Enforcing Data Security, Load Balancing And Auditing In Cloud Computing

Nikhitha K Nair[1], Navin K.S.[2], Soya C.S[3]

[1]M.Tech, Department of Computer Science and Engineering
Sarabhai Institute of Science and Technology
Vellanad, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering
L.B.S. Institute of Technology for Women
Poojapura, Kerala, India

[2]Associate Professor, Department of Computer Science and Engineering
Sarabhai Institute of Science and Technology,
Vellanad, Kerala, India

ABSTRACT--- ***Cloud computing is one of the emerging technologies that provide users with efficient storage and easy sharing of resources in a single platform. With the advent of this drastic technology, users became active in performing their applications with sharing with other use. This technology also brought in front the issues relating to the security, privacy and confidentiality. In this paper, proposed system focuses on performing dual security using encryption schemes, auditing using third party auditor and load balancing through agents in a single platform.***

Keywords--- Cloud Computing; Dual Security; Load Balancing; Third Party Auditor.

1. INTRODUCTION

Cloud Computing is the process by which data are entrusted to various information systems. These information systems are managed by third parties on remote servers in the cloud. Cloud facilities are being provided through virtualization technology.

Virtualization became most powerful tool to be used in the information technology in all these years. Many businesses have taken the advantage of this virtualization for consolidating hardware and software services. Now a day's many attackers have begun attacking the virtualization software itself.

The hypervisor or the Virtual Machine Manager (VMM) is the software layer that sits between the Virtual Machine (VM) and the underlying physical hardware. The Virtual Machine Manager performs the responsibility of allocating the resources to the Virtual Machines (VM) and isolates the virtual machines from each other and from the underlying host.

Cloud Computing has proven advantageous in providing customers with flexibility in obtaining computation and storage resources on demand. It provides flexibility in accessing the resources and data that are stored in cloud with great efficiency.

Even though cloud computing can be seen as a promising service platform for the next generation web, there are some challenges that restrict the cloud computing from wide acceptance. The most prominent issues include security and privacy.

Apart from traditional computing models where users have full control over the data storage and data accessibility, cloud computing restricts the users from the full control of the stored data. Here cloud service provides perform management of physical data and machines while users can have control only on the virtual machines. Therefore there will be compromise regarding the correctness of data stored in the cloud.

In detail study, the cloud computing security fall into two major classes namely Cloud Storage Security and Cloud Computation Security. Here the Cloud Storage Security emphasis on ensuring the correctness of data that is being stored in the cloud while Cloud Computation Security refers to ensuring the correctness of computation performed by the cloud service providers.

Auditing is another scenario that enhances the integrity of data stored in the cloud. Auditing on cloud data can be done by internal auditor and external (third party auditor).Third party auditor always tries to ensure that integrity is maintained on the data that is uploaded by the data owners in the cloud.

Load balancing in cloud data is the most challenging problem that is faced by the cloud. The cloud allows large amount of information to be stored and provides accessing of bulk of resources to different users. These can create load on the cloud servers. Load on the cloud servers can be under-loaded or over–loaded. But both these conditions are to be considered in order to solve the load balancing problem. Load balancing should be done in a manner that no node is over loaded or under loaded.

2. SECURITY ISSUES FACED BY THE SERVICE MODELS

The three delivery models are being utilized by cloud computing for delivering services to the end users. The three delivery models include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These service models maintain different level of security requirements in the cloud environment.

Infrastructure-as-a-Service (Iaas) forms the foundation of all services that are provided by the cloud. The Platform-as-a Service (Paas) is built on it and Software-as-a-Service (SaaS) in turn built on the PaaS.

Infrastructure-as-a-Service allows users to utilize the infrastructure as a service without bothering about the underlying hardware complexities. In a broad sense, IaaS only able to provide only basic security features such as load balancing but applications need higher levels of security.

In Software-as-a-Service (SaaS) which is a deployment model, where all applications are made available to clients on demand through the internet, which are hosted remotely by the service providers. This provides the customers with benefits such as increased efficiency and reduced costs. Due to the lack of visibility regarding how the data is stored and the way the security is provided, most of the enterprises are unsatisfied with this SaaS model.

Platform-as-a-Service (PaaS) is a layer which is above the Infrastructure-as-a-Service (IaaS) which offers an integrated set of development environment which helps the clients to develop their own applications without worrying about what is going on below the service. It offers the developer with the software which helps in management of complete software development life cycle, from its planning phase till testing and maintenance phase. But these advantages could help the hacker for leveraging the PaaS for malware commands and go to the IaaS applications and destroy them.

3. SECURITY ISSUES IN PLATFORM AS A SERVICE

In Paas, the control should be made for the clients by the provider in order to build applications on the platform. The provider should give strong security assurances to the clients that the data will remain inaccessible between the different applications.

Different metrics should be used for assessing the effectiveness of application security programs. Patch coverage and vulnerability scores are the available security specific metrics among the direct applications. These metrics focuses on the application coding quality.

Intruders can easily attack the visible code, infrastructure and perform extensive black box testing. So strict attention should be made on how the intruders react to new cloud application architectures.

4. SECURITY ISSUES FACED BY THE INFRASTRUCTURE AS A SERVICE

The Infrastructure-as-a-Service (IaaS) are more prone to security issues depending on the cloud deployment model. In this case, public clouds are more prone to these security issues than private clouds.

In a cloud environment, data transmission takes from the source to destination through a number of third-party infrastructure devices. There is more possibility in the case of routing the data through the intruder's infrastructure.

Cloud environment still uses normal security measures and protocols for providing security to the cloud data but cloud systems really requires higher degrees of security since large users and resources are involved. Encryption techniques and secure protocols help to provide security to a great extent but they can never be context oriented.

5. SECURITY ISSUES FACED BY SOFTWARE AS A SERVICE

Here the users fully depend on the cloud service providers for getting the proper security measures. Some of the elements that must be considered in the SaaS development and deployment process include:

- Availability
- Data security
- Data access
- Authentication and Authorization
- Data Confidentiality issue
- Network Security issue
- Data integrity issues
- Data segregation issue
- Data locality issue
- Web application security issue
- Data breaches
- Back up issues
- Vulnerability in virtualization
- Identity management and sign-on process

5.1 Availability

The SaaS performs the function of ensuring that the services are provided to the appropriate enterprises on time. Architectural changes should be brought both at the infrastructure and application levels in order for adding high availability and scalability. Multi-architecture plays a prominent role and it should be adopted with load balancing schemes.

5.2 Data Security

In the case of SaaS model, the data related to enterprises will be stored outside the enterprise boundary. Also, it is the responsibility of the SaaS vendor to use additional security checks to provide additional security and also to prevent various breaches due to the security vulnerabilities in the applications. Various encryption techniques can be used in order to provide data security.

5.3 Data Access

The security policies that are being provided to users in order to access the data give rise to different data accessibility issues.

5.4 Authentication and Authorization

User credentials may be stored in SaaS provider's databases. So the SaaS customers should always remember to activate or deactivate their accounts when the employees leave the company and then create accounts when they return. Authentication and Authorization issues to be considered are a challenging task.

5.5 Data Confidentiality Issues

Whenever there is sharing of information between an individual, a business or government agency in the cloud, then confidentiality issues arises. Laws should be made in order to overcome such issues.

5.6 Network Security

In the network security scenario, all the data which is flowing through the network should be provide security in order for preventing sensitive information leakage. So network traffic encryption techniques such as SSL and TSL can be used for providing security.

5.7 Data Integrity Issues

Data integrity issues can be handled by following ACID (Atomicity, Consistency, Isolation and Durability) properties. Most of the databases have the property of supporting ACID transactions and can maintain data integrity.

5.8 Data Locality

A SaaS model can be called as secure if it can provide reliability on the location of data of the consumer.

5.9 Data Segregation

The SaaS model should be capable of providing a clear boundary for each user's data to be stored. Both the application level and physical level boundary should be defined for storage of data by the client. The SaaS should have intelligence in segregating the data from the different users.

5.10 Web Application Issues

SQL injection is known to be the one type of attack that causes vulnerabilities to the web application. In such a case, the entire data which is behind the application is at risk.

5.11 Data Breaches

Breaching into the cloud environment can attack all the data of the user since in the cloud data from various users and organizations lie together.

5.12 Backup Issues

During any disaster, backups of information play a major role. The vendors of the SaaS models should ensure that they maintain backups of all the important information.

5.13 Vulnerability in Virtualization

There is a requirement of ensuring the different instances of application which is running on the same physical machine are isolated from each other.

5.14 Identity management and Sign-on process

The identity management plays of role of administrator by identifying the individuals associated with the system and putting restrictions for users in accessing the resources in that system.

6. AUDITING

Auditing of data that is stored in the cloud now became a usual practice. Auditing can be done by a private auditor or it can be done by internal auditor. The internal auditing process done by an internal auditor is commonly done in every organization. Third party auditing done by a third party auditor follows strict rules and regulations for the auditing process than by an internal auditor. The purpose of auditing is to ensure the correctness in the cloud data.

Auditing process ensures integrity in the cloud data. This process also checks for the authorization and authentication issues. Signatures are most probably used to deal with the authorization issues.

7. LOAD BALANCING

Load balancing is another phenomena which is challenging in the field of cloud computing. The cloud computing provides a platform where large information or resources can be stored and shared by different users. These increases load on the cloud data.

Load balancing is the property to balance the load on the cloud data. Both under-loaded condition and the over-loaded condition becomes real world problem that has to be dealt with equal importance.

The balancing of load in the cloud data should be done in such a manner that tasks requesting for the resources does not remain idle or overloaded. Agents can be used to reduce the overloaded situation in the cloud data.

8. RELATED WORK

In paper [2] attempted to solve the problem of ranked search done on the keywords in order to achieve utilization of encrypted data stored in the cloud.

In paper [3] provides a description about the various Cryptographic cloud storage service along with the benefits of using such a service.

In paper [5], the more emphasis is being given to the multi-keyword ranked search when user wants to download the data that is being stored in the cloud. Here Multi-keyword Query Encryption scheme is being used which have the tendency to greatly reduce the maintenance overhead during the expansion of keyword dictionary.

9. PROPOSED SYSTEM

The proposed system attempts to bring all the three conditions which include Security, Auditing and Load balancing.

In the proposed system, security in the cloud data has been enhanced by using encryption techniques. The encryption techniques are commonly used now days to enhance security to some extent. The dual encryption technique enhances security on the cloud data. The encryption schemes used in the proposed system includes swap XOR and AES encryption scheme.

Also auditing plays a major to ensure correctness on the data that is stored in the cloud by the data owners. In this proposed system, instead of using internal auditors for auditing purpose, third-party auditors are being used. The third-party auditors audit the cloud data upon the request from the users.

Load balancing has been done by the agents which are software programs that act to reduce the load on the cloud. Whenever there are large amount of tasks to be done by the cloud providers, then the agents act in between them and handle some of the tasks that are to be done by the cloud. In this way, agents help the cloud providers in performing bulk of tasks.

10. METHODOLOGY

The system works as follows. The data owners are the entities who want to upload their data in the cloud and data users are the entities who download the data that is stored in the cloud.

Here first the data owners upload their information in the cloud. For security, they use AES encryption standard and they store the encrypted data in the cloud. Here only one key (private key) is generated since it is a symmetric encryption scheme. The private key is owned by the data owner.

Then after storing the encrypted data in the cloud, the cloud performs dual encryption on that data using swap XOR scheme. When the data users want to download the data that is being stored in the cloud, then he should decrypt the dual encrypted data using the private key. In this way the security is enhanced on the uploaded data in the cloud.

The data users can request the third party auditor to undergo the auditing on the data that is stored in the cloud so that the downloaded data is correct in every sense. The third party auditor requests the cloud indicating the request from the data user regarding the cloud data to be downloaded.

The cloud provider then checks the details regarding the stored requested data and send response to the third party auditor. The third party auditor verifies the details and sends the report to the client regarding the correctness of verification. In this way, the auditing process is being performed.

Load balancing is being performed by connecting different computers and making one system as a server and other as client machines. When the client sends bulk of requests for the resources, then cloud server becomes over loaded. Then some of the tasks are sent to the agent machines which are later performed by them.

In this way different scenarios are being created to perform security, auditing and load balancing situation.

11. CONCLUSION

Cloud computing provides a platform the users to handle data storage and data sharing efficiently. Many issues relating to security and privacy that can affect the cloud data has been considered here. The proposed has considered enhancing security on the cloud data by using dual encryption schemes. At the same time, auditing process is also carried over with the help of third party auditor to ensure correctness in the stored data. Load balancing problem in the cloud has been handled with the help agents.

12. REFERENCES

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," *Proc. IEEE INFOCOM*, pp. 829-837, Apr, 2013.

[2] Cong Wang, Ning Cao, Kui Ren and Wenjing Lou," Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data" , IEEE Transactions on Parallel and Distributes Systems ,Vol.23, NO.8, AUGUST 2012.

[3] S. Kamara and K. Lauter,"Cryptographic cloud storage," in *RLCPS, January 2010, LNCS.Springer, Heidelberg.*

[4] Ankatha Samuyelu Raja and Vasanthi A, "Secured Multi-keyword Ranked Search over Encrypted Cloud Data ", International Journal of Advanced Research in Computer Science and Software Engineering-Volume 2, Issue 10, October 2012.

[5] Zhiyong Xu, Wansheng Kang, Ruixuan Li, KinChoong Yow, and Cheng-Zhong Xu,"Efficient Multi-Keyword Ranked Query on Encrypted Data in the Cloud", IEEE 18th International Conference on Parallel and Distributed Systems.

[6] William Stallings,"Cryptography and Network Security", 4/E. Pearson Education India, 2006.

[7] R.G.Rajan, V.Jeyakrishnan, "A Survey on Load Balancing in Cloud Computing Environments", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2013.

[8] N. Sran, N. Kaur, "Comparative Analysis of Existing Load Balancing Techniques in Cloud Computing", International Journal of Engineering Science Invention ,Volume 2 Issue 1, PP.60-63,ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726, January. 2013

[9] Wang, S. C., Yan, K. Q., Liao, W. P. & Wang, S. S. "Towards a load balancing in a three level cloud computing network", Proceedings of 3rd International Conference on Computer Science and Information Technology (ICCSIT), IEEE, July, 2010, 108-113.

[10] Randles, M., Lamb, D., Bendiab, A. T. "A Comparative Study into Distributed Load Balancing Algorithms for Cloud Computing ", IEEE 24th International Conference on Advanced Information Networking and Applications Workshops 978-07695-4019-1/10, 2010.