Secure Computing of Multi Tenant Using Encryption

Parul Kashyap[1], Rahul Singh[2]

[1]Research Scholar, Department of Computer Science & Engineering, Shri Ramswaroop Memorial University, Lucknow Deva-Road Barabanki UP, India 225003

[2]Assistant Professor, Department of Computer science & Engineering, Shri Ramswaroop Memorial University, Lucknow Deva-Road Barabanki UP, India 225003

***Abstract*— Most recent Computing models aim to provide a firm, moneymaking deliverance of patch up to users of these computing models such as grid computing, cloud computing. Infrastructure, software, platform and storage are most delivering services of cloud computing. It is a challenge on the way to Cloud computing for providing security for data of multiple tenant of the identical physical machine in the course of virtualization. In this paper, we focus on database security of multitenancy model using by different organizations. From a security point of view separate database to each tenant is fine, but it is not cost effective, so single database is used by all tenants of the same physical machine. Sharing of database leads to illicit access of tenant's data by another tenant which is a severe violation of security. So to tackle this dilemma we use the cryptography RSA algorithm. In this algorithm we use two keys, public and private for encryption and decryption. This algorithm is occurring on CSP (cloud security provider). After concluding this study we provide more cost effective and secure database sharing among the tenants.**

***Keywords*— Multi Tenancy Model, RSA, Cloud Computing, Data Isolation, Virtualization**

I. INTRODUCTION

The modern era of computing includes large number of techniques, where cloud computing is a valued tool for grid, utility computing. This computing promptly adopted by organizations to amplify their profit altitude. Cloud computing comprises of different IT capabilities basically, three types of services are provided to the customers. Firstly, SAAS (software as a service) which concludes web services. These services require installation, e.g. yahoo Flickr, Google doc, etc. secondly, PAAS (platform as a service) which concludes platform for computing services as websites e.g. API's for Google maps. Thirdly, IAAS (infrastructure as a service) which concludes infrastructure as a services e.g. Amazon EC2 [1]. SaaS of cloud computing consists of a number of applications which can be grouped into development models contains a variety of characteristics: configurability of metadata, scalability, and multitenancy [2, 3]. The first development model characteristics specify that dealer provides different instances of different customer, but all the instances use the identical code. The customer can change their instances as per their need. In the second model of development specify that individual customer has its own individual instance software. This model has some security issues, but less compared to other models. Lastly the multitenancy characteristic of development model serves identical instance to all the customers of requesting the services[4, 5].

There are large numbers of features presented by cloud like elasticity, metered service, on demand service, broad network access which gets shared by no. of users of organizations which leads to an important building block element called Multitenancy http://www.cloudsecurityalliance. Multitenancy feature works at all layers of cloud. At IAAS layer infrastructure gets a share, whereas at the SAAS database of tenants are sharing. The Multitenancy helps to find out the operations and service provided to or for the tenants. The main aim of multitenancy is to take advantage of associated economy of extent which translates into the stash for the end user. The viable nature of cloud computing is lowering the rate of investment in its sector. By introducing multitenancy factor, it is sinking the rate of investment. Multitenancy is just like a college which covers up various departments. Each department contains teachers, students each get distinguished by their unique identification in an archetypal multitenancy circumstance, customers become tenants and are provided with a point of control to make friendly hardware and software to able bodied their specific requirements. But this multitenancy feature also introduces some set of security issues which causes serious problem to plan maker and cloud service providers. As the database share by the tenants for storage it limits its usage and increases its security issues. For this we have to use a secure architecture of Multitenancy where each tenant separated with other tenant from security point of view. Database, virtual segmentation, virtual machine, etc. should secure to reduce its ill effect on tenants[5].

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. SECURITY ISSUES OF MULTI TENANT

Multi-tenancy [6] consists of running a large number of application which causes a physical server partitioning and process customer demand with virtualization. This virtualization enables to share processor, memory, input output. Through virtualization, a physical server divides in number of virtual machines http://www.microsoft.com/technet/security/bulletin/ms07-

049.mspx. These VMs also requires integrity in different fields for security purposes. The expertise difficulties of multitenant model include:

Data isolation- data of the different virtual machines belongs for holding data of users should not mutually interleave.

Architecture extension- the demand of customers increases or decreases as per demand so, the architecture should be flexible and scalable.

Configuration self definition- means that cloud computing should support unusual customers significant disturb on its once-over proposal configuration.

Performance customization- various customer demand guaranteed to fulfil under different workload on the performance of the multitenant model.

For any modern technology data security is the major dispute. This dispute become more difficult when it deals with the SAAS users which totally relay on security [7-9] .In this paper issue related to data isolation get discussed. Data of different virtual machines should not be interleaved with other virtual machines for the level of security. Because when customer arises for fulfilling their demand they should firstly focus on their data that in what place it going to store. For security reason data storage is also an important subject. For providing security for data, it should be provided at the level where all data resides. These levels are shown in figure 1-

Fig.1 Levels of Data

Segregations of data among tenants- refer the willingness of tenants to share their data or not.

Security at the virtual level- It is the level where flexibility from the point of storage requires on demand and also attached to the instances in a flexible manner. E.g. Amazon elastic block in Amazon EC2 instances. Here data is encrypted to maintain its integrity for their legitimate VMs users.

Security at client level- This layer protects data from legitimate users who may have further secretarial rights in the cloud policy for assorted supplementary reasons.

Security at function level- This layer is hassle free from protection techniques. Less no of attacks occurring at this level, so it requires less fined grained security techniques http://www.microsoft.com/technet/security/bulletin/ms07-049.mspx..

This paper basically on data isolation among the tenants that how one tenant data, isolate from other tenant and where it store.

III. PROPOSED WORK

In Multitenant application data isolation of tenants is a great issue. So, for security purpose separate database grant to each tenant, but it is less cost effective and time consuming. To reduce these entire consequences single database is the best step. Where each row store tenant data with their tenant's id, each row get separated by its id. In this surrounding area, security concerns dart high that misconfigure application code or an inaccuracy in an admittance control list may put tenant information in the danger of thievery and use wrongly. For scheming access to database data, there are reasonably a small number of tools and technologies available. The new applications implemented is use for validation and approve of the access request so that only firm rows or fields are changeable based on security policies that guarantee access is defensible. In this way the cost and time of implementing database get reduces. But still there is some possibility of data leakage of tenant by another tenant. To recover from this insecurity we use the concept of cryptography. Cryptography is the technique through which encryption/decryption of data gets performed. The RSA algorithm is one of the best algorithms of cryptography.

IV. METHODOLOGY

RSA is extensive using Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who foremost perceptibly described it in 1977. Basically RSA is a block cipher in which every request arising from the user is matched up with the integer. RSA consist of two keys public and private key, public key is to encrypt the data whereas private is used to decrypt the data. The public key is known to the user and service provider and private keys hold by the user or tenant for decrypting the data which he encrypted with the public key. As the different key used for encryption and decryption so, it provides more security to the data compare to other cryptographic techniques. In our proposed work, we are using RSA algorithm to encrypt the data of tenants before store in database. By this only who is authorize can only access the data[10]. There are sequences of steps for providing security in the database in figure2:

Step1- firstly, when data arise from the tenants for storing in a database, it passes from cloud security provider (CSP) where it encrypted using the RSA algorithm.

Step 2- At CSP public key and private key generates by RSA. Using public key data encrypts, this public key is known to CSP and the tenant.

RSA algorithm involves three steps-

1. Key-generation
2. Encryption
3. Decryption

RSA ALGORITHM:

Key-generation-

1. Select a and b (a, b prime no. randomly of similar bit length).
2. Compute n = a * b.
3. Calculate Ø (n) =a*b where Ø (n) is not equal to 1.
4. Select an integer e such that 1 < e <Ø (n) and greatest common divisor of me, Ø (n) is 1.

   Now e is released as Public-Key exponent.
5. Evaluate d = e-1(mod Ø (n)) i.e., d is the multiplicative inverse of e mod Ø (n).
6. D is kept as Private-Key components, so that d * e = 1 mod Ø (n).
7. Public-Key= (e, n)
8. Private-Key= (d, n)

Encryption-

1. c= me (mod n)

Decryption-

1. m= cd (mod n)

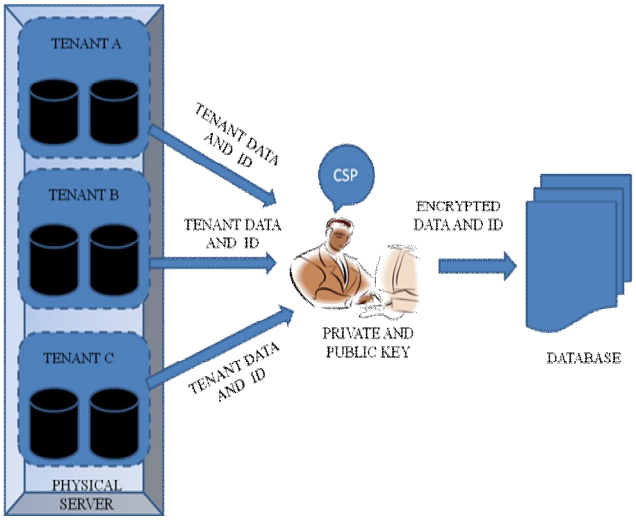

Fig.2 Proposed Model

Step 3- After encrypting data CSP move encrypted data forwards to a database where encrypted data get stored with tenant id.

In this way when tenant presents its data to store in database, CSP encrypts data using public key which generates by implementing the RSA algorithm. This public key known to the tenant and CSP, both, but when decryption request arises data get decrypted using private key which is known to tenants only.

V. Conclusions

For on demand service cloud computing is still a new paradigm. When the organization decides to move a cloud for their flexibility, control of data has become a major issue. Thus, it requires a specific amount of security so that a trusted environment can maintain in the organization. Multi tenancy is one of the intrinsic aspects of cloud computing which provides many benefits to the users in the stipulations of resources but it also contains security issues. Therefore, in this paper, we proposed the way of providing security to the users of a single database. RSA is one of the preeminent techniques of cloud computing, which cover up this security issue by encrypting data of the database before storage.

Acknowledgment

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings

References

[1] J. G. Walz, D A. , *"Time to Push the Cloud,"* IEEE Computer Society, September/October 2010.

[2] J. Ju, Y. Wang, J. Fu, J. Wu, and Z. Lin, *"Research on Key Technology in SaaS,"* IEEE Computer Society, pp. 384- 387, 2010.

[3] C.-P. Bezemer and A. Zaidman, *"Multi-tenant SaaS applications: maintenance dream or nightmare?,"* In: Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), Antwerp, Belgium. ACM New York, NY, USA, pp. 88- 92, 2010.

[4] F. Chong, G. Carraro, and R. Wolter, *"Multi-tenant data architecture,"* Journal of Internet Services and Applications pp. 11-13, 2006.

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

[6] J. Chea, Y. Duanb, T. Zhanga, and J. Fanaa, *"Study on the security models and strategies of cloud computing,"* International Conference on Power Electronics and Engineering Application, 2011.

[7] J. W. Rittinghouse and J. F. Ransome, *"Cloud Computing: Implementation, Management, and Security,"* CRC press Taylor & Francis Group 2009.

[8] S. Subashini and V. Kavitha, *"A survey on Security issues in service delivery models of Cloud Computing.,"* Journal Network and Computer Application, vol. 34, 2011.

[9] J. Viega, *"Cloud Computing and the common Man,"* IEEE Computer Society vol. 42, pp. 103-108, 2009.

[10] P. Kalpana, *"Data Security in Cloud Computing using RSA Algorithm,"* International Journal of Research in Computer and Communication technology, vol. 1, 2012.