iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: IV Month of publication: April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4717

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

An Approach to Secure Multi-Tenancy in Cloud Computing

Rajalakshmi S[1]
[1]Student BCA, Department of Computer Science, M. O. P. Vaishnav College for Women, Chennai.

Abstract: Cloud Computing provides a multi-tenant feature to host multiple tenants. In architectures that are based on cloud, organizations, consumers and customers share infrastructure and databases to gain advantage of price and performance. Basically, "cloud" can be referred as an internet-based environment for computing resources consisting of servers, software applications that are accessed by any individuals with internet connectivity. The advantage of delivering service to multiple tenants on the same physical machine through virtualization can become a challenge as it also has to provide security to all the data of multiple tenants. The overall objective of this study is to explore specific risks due to multi-tenancy in cloud computing and provide solutions to overcome the risks to avoid loss of data, misusing the data or violating the privacy guidelines.

Keywords: Cloud Computing, security, data, multi-tenancy

I. INTRODUCTION

Cloud computing is a technique adopted by many firms to decrease IT costs and provide clients with faster responses thereby increasing profit margins. Clients receive the services through three major service models namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In today's world there are no standard business model for cloud computing; instead the companies experiment with four ideas – private, public, community and hybrid models. The different characteristics of cloud such as on-demand service and broad network access allow services to be shared among various users within the same organization or among different organizations leading to multi-tenancy. Multi-tenancy allows access to data and applications within a cloud environment and allows businesses to benefit from reduced costs.

Cloud computing security architecture must ensure that one tenant does not have access to the resources of another tenant. Every tenant must be separated securely using segmentation, access control and certain other techniques. Multi-tenancy must address in all layers for security analysis. In a typical multi-tenancy situation, the users are the tenants and are provided with a level of control in order to customize and tailor software and hardware to fit their specific needs [1].

II. SECURITY THREATS TO MULTI-TENANCY

The fundamental security issue with multi-tenancy is that, multiple tenants share the same computer hardware. Indeed, using a multi-tenancy approach for the development of public cloud infrastructure presents a number of challenges in terms of compliance, security and privacy [1]. The main challenge of using this form of multiple services is ensuring data isolation. The management of data is critical as several users will be use the same system, each requiring their own privacy and confidently. The lack of isolating the network among tenants makes the public cloud vulnerable to attacks. The inadequacy of efficient bandwidth and traffic isolation makes multi-tenancy in cloud computing vulnerable, since malignant tenants may launch attacks towards co-resident tenants within the same cloud server centre [5]. Current approaches to access control on clouds do not scale well to multi-tenancy requirements because they are mostly based on individual user IDs [6]. By its very nature multi-tenancy has increased security risks due to the sharing of software and data by multiple tenants. As these collocated tenants may be competitors, if the barriers between tenants are broken down, one tenant may access another tenant's data or interfere with their applications. Indeed, cloud providers are responsible for ensuring that one customer cannot break into another customer's data and applications [6]. In a multitenant environment, side-channel attacks pose significant risks in a cloud computing environment. Side-channel attacks occur based on information obtained from bandwidth-monitoring or other similar techniques or due to lack of authorization mechanisms for sharing physical resources. Indeed the multi-tenancy architecture has increased the risk of database exposure and thus, data protection today is more crucial than ever. Another obvious risk of multi-tenancy is resources being assigned to consumers whose identities, and intentions, are unknown. Practically all virtualization platforms on the market today have a trusted virtualization layer that, if compromised, leads directly to full compromise of any of the virtual machines running on the physical host [7]. This could result in the inability to monitor activity on the virtual machine, and possibly allowing a malicious user to alter the state of the virtual machine. Another important security risk inherent to multi-tenant systems is uncoordinated change controls and misconfigurations. When multiple tenants are sharing the underlying infrastructure it is possible that changes may lead to a security breach, allowing one tenant to gain access to another tenant's data or resources. A security risk may result from combined tenant data. To reduce cost, providers may store data from multiple tenants in the same database table-spaces and/or backup tapes. In this scenario a data deletion request may become a challenge resulting on portions of data not being properly deleted. (Full multi-tenancy)

A. Addressing The Concerns

Software providers argue that their software is provided with the highest level of security available. There is a scope for human error when a database administrator accidentally grants access to an unauthorized person. There is also a threat of hackers – who breaks the encryption of multi-tenant database will be able to steal the data of hundreds of businesses who have data stored on it. We should address the concerns of cloud computing in order to provide secure multi-tenancy enforcing separation at one or more layers:

1) *Server Layer* – Server virtualization and operating systems separate tenants and application instances on servers and therefore control utilization of access to server resources
2) *Application Layer* – Separate or multiple instances of same application provide multi-tenancy at this level
3) *Network Layer* – Techniques like zoning, VLANs can be used for network separation. IP security provides network encryption at the IP layer for additional security
4) *Storage Layer* – Data should be protected from tenants so that data of various tenants is secured(Data partition encryption)

III. LITERATURE SURVEY

Some of the proposed methods have been discussed in the literature survey for handling security issues in cloud computing.

Popovi and Hocenski, discussed about the security issues, requirements and challenges that are faced by cloud service providers during cloud engineering [4]. Behl explores the security issues related to the cloud environment. He also discussed about existing security approaches to secure the cloud infrastructure and applications and their drawbacks [5]. Sabahi discussed about the security issues, reliability and availability for cloud computing. He also proposed a feasible solution for few security issues [6]. Mohamed E.M et.al presented the data security model of cloud computing based on the study of cloud architecture. They also implemented software to enhance the work in Data Security model for cloud computing [7]. Wentao Liu introduced some cloud computing systems and analyses cloud computing security problems and its strategy according to the cloud computing concepts [8]. Mathisen, E discussed about some of the key security issues that cloud computing are bound to be confronted with, as well as current implementations that provide a solutions to these vulnerabilities [9].

(Challenge paper)

IV. DATA SECURITY CHALLENGES

Data leak prevention is the most important factor with 88% critical and important challenges and similarly, data segregation and protection has 92% impact on security challenges. When multiple organizations share resources, there is chance of risk for misuse of data. Protection of data is the most important challenge in cloud computing. The three main areas of data security are:

A. Confidentiality

Critical vulnerabilities must be checked to ensure that data is protected from any attacks by conducting security tests to protect data from malicious users.

B. Integrity

Users should not store personal data like passwords to ensure integrity to provide security to client data.

C. Availability

An important issue faced by several organizations which depends on the agreement between vendor and client.

D. Data Breach

Another important issue in cloud is data breach. The entire cloud environment is prone to attack if a malicious user enters the cloud which consists of large data from various users. The data breaches may either be accidental issues or due to insider attack.

V. PROPOSED METHODOLOGY

To overcome the issues faced by multi-tenancy in cloud computing, an application can be designed for improving cloud security using partition method. In this application, the data of the clients are encrypted. After encryption, the data is partitioned into many parts and sent to different cloud servers. When client requests for the stored data, it is retrieved from the cloud servers and decryption is done to merge that data. The merged data must be returned to the client as their original data. The application should have simple user interface.

A. Concept

The partitioning of data makes storing of the data in easy and effective and provides a way for flexible access and there is less cost in data storage. Both the time as well as space is considerably reduced during cloud storage. The partitioning method is used for the data storage to avoid the local copy at the client side. This method ensures identification of misbehaving server; high cloud storage integrity and improved error localization.

B. Partition Algorithm

1) Load Input file
2) Check for the file size
3) If file_size = = invalid ,
4) then declare as invalid_size
5) else,
6) size = s
7) Split file into ‘n’ partitions with an index value
8) Return files

C. Merging Algorithm

1) Collect all decrypted file partitions
2) Check file status
3) If (!file)
4) then file is missing
5) else
6) Count the index value

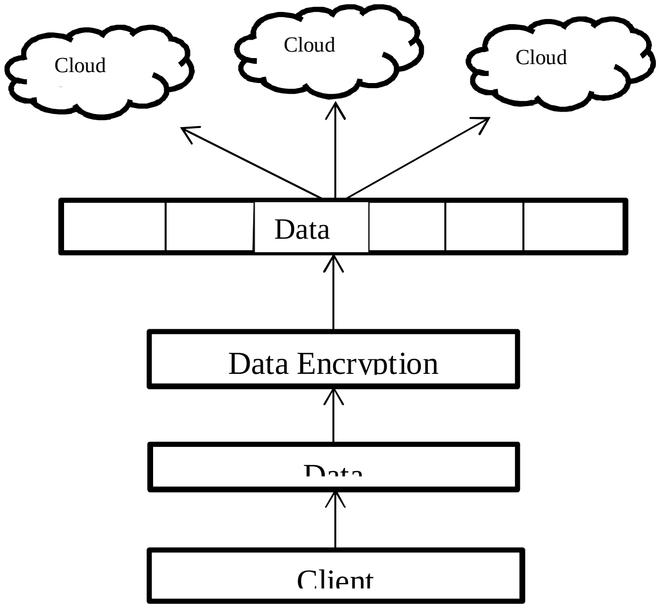

Figure to illustrate Partition Algorithm

D. Future Work

The proposed work aims in the design of secured data storage and error tolerance in cloud storage and is particularly beneficial for multi-tenant systems. The remote data integrity checking detects the threats and misbehaving server. In future, a higher level of security can be provided by using advanced encryption and decryption algorithm and searching mechanisms for outsourced computations in cloud services. Multi-tenancy in cloud computing is an inherent feature, providing many advantages in terms of resources usage in cloud environment, but at the risk of security. So in this paper we have proposed a technique which allows tenant's data to be secure when data is stored in partitions in different cloud servers.

VI. CONCLUSION

Cloud computing is the new emerging technology that presents a good number of benefits to the users, but it faces a lot of security issues due to multi-tenancy and data security challenges. The proposed methodology provides an effective means for securing data of multi-tenants by involving a considerable low amount of space and cost. However, database administrators need the tools and the knowledge to understand which tenant should be deployed on which network in order to maximise capacity and reduce costs. To provide a secure data access in cloud, advanced encryption techniques can be used for storing and retrieving data from cloud. Also, proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.