Securing Multi-tenancy systems through multi DB instances and multiple databases on different physical servers

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 Nov 7, 2018
Accepted Nov 21, 2018

Keywords:

Cloud computing
Multi-tenancy
SaaS
Shared data services

ABSTRACT

Use of the same application by multiple users through internet as a service is supported by cloud computing system. Both the user and attacker stay in the same machine as both of them are users of the same application creating an in-secure environment. Service must ensure secrecy both at the application and data layer level. Data isolation and Application isolation are two basic aspects that must be ensured to cater for security as desired by the clients that accesses the service. In this paper a more secured mechanism has been presented that help ensuring data isolation and security when Multi-tenancy of the users to the same service has been implemented.

Corresponding Author:

M Trinath Basu,
Department of Computer Science and Engineering,
KLEF University, Vaddeswaram,
Guntur District, India.
Email: miriiyala68@kluniversity.in

1. INTRODUCTION

Cloud notated service whether it comes to software, platform or infrastructure can be availed on demand through cloud computing systems hosted by service providers. Software as service (Saas) is one of the service model offered by the cloud computing service providers (CSP) through various application software packages can be made to be availed by the customers as services. The services can be availed by directly referring or acquiring the same through Virtual Machine. Several users who are given the access to the same VM can share the same application hosted by CSP. The users who are given with the access to the same application will share the same database. Several users who are in the same physical environment can encroach and attack each other spoiling each other’s processing or data and both. A Service provider makes available several Virtual machines of the same physical machine to one or more users.

The resources which are attached to different machines can be allocated to each of the virtual machine on sharable basis. Hypervisor installed on Physical machines manages all virtual machines. A virtual machine can be assigned to one or more users in which case the applications that are assigned to a VM can be shared among several users. The users also share the databases that are connected to the application access of which is given to several users. When several users are given access to the same application which is assigned to a virtual machine, then such a system is called multi-tenancy system [1]. Users are quite concerned amount the secrecy of the data and software stored in an unknown infrastructure hosted by CSP. The users of a multi-tenant system use the same data bases accessed by the application creating a risky environment making it possible for each user to attack the data of the other.

The users have no control on the data the moment the same is placed in a cloud. The users as such cannot monitor or control the way the data is stored and accessed on the cloud. A virtual machine is a software realization which is configured through a chosen operating system and any other program as desired by the user. On VM either user developed or CSP provide software can be made to run through user requested configuration. Resources that are attached to several physical machines are allocated to the VM. Specialized software called hypervisor creates, monitors and controls VMs within a single physical machine. The VMs can be loaded with different application software which can be given with the access by multiple users. VMs are configured with all the computing facilities contained within physical machines. The resources as such constitute CPU, Memory, Storage, network etc. 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 with 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 thereby 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. 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 of the 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 that 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-tenancy which includes Virtualization, 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 Application hosted on a physical machine needs to access the same database in multiple ways. Database management software, through which the application accesses the database, can be made to be running in either single or multiple instances mode. In the case of a single instance mode the data as such can be organized as a single database, multiple partitions or user spaces in the same DB, Multiple partitions of the same DB made to be resident on different physical machines. Several users' data is accessed through single instance of database management software. The database management software can be organized into several instances; each instance is allocated to a single user there by isolating the users at the application level. The multiple instances can be organized to use a single DB, multiple DBs on the same machine and many machines respectively. The arrangements are shown in Figure 1.

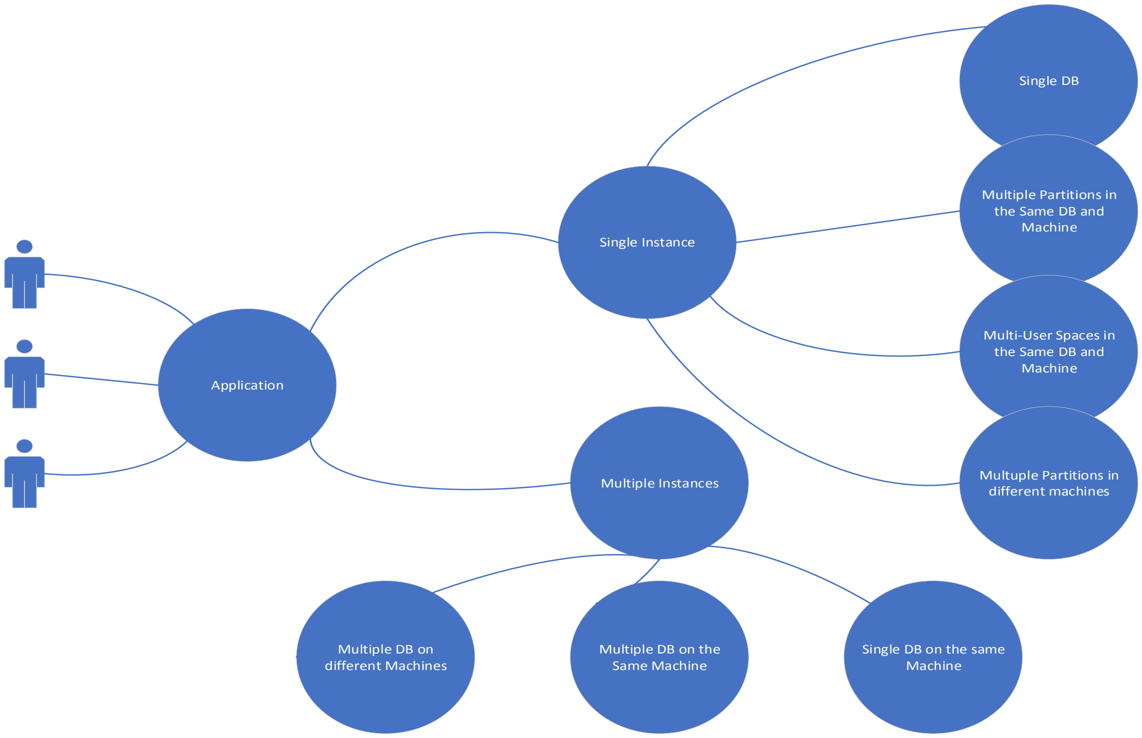
Single DB
Multiple Partitions in the Same DB and Machine
Multi-User Spaces in the Same DB and Machine
Multuple Partitions in different machines
Single Instance
Application
Multiple Instances
Multiple DB on different Machines
Multiple DB on the Same Machine
Single DB on the same Machine

Figure 1. Data organization mechanisms under cloud

Each of the data arrangement has the strength of enforcement of data isolation at a specific level. In this paper ensuring the secrecy through multi-instances and multiple databases situated in different machine has been presented. This approach gives high level of secrecy both at the application and the data level even though the method is costly due to running of multiple instances of DBMS software on the same machine. 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. 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 [3], [2]. 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. More number of issues arises due to Multi-Tenancy for simple 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 mean 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 attacker 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 defenses as such cannot protect the data that is attacked within the purview of a physical machine. Many issues are to be addressed when data of multiple users is stored within the same repository. Mechanisms are to be introduced such that the data and the application are secured from user's perspective. 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 in multi-tenancy is to allow an application to be executed in single machine where it has to be connected to a single data base which is working in a same virtual machine so that we can 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. 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.* [4]. They have covered both consumer and enterprise scenarios and they have used nonstandard encryption algorithms such as searchable encryption and attribute encryption.

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. An algorithm that uses user attributes and their signature has been presented by Zarandioon*et al.* [5]. 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. 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 geo location of the data where it has been stored. Many methods have been presented in the literature that aims at isolating data storage, allocating separate data storage for each tenant etc. [6] Each method releases a different security issue altogether that involves use of different types of encryption techniques. 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.

Access control is one of approaches that can be enforced to prevent unauthorised 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 [7]. 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 [8]. Have presented a comparison of the attribute based encryption (AES) of the data to be stored in the cloud [9]. However the methods will be directed towards achieving the access controlling of the data than dealing with issues related to multi-tenancy. [10] 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. 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 [11].

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. 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 [12]. 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. 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 [13]. 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.

Manjinder Singh *et al.*, [14] 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. 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. Wood et al, [15] 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. 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.

3. INVESTIGATIONS AND FINDINGS

Many approaches have been presented in the literature for securing the data in a single database in which the data related to different customers has been stored and processed by a single application. All the approaches used for dealing with the data 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. There are many techniques that can be used to segregate the data such that very high level of data isolation can be achieved. Both the application level and data level isolation when achieved will make the entire multi-tenancy system to be fully secured from the perspective of all the users. Application level security can be achieved through suing several instances of the DBMS software and allocation each instance to each user. Making available multiple instances of the DBMS software is quite expensive but will provide high level of security. Creating several databases each operated through its corresponding DBMS instance gives very high level of data isolation. The isolation level will further increase when the databases are situated in several physical machines. The databases in this case are physically distributed. The arrangement of multiple instance of DBMS software and the data is shown in the Figure 2.

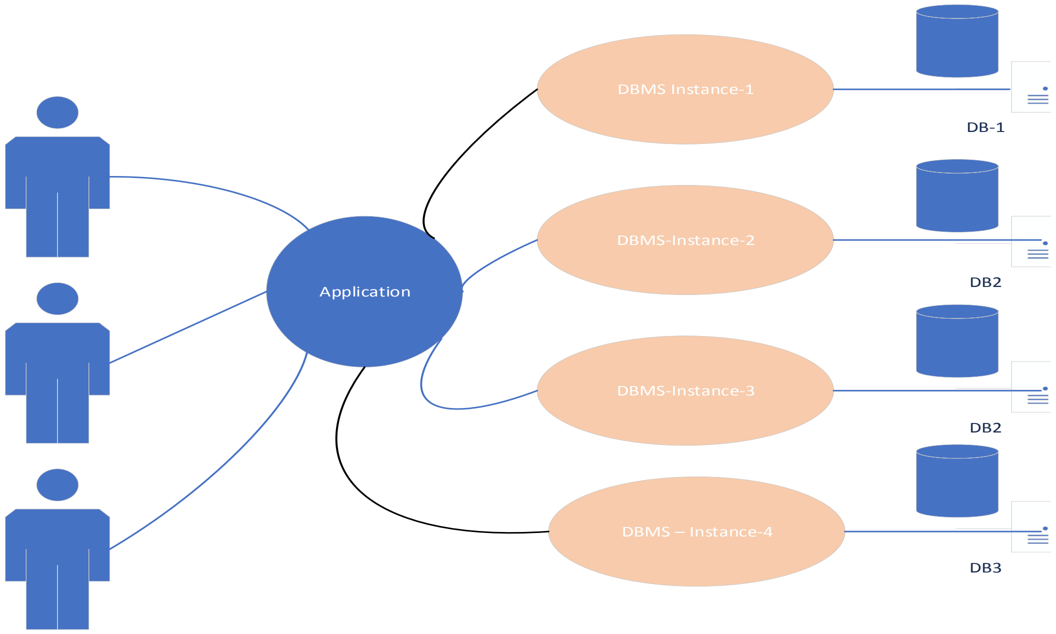

Figure 2. Multi user spaces segmented database working under SaaS

Each of the databases is recognized by the IP Number of Physical machines on which DB is created. Every user identified by the cloud computing system using some kind of ID which is assigned by cloud computing system. When a user makes a request for a VM to run a SaaS service the hypervisor shall make a request to the application to create a database on different server on which no other database is created. The application server is also guided to create a spate instance of DBMS software and then attach a newly created database on a different machine. Thus the Instance and the database are binded tightly. Thus the user, instance and DB are completely inter-linked tightly. An encryption algorithm is dynamically selected on the CSP side based on the Name of the instance and the IP address of the physical machine on which the DB is created. A hash is developed using the name of the instance and IP address and the hash is indexed into encryption algorithm using a lookup table. Similarly, on the User side an algorithm for encryption is chosen based on either a lookup table or dynamically selected based on the combination of public key pair of the user and CSP. The method is based on double encryption both on user side and CSP side and the data is decrypted only on the user side. The key and the encryption algorithm are used to encrypt the data on the user side before it is transmitted to the VM concerned based on the logical port number provided by Cloud computing system at the time of registration of the user. The cloud computing system uses its own public key and the encryption algorithm selected based on the name of the user space and encrypts the data before it is written to the concerned user space. These methods ensure the isolation at the application level and data level. Within the Application level a thread is created for each of the user for transporting the data either way there by ensuring the application layer isolation. 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.

3.1. Algorithm

Initialization process

1. Client request for an instance and a database is sent to the Hypervisor
2. The application running on the VM will create an instance of the DBMS, locates a physical machine and then creates the Database on the chosen Physical machine. A bonding is established between the Application, DBMS instance and the Database
3. A hash value is generated based on the name of the instance and the IP number of the physical machine on which the DB is created. The hash value is indexed into the kind of Encryption algorithm that must be used for data encryption on the CSP side. A different encryption algorithm is selected every time hash indexing is done.
4. Public key pair generation is done on the CSP side and the public key of the User is exchanged
5. The user ID, Key and the encryption algorithm are stored along with user ID within the cloud

Client-side process

1. Tenant ‘Ci’ generates a large Prime Cp from his own credentials generally using his own ID and sent to Cloud Service Provider.
2. Tenant Ci computes N=2*Cp
3. Tenant Ci generates Cyclic group ZN* of order Ø(N) (Euler Quotient function)
4. A subgroup ZØ(N)* subset of ZN* of order Ø(Ø(N)) is generated by Ci with generator g ∈ Zn*
5. 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*
6. Tenant Ci Computes N= Cq* Cr
   Ci chooses ‘e’ such that gcd (e, Ø(N)) =1
   Ci determines ‘d’ such that ed≡ 1 mod Ø(N)
7. 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>
8. Tenant Ci encrypts the data of each record R(ER) ER= Re mod n
9. Tenant Ci sends ERj to CSP to store in the database Pi.

Processing on the Cloud side

10. CSP fetches the related Encryption algorithm and the key with the help of user ID
11. CSP also fetches the database into which the data must be written
12. The data record received from the client is encrypted again using the key and encryption algorithm
    EER = ERTPb mod n
13. CSP stores ER in user space Pi of Ci

Data storage Retrieval process

14. Tenant encrypts the Primary data using his own key and algorithm and send the same to the cloud along with his own ID
15. CSP receives the primary data and encrypts the same using the key and dynamically selected algorithm which is connected with the instance name and location of the database.
16. CSP fetches the requested record from the related database and through the connected DBMS instance using encrypted primary key data.
17. 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.
18. After receiving Tenant Ci computes R = EERrst mod N to obtain original Record.
19. 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. EXPERIMENTATION AND RESULT

The above mention algorithm has been implemented within the Eucalyptus and even the brute force method applied to access the data did not reveal the secrecy of the data stored in the database. It has not been possible to even locate the database 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 users are using the same application resident 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 creating a separate database on a different physical machine thus achieving booth logical and physical isolation. The application level isolation is achieved through creation of multiple database instances. The method is expensive that more number of DBMS instances has to be created and more number of physical servers is to be used for locating the databases. However, the method is full proves that it secured the data and the application 100%. Double encryption by both the user and CSP ensure using different keys and algorithms ensure complete secrecy. Decryption is done the user side only reviving computational overhead on the CSP side.

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*, vol. 3, issue. 11, pp. 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,* vol. 4, issue. 7, pp. 1-5, 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, pp. 1-9, 2014.

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

[5] 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,* pp. 48-55, 2010.

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

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

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

[9] Goikar Vandana T., Jagdale Supriya K., Parade Priya B., Pawar Sumedha D., "Improve Security of Data Access in Cloud Computing using Location," *IJCSMC*, vol. 4 issue. 2, pp. 1-10, 2015.

[10] Bhawna Sehgal Er. Jasbeer Narwal, "An Analysis of Performance for Multi-Tenant Application through Cloud SIM," *International Journal of Emerging Research in Management &Technology*,vol. 4 issue. 6, pp. 1-5, 2015.

[11] K. Wood, M. Anderson, "Understanding the Complexity Surrounding Multitenancy in Cloud Computing," *Eighth IEEE International Conference on e- Business Engineering,* vol. 1, pp. 119-124, 2011.

[12] Paul Feresten, Storage Multi-Tenancy for Cloud Computing, SNIA, 2010. Mohamed Almorsy, John Grundy, and Amani S. Ibrahim, "TOSSMA: A Tenant-Oriented SaaS Security Management Architecture," *IEEE Fifth International Conference on Cloud Computing*, pp. 1-9, 2012.

[13] 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, pp. 1-7, 2015.

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

[15] 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.