloud where user data will be distributed and executed in those clouds simultaneously. It is observed that multi–clouds improve performance provided by single cloud environment by dividing security, trust and reliability among different clouds. Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment. Users of online data sharing or network facilities are aware of the potential loss of privacy [1].

Moving databases to a large data centre involves many security challenges [5] such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Subashini and Kavitha [3] present some fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources. In different cloud service models, the security responsibility between users and providers is different. According to Amazon [6], their EC2 addresses security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data.

According to Tabaki et. al., [7], the way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data [7].

Jens-Matthias Bohli [8] et. al., proposed four types of architectural patterns for multi-cloud computing paradigm for improving security and privacy of user and provider. They are Replication of application, Partition of application System into tiers, Partition of application logic into fragments, and Partition of application data into fragments. First approach specifies replication of application which helps to verify integrity of data after execution in cloud is over. Second approach helps to protect data and logic by separating them. Third approach protects data and application confidentiality by breaking application logic in parts and executing it over multiple clouds. Similar approach is given in last architecture where data is broken into parts and executed over various clouds which helps to protect from malicious cloud service provider.

Load balancing is one of the main Challenges in cloud computing which is required to distribute the workload evenly across all the nodes. Load is a measure of the amount of work that a computation system performs which can be classified as CPU load, network load, memory capacity and storage capacity. It helps to achieve a high user satisfaction and resource utilization ratio by ensuring an efficient and fair allocation of every computing resource. Proper load balancing aids in implementing fail-over, enabling scalability, over-provisioning, minimizing resource consumption and avoiding bottlenecks etc [9].

3. PROPOSED WORK

The proposed system focuses on the concept of multiple cloud storage along with enhanced security using encryption techniques. Instead of storing complete file on single cloud system, the proposed system will split the file in different chunks then encrypt it and store on multi-cloud. Here every encrypted file split will be dependent on other, i.e., after file splitting is completed hash value or message digest of the each split is determined using Secure Hash Algorithm (SHA). A message digest is a code which is created algorithmically from a file and represents that file uniquely. If the file changes, then the message digest changes. This hash code can be used as the key for encrypting the file split. Suppose a file named X is splits into n chunks, say $x_1, x_2, x_3, \ldots, x_n$ and hash code corresponding to each split is $h_1, h_2, h_3, \ldots, h_n$ respectively. Then first split x_1 will be encrypted by using the key provided by the user U_k. The second split x_2 will be encrypted using hash code of the first file split h_1, third file split is encrypted using hash code of the second file split h_2 and so on.

Here every split is dependent on other splits. When the original file uploader wants to access the file, he has to input the same user key U_k which is given by him during the file uploading or encryption. The user key should be the same in order to decrypt the first file split x_1. After splitting the first chunk we need to determine the hash code of the first file split h_1 which can be calculated only after decrypting x_1. This means that, second file chunk can be decrypted only after decrypting first file split. Similarly third file split is decrypted only after decrypting second file and also after determining hash code it. Thus every file split is dependent on other. So for decrypting every file split (except first split), user key and location of the first split should be known.

In a cloud computing environment, nodes can be upgraded, deleted or added as well as files can also be created, deleted and appended. This leads to the problem of load imbalance in a distributed file system. Load balancing process distributes the workloads across multiple resources. It aims to minimize resource use, improve throughput and reduce response time.

Security can be further increased by file dependency feature. If the attacker gain access to any of the file split he may not able to read or decrypt the file, because every file split is dependent on another. So we can secure our sensitive information more efficiently. So even if the cloud is unreliable the data is secured by three ways.

(i) The data is split into multiple parts so it is not readable.

(ii) The data is encrypted using AES encryption algorithm so it will be very hard to decipher it without key.

(iii) Each file split is dependent on each other. So to decrypt one file, the key should be known which is determined only after decrypting other file split.

A. System Architecture

Figure shows system architecture of proposed scheme. The proposed scheme works in following way. When a user wants to upload a file into the cloud he should register in the website first. After registering he will be able to upload file in to the application. When uploading is completed, the system will split file in to three parts (number of splits can have any number according to the application design). Hash value of the each split is calculated using Secure Hashing Algorithm (SHA). 128 bit key value is selected from hash of the file which will be used as key for encryption. After getting the key, each file split is encrypted using Advanced Encryption Standard (AES) algorithm where encryption key will be the corresponding 128 bit key selected from hash code of the each split. This encrypted data will be stored in each server.

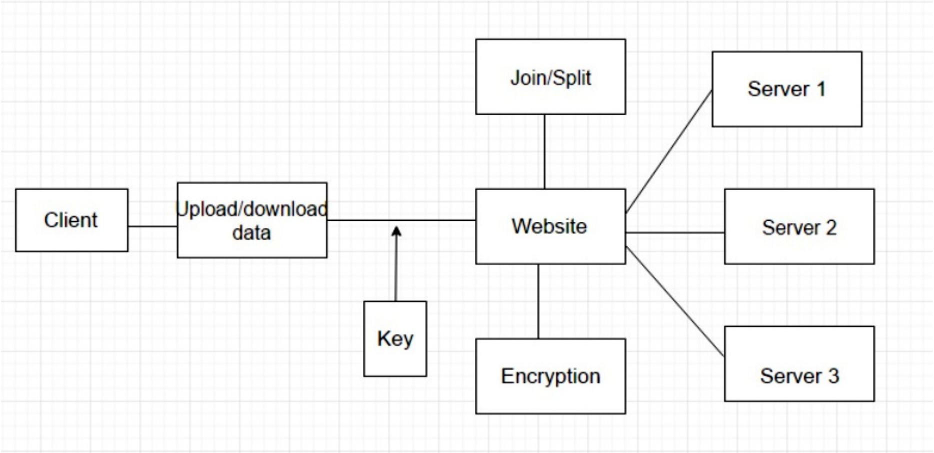

Figure 1: System architecture

When the user wants to download the same file, the file will be decrypted using the same key which is used for encryption. After decryption, each split is combined to form a single file which will be in the same format uploaded by the user.

4. CONCLUSION

Cloud computing is completely internet dependent technology where client data is stored and maintained in the data center of a cloud provider. To overcome the security challenges present in the single cloud, the concept of multi-cloud is used. The proposed system will split the file into different chunks when a file is uploaded by the user. Security is provided by using the AES encryption algorithm. Here first file split will be encrypted using the key provided by the user. From second split onwards each file will be encrypted using the hash code of the previous file split as the key which can be determined by using SHA algorithm. Thus security can be further enhanced by file split dependency. Due to the dependability between each file split, when an attacker gains access to one server he may not able to read the file, because its decryption key is dependent on any of other file split and the attacker is unaware of the location server where other split is stored. Thus concept of multi-cloud approach can be used to enhance the security in cloud.

REFERENCES

[1] Prof. Deepali M. Khatwar and Rashmi S. Ghavghave, Load balancing and security in multi-cloud IaaS using distributed file system- A review, volume 2, Issue 4, December 2014, pp. 1051-1055.

[2] C. Wang, Q. Wang, K. Ren and W. Lou, Ensuring data storage security in cloud computingARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.

[3] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[4] Mohammed A. AlZain; Ben Soh and Eric Pardede, Evaluation of multi-cloud computing TMR-based model using a cloud simulator, Fuzzy Systems and Knowledge Discovery (FSKD), 2014 11th International Conference on Year: 2014, pp. 6-11.

[5] C. Wang, Q. Wang, K. Ren and W. Lou, Ensuring data storage security in cloud computingARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.

[6] G. Brunette and R. Mogull, Security guidance for critical areas of focus in cloud computing, Cloud Security Alliance, 2009.

[7] H. Takabi, J.B.D. Joshi and G.-J. Ahn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[8] Jens-Matthias Bohli, Nils Gruschka and Meiko Jensen, Security and Privacy-Enhancing Multicloud Architectures, IEEE Transactions on dependable and Secure Computing, volume 10, July 2013, pp. 212-225.

[9] Dharmesh Kashyap and Jaydeep Viradiya, A Survey Of Various Load Balancing Algorithms In Cloud Computing, International journal of scientific & technology research volume 3. Issue 11, November 2014, pp. 115-119.