IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

An Innovative Method to Provide Confidentiality in Multi-Tenant Cloud Environment for Shared Resources

Suresh P [1] Asst professor Nanditha N E [2] Student SVCE Bengaluru India, Lakshmi P S [3] Student SVCE Bengaluru India, Nisarga K N[4] Student SVCE Bengaluru India

ABSTRACT:
Cloud computing can be an enabler for businesses to build custom services using OnDemand IT infrastructure that is flexible, scalable, and cost-effective. However, the biggest hurdles to broader adoption are security and privacy concerns. Public cloud migrations place users outside direct control over their data and applications, thereby putting such data and applications in the hands of CSPs, which operate as distinct administrative bodies. Though CSPs provide highly reliable and robust infrastructures, cloud environments are still vulnerable to various vulnerabilities that include hardware failures, bugs of the software, malware, administrative errors, and even malicious insiders. This makes the scenario more complex because hardware virtualization allows a single physical infrastructure to be used by multiple users and supports applications running in parallel. This multi- tenancy model improves resource utilization but adds complexity for secure and private interactions of users. Thus, while ensuring data security and privacy, the cloud does not have an innate sense of security, and scalability and cost savings offered by the cloud in most cases are not enough without such a guarantee. Security and privacy with multi-tenancy is one of the major challenges that cloud adoption in public environments may face. Such solutions require effective development to address these concerns and maintain their scalability within a dynamic and rapidly growing computing environment. Current approaches thus remain limited in this direction of achieving robust and scalable yet continuous security measures, which only emphasizes the need for innovative strategies that will ensure trust and safety in cloud computing.

KEYWORDS: Cloud computing, Data security, Trust and safety, Privacy.

I. INTRODUCTION

Cloud computing has been regarded as one of the most accessible and widely followed technologies and has come out as a model of Computing as a Service. Users pay for applications, computing power, and storage resources on a "pay-as-you-go" basis. It is defined as a system wherein the data center resources are shared using the technology of virtualization, offering elastic, on-demand, and instant services to the users while billing them like a utility. The benefits that cloud computing offers are immense but, at the same time, have significant problems-most significantly in the realm of security. Information security refers to defence against unauthorized access, use, disclosure, modification, or destruction of data and systems. According to the CSA, seven key threats which fall on businesses in embracing cloud computing include: Abuse and Malicious Use of Cloud Services, Insecure APIs, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss or Leakage, Account and Traffic Hijacking, and Unknown Risk Profiles. For example, Gartner also identifies other critical security concerns, including: Outsourcing Risks, Regulatory Compliance Issues, Data Location Concerns, Shared Environments, Business Continuity and Disaster Recovery, Challenges in Investigating Illegal Activities and Long-term Viability. In the International Data Corporation survey report by 2008, it concluded that, security (88.5%) and availability (84.8%) were the top two concerns affecting the application of cloud computing by business entities. This is one of the core features of cloud computing in which an instance of one software can serve multiple clients at the same time often spread across various servers. This capability does reduce cost and improve access to data and applications but creates some very distinct security challenges. In this line of thought, multi-tenancy authorization systems for middleware services are key to PaaS layer. It uses access control mechanisms, whereby all kinds of data by different cloud services are protected and ensure secure sharing between various service providers. Although data privacy is important, it was never a strongly perceived issue by policy makers and CSPs. Current regulations, especially from the EU, state basic privacy standards but remain lacking in detail and specificity, especially where

cloud environments are concerned. Cybercrime threats continue to mushroom, therefore underscoring the necessity for robust cloud security frameworks and guidelines especially relating to cloud-specific challenges. In federated clouds, SSO mechanisms are widely applied for authentication but mainly fail to support fine-grained authorization. As a correlating example, Nebula is NASA's private cloud system, integrated with Role-Based Access Control (RBAC)for precising access control, but fails to manage partnerships well. IBM and Microsoft have looked toward database schemas to share resources among clients in data-centric clouds, yet such methods are specific to services. Traditional access control approaches, such as RT and dRBAC, rely upon credentials to enable secure collaboration but have significant issues with centralized credential management, which may not be very aligned with the decentralized systems of clouds. To establish a trusted public cloud environment, these critical security concerns should be addressed, and more importance be granted to them. Research into innovative security solutions tailored to the dynamic and complex landscape of the cloud should then be encouraged.

II. LITERATURESURVEY

2.1. Cloud Computing Service Models:

There are essentially three types of cloud computing services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

1. Software as a Service (SaaS): SaaS is a model where software applications are provided to users over the internet on demand, and users can access a single instance of the software centrally hosted. The provider manages and maintains the software, and hence, users are not required to manage it locally. This multi-tenant architecture allows many users to share a single instance of the software, so they get updates as applied without the need for buying expensive licenses. Since it is a network-based service, availability of a network with no interruptions is a pre-condition to use the SaaS. Examples include Google Apps, NetSuite, and Oracle CRM on Demand.

2. Platform as a Service (PaaS): PaaS offers virtualized hardware platforms for deploying and running applications. It aids in scaling by allowing users to request extra resources whenever they need to. In developing their applications, users are permitted access to development tools; users have full control over any deployed application but they do not manage the underlying servers or networks or operating systems. PaaS enables programming in multiple languages; hence application portability is easy. Examples include Google App Engine and Long Jump.

3. Infrastructure as a Service (IaaS): IaaS provides access to a pool of hardware resources such as servers, routers, and switches, with users being able to perform multiple computational tasks, for example, processing and storage. Users install and run what software they wish, including operating systems and applications, but have no responsibility for the underlying cloud infrastructure; they maintain control over the applications and devices hosted on the infrastructure.

These service models involve security of great importance. In SaaS, the third-party software is hosted by the CSP and accessed by various users. If a malicious actor manages to compromise the hosting location of the software,

such actor can consequently bring disruptions to availability for all users. Just as in other security vulnerabilities for every type of CSP service, there are potential attacks, requiring strong security.

2.2. Challenges in Multi-Tenancy Security:

Multi-tenancy in cloud computing presents unique security challenges, as both attackers and victims often share the same physical server. Traditional security measures, primarily designed to monitor network layers, cannot effectively address threats that originate within shared servers. The exploitation of multi-tenancy typically involves co-locating an attacker's virtual machine (VM) with the victims on the same physical machine (PM). For instance, research has demonstrated this vulnerability through an attack on Amazon EC2, where network probing and brute force techniques were used to strategically place the attacker's VM next to the victims. The attacker had a 40% chance of success for a minimal financial investment. Once co-located, a side-channel attack was executed, exploiting system characteristics to extract sensitive data from the victim's VM. Side-channel attacks are particularly dangerous because they cannot be detected by hypervisors or operating systems, allowing malicious tenants to target neighbouring tenants undetected. While it is not possible to entirely eliminate the risks associated with multi-tenancy without sacrificing its benefits, the impact can be mitigated. This can be achieved through intelligent resource allocation strategies that complicate co-location for attackers. By increasing the time, effort, and cost required for attackers to exploit multi-tenancy, the likelihood of successful attacks can be reduced, thereby enhancing security. Such measures strike a balance between maintaining the advantages of multi-tenancy and minimizing its inherent risks.

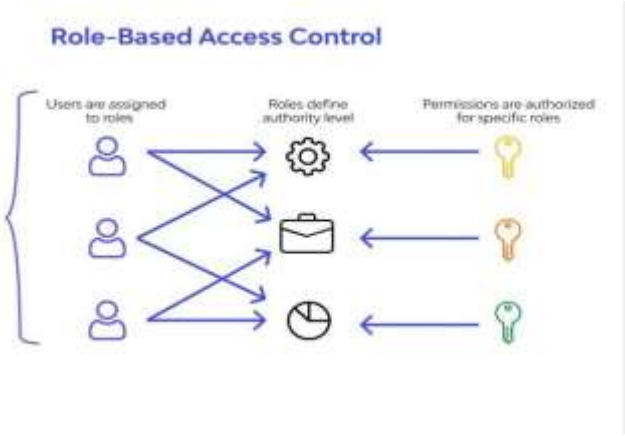
2.3 Privacy Statutes and Legislation:

Ensuring data privacy and fulfilling the regulatory compliance requirements in cloud computing is challenging, especially with the multi-tenant systems. There is no such universal framework regarding privacy and protection hence compliance cross-border data transfers become difficult. Users feel safe and sound with the stringent local privacy laws, but unknowingly fall prey to breaches of privacy, due to cross-country border storage or transfer of data. For instance, the Patriot Act permitted the United States government to search data, preventing users from storing information in those areas. Conversely, EU rules significantly limit data movement due to circumvention of privacy laws. The EU has established robust and harmonized privacy regimes that are based on intergovernmental collaboration between governments, corporations, and sectors. It follows that there is an assurance of uniformly applied privacy practices across sectors. In contrast, the US has a sector-specific approach, whereby HIPAA is applied to health-related entities and the Sarbanes-Oxley Act (SOX) for financial entities. Such piecemeal approach often lacks an all-inclusive safeguard wanted by the EU nations, while the EU considers the US a region of higher risk when it comes to data privacy. The US has developed the Safe Harbor Privacy Principles, somewhat akin to the EU Directive 95/46/EC, but because it is voluntary it remains to be implemented. Asia-Pacific remains playing catch-up with the EU and the US. The Asia-Pacific Economic Cooperation's Privacy Framework is merely a list of best practices not backed by law. However, major differences in cultures and economies within the Asia-Pacific region blur the lines toward standardizing international thinking on privacy regulations. This inequality underscores the necessity for globally harmonized privacy frameworks to facilitate the safe adoption of multi-tenant systems. Identity protection, data placement regulation compliance, and geo- redundancy are very important especially for sensitive and personal data kept in shared environments. For instance, Principle 8 of the UK Data Protection Act 1998 prohibits transfers of data outside the EU unless adequate safeguards are in place, with very few countries such as Switzerland and Hungary fulfilling these requirements. Worldwide cooperation is needed to strengthen privacy protections and instill confidence in cloud computing.

III. PROPOSED AUTHORIZATION MODEL: AUTHORIZATION AND ROLE BASED ACCES CONTROL

Multi-tenancy supports shared infrastructure, resources, and applications through many users having tenancy capabilities in cloud services. This has drastically reduced the operational cost and maximized resource usage efficiency. Still, it has remained very challenging to enforce proper security and access control in multi-tenancy-

based environments. The access management mechanisms used widely for such shared resources are based on role-based access control, especially in multi-cloud environments. This strategy provides a strong, scalable, and secure mechanism to ensure that only those authorized users can access the resources and services to which they have an entitlement to use as given by their defined roles.



Role-based access control is highly used in managing user access in the cloud environments. RBAC ensures that a user's role in an organization or system forms the basis of determining accessibility to resources. Every role defines what kind of permission or privilege should be granted on the resources offered by the cloud. Just like in any other technology, within a multi-tenant environment, different users may access the same applications coming from different organizations or business units, but each one can only perform actions pertinent to his job function or business need. This will ensure that sensitive data or services are accessed only by the right user. Users may have to operate on more than one cloud platform, which adds another layer of complexity as each possibly would have their version of access control, policies, and security. Therefore, a centralized multi-cloud role-based access control system is the need for effective user access management. The multi-tenancy authorization mechanism in cloud computing, based on RBAC, would ensure that only relevant services are accessed by the users with significant security measures and compliance to varying service-level agreements. Multi-tenant cloud systems mean that many tenants on the same platform share the same infrastructure. The authorization process in a multi- tenant cloud system is an essential security and privacy mechanism. The moment a user applies for access to any service or resource, the cloud system authenticates the user to check whether they actually are who they claim to be. After this authentication process, the system checks whether such a user has the permissions to obtain the requested service. Once authorized by the system, it proceeds to allow access either by direct access or by secure ticketing. One of the key challenges for multi-cloud systems is managing access control across different cloud platforms. Each cloud may employ different types of authentication and authorization mechanisms such as Kerberos, X.509 certificates, or OAuth, and various ways of defining roles and permissions. To face up to this challenge, a centralized authorisation system like the ARDC, which supports the Authorization and Resource Distribution Controller, can be used to manage the authentication and authorization processes across multiple clouds. The ARDC ensures access to only the users who have the right roles and privileges for a service or any resource by the authenticating that requesting of access from any user is done in place. It uses techniques of cryptography, symmetric key, to effectively communicate with the cloud servers by ensuring access is granted to only authorized users. Cryptographic keys are shared between the ARDC and each cloud to permit mutual authentication of users and their different roles across distinct environments. The use of cryptography assures the authorisation process is secure, tamper-proof. See synchronous key cryptography and key management below. The heart of secure authorization processes in multi-tenant cloud systems lies in symmetric key cryptography. Symmetric cryptography employs the same key for both encryption and decryption purposes. This makes the method very efficient and fast for securing data and communication between systems. However, key management is absolutely important in holding a system secure. It is possible to breach the security of the entire system due to improper management of cryptographic keys. Key management consists of key generation, distribution, storage, updating, and revocation in a secure manner. The complexity of the management is further increased in the case of cloud computing due to the dynamic nature of cloud resources and users. As the users may join or leave the system frequently, key updates or revocations are required very frequently. Moreover, the infrastructure of the cloud consists of multiple servers and platforms, each having a different key set. To ensure that the keys are indeed dealt with and preserved appropriately during the system's lifetime, a central key management system is needed. Although the ARDC makes use of symmetric key encryption to authenticate user credentials and to issue tickets, it, through the central management of the keys, spreads out its cryptographic keys across the various cloud-based platforms in a secured manner. When a user wants to access a service, the ARDC uses the encryption keys distributed to the cloud servers to authenticate it. If all checks regarding the authentication of the user are completed successfully, ARDC generates a ticket that the user can present before the target cloud server for authentication again. Role-based access control is an effective method for handling access in the multi-tenancy environment where several users belonging to different organizations share common resources. In RBAC, roles determine a set of permissions to be granted on the system; then the user is assigned one or more roles in a job. For example, an administrator role would have access to all resources while a user role might only give access to certain data or services. This multi-tenant cloud system further enhances this role-based access control by managing users of different tenants without losing isolation and security. The system assigns each user a role, which describes which resources they have rights to and also the permissions associated with those resources. A hierarchical permission model can have roles that inherit permissions from other roles. For example, one "manager" role could inherit from the "user" role but be given some additional privilege to update the data. RBAC in multi-tenant environments extends the security aspects of user isolation. Here again, users in separate tenants are managed. For this purpose, the system grants each user a given role, which is defined as what kind of resources he needs to have access to and what privileges are

attached to them. It's also possible to make roles hierarchical so that some roles will inherit permissions of other roles. For instance, a "manager" role may inherit from the "user" role but contains additional privileges to enable actual modification of data. In multi-cloud environments, access control is therefore managed using a 5-variable pattern, including parameters such as the issuer, subject, privilege, interface, and object. These parameters therefore provide a much more fine-grained control of access and may also be used to specify with exactitude what a user is authorized to perform, under what conditions, and through which interfaces.

IV.CONCLUSION

The following is the securing of access to resources and services, more so in multi-tenant cloud environments, which ensures privacy, security, and compliance with regulatory requirements. An RBAC system offers scalable and flexible mechanisms for managing access based on roles and privileges. Multi-tenant systems can provide secure and authorized access of resources by users to their necessities through federated authorization, symmetric key cryptography, and privacy policies. A highly effective kind of a role-based authorization system is seen in multi-cloud environments in which the users often have a need to access various services from multiple providers of cloud. The use of a central authorization mechanism, which is the ARDC, makes it easy for the management of roles and permissions. This therefore assures security and privacy for every one of the tenants with adequate security mechanisms properly implemented. The achievement of multi-tenancy in cloud computing will then thus be fully accomplished while being secure and efficient for the respective users and organizations.

REFERENCES

1. Vaishnavi Waghmare, Harsh Khandve, Nitin Kamble. “Privacy in Multi-Tenancy Cloud”. 2021 International Journal of Innovative Research in Computer and Communication Engineering

2. Wahidah Hashim, Noor Al-Huda K. Hussein. “Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures”. 2024 SHIFRA

3. Dr. A Yashwanth Reddy, Dr. M Upendra Kumar. “Design and development of multi tenancy security issues in cloud computing”. 2021 International Journal of Multidisciplinary Research and Growth Evaluation.

4. 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.

5. Hussain AlJahdali, Abdulaziz Albatli, Peter Garraghan, Paul Townend, Lydia Lau, Jiee Xu. “Multi-tenancy in Cloud Computing”. 2014 IEEE 8th International Symposium on Service Oriented System Engineering

6. Bo Tang, Ravi Sandhu, Qi Li. “Multi-tenancy authorization models for collaborative cloud services”.2014 Concurrency and Computation: Practice and Experience