Multi-tenancy and Logical isolation

Ashwini kumar[1], Prof.Barnali Chakraborty[2]

[1] PG Student, Department of Computer Application, AMC Engineering College Bengaluru, Karnataka, India
[2] Professor, Department of Computer Application, AMC Engineering College Bengaluru, Karnataka, India

ABSTRACT

Shared working is of very much importance for the organizations because it will be cost effective for them due to the flexibility and availability of multiple resources. Multiple providers into the business of share platforms which will be provided to the Global clients but we have recognized that when the multi tenancy references of the software architecture is being used it will have multiple types of security issues. A single instance of the software runs on to the server and with the help of this multiple users can utilize it so in this perception multiple types of security issues has to be properly identified.

Effective security solutions should be stated by the cloud providers and the vendors those were associated on to the podium to provide the services because now multiple parallel accounts of multiple users has to be maintained. In paper we are discussing all types of associate head security difficulties which are related with the multi tenancy architecture and how effective security solutions to be stated by the service providers.

Elaboration in reference to the security types is stated which will help us the advance attack model designs that the substantial security references can be implemented. Multiple new organizations those who are starting up the business require a secured place for performing their operations the reason why the study of multi tenancy security references is quite important.

Keywords: - *logical isolation , security attack models, multi-tenancy, security, cloud*

Introduction

When any type of service platform is being designed it will be having all types of services that it will be providing it to the customers, multiple new organizations are having the requirement of real time working platform so that they can do their activities properly with cost effective control. The service providers are required to provide various types of services from a service platform the reason why the multi tenancy architecture will be used with the instances of the software and utilities will be provided and accordingly multiple account holders will be having the accessibility.

When we are providing the accessibility to multiple users we have to accomplish all types of security references properly because now we have to check the attack models which may affect the working in the real time. When we are providing the shared environments all types of workability will be performed on a single platform but eventually the logic isolation has to be referenced. Multiple possessions which are related with the working for example use a management, instances of utility designing and various types of security perceptions have to be separated logically.

The system of multi tenancy is desperately important for the organizations because they don't require more Complex scenarios of setting up the infrastructure because now built on the real time platform the setups can be initiated on all types of common computing IT services are present. With the help of system applicable the control is very much flexible because all types of controls can be operated from a single system which is much important for the organizations and even any kind of scalability which is needed by the organizations to perform their activity is also supported.

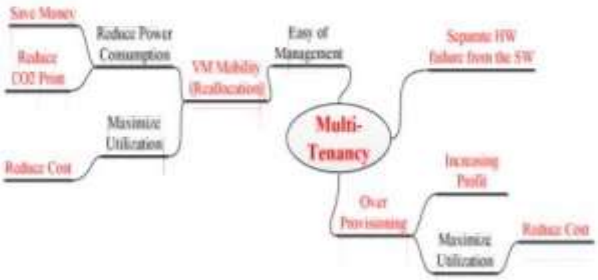

Figure-1

Multi-tenancy optimization

Some of the important advantages of multi tenancy architectures being listed below -

- All the users much comfortable in reference to data management because they don't require into which will hardware for managing their data and all the reference of data will be hosted
- The designs are represented in a way that scalability is maintain so any number of projects and work undertaken which are required will be supported
- It is less expensive because it is on to service version so while paying the service fee the system can services because it will be done by the service provider services because it will be done by the service provider
- Administration and tracking is made easier because not will be done from a single system which will be very much cost affective
- All new technology based resources which are needed are available on to the services term making it easier for the usage
- The billing references will be very much flexible in this model because conferring to the properties which are being used the service providers will be providing the bills so we can say it is flexible for the small industries and for the new startup organizations

Security concerns

Security concerns data related with the service platforms are stated as following -

When the service provision is being used a strict authentication and access control for the safety of the applications which are being secondhand have to applied so we can say that proper knowledge about the authentication and access control should be required for better management and workability when the multi-tenancy architecture is being used

Downtime problems are also recognized because depending to the providers the related resource setups if not done properly and when multiple users are utilizing the same case of the software it may turn in more down times

Security breach is also important problematic for the data leak because if all types of perception understanding is not done properly then the hackers can break up to the system and the related information will be compromised

Literature review

Attack Models

Various types of attack model references are identified in reference to the facilities which are provided by cloud providers and these are designed in a method that it will compromise to the security. Multiple types of security considerations and concerns are being recognized because now various types of attack models are design to get into the system for the data breach.

When the attack model farming design it will be for compromising the software facilities that been provided and to exploit the security mechanism which is being implemented. The cloud providers are required to be associated with updated references of understanding about the attack models so that the services can be properly optimized.

Few of the basic references of attack models associated are listed as following

Data breach attack

When weak encryptions are being used unauthorized access of the sensitive data can be acknowledged with the help of database attack models, the hackers can break the encryptions and the data will be compromised

Denial of Service (DoS)

Illegitimate request will be referenced in such a manner that cloud services will be having the downtime and the performance of the system will be degraded. Excessive consumption of the resource references will be reference to disturb services used by the cloud providers under this attack model

Malware and Code Injection

Multiple types of malicious codes will be injected within the cloud platform by the hackers and in this way they will be getting the access. Under this system on authorized access of multiple sensitive data on cloud services will be acknowledged. The services will be also disturb with the support of this attack because now the access will be transferred to the hackers and they can manipulate the activities

Identity and Access Management (IAM) Attacks

Under the cloud services multiple types of users will be having the privileges to work but with the help of identity and contact management the credentials of individuals will be on the risk, individual rights that are been provide it will target and accordingly the access for the crowd platform will be gained by the hackers

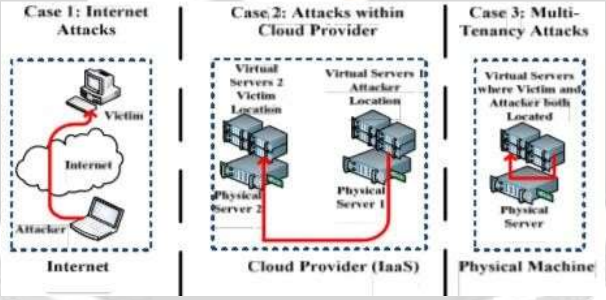
Case 1: Internet Attacks
Victim
Internet
Attacker
Internet
Case 2: Attacks within Cloud Provider
Virtual Servers 2 Victim Location
Virtual Servers 1 Attacker Location
Physical Server 2
Physical Server 1
Cloud Provider (IaaS)
Case 3: Multi-Tenancy Attacks
Virtual Servers where Victim and Attacker both Located
Physical Server
Physical Machine

Figure -2

Different scenarios

<u>Related work</u>

In terms of application instances, sharing various types of resources through the cloud and government will be extremely cost-effective and efficient; however, it must be properly implemented for resource and work load management. When sharing resources in a cloud environment is required, the references of request and Threads must be properly acknowledged (Momm and Krebs, 2011).

The proper aspects of resource allocation, load balancing techniques, and scheduling in need to be integrated in order to properly identify the security concerns and the related head multitenant cloud system. Lee, J., S. Kim, and H. Park 2019)

Access control must be properly recognized so that the security mechanism can be properly established and the users should not face the problem in real time. Multiple types of security concerns are stated within a cloud based on data isolation based on vulnerability and based on 2020)

Experimental analysis

The service providers are required to identify all types of cross tenant attacks on the cloud environment and according the related controls has to be managed. All types of related working requested standards should be identified an accordingly the user should be updated for the provisions of working when they will be provided with the account on to the system.

Secured Communication protocols and high-end encryption algorithms will be utilized within the system so that all across the communication the users and all types of data that will be hosted by users will be having a high-end security. All types of information transfer which will be done on the cloud platform should be encrypted and this way the related references of tracking the date a can be minimized

Various types of factor authentications will be included for the accessibility so we can say that initial techniques and multiple types of security setups will be utilized. The Gateway security factors and multiple authentication factors can included so each and every user related to the organization for the cloud related working will be authenticated properly. OTP references will be channeled and in the same way multiple types of layers of authentications will be highlighted making it easier to manage individual identities within the cloud platform identified. Permissions which are being provided to the users will be regularly identified and will be monitored to check that how the related user is behaving

Data isolation techniques will be used where all the related account holders of the cloud will be isolated from one another. All the related data will be individually organized on to the cloud so that data isolation can be acknowledged.

Data isolation should be properly implemented within the system because now all the account holders can be treated as an individual identity with various types of integrated formulations of policies to be acknowledged

Intellectual property references to cloud to established because this will help us to make sensitive data more managed properly. Any sort of personal information or sensitive data will be checked for the transmission and for the authentications. Any form of payment details or card details should be prevented from the unauthorized transmission on to the cloud platform so we will be using the data loss prevention techniques

Multiple types of auditing and tracking references should be also used by the service providers so that they will be having a basic understanding about the actions that are being achieved on to the cloud platform by the users

Up gradation of the software and all the relative possessions which provided to the users will also help in managing the security because when the security references update within the independent tools it will help the service providers to accomplish a proper scenario understanding

Results

We have recognized that proper type of escalation system should be intended by the cloud providers so that any type of security issues if encountered by the users can be easily rectified. The identification of the safety problems which are being stated by the clients should be properly taken into the consideration.

Proper auditing is also required so that all types of basic formulations of updating the software and providing all types of Identity security references should be easily highlight.

All types of proper management stating to the identity associations and transfer of the data which is being acknowledge with the system is also required to be identified properly by the service providers to provide detailed security.

Multiple types of related updating techniques and encryption references for the data isolation will be utilized by the service providers in this way we can achieve all proper aspects of considerations in reference to the multi tenancy service provisions.

Conclusion

We can conclude that in modern business scenarios when multiple new businesses are arising they require a proper secured cloud references to work and manage their activities, the service provider should be very much concern about the data security and isolation techniques is a must to be followed by the service providers. We can conclude that when numerous types of Identity management references are clearly stated within the system individual identities and users can be easily accomplished and controlled.

We have to use the data isolation techniques in a proper way so we can manage individual account data properly. People references of security techniques connected to the encryptions and multiple types of associated monitoring reports are also required to be established with the aid of this the control on to the unauthorized attacks on the cloud facilities can be minimized.

We should be having a proper response system with the any type of problem arises it can be rectified faster and the blocking of the hackers has to be initialized on a very fast scale so that we can provide a confident working platform to the end users.

can be rectified faster and the blocking of the hackers has to initialized on a very fast scale so we can provide a confident working platform to the end users.

References

1. Title: "Scalability Challenges in Multi-Tenant Cloud Environments" Authors: Chen, H., Liu, G., & Wang, Z. Year: 2019
2. S. Subashini, and V. Kavitha, “A Survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications (2011
3. D. Reed, and D. Silva, “Perspectives on cloud computing: interviews with five leading scientists from the cloud community,” Journal of Internet Services and Applications, vol. 2, no. 1, pp. 2–9, Jun. 2011
4. G. I. Davida, D. L. Wells, and J. B. Kam, “Security and Privacy,” IEEE Concurrency, vol. 8, no. 2, pp. 24–21, 2000
5. S. Pearson and A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing,” 2010
6. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds”, in Computer and Communications Security (CCS), 2009
7. Title: "Performance Isolation in Multi-Tenant Cloud Environments" Authors: Li, C., Wu, Z., & Zhang, J. Year: 2020
8. Hussain AlJahdali, Abdulaziz Albatli, Peter Garraghan, Paul Townend, Lydia Lau, Jie Xu-2014
9. Title: "Data Privacy in Multi-Tenant Cloud Environments: A Systematic Review" Authors: Chen, Y., Wang, L., & Zhang, H. Year: 2017
10. Dimitrios Zissis, and Dimitrios Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems (2011)
11. David Teneyuca, “Internet cloud security: the illusion of inclusion,” SciVerse ScienceDirect (2011).
12. R. Chakraborty, S. Ramireddy, T. S. Raghu, and H. R. Rao, “Assurance Practices of Cloud Computing,” pp. 29–27, 2010