IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 11, November 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 11, November 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0911022 |

Privacy in Multi-Tenancy Cloud

Vaishnavi Waghmare[1], Harsh Khandve[2], Nitin Kamble[3]

Student, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[1]

Student, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[2]

Senior Faculty, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[3]

ABSTRACT: Cloud computing is a new computer technology that allows companies to create their own services by utilizing on-demand IT infrastructures. Although the advantages of cloud computing are numerous, security and privacy issues are the primary roadblocks to widespread adoption. Because cloud service providers (CSPs) are separate administrative organizations, consumers lose direct control over the systems that handle their data and apps when they migrate to the commercial public cloud. Despite the fact that CSPs' infrastructure and management capabilities are far more powerful and reliable than those of personal computing devices, the cloud platform is still vulnerable to both internal and external security and privacy threats, such as media failures, software bugs, malware, administrator errors, and malicious insiders. Furthermore, thanks to hardware virtualization, several users can now share the same physical infrastructure, running their separate application instances at the same time. While this unique multi-tenancy feature boosts resource efficiency, it also introduces new security and privacy issues for user interactions. 3 As a result, we contend that the cloud is inherently insecure from the user's perspective. We can't expect consumers to hand over control of their data and computing applications to the cloud based purely on cost savings and service flexibility unless we provide a robust security and privacy guarantee.

One of the most significant difficulties for the public cloud is multi-tenancy security and privacy, and finding solutions is vital if the cloud is to be broadly used. However, there is currently minimal work that not only solves these issues, but also continuously and scalably maintains the scalability of this dynamic computing environment.

KEYWORDS: Cloud computing, security, multi-tenancy, privacy, management capabilities

I. INTRODUCTION

Cloud computing is now widely recognised as one of the most popular technologies accessible; it is an example of Computing as a Service. Customers who use Computation as a Utility pay for apps, computing, and storage resources on a "pay-as-you-go" basis. Cloud computing is defined as "a system in which a data center's resources are shared via virtualization technology, while also providing elastic, on-demand, and immediate services to users and billing usage as a utility bill."

The advantages of Cloud Computing are accompanied by difficulties to the paradigm; one of the most difficult of them is security. Information security refers to preventing unauthorised access, use, disclosure, interruption, modification, inspection, recording, or destruction of data and information systems. According to a study conducted by the Cloud Security Alliance (CSA), there are seven major risks that businesses will encounter while implementing cloud computing. Cloud Computing Abuse and Malicious Use, Insecure Application Programming Interfaces (API), Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service, and Traffic Hijacking, and Unknown Risk Profile are among the threats. Outsourcing Services, Regulatory Compliance, Data Location, Shared Environment, Business Continuity and Disaster Recovery, Hard Environment for Investigating Illegal Activity, and Long Term Viability are among the seven Cloud Computing security threats listed by Gartner. Furthermore, in a 2008 survey of Cloud providers conducted by the International Data Corporation (IDC) to investigate the obstacles or concerns for adopting Cloud Computing in businesses, security was ranked first with 88.5 percent of the votes, followed by availability, which is one of the information security principles, with 84.8 percent of the votes.

Multi-tenancy support refers to a software instance's capacity to provide services to several parties at the same time. At this post, we'll look at a multi-tenancy authorization system that's good for middleware services in the PaaS layer. The authorization system establishes access control methods for all types of data in all cloud services that use the cloud infrastructure. End users will be able to access each cloud provider's services, and some of these cloud services may be shared with other cloud service providers.

Policymakers and Cloud Service Providers have yet to completely acknowledge data privacy as a serious issue (CSP). This is reflected in the regulations and legislation governing privacy and user protection rights, which, while

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 11, November 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0911022 |

applicable to cloud computing, do not specifically relate to cloud computing. There are currently no discernible guidelines for CSPs to follow. European Union (EU) directives, for example, establish a minimum degree of privacy that must be met by any partner country and limit data movement outside of the EU. At a time when reports imply that cybercrime is one of the most serious security risks, more study is needed to develop more cloud security defences.

The capacity to operate several clients on a single software instance placed on multiple servers is referred to as multi-tenancy. These systems have lately gained popularity as a result of their multi-tenancy characteristics, which allow enterprises to save money while still having access to data and applications. This article discusses some of the difficulties surrounding multi-tenancy, as well as examples of its application and recommendations for improving multi-tenancy security.

In federated cloud environments, CSPs currently use Single Sign-On (SSO) mechanisms to enable authentication and rudimentary authorisation, but fine-grained authorizations are often not supported. Role-based access control (RBAC) has been integrated into NASA's Nebula private cloud system. Traditional RBAC allows for fine-grained access control techniques in clouds, but it does not allow for the management of partnerships. IBM and Microsoft proposed leveraging database schema to share resources in data-centric clouds, but this technique is specific to databases and cannot be used to other types of services. Traditional access control techniques, such as RT and dRBAC, use credentials to securely communicate among collaborators in collaboration models. Because of the presence of centralised facilities, credential management remains a challenge that could be avoided in cloud contexts.

Here, we list many major security concerns, emphasise their importance, and encourage additional research into security solutions that will aid in the creation of a trustworthy public cloud environment.

II. LITERATURE SURVEY

2.1. SERVICE LAYERS OF CLOUD COMPUTING

Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are three types of cloud computing services, as depicted in fig.1.

1. Software as a Service (Saas): The applications requested by consumers are offered on demand in a SaaS platform. Users can access a single instance of the software through the internet. The software is managed and maintained from a central location rather than at the user's node. Because a single piece of software may be shared by multiple users, this form of service is known as one-to-many or multi-tenant architecture. The SaaS platform assures that consumers have access to the most recent software and that they do not have to purchase the expensive software outright. However, because this is a network-based service, the network must be up and operating at all times in order for the user to use it. Google Apps, NetSuite, and Oracle CRM on Demand are all examples of SaaS.

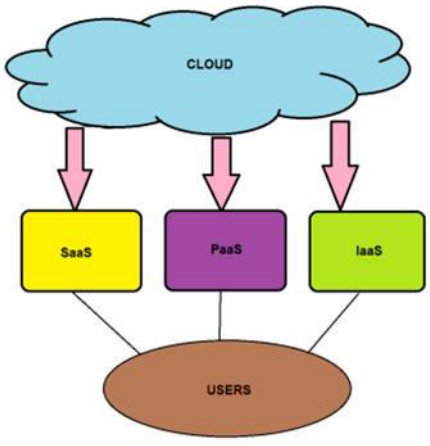

Fig. 1: Cloud Services

2. Platform as a Service (Paas): Unlike SaaS, a PaaS platform provides the user with the full hardware as a virtualized entity, allowing the user to deploy his own applications on the given hardware. PaaS also has a high level of scalability; users can request extra hardware and resources. In a PaaS, the service providers support a variety of programming languages that may be used by the user and ported to other platforms. The user can control his infrastructure using the programming tools given, but he does not have access to the server, network, or host Operating System. PaaS providers include Google AppEngine, LongJump, and others.

3. Infrastructure as a Service (Iaas): IaaS provides a pool of servers, routers, switches, and other devices that are required for application components that can run at high speeds. The user interacts with the infrastructure, which is where the service provider provides the functionalities. It gives you the capacity to process, store, and conduct other

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 11, November 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0911022 |

basic computations on the resources you have. Any software, including operating systems and applications, can be installed and executed by a user. The user is not required to operate the cloud infrastructure, but he or she does have control over the devices and apps (software).

Regardless of the service supplied by the cloud service provider (CSP) to the clients, security is critical. When a SaaS service is proposed, the CSP will host third-party software that all of its clients will have access to. If a malicious user gains access to the software's location, however, the malicious user will have the ability to render the resource unavailable to all other users. Other attacks can also be carried out using the CSP's various services.

2.2. MULTI - TENANCY SECURITY CHALLENGES

Multi-Tenancy in Cloud Computing is distinguished by the fact that both the attacker and the victim share the same server (i.e. physical machine (PM)). Traditional security tactics and measures cannot mitigate such a configuration since they are not designed to reach within servers and their monitoring techniques are limited to the network layer.

To secure such a flaw, we must first address the following question: how is Multi-Tenancy exploited? [12] provides an answer by generating an attack against the Amazon EC2 Cloud to explore data leaks. Network probing is used to carry out the attack, and then a brute force attack is developed to take advantage of the Multi-Tenancy effect by allocating the attacker's VM next to the victim's VM. The findings suggest that an attacker has a 40% chance of allocating his VM beside the victim's VM by investing just a few bucks. After accomplishing Multi-Tenancy, a side channel attack is created to extract the data of the victims. A side channel attack is any assault that takes use of the system characteristics.

Because the type of attack that could be used, such as side channels, cannot be recognised by the hypervisor or even the operating system, any tenant can target its neighbour.

So, while there is no way to completely eliminate the Multi-Tenancy impact while maintaining its benefits, the effect can be lessened, which is what this work is attempting to demonstrate. Multi-tenancy cannot be eradicated, but a clever resource allocation strategy can reduce the danger of Multi-Tenancy; in other words, a resource allocation technique can make obtaining Multi-Tenancy more difficult for customers while still being easily managed by Cloud providers. Multi-Tenancy is intriguing since it requires the attacker to expend effort, time, and money in order to accomplish it for selected victims. As a result, by making Multi-Tenancy difficult for clients to acquire, we are limiting the number of prospective attackers.

2.3 PRIVACY REGULATIONS AND LEGISLATION

Maintaining the levels of data and privacy security required by present regulations in cloud computing infrastructure, as well as complying with cross-border data transmission limits, is a new problem. The lack of standardised privacy and protection standards has caused serious issues, particularly in the deployment of multitenant systems. The issue for the end user is that there may be stringent rules and privacy in their native nation, making them feel safe. However, if data is transported over national borders and stored in the same manner as before, the user may be exposed to privacy breaches without even realising it. Some users, on the other hand, may be afraid to store their data at sites in certain countries because local laws allow access to data for the government of that nation, such as the Patriot Act in the United States. Some regulations, such as those in the European Union, impose restrictions on data mobility in order to prevent organisations from circumventing legislation by sending data across borders.

The European Union's (EU) privacy regulations take a strong and comprehensive approach that has been established and influenced by both public and private sector governments and corporations. A standardised framework arose as a result of contributions and understanding the demands of many sectors, ensuring that privacy codes of practise may be integrated across all industries across the EU. With minimal government participation, firms and industry associations in the United States have been left to design particular industry sector privacy legislation. As a result, rather having a single uniform privacy agreement, more specialised sector-specific privacy law is enforced, such as HIPAA for health agencies in the United States and the Sarbanes-Oxley (SOX) Act for financial companies.

This is a challenge for EU countries, since they prefer to operate within a stronger framework and value data protection and privacy very highly [24]. As a result, the EU considers the US to be hazardous and lacking in the necessary privacy protection requirements. To circumvent these impediments, the United States has adopted the US Safe Harbor Privacy Principles, which aims to ensure that US-based enterprises comply with EU Directive 95/46/EC on personal data protection. However, businesses can choose whether or not to accept this legislation at this time. The Asia-Pacific area is driving technical progress. However, it lags behind the EU and the US in terms of legislation, with the APEC Privacy Framework being an optional best practise rather than a legal requirement. Differences in economies and cultures in comparison to the west have resulted in disparities in practise and attitudes, making it more difficult to build a consistent and possible international privacy legislation agreement. From these three instances of privacy policies and attitudes, it is apparent that more work is needed to ensure that people worldwide may benefit from multi-tenancy stems while remaining safe.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 11, November 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0911022 |

Identity protection is a crucial aspect of any system. When using cloud computing, regulatory compliances regarding data placement and geo redundancy are also important factors to consider. The security of a user's personal, confidential, and sensitive data is critical, particularly in a shared setting. Indeed, Principle 8 of the UK Data Protection Act 1998 prohibits data transfers outside the EU to countries that do not provide appropriate data protection through regulation, with only Hungary and Switzerland designated as providing adequate protection.

III. PROPOSED AUTHORIZATION MODEL: AUTHORIZATION AND ROLE DISTRIBUTION CENTER (ARDC)

The proposed model namely "authorization-role distribution center" is explained in following figures 1 and 2 for multi-tenant architecture in multi cloud environment systems.

The following is the algorithm for authorization and roles distribution center (ARDC) ARDC Algorithm
Step1: Request || N1
Step2: EKA [KS || SLA || Request || N1 || EKB (KS, SLA, IDA)]
Step3: EKB [KS || SLA||IDA]
Step4: EKS [SLA || N2]
Step5: EKB [f (N2)]
Steps 1 to 3: Role Distribution & Steps 3 to 5: Authorization
Authorization system in a Multi-tenancy scenario is explained in the following figure.

3.1. THE OPERATIONS OF ARDC

Multi-tenancy can be achieved across platforms of cloud services using the proposed authorization mechanism. It is presented using two diagrams. Figure 1 shows how to distribute roles and authorizations to end users. In Fig2, a section of the authorization systems in a multi-tenancy system in a single cloud is shown in detail; it may also be applied to several clouds in the same way.

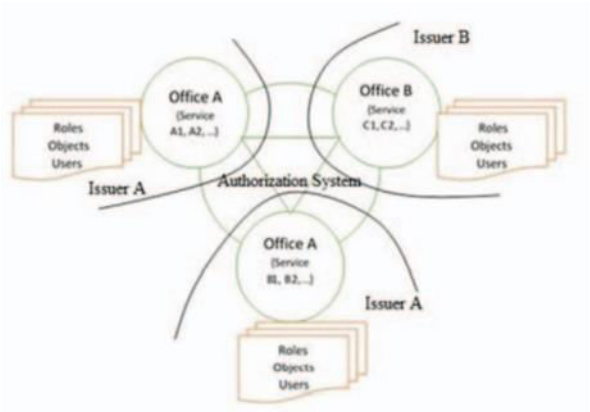

Fig2: Authorization system in a Multi-tenancy scenario

Steps 1, 2, and 3 are utilised in Fig. 1 to spread a user's responsibilities with their approved services (Service Level Agreement - SLA) in a single cloud. If the same service is to be used in another cloud, the next three procedures (3, 4, and 5) are used to obtain SLA from that cloud. This model can also be used to expand multi-tenancy to multiple clouds. The suggested model demonstrates how symmetric key cryptography and Kerberos algorithms can be used to provide multi-tenancy authorization in a multi-cloud system. The multi-tenancy procedure is described in Figure 2, which assumes different parameters for different techniques or privileges. Multi-tenancy in multi cloud systems can be achieved by combining the two numbers into one. Fig1 Cryptographic techniques are frequently utilised in wired and wireless networks for secure communications. Cryptographic keys are used in almost all cryptographic processes, including symmetric and asymmetric cryptography. All cryptographic systems, however, will be rendered useless if key management is inadequate. The management of keys is also an important aspect of security. The goal of key management is to ensure that cryptographic keying materials are handled in a secure manner. Key management

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 11, November 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0911022 |

includes the creation, distribution, and maintenance of keys. The methods for key storage, key update, key revocation, key archiving, and so on are all part of key maintenance. The computational load and complexity for key management in Cloud computing are heavily influenced by the node's available resources as well as the dynamic nature of distributed computing. A typical ARDC procedure (shown in Figure 1) involves a user requesting to access a service from a specific cloud. To verify that requesting users are who they say they are, the ARDC will deploy cryptographic techniques. It will also determine whether a specific user has the authority to utilise the requested service. If the authenticated user passes all of the requirements, including the service level agreements (SLA), ARDC can issue a ticket allowing access to the requested service in exchange for accepting the cloud's SLA. The majority of ARDCs use symmetric key encryption. The ARDC in this example shares a key with each of the other clouds. Based on a first cloud server key, the ARDC generates a ticket. The client receives the ticket and sends it to the cloud server that was defined. The target server can check the submitted ticket against the SLA and give access to the user based on the SLA and the user's identity authentication. Kerberos is one of the security systems that uses ARDCs. Kerberos splits ARDC tasks between two parties: the AS (Authentication Server) and the TGS (Transfer Gateway Server) (Ticket Granting Service). ARDCs frequently work in cloud environments, where some users may have permission to use particular services at some times but not at others. Fig2 In order to control access to resources in a cloud system (as shown in figure-2), an authorization model must first decide if a subject has the privilege to conduct a given action over the controlled object. However, with multi-tenancy support, all users can share the same authorisation service at the same time. The processing system can become with issuer, subject, privilege, and object parameters as a result of this. This can be strengthened by adding another parameter to secure various items, namely the cloud interface. To retain linkages between roles and users, RBAC and hRBAC have merged user privileges into a set and assigned it to an end-user. For instance, the system may understand (user1, role (user2, role), and role) to mean that any privileges provided to role (user1, role) will be granted to role (user2, role) (user2, role). In cloud computing, you conduct any action on a privileged subject using a three-variable pattern expressed as (Subject, Object, and Privilege). This can be extended by adding an extra tuple as issuer, which allows many authorised users to work at the same time. In addition, to secure objects with respect to the interface used to interpret the object, an extra variable named interface is added, making it a 5-variable pattern with five variables (Issuer, Subject, Privilege, Interface, and Object). One of the X.509, Kerberos, or other authentication methods is used to authenticate the user and issuer management. The scope of privilege can be extended to a certain object, as well as all additional objects that are followed by the main object via object hierarchies. Consider a cloud computing scenario with a multi-tenancy authorization system (see Fig2) involves in different organizational businesses, with 2 dissimilar cloud services. Cloud services belonging to distinct companies can use an altered information model with information related to users, privileges, roles, issuers and resources. The system requires their association in sharing of authorized data. Consider an e.g., the system can interpret the command (IssuerA, role (IssuerB, users), Read, ServiceA.1, \root\) as IssuerA grants anybody with role (IssuerB, users) Read access to the \root\ folder of the file system provided by ServiceA.1. Note that role (IssuerB, users) is controlled by IssuerB. Similarly, for the remaining users and operations, The ARDC will adhere to the privacy policy. Multi-tenancy, access control methods, object-based hierarchies, and federation are all enabled by this approach. This paradigm is used by different issuers to define the authorisation SLA information in the system. If an authorization request is made, the system examines all authorization information to determine whether the request is valid; otherwise, access to the resource is denied.

3.2. PROBLEMS AND SOLUTIONS

Because of their architectural, security, and deployment levels, or by not supporting alternative interfaces, problems may develop in the initial setup of a cloud environment for accessing roles and authorisation, including its SLAs. Amazon Web Services or OpenNebula can help with this. It uses open industrial standards like the EC2 API, VPC, EMR, Load Balancer, and Open Cloud Computing Interface to avoid cloud 410 2017 International Conference On Big Data Analytics and Computational Intelligence (ICBDACI) provider lock-in (OCCI).

Security is more of a problem these days in any connection over a virtual network with its firewall. Secure socket layer (SSL), transport layer security protocols, and RSA key pair methods should all be used to safeguard it. This occurs at the data link layer of the OSI model's address resolution protocol (ARP).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 11, November 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0911022 |

A private cloud is deployed and managed using OpenNebula. Any private cloud provider does not make any API available to the public, and hence uses it only internally. When third-party users want to use external resources like those in the public cloud, they can choose from a pre-defined range of APIs.

Eucalyptus is a premium and free software for private and hybrid cloud environments that works with Amazon Web Services. This allows users to scale up or down resources like as computation, storage, networking, and so on.

IV. CONCLUSION

In a cloud computing context, the proposed paradigm is highly scalable in terms of resources. Users of the cloud would be able to exercise control over approved data exchanged within various organisational enterprises under this paradigm. The authorisation has been improved while sharing data across cloud platforms thanks to the five variable pattern. One of the most significant barriers to cloud computing's success is security and privacy. In this context, we've identified a number of key security concerns that aren't being addressed by current research efforts. This post is meant to be a rallying cry for more research into the several challenging security concerns that will have an impact on the public cloud's future. Clearly, there is still a lot of work to be done before a secure public cloud environment becomes a reality.

REFERENCES

1. Li, Xiao-Yong, et al. "*Multi-tenancy based access control in cloud*." 2010 International Conference on Computational Intelligence and Software Engineering. IEEE, 2010.
2. Ren, Kui, Cong Wang, and Qian Wang. "*Security challenges for the public cloud*." IEEE Internet computing 16.1 (2012): 69-73.
3. AlJahdali, Hussain, et al. "*Multi-tenancy in cloud computing*." 2014 IEEE 8th international symposium on service oriented system engineering. IEEE, 2014.
4. Wood, Katie, and Mark Anderson. "*Understanding the complexity surrounding multitenancy in cloud computing.*" 2011 IEEE 8th International Conference on e-Business Engineering. IEEE, 2011.
5. Yang, Shin-Jer, Pei-Ci Lai, and Jyhjong Lin. "*Design role-based multi-tenancy access control scheme for cloud services*." 2013 International Symposium on Biometrics and Security Technologies. IEEE, 2013.
6. Calero, Jose M. Alcaraz, et al. "*Toward a multi-tenancy authorization system for cloud services*." IEEE Security & Privacy 8.6 (2010): 48-55.
7. Anwar, Mohd, and Ashiq Imran. "*Access control for multi-tenancy in cloud-based health information systems*." 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing. IEEE, 2015.
8. Tang, Bo, Ravi Sandhu, and Qi Li. "*Multi‐tenancy authorization models for collaborative cloud services*." Concurrency and Computation: Practice and Experience 27.11 (2015): 2851-2868.
9. Zhang, Zhaohai, and Qiaoyan Wen. "*An authorization model for multi-tenancy services in cloud*." 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems. Vol. 1. IEEE, 2012.
10. Rao, M. Varaprasad, G. Vishnu Murthy, and V. Vijaya Kumar. "*Multi-Tenancy authorization system in multi cloud services*." 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC). IEEE, 2017.
11. Jasti, Amarnath, et al. "*Security in multi-tenancy cloud*." 44th Annual 2010 IEEE International Carnahan Conference on Security Technology. IEEE, 2010.
12. Prasad Saripalli, and Ben Walters, "*QUIRC: a quantitative impactand risk assessment framework for cloud security*," IEEE 2rd International Conference on Cloud Computing (2010).

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details