Secure Dynamic Virtual Machine Allocation In Cloud

Shilpa O. Gore[1], Janhavi D. Katkar[2], Swati U. Kavale[3], Prof. Ms. Rupali M. Pandharpatte[4]
Dept of EEE
K.J. College of Engineering and Management Research.

Abstract- *Cloud computing is one of the emerging technology today which is used by most of the social media sites to store their data. The major challenge for a cloud is securing the data and providing proper load balancing. These aspects are considered in our proposed system and also try to avoid data theft and overloading of data in cloud till some extent. In our proposed system, the data uploaded by a user is shuffled between the numbers of physical machines within cloud after a particular interval of time, so the attacker will not have access to data, thus enhancing the security aspect. Proposed system balances load on servers as well as avoids data duplication. In proposed system we are also going to use the AES algorithm for the purpose of encryption of data. The SHA-2 algorithm is used to generate hash code on the content of file so as to check duplication of data and can retrieve data using hash code. The Weighted Round-Robin algorithm is used for allocating the VM on cloud within the PM. The migration/routing of data is the main factor used for security for which we are going to use forward chaining. The proposed system can balance load and provide security to avoid access to data.*

Keywords- Cloud Computing, Load Balancing, Security, Server, Data-Center, Virtual Machine, Physical Machine, SHA-2, AES, Weighted Round-Robin, Forward Chaining.

I. INTRODUCTION

Cloud Computing enables on-demand network access to a shared pool of configurable computing resources such as servers, storage and applications. These shared resources can be rapidly provisioned to the clients on the basis of paying only for whatever they use.Cloud storage refers to the delivery of storage resources to the clients over the internet. Private cloud storage is restricted to a particular organization and data security risks are less compared to the public cloud storage. When the utilization of private cloud storage increases, there will be a behind this application/project is to developa secured system which will balance the load increase in the storage demand, which results in server down. It leads to expansion of cloud storage with additional storage servers. During such expansion, load on the servers should be balanced. In order to achieve security over data theft, the data is migrated among various servers. The key idea across the servers during the expansion of private cloud storage.

II. RELATED WORKS

1. A New Framework for Cloud Storage Confidentiality to Ensure Information Security

In this paper, Integrity, Confidentiality and Authentication issues in the cloud environment are targeted. They are using quite obvious algorithms for achieving confidentiality and integrity i.e. AES and SHA-1.But for authentication they are using a different approach as they have stated in their literature survey that in previous cloud security mechanisms diffie hellman algorithm was used, but it was prone to man-in-middle attack. So, they are using Station-to-station key agreement protocol for authentication. The advancement in their proposed system over existing is every server has a functionality to work as both storage server as well as encryption or authentication server. As a result Efficiency is increased in their proposed model over equal amount of computational power and time. The only disadvantage we found in this paper is that it assumes that the attacker can never decrypt the data as it is encrypted using AES.[1]

2. Secured Cloud Architecture for Cloud Service Provider

In this paper also they are targeting three main issues in cloud security which are Confidentiality, Authentication and Integrity. For Confidentiality they are using AES algorithm but they are ignoring the fact that the data can be decrypted. for authentication in cloud networks they have proposed an OTP mechanism which is promising because whenever user will want to register or login to upload or download file user first has to enter a valid OTP sent by CSP on its mailbox. As the OTP is unique for each login and confirmed using a secure and trustable application i.e. mailbox, reliable authentication is achieved. They have also used Modified version of SHA-2 because it will remove threat of Pre Image and collision attack.[2]

3. Advanced Persistent Threat Defence System Using Self-Destructive Mechanism for Cloud Security

In this paper author has given a solution on behaviour of a system in case of detection of Advanced Persistent Threat which can lead to data stealing. For encryption, they are using

Time Interval given by encryptor. In proposed system, on detection of advanced persistent threat or after expiration time specified by data owner is reached, the secret key will be automatically destructed or vanished from the database and hence no one will be able to decrypt the data. Also, the decryption is only possible within a time interval specified by encyptor or data owner, if any attempt is made to decrypt the data outside that time interval, the secret key will be vanished. The main focus of this paper is to avoid data stealing in any situation, but the disadvantage is that it doesn't give enough attention to data loss cause due to unavailability of secret key.[3]

4. Enhancement of Cloud Computing Security with Secure Data Storage using AES

In this paper, author has explained basic categories of encryption algorithms which are symmetric, asymmetric and hash functions. Author has surveyed encryption algorithms such as Symmetric: DES, Triple-DES, Blowfish and Asymmetric: RSA, DSA, Diffie Hellman. Symmetric algorithms has an advantage of speed and computational efficiency. Blowfish requires more memory than AES. DES have very small key size (56 bit) and hence can be easily decrypted. AES offers a range of key sizes like 128,192 and 256 bits which increases its performance exponentially over DES. In AES, number of rounds depend on key size like 10 rounds for 128-bit key, 12 rounds for 192-bit key, 14 rounds for 256-bit key and likewise. In each round except the last one, following operations are performed: SubstractBytes, ShiftRows, MixColumns and AddRoundeKey. Because of reasonable memory requirement, speed, flexibility and scalability, AES is found to be most efficient encryption algorithm.[4]

5. Static Load Balancing Algorithms In Cloud Computing: Challenges & Solutions

In this paper, Author has explained static load balancing algorithms. Advantages and disadvantages of Round-Robin, Weighted Round-Robin, Opportunistic, Min-Min, Max-min algorithms are discussed. In Round-Robin algorithm, all the servers are randomly placed in a queue. For each user request, virtual machine is allocated to first server in the queue. Once the virtual machine is allocated, server goes back at the end of the queue. Advantages of Round Robin are better response time and no starvation. But as there is no criteria for Virtual machine allocation, some servers may be over-utilized and some servers may remain under-utilized. Weighted Round Robin overcomes disadvantages of Round Robin by assigning weights to all the servers. Virtual machine will be allocated to a server having maximum weight and hence the load on the servers is balanced. Opportunistic Load Balancing Algorithm will assign a virtual machine randomly to any of the available servers without considering any other parameter. Min-Min Load Balancing Algorithm and Max-Min Load Balancing Algorithm suffers from starvation.[5]

III. SECURE DYNAMIC VIRTUAL MACHINE ALLOCATION IN CLOUD

In our system, along with encryption we have proposed a different approach to ensure security in cloud systems. We are using AES for encryption but at the same time we are considering the fact that data can be decrypted and hence we are moving the data among the servers before the minimum decryption time. For calculating minimum decryption time, we are setting the size of smallest file in the cloud. For moving the data, we are using Forward Chaining algorithm. For resource allocation we are using Weighted Round Robin and for integrity check SHA-2 respectively.

The algorithms used in our system are:

1. AES
2. SHA-2
3. Weighted Round Robin
4. Forward Chaining

1. AES:

The AES is Advanced Encryption Standard.It is asymmetric key algorithm, meaning the same key is used for both encrypting and decrypting the data.

In this, When file is received it is divided into blocks of size 128 bit. Further it goes under 10, 12, 14 rounds using 128,192,256 bits key which is generated using 128 bit block.[1][2][4][7]

2. SHA-2:

SHA-2 is Secure Hash Algorithm 2 this contains advance features over SHA-0, SHA-1. This algorithm is used to check integrity of data. If previously uploaded file contains same data which current file have then SHA-2 will tell about the integrity. SHA-2 contains set of cryptographic hash functions SHA-224, SHA-512, SHA-512/224, SHA-256, SHA-384, and SHA-512/256with digests (hash values) that are 224, 256, 384 or 512 bits.[2]

3. Weighted Round Robin:

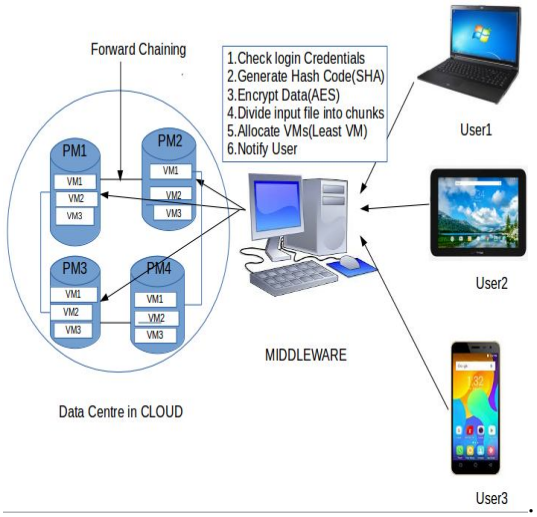
In this algorithm, a weight is assigned to each server. Though any criteria can be used as a weight, most commonly used criterion is the server's traffic handling capacity. Traffic handling capacity means how many more requests are sent that server's way, compared to other servers on the cloud. We are using server's available memory as a weight. So in our system virtual machine will be allocated to the server having maximum weight i.e. maximum available memory.[5]

4. Forward Chaining:

Forward chaining algorithm is used to take decision using inference rules. It starts with the data available to the user and uses inference rules to extract more data until it reaches to the goal. An inference engine which uses forward chaining searches the inference rules until it finds If clause is known to be true. When inference rule is found, the engine can conclude, the Then clause, results in the addition of new information to its data. Inference engines will go through this process until it reaches to the goal.[6]

IV. PROPOSED WORK

This System has a functionality to ask information for the client to login and send the username, password and private key to the user with the help of the admin. Those have login credentials as well as a private key for the login only thosecan easily perform upload, delete, and download operations. The Hash Code is created code according to the data using SHA-2 algorithm and this hash code is used to check whether the same file already exist or not. If the hash code is same then 'Duplicate File' message will arrive otherwise code is unique then file will be encrypted using AES algorithm and then encrypted file get split into three different chunks and stored in cloud servers. The migration/routing of data is the main factor used for security for which we are going to use Forward Chaining which will route the data among the servers at the particular clock tick. If the user tries to Delete or Download the file without Private Key and its login credential it gets fails. If login credentials are matched then all the chunks get merged into a single file and Delete/Download Operations get performed.



Advantages:

1. Avoid Data Theft.
2. Reduces Load.
3. Avoid Duplication of data.
4. Data cannot be misused.

V. CONCLUSION

The proposed webapplication has various characteristics like it does proper resource utilization ultimately load on servers is balanced and it also avoids duplication of data in cloud. The security to data theft is provided using migration of data within the servers.

REFERENCES

[1] Deepak Singh, Harsh K Verma, "A New Framework for Cloud Storage
Confidentiality to Ensure Information Security", Symposium on Colossal Data
Analysis and Networking (CDAN), 2016.

[2] Mr. Nilesh R. Patil, Prof. Rajesh Dharmik, "Secured Cloud Architecture for
Cloud Service Provider", 2016 World Conference on Futuristic Trends in
Research and Innovation for Social Welfare (WCFTR'16), 2016.

[3] J. Vijaya Chandra,Dr. Narasimham Challa,Dr. Sai KiranPasupuleti,"Advanced Persistent Threat Defense System Using Self-DestructiveMechanism for Cloud Security",2nd IEEE International Conference onEngineering and Technology (ICETECH), 17th, 18thMarch 2016, Coimbatore,
TN, India,2016.

[4] Vishal R. Pancholi, Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES", The International Journal for Innovative Research in Science & Technology, February 2016, 18-21.

[5] Nadeem Shah, Mohammed Farik, "Static Load Balancing Algorithm in Cloud Computing: Challenges & Solutions", International Journal of Scientific & Technology Research, October 2015, 365-367.

[6] Dony Novaliendry, Cheng-Hong Yang, A. Y. Denno Guara Labukti, "The expert system application for diagnosing human vitamin de_ciency through forward chaining method", Information and Communication Technology Convergence (ICTC), 2015.

[7] Qian Sun, Qingni Shen, Cong Li, Zhonghai Wu, "SeLance: Secure Load Balancing Of Virtual Machines In Cloud", IEEE TrustComp-BigDataSE-ISPA, 2016, 662-669.