Study on Multitenancy security in Cloud Computing

Deepti Dave[1],
[1]*Senior Faculty-IT, iNurture, Bangalore, India*
Ajeenkya, D Y Patil, University.

Abstract **-** Security within the cloud is of utmost importance as the interest and indeed utilization of cloud computing techniques has increased with time. Specifically, Multitenancy has introduced exceptional security risks to cloud computing as a result of many tenants using the same physical computer hardware. The motive of this research paper is to present an over view of some of the specific risks, arising in cloud computing due to multitenancy.

Keywords **-** Cloud computing, Multitenancy and Cloud security.

I. INTRODUCTION

Cloud computing attributes to services along with applications that executes on a distributed network utilizing virtualized resources and accessed by common Internet protocols and standards, related to networking. It is distinguished by the fact that resources are limitless and virtual; and that particulars of the physical systems on which software runs are abstracted from the user.

Some of the big sharks in cloud are Amazon and Google, who have captured prominent place in cloud market. Cloud computing states to a model for enabling suitable, on-demand network access to a shared pool of configurable computing assets. These resources can be rapidly allocated and released with trifling management effort or cloud service provider interaction. The mainstream service provider provides multitenancy to capitalize on the associated economies of scale which also translates into savings for end user. Due to competition in cloud market, cloud service providers have to lessen the total cost of ownership of their IT infrastructure, thus introducing multitenancy a prominent way to minimize total cost of ownership.

Cloud computing comes with huge advantages to the organizations, but moving from conventional storing to cloud computing is not an easy task. This paper elaborates on types of clouds, its benefits, multitenancy and its challenges. Fig.1 denotes the cloud computing features, which uses the Internet and remote servers to preserve data and applications.

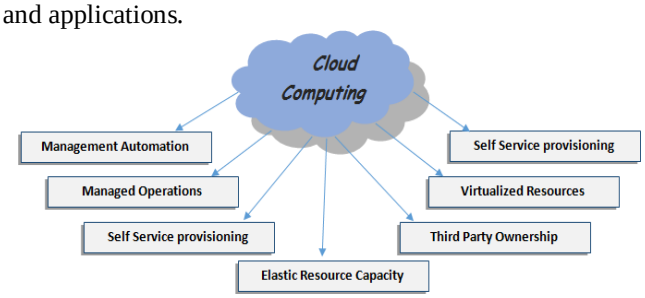

Figure 1: Cloud computing features.

II. MULTITENANCY

Multitenancy refers to the practice of engaging multiple tenants on the same physical hardware to cut down costs to the user by leveraging economies of scale. Tenant is a user on the cloud. Though, through multitenancy cloud cost has been reduced but it has introduced various security risks, which is still yet to be fully acknowledged as a serious problem by cloud service providers and policy makers. This paper illustrates the risks associated with multitenancy and actions which can be taken mitigate them. Fig. 2 depicts three different database designs used for attaining multitenancy data architecture [1].

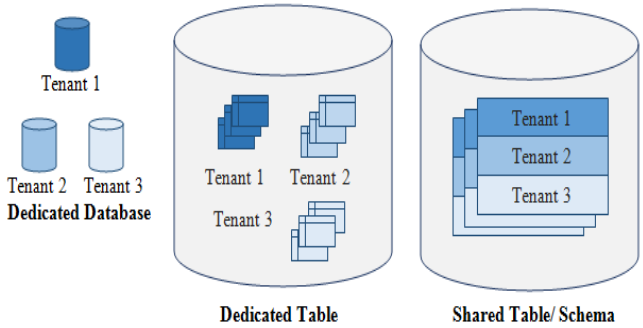

Figure 2: Multitenancy

A. Dedicated Database - Dedicated database approach allocates a new database for every novel tenant. To attain isolation, separating tenant data in different database is the modest method. It will allow users to expand their database of their choice if their storage logic permits for it. The main downside of this architecture is its costs for hardware and maintenance. Moreover, this architecture helps for those clients that require good data isolation and also when the number of clients are limited.

B. Dedicated Table - Dedicated schema approach comprises of keeping all tenants in a single database and detaching every tenant by creating a separate schema for its tables. As a result, every tenant will have its own set of tables within the same database. The advantage of using this schema is that it keeps the hardware cost less by utilizing the same database for all tenants.

C. Shared Table/ Schema - Shared Table technique includes storing all tenants' data in the same database using the same schema for all tables. For identification, a separate column is present to associate each record with its own tenant. The name given to that column is **TenantId** and with the help of foreign key, it points to a specific tenant. The benefit of this architecture is the low hardware cost.

Todays need is to provide facility of multitenancy with the provision of security.

Virtualization + Resource Sharing = Multitenancy. (1)

Equation 1 represents that to implement multitenancy, both virtualization and resource sharing is required by cloud service provider.

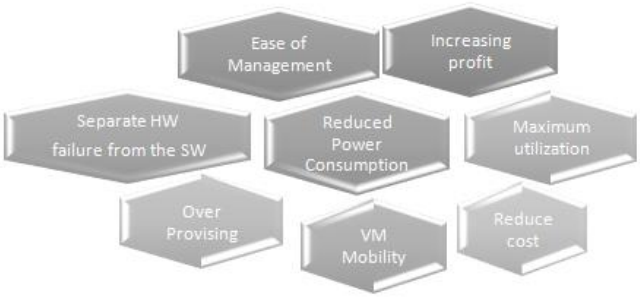

Figure 3: Benefits of Multitenancy

Fig 3 depicts possible aids of multitenancy. These aids are co-related to either virtualization, resource sharing or by involving both of them. For example, splitting the hardware failure from the software failure is attained by virtualization. While, sharing the resource will enhance the utilization which will lead to a lessening in cost by making the resource available for many customers.

III. MULTI-TENANCY SECURITY CHALLENGES

In multitenancy, both the attacker and the victim share the same server or physical machine. Such a setup cannot be eased by conventional security methods, as it is not designed to penetrate inside servers and their monitoring procedures are restricted to the network layer [4],[5].

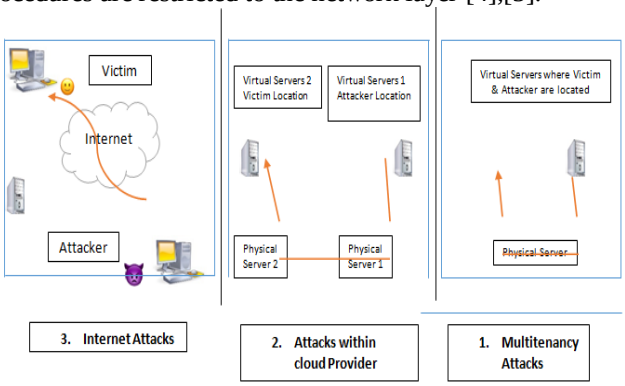

Figure 4: Comparison between Multitenancy and conventional cases.

Fig. 4 illustrates different scenarios of intruder and victim locations and networking among them. In the first case, the attacker and the legitimate user both are regular Internet users. In this case, the conventional network security techniques are efficient enough to defend against any attack. In second scenario, both attacker and the victim are customers in the same cloud provider but each one of them is located on a different server. This type of structure is due to the utilization of the virtualization layer in the cloud computing model; to secure such a setup, virtual network security devices and techniques must be implemented by cloud providers.

The third scenario defines where both the victim and the attacker use the same cloud and share the same server. This is the same scenario of multitenancy. Achieving security in such a system is not an easy task, as network communication between the attackers VM and the victims VM is limited within the physical machine. Hence, traffic will not leave the physical machine, which is harder to be mitigated by virtual network security defenses as opposed to case two.

IV. CONCLUSION

In cloud computing environment, multitenancy means users and firms share same infrastructure and databases. Also the major plus point is of reduced price and high performance. Tenants can share hardware on which their virtual machines or servers run, or they may even share database tables where the data of customer X is on one row and that of customer Y is on another. Security measure must be implemented so that tenants do not pose a risk to one another in terms of misuse, privacy violation or data loss. Multitenancy protections from attackers must be provided by cloud service providers through all layers of cloud i.e. IaaS, PaaS, SaaS.

V. REFERENCES

[1]. https://medium.com/@MentorMate/increase-efficiency-with-multi-tenant-cloud-software-architecture-4261fca6025e. Accessed on 10/5/2019.
[2]. "Multi-Tenancy in Cloud Computing", IEEE 8th International Symposium on Service Oriented System Engineering, Hussain AlJahdali, Abdulaziz Albatli, Peter Garraghan, Paul Townend, Lydia Lau, Jie Xu, School of Computing University of Leeds Leeds, United Kingdom, 2014.
[3]. "A Survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, S. Subashini, and V. Kavitha, 2011.
[4]. "Information flow control in cloud computing", Ruoyu Wu, Gail-Joon Ahn, Hongxin Hu, and Mukesh Singhal, (9- 12 Oct. 2010).
[5]. "Monitoring a virtual network infrastructure," Augusto Ciuffoletti, (October 2010).