Indonesian Journal of Electrical Engineering and Computer Science
Vol. 13, No. 1, January 2019, pp. 65~71
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v13.i1.pp65-71

Securing SAAS service under cloud computing based multi-tenancy systems

JKR Sastry, M Trinath Basu
Department of Computer Science and Engineering, KLEF University, Vaddeswaram, Guntur District, India

Article Info

Article history:

Received Jun 15, 2018
Revised Sep 20, 2018
Accepted Oct 4, 2018

Keywords:

Cloud computing
Multi-tenancy
SaaS
Shared data services

ABSTRACT

Cloud computing technologies are being used by many who need computing resources such as software, platform and infrastructure as per their business requirements in terms of provisioning and pay for the usage as per actual consumption of the services based on the SLA signed by the user and cloud service provider. Software running on a physical machine is being provided as services to the end users. For the reasons of cost economies access to software that uses a database is being provided to multiple users. The access to the software is provided either directly or through a virtual machine. The software being provided as service uses the same database for many of the users who have requisitioned for the same. As a result, there could be encroachments by the users into the data of others. There is a need to secure the data belonging to several users while all of them access the data using the same application. In this paper an efficient method is presented for securing the data processed by software which is offered as a service to multiple users either directly or through virtual machines.

Corresponding Author:

J.K.R. Sastry,
Department of Computer Science and Engineering,
KLEF University,
Vaddeswaram, Guntur District, India.
Email: drsastry@kluniversity.in

1. INTRODUCTION

Cloud computing provides several services to multiple tenants using the same physical machine through implementation of concept called virtualization. Providing security and privacy to data owned by several tenants is a challenge when the resources connected to the same machine have to be shared among several tenants. In cloud computing, the software marketed by the cloud computing service provider is made available to the user through implementation of a service model called SaaS.

Many users are allowed to use the same application and therefore give scope for encroachment into a data segment which is not related to some users. Customers cannot monitor or control the way the data is going to be dealt by the service provider as the user has no idea of the infrastructure being used to store the data. Multi-tenancy implies that a set of users are allowed to utilize the same application hosted by the service provider. The user is not concerned with the kind of underlying infrastructure being used by the application [1].

SaaS is a kind of delivery models implemented by cloud computing service providers. Customers access the application through Internet. The software and the related data are centrally hosted by the service provider. A virtual machine (VM) is a kind of implementation of software. The VM can be configured with an Operating system or any other program which actually runs on the Physical machine on which the VM is provisioned. The software that is configured on the VM uses the all the computing facilities existed on the physical machines that include memory, storage, network etc.

A Software called Hypervisor which is installed on the physical machine on top of operating system is responsible for managing all the resources that are shared by the applications running on different virtual machines. Many resources supported on the physical machines as such must be managed such that one user do not conflict another user in relation to the shared resources allocated to them. The resources that can be shared among the users include virtual machines, storage, memory, network bandwidth etc. The accessibility of the sharable resources among several tenants must be controlled through use of techniques such as access control, Virtual storage controller and use of VLANS. Cloud computing systems also are subjected to attacks which include side channel attack, brute forcing attack, network probing etc., from which the data and the applications must be protected. The most important thing is to achieve data isolation. Multi-tenancy is an important feature of SaaS in cloud computing. Multi-tenants can share single instance of the same application there by share the same data storage area. Multi-tenancy provides the user the ease of operations and reduces delivery cost for a huge number of tenants.

Cloud computing should support Isolation of tenant data, workspace (memory), Process execution, Tenant-aware security, monitoring, management, reporting and self-service administration, Isolation of tenant customizations and extensions to business logic, tenant-aware version control, Tenant-aware error tracking and recovery etc. so as to ensure that the data is actually protected. Multitenancy can be achieved through various models that include shared nothing, shared hardware, shared OS, shared database, and shared everything and custom multitenancy models.

Data related to many users could be stored in the same database and managed through the same application that has been given access to many users. Some many users may be given access to the same tables existing in the same database. The users for the same applications also are given the option of configuring the application as per their business requirements. The main issue in the case of multi-tenancy is the data risk, one user tampering the data of others. Multi-tenancy is all about isolating the data in such a way that the owner of the data only will have access and keeping complete confidentiality.

Data Management as such will be the key issue keeping in view of confidentiality and privacy of the data. Many rules and regulations must be in-built into cloud computing multi-tenancy environment so that the needs and the regulatory requirements of different users can be met. Nevertheless, it is critical that the need to segregate the data and provided proper access controls so no unauthorized access can be gained. Many Challenges are to be met when one implements Multi-Tenancy.

End users requires Performance isolation, Availability of all the resources, Scalability in terms of tenets requirements, support for value added applications and need for privacy and security of the data accessed by applications, ability to customize the applications to run the way their applications are designed for the customers. Solution developers are concerned with the issue of access control, customizability considering database, Business logic, user interface, workflows, tenant provisioning, and usage based metering. Service providers' needs to deal with data sharing, backup, and restoring tenant data, enhancing the usage of the hardware, reducing the operational cost, development of human resources, reduce the development effort, reduce the time to market, enablement of the mutli-tenancy support to the users without the need to make any code changes.

Multi- tenancy can be implemented considering virtualization, sharing operating systems and applications. Many methods have been implemented to achieve multi-tenancies which include visualization, data isolation, and managing databases. Virtualization is creating more logical machines that run on a single physical machine which is connected with more number of resources and also that many operating systems run on a single machine. The resources connected to the physical machine are shared among the virtual machines.

A configured virtual machine can opt to run a specific operating system. A separate virtual machine can be allocated to each of the tenant. Implementing virtualization require running a separate software such as VMware on the physical machine. The software is responsible for providing services that include scalability, flexibility, resource sharing. When making available the access to a database, various aspects have to be supported that include separation of the services provided to different tenants, scaling the access to the databases based on the number of tenants, confirming to the SLA terms and conditions, support for tenants customization like support to tenant defined triggers and stored procedures. Each tenant to whom a virtual machine is provided, additional services needs to be provided relating to backup and retrieval of data, enforcing the application upgrades, security enforcement and support for implementing law and act. Multitenancy is all about several tenants sharing the same application that is developed using database management software [2]. The accessibility of a database can be provided though many database management mechanisms that include the following:

a) Allocation of separate databases resident on the same machine.
b) Allocation of databases on different machines.
c) Allocation of segmented database.

d) Allocation of Horizontally partitioned databases resident on the same machine.
e) Allocation of Horizontally partitioned databases resident on the different machines.
f) Allocation of shared database with separate schema.
g) Allocation of shared database and shared schema.

A database with its associate schema can be allowed for accessing by several users. This kind of sharing is usually implemented within an enterprise setup. However this kind of a scalability of a single database leads to unauthorized access to the data. The grant permission adopted by the users limits the access by the users. If access permissions exist, there could be data encroachments by the users. The administrators of the database will have access to the entire data losing the secrecy of the same. More mechanisms have to be adapted so as to ensure the secrecy of the data.

Multi-tenancy within SaaS is achieved through use of a database with data isolation achieved at application layer. The service providers shall have to build into the application, the mechanisms that implement data isolation considering each of the users who have been given access to the application. One of the isolation method that can be implemented is the data access is implemented for each user through a separate instance of the same data access class.

The threat of data corruption, data loss, data inconsistency is expected to increase when more number of users accesses the same data with different pointers to the data [2-3]. The services implemented through cloud computing infrastructure bypass the security controls (Personnel, physical and logical) exercised by the users. This leads to a risk when data control responsibility is left to cloud computing system.

Much number of issues arises due to Multi-Tenancy due to the reason that same hardware is used for all the users who are given with the access for the same application. However some kind of separation between the users exists at the application and Virtual layers [1].

In the case of Multi-Tenancy both the Victim and attacker uses the same application that runs on a single server. The risk caused by the attacker cannot be mitigated by traditional methods as these methods cannot penetrate into the servers. The monitoring to find attacking if any is limited to network layer only. There are three different ways the attacker and the victim can be situated within the cloud.

In case one, the attacker and the Victim are simply the internet users which simply means traditional security methods can be used to protect each other's data. In case two, the victim and the attacker are in the same cloud but on different servers. The victim and the attacked are physically separated due to allocation of different virtual machines to each one of them. In this case Virtual security measures are to be employed by the service provider. In another case the victim and the attacker are on the same cloud but share the same server which is the case of multi-tenancy.

Securing this kind of situation is hard as no network as such exits for communication to happen. The traffic as such happens within physical machine only. Virtual network security defences as such cannot protect the data that is attacked within the purview of a physical machine. Many issues are to be addresses when data of multiple users is stored within the same repository. Same cryptographic algorithms are used to store the data in the common storage. No physical separation either physical or logical exists. Also there exists an opportunity to attack the data when data is retrieved from the database and decrypted to plain text for processing. The processing job can be interrupted to access the plain text and thus can be attacked. There should be composite and complete privacy and security to the data of multiple clients stored in the same database being accessed by the same application which is shared by many customers.

2. RELATED WORK

The main issue that must be addressed when multi-tenancy is used is to protect the application and the hardware on which the application is deployed as the clients are allowed to share both the elements. Multi-tenancy thus possesses many challenges to secure and preserve the privacy of the data owned by different users. Many methods have been presented in the literature that aims at isolating data storage, allocating separate data storage for each tenant etc. [9].

Each method releases a different security issue altogether that involves use of different types of encryption techniques. The service provider can provide an interface within the application using which the users can configure the application for imposing some security constraints. The security enforcement can be externalised without imposing any load on the application Mohamed Almorsy et al [13]. Cloud computing architecture must include various issues related to enforcement of the security issues. The very first attempt to include security in to cloud computing infrastructure was attempted by Kamara et al. [14].

They have covered both consumer and enterprise scenarios and they have used nonstandard encryption algorithms such as searchable encryption and attribute encryption. An algorithm that uses user attributes and their signature has been presented by Zarandioon et al. [15].

The algorithm is included into a protocol call K2C (Key to Cloud - user centric privacy preserving cryptographic access control protocol. The end users can securely share, manage and stores their data in the cloud computing infrastructure which is basically unstructured. Encryption algorithms are quite frequently employed to secure the user data. The encryption algorithms can be used to transform the users' critical data so that the data can be made to be in-accessible to unauthorized users even in the situations of availability of such data to unauthorized users. Access control is one of approaches that can be enforced to prevent un authorized access to data. Access control enforced for controlling the access while the users are in multi-tenancy mode is not an effective methods as the access control is merely achieved through using IDs [12].

Data Isolation is the critical issue that must be addressed when it comes to multi-tenancy. Effective data management systems must be implemented to control the access to the data by multiple users through access to the same application. Appropriate and extensive privacy and security to the data must be implemented. The public clouds as such can be attacked through several means as no network isolation is implemented [10].

Users who are attackers can launch attacks on co-resident users as no traffic or bandwidth isolation is implemented as the multi-tenancy is an issue that is implemented within a single server [11]. DPET (data Partition encryption techniques is one such method)[2]. In this method each record is encrypted twice before storing the same in a portion that is allocated to the tenant. Entire database is portioned (user space) and one portion is allocated one tenant only. A scheme is used for portioning and allocating the partition to a specific tenant. The record is encrypted using a public and private key known to both the tenant and CSP (Cloud service provider).

The kind of encryption algorithm to be used is randomly selected. First the record is encrypted by tenant using public key and then encrypted by the CSP using their own public key. The private key of the tenant is used at the time of decryption. The key pair to be used for each of the tenant is different and the same is stored in the data segment related to the tenant concerned. The DEPT algorithm while provides certain level security, the data processed within the server can be still be attacked by the co-resident users due to lack of traffic and bandwidth isolation. An attack model has been presented which is based on a threat model that takes advantage of Multi-Tenancy situation is presented by [3].

Mitigating the attacking is the best course of action. The information related to resource allocation, resource utilization and accessing can be known from the logs maintained by the clouds. The scanning of the logs and applying brute force methods the details of locations where data is stored could be known and therefore can be attacked. [4] Have shown the kind of issues that must be addressed when muti-tenancy is implemented in IaaS layer. When new hardware is added with an intention of increasing the performance, sometimes it leads to many of the security issues as well.

The authors have presented a model using which the performance of a cloud can be computed. Security of the data stored on the cloud computing system can be achieved through implementing access control systems considering both authentication and authorizations; they have presented a mechanism to encrypt the data based on the location of the user and geolocation of the data where it has been stored. [5] Have presented a comparison of the attribute based encryption (AES) of the data to be stored in the cloud. However the methods will be directed towards achieving the access controlling of the data than dealing with issues related to multi-tenancy.

Data privacy and security of the data stored in cloud can be achieved through implementing access control mechanisms. A comparison of currently existing AES-Based schemes of data access control has been presented [6]. A list of unsolved problems through AES has been enlisted. Even though the AES based current existing control schemes could satisfy the requirements of data access control for cloud storage, there are still problems such as revocation of the user, reduction of the computational effort, implementation of hierarchical structure of the user etc. There are many problems such as revocation of the users, computational efficiency, hierarchical structure of the users etc., which are related to securing the cloud storage while attribute based encryption could solve many access control related issues with respect to cloud storage.

An analysis of data storage in cloud computing and the kind of security enforcement that can be built into cloud computing system has been provided [7]. They have emphasized that the main concept is to provide integrity to the cloud storage area with distinct data models and security algorithms. They have presented cloud data storage architecture along with the cloud data models. Manjinder Singh et al., [7] have emphasized that one has to ensure data integrity to the cloud storage through use of different data models and security algorithms. They have presented an architecture that includes the security models within the cloud computing system. They have presented a modified RSA based algorithm that has been provided with a different key generation and decryption system for ensuring the cloud storage security.

The challenges that one has to face in providing the security within the cloud computing are presented in detailed by Katie Wood et al., [8]. They have focussed specifically around cloud deployment and data storage, in particular relation to privacy concerns due to multi-tenancy. Katie Wood et al, [8] have

presented series of challenges that one must face when security to the cloud storage has to be ensured. They have concentrated main on securing the cloud storage considering the multi-tenancy implemented through SaaS.

3. INVESTIGATION AND FINDINGS

Many approaches have been presented in the literature for securing the data in a single database in which the belonging to different customers has been stored and processed by a single application. All of them suffer from one kind of risk are other. The data stored in the database can be double encrypted by the user and then the service provider so as to guarantee the confidentiality from both perspectives.

Then in that case the way the encryption algorithms are selected or the way the keys are generated is the most crucial aspect of securing the data stored in the database. Data isolation is most significant aspect of securing the data. The data as long as it is in single database, will be insecure at least at physical storage level. Physical data isolation can be done by distributing the data into different storage areas connected to different physical machines. The database is assigned to physical data storage situated in different machines. Database can be portioned horizontally and each partition is made to be situated on the storage situated in different machines. Each partition is allotted one single user. Since the data of different users is situated in different machines, data isolation is achieved thereby there is no chance of one user encroaching into the storage area of some other user. The arrangement of such an implementation is shown in Figure 1.

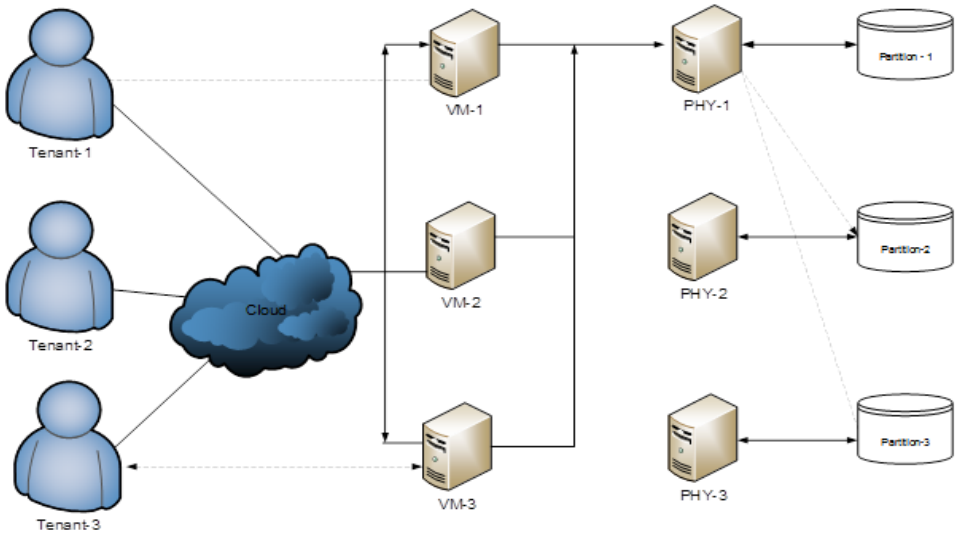

Figure 1. Multi-portioning the database

Each of the partition is recognized by the IP address of the Machine where it is situated and the location where the partition is situated. A user id is identified by an ID assigned by the Cloud computing software. When a user makes a request for a VM to run a SaaS service the hypervisor shall make a request to the application to allocate the partition and provide the details of the Physical machine (IP address) and the location where the partition exists within the physical machine.

The user can encrypt his own data using their public key. The public key of the user can be generated on the user side. The algorithm to be used by the user for undertaking the encryption can be fetched dynamically at the user side based on his ID. The key and the encryption algorithm are used to encrypt the data on the user side before it is transmitted to the hyper wiser for storing the same on the user related portion. The hypervisor shall lookup for an algorithm based on the IP address of the physical machine and the location of the partition within the physical machine, using which an encryption algorithm and a key is generated and the same are used for encrypting data on the cloud side. Thus the data protection is implemented and privacy maintained on both the ends of the client and CSP. The description of the data however can be undertaken on the client side using the private key of the user.

Algorithm

Initialization process

a) Client request for partition in the database. The request sent to the Hypervisor.
b) The hypervisor gets the details of the partition in terms of the IP address and the location of the partition from the guiding application software. A different IP address is chosen every time a request is initiated.
c) The key and the encryption algorithm to be used on the cloud side are generated based on the TCP/IP address and the location of the partition.
d) The user ID, Key and the encryption algorithm are stored along with user ID within the cloud.

Client side process

a) Tenant 'Ci' generates a large Prime Cp from his own credentials generally using his own ID and sent to Cloud Service Provider.
b) Tenant Ci computes N=2*Cp
c) Tenant Ci generates Cyclic group ZN* of order Ø(N)(Euler Quotient function).
d) A subgroup ZØ(N)* subset of ZN* of order Ø(Ø(N)) is generated by Ci with generator g ∈ Zn*
e) Tenant Ci randomly picks up two private keys Tq and Cr ∈ ZN* Cq≡ gk1 mod N and Cr≡ gk2 mod N where k1,k2 ∈ ZØ(N)* where g is generator for ZN*
f) Tenant Ci computes N= Cq* Cr
g) Ci chooses 'e' such that gcd(e, Ø(N))=1.
h) Ci determines 'd' such that ed≡ 1 mod Ø(N)
i) Tenant Ci computes CPr = e.rst such that e.rst ≡ 1 mod Ø(N) and CPb =d.rsd such that d.rsd ≡ 1 mod where CPr : Tenant Private Key, CPb: Tenant public key Public key <N,CPb> Private key <CPr,d,e>
j) Tenant Ci encrypts the data of each record R (ER) ER= Re mod n
k) Tenant Ci sends ERj to CSP to store in its Partition Pi.

Processing on the Cloud side

a) CSP fetches the related Encryption algorithm and the key with the help of user ID.
b) The data record received from the client is encrypted again using the key and encryption algorithm
c) EER = ERTPb mod n
d) Fetch the partition details PT of the client using the lookup table with the help of user ID
e) CSP stores ER in partition Pi of Ci

Data Retrieval process

a) Tenant encrypts the Primary data using his own key and algorithm and sends the same to the cloud along with his own ID.
b) CSP fetches the record from the partition related to the client using the encrypted key data which is further encrypted using the client's encryption algorithm and the key which is generated and stored in the lookup table on the CSP side. The details of the partition related to the client are stored within the Application software or the hypervisor.
c) The queried data is sent to the client. It should be noted that no decryption is done on the cloud side. Querying is done using the encrypted key values only.
d) After receiving Tenant Ci computes R = EERrst mod N to obtain original Record.
e) If Tenant Ci does not get Record R from above data then Ci assumes R is modified by CSP or intruder, so R is discarded and requests for fresh record.

4. RESULTS AND ANALYSIS

The above mention algorithm has been implemented within the Eucalyptus and even the brute force method applied to access the data siting on the database software side did not reveal the secrecy of the data stored in the database. It has not been possible to even locate the partition or gain handle on the algorithm and the key used for undertaking the encryption on the CSP side.

5. CONCLUSION

When application software that uses a database has to be provided as data service to multiple users through virtual machines, the issue of Multi-tenancy arises. The data can be attacked by the users due to the reasons of multi-tenancy. One user can attack other as both the VM related to the clients are situated on the same server. Therefore it becomes necessary to implement methods / Mechanisms that help in protecting the data when the same services are provided to several users. Data isolation is the key to protect the data which can be achieved through locations and the partitions of data related to a specific user on a different physical

machine or in a completely different location on the same physical machine. More complex but simple to implement system can be achieved through double encryption carried on the customer and cloud side. The key and the encryption algorithm are selected dynamically using the reference data.

REFERENCES

[1] M.Saraswathi, Dr.T.Bhuvaneswari, "Multitenancy in Cloud Software as a Service Application", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol3,issue11, page 1-4,2013.

[2] K.Venkataramana, Prof. M. Padmavathamma, "Multi-Tenant Data Storage Security In Cloud Using Data Partition Encryption Technique". *International Journal of Scientific & Engineering Research*, vol4,issue7,page1-5,2013.

[3] Hussain AlJahdali, Abdulaziz Albatli, Peter Garraghan, Paul Townend, Lydia Lau, Jie Xu, Multi-Tenancy in Cloud Computing, *IEEE 8th International Symposium on Service Oriented System Engineering (SOSE)*, doi.org/10.1109.SOSE.2014.50,page1-9,2014.

[4] Bhawna Sehgal Er. Jasbeer Narwal, "An Analysis of Performance for Multi-Tenant Application through Cloud SIM", *International Journal of Emerging Research in Management &Technology*,vol4 issue6,page1-5,2015.

[5] Goikar Vandana T., Jagdale Supriya K., Parade Priya B., Pawar Sumedha D., "Improve Security of Data Access in Cloud Computing using Location", *IJCSMC*, vol4 issue2, page1-10,2015.

[6] Tengfei Li, Liang Hu, Yan Li, Jianfeng Chu, Hongtu Li, and Hongying Han, "The Research and Prospect of Secure Data Access Control in Cloud Storage Environment", *Journal of Communications*, VOL 10,ISSUE 10,PAGE 1-7,2015.

[7] Manjinder Singh, Charanjit Singh, "Multi Tenancy Security in Cloud Computing", *International Journal Of Engineering Sciences & Research Technology*,Vol 4,Issue 116,Page 1-7,2017.

[8] Katie Wood and Dr Mark Anderson, "Understanding the complexity surrounding Multitenancy in cloud computing", *Eighth IEEE International Conference on e-Business Engineering*, 10.1109/ICEBE.2011.68,2011.

[9] http://www.gartner.com/id=2058722.

[10] K. Wood, M. Anderson, "Understanding the complexity surrounding multitenancy in cloud computing", *Eighth IEEE International Conference on e- Business Engineering*,VOL1,PAGE NO 119-124,2011.

[11] Paul Feresten, "Storage Multi-Tenancy for Cloud Computing", *SNIA*,2010.

[12] W. Tsai, Q. Shao, "Role-Based Access-Control Using Reference Ontology in Clouds", *Tenth International Symposium on Autonomous Decentralized Systems*, VOL 11,PAGE 121-128,2011.

[13] Mohamed Almorsy, John Grundy, and Amani S. Ibrahim, "TOSSMA: A Tenant-Oriented SaaS Security Management Architecture", *IEEE Fifth International Conference on Cloud Computing*, PAGE 1-9,2012.

[14] S.Kamara, Kristin Lauter, "Cryptographic cloud storage", *FC'10 Proceedings of the 14th international conference on Financial cryptography and data security*, PAGE 136-149,2010.

[15] Jose M. Alcaraz Calero, Nigel Edwards, Johannes Kirschnick, Lawrence Wil cock, and Mike Wray, "Toward a multi-tenancy authorization system for cloud services", *IEEE Security and Privacy*, PAGE 48-55,2010.