Journal of Advances in Science and Technology
Vol. 19, Issue No. 2, April-2022, ISSN 2230-9659

Cloud Computing for Secured Communication

Ghanshyam Shivcharan Nikhade[1]*, Dr. Tryambak Hiwarkar[2]

[1] Research Scholar, Department of Computer Science, Sardar Patel University Balaghat M.P.

[2] Professor, Department of Computer science and engineering, Sardar Patel University Balaghat M.P.

Abstract - Nowadays, group oriented applications such as video-conferencing, TV over internet, Video on demand and e-learning has been developed which acquire multicast communication. Support for multicasting in apps means the data may be sent to a larger audience. The group's members must have safe and simple means of communicating with one another. Encrypting the message before sending it out to the whole team is a must if you care about data security. A secret or group key must be shared amongst the group members in order to encrypt and decode the material. Members of the group who have been given the group key are the only ones who can read the encrypted material. In recent years, cloud computing has evolved as a viable platform for multicast data sharing across a community of users. Since a third company is responsible for protecting your data on the cloud, data security is another major obstacle. However, a secret key must be produced and sent securely to cloud users when sharing the data with a group of people.

Keywords - Cloud Computing, Cloud Infrastructure, Secured Communication, Cloud network.

----------X----------

INTRODUCTION

Cloud computing has originated with the exponential development of internet connectivity and infrastructure access. Cloud is a modern model for providing diverse applications to people on the internet, also referred to as the 'cloud,' for example web production frameworks, servers, storage and content. Cloud infrastructure often offers customers and companies different tools to use cloud technology in an easy and reliable way, without growing computing resources costs.

Business may select between private, public or hybrid cloud implementation, depending on specific business requirements and security considerations. Most organizations follow this fast-growing paradigm to satisfy their computing requirements and develop their market. Cloud infrastructure offers tools for digital networks and other software used both by a customer and the businesses of the cloud service provider, such as network capability, storage and server utility.(1) Instead of buying new hardware or services for its commercial uses, this enables consumers to use the cloud network as a commodity, technology and software as a service.

Many famous companies supply this equipment and provide cloud services. Here are some of the biggest names on the market:

- **Google:** Google's own private cloud is to include Google Docs, email, analytic websites, charts, Google Cloud Storage, among even more for features such as Google App Engine (Python, Java, Go).

- **Microsoft:** Microsoft offers its offline software apps and, in particular, the Microsoft Office 365 web platform enables its customers to shift the information and market analytics resources.

- **Amazon:** Amazon Web Services (AWS) provides reliable cloud services to support companies' expansion. It provides Elastic Cloud Computing (ECC), Simple Storage Service (SSS), content distribution and other capabilities.

- **Salesforce.com:** Salesforce.com enables customers to run cloud apps. Force.com, vmforce.com and Java developers are able to design and install company applications in the cloud.

Cloud Computing

Exploring a public scheme always starts with defining the key concepts and how the public understands them. Studying such cutting-edge and up-to-date literature yields the following functional descriptions, which form the basis for a wide variety of novel approaches to cloud computing: (2)

"Cloud computing ('cloud') is an emerging word that depicts the growth of numerous current technologies and approaches to computing into something else,"

writes NIST (National Institute of Standards and Technology). The cloud "decouples" IT resources like applications and data from their physical location and the means by which they are delivered.

Cloud Computing Architecture

Cloud infrastructure design focuses mostly on device product configuration for cloud, hardware, middleware and applications, cloud consumers, cloud storage, and networking. Both these modules are mainly arranged with regard to the use of the cloud consumers and end users.

A new paradigm focused on the possibility of holding large amounts of data and software is the cloud computer architecture. The aim is also to include these stored data and applications focused on consumer demands and flawless hardware and software access without substantial expenditure in own software, hardware or infrastructure. Figure 1 shows the cloud infrastructure architecture and the cloud design elements. (3)

Access Control Techniques in Cloud Computing

To resolve the security issues in cloud computing applications, access control policies are used as one of the security mechanisms to permit, deny or restricts the access to the cloud computing systems. Also, the existing access control techniques attempted to identify the users who are trying to access the system without proper authorization. According to Anderson (2010), Access Control is the security model which provides several constraints on the user's actions, which is performed in a system based upon the rules described by the access control mechanism. Figure 1 depicts the access control view point.

Figure 1: Access Control View Point

Multiple access control mechanisms are usable, some of which are listed below:

a) Discretionary Access Control (DAC)

Access to knowledge regarding artifacts is provided by the DAC model which grants permission to the owners (restrict or access their personal objects) depending on the skill or user identification or participation of a club. (4) The DAC is deemed less secure and commercially used by the UNIX-based systems due to its flexibility in comparison with other access control methods. The DAC flow in cloud computing is shown in Figure 2.

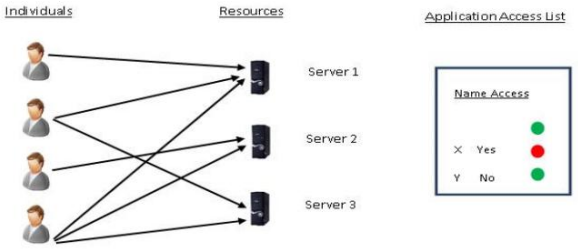

Figure 2: Discretionary Access Control

b) Mandatory Access Control (MAC)

The MAC model (Anderson 2010) provides a central authority with access to a subject's decisions that request access to artifacts or knowledge within objects. MAC grants a class of access to any topic and entity to protect access to artifacts and the knowledge that passes within objects. A class of access is a type of authentication used to protect the flow of knowledge between dominating objects and objects. Item classifications are security codes used to identify items depending on their sensitivity. The safety standards used to reflect confidence or rules of subjects are the focus of the clearances. In cloud storage, Figure 3 displays the MAC.

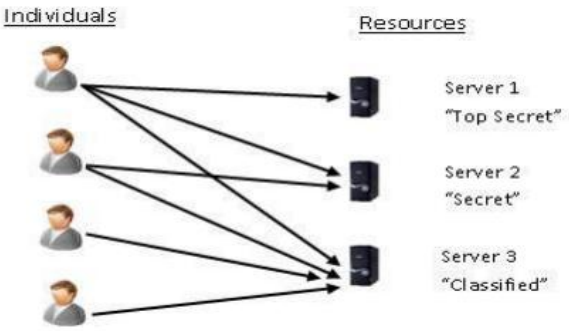

Figure 3: Mandatory Access Control

c) Role-Based Access Control (RBAC)

The consumer with allocated roles shall have access to the object. The functions are determined on the basis of the job function. (5) The device functions and not the user are all the objects involved. The RBAC function in cloud computing is seen in Figure 4

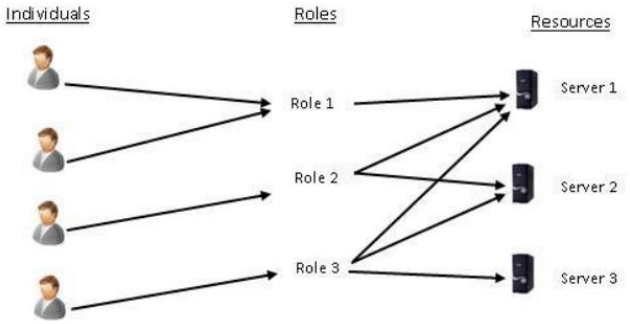

Figure 4: Role-Based Access Control

Key management infrastructure in cloud computing

Control of cloud core The Cloud Core Management Client (CKMC) and Cloud Core Management Server infrastructure (CKMS). Like software, platformer, infrastructure and other basic cloud services, CKMC leaves cloud apps (as a Service). CKMS interacts with CKMC through the interoperability protocol cloud key management, which interacts with the SKMS framework and the PKI, utilizing the symmetric key management protocol and asymmetric key management protocol, as seen in Figure 5.

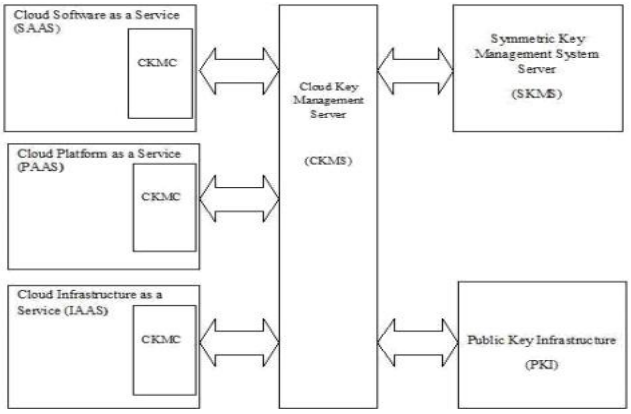

Figure 5: Cloud key management infrastructures

A single comprehensive protocol for communication between cloud key manager servers and cryptographic clients is established in the Cloud Key Management Interoperability Protocol (CK-MIP). Defaults to the crucial need of an extensive key management protocol by specifying a protocol that can be used by every cloud cryptography client, from the multi-locator implementations to the cloud stores. (6) It is integrated into the cloud storage infrastructure and can deploy efficient centralized key management for all of its security, authentication of certified devices, digital signatures and other encryption capabilities. A cloud infrastructure solution can consolidate main administration in a single enterprise key management system by providing provider assistance from CKMIP. It eliminates operating and maintenance costs while improving the organizational controls and regulation of a security policy by every cloud cryptographic customer, from multi-tenant deployment to cloud storage. It is integrated into the cloud storage infrastructure that enables efficient centralized key management for all its encryption, user authentication based on certificates, digital signs and other cryptographic functions. A cloud storage solution may consolidate key management inside a single company key management framework with provider assistance from CKMIP. It lowers maintenance and maintenance expenses thus reinforcing operational controls and protection policy regulation.

Security in Cloud Computing

Whether it's an IaaS, SaaS, or PaaS provider, in the cloud computing model, the cloud provider is responsible for developing, deploying, and managing the corresponding resources, applications, and services. (7) The best way to get the most out of your infrastructure and software is to take use of multi-tenancy and virtualization. Virtualization allows several users to share a single server, computer facility, data centre, and operating system. By pooling their resources, cloud providers are able to service a huge user base. As a result of multi-tenancy and virtualization, the cloud environment faces a number of security challenges, including those related to data protection, communication, and the management of resources for isolation and virtualization. (8)

Data Protection: At any given time, several users tap into the cloud's resources. Providers control the common infrastructure where users' data is kept and processed. Someone with bad intentions might potentially alter user data. The necessity of data privacy and protection in cloud environments is heightened by factors such as a lack of knowledge regarding where data is stored, regulatory concerns arising from cross-border storage, and similar factors. As a result, fundamental security concerns in cloud computing revolve around data protection issues such data confidentiality, data integrity, and data availability.

Application Security: Security concerns are unique to cloud computing environments and must be taken into account when developing or deploying application software. The remote app you're using must be genuine and virus-free. The cloud's adaptability, transparency, and public availability pose risks to application security. Another issue is how to ensure the programmes' security when they are run on remote computers. (9)

Network Security: A cloud computing can have type public or private, based on the deployment model. Service and applications are accessed from remote locations in a cloud environment. Continuous availability of cloud service without any disruption due to network security problems like Denial of Service (DOS), and other attacks are important security challenges.

Virtualization Security: The hypervisor and other management components of virtualization technologies provide the door to new types of assaults. Virtual servers and apps cannot be evaluated for safety in any meaningful way. A man-in-the-middle attack might arise at the moment of authorization for any service when using multi-tenancy in cloud infrastructures to share 7 physical resources amongst VMs (Virtual Machines).

Identity Management: Registration is when identities are created for use with cloud services. To access a cloud service, each user must first log in with their own unique identity. It's a serious problem because unauthorized users can access cloud-based services and data. A bad actor can get access to a cloud service by masquerading as a genuine user. Frequently, these bad actors take over a cloud service, making it unavailable to genuine users. It's also possible for the user to go too far when making use of the service in question.

Access Control Techniques in Cloud Computing

Access control rules are one of the security strategies used to allow, prohibit, or limit access to cloud computing systems, helping to address the security concerns that have been raised about cloud computing applications. Existing methods of access control have also made an effort to track down those who are trying to log in to the system without authorization. According to Anderson (2010), an access control mechanism describes a security model that places restrictions on the activities a user may do within a system. (10)

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)

Challenges & Issues In Cloud Computing

Cloud computing has a multi-tenancy feature which increases the challenge to cloud adoption. Service providers must address the number of following challenges as shown in the Figure in the cloud:

- **Loss of Governance:** When using cloud computing, customers cede authority to the service provider, which can compromise the safety of their data and applications in a number of ways. This means that service level agreements (SLAs) may not impose any security obligations on the provider. Thus, the phrase "policies" is used by all businesses to avoid blame for unauthorized access, usage, fraud, and deletion of client data and apps.

- **Lock-In:** One more hurdle is the lack of knowledge in terms of procedures, standards and tools to deliver the compactness and interoperability of information between the cloud services and cloud vendors. This forces the client to be fully dependent on the service providers.

- **Isolation Failure:** Cloud computing has a great feature of multi-tenancy and resource sharing but it also fails to separate the storage devices and reputation among different occupants. This increases a security concern when a stored data is being attacked by an intruder such as guest-hopping attacks. (11)

- **Malicious Insider:** This is the most challenging deal with in cloud computing because if it happens, the damage is uncountable. A risk of insider attack is aggravated by certain roles generated by the construction of cloud computing. Examples of these roles are security service providers, the cloud service provider system administrator etc.

- **Security:** Security is a major issue which is hindering Cloud computing acceptance because the cloud has a distributed nature which makes it more vulnerable to attacks like replay attacks, man-in- the-middle attacks, sniffing and spoofing of information. Security issues such as data loss, phishing, botnet (running remotely on a collection of machines), resource location, multi-tenancy, authentication & trust, system monitoring & logs are posing serious threats to organization's data and software.

- **Costing Model:** Consumers of the Cloud must weigh the pros and disadvantages of sacrificing one or more of processing, communication, or integration. The cost per computing resource unit used is likely to increase after migrating to the Cloud, despite the fact that the Cloud can significantly reduce infrastructure costs. This is because data communication costs or the money spent sending and receiving an organization's data in the public and community Cloud, will rise. When a company adopts a hybrid cloud deployment architecture in which data is stored in a combination of public, private, and community clouds, this issue becomes more pronounced. (12) Tasks that need a lot of processing power are a natural fit for on-demand computing.

CONCLUSION

This study proposes and implements spatio-temporal restrictions for storage and retrieval with access control, allowing for safe and dynamic cloud-based collaboration. Cloud-based security paradigm to assist online students in safely accessing cloud-based learning resources. In addition, an access control method is implemented in this work to

safeguard the resources from unauthorized users. To achieve this, a unified access policy and a protected group key management system were designed and implemented in this study. In this way, only approved users are granted access to the cloud's resources. As a result of this suggested technique, cloud users can benefit from faster and cheaper access to cloud-based resources.

REFERENCES

1. Sahil Arora, Ashish Raj (2014) on "Securing the Cloud with Encryption and Key Management", International Journal of Engineering Research & Technology (IJERT) IJERT ISSN: 2278-0181 www.ijert.org Vol. 3 Issue 7

2. Bibin K Onankunju (2013) on "Access Control in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 9

3. Jaebok Shin, Yungu Kim, Wooram Park, Chanik Park (2013) on "A Method for Data Access Control and Key Management in Mobile Cloud Storage Services", IEMEK Journal of Embedded Systems and Applications 8(6), DOI:10.14372/IEMEK.2013.8.6.303

4. Ramaswamy Chandramouli, Santosh Chokhani (2013) on "Cryptographic Key Management Issues & Challenges in Cloud Services", Computer Security Division Information Technology Laboratory

5. Ivan Damgard, Thomas P. Jakobsen (2013) on "Secure Key Management in the Cloud", 14th IMA International Conference on Cryptography and Coding

6. Chandran, D, Kempegowda, S 2010, 'Hybrid E-Learning Platform Based On Cloud Architecture Model: A Proposal', IEEE International Conference on Signal and Image Processing (ICSIP), pp. 534-537.

7. Chengcheng Zhang & Fei Wang 2010, 'E-Learning Instructional Platforms Based on Network and Multimedia Technology', Proceedings of the Second International Workshop on Education Technology and Computer Science, IEEE, Vol. 2, pp. 464-467.

8. Chin Bang & Yao 2010, 'Adaptive Context Aware and Intelligent Searching in Mobile Learning Applications', Proceedings of the Second International Conference on Computer and Automation, IEEE, Vol. 5, pp. 802-806.

9. Chuang, S, Chang, K & Sung, T 2011, 'The Cost-Effective Structure For Designing Hybrid Cloud Based Enterprise E-Learning Platform', IEEE International Conference on Cloud Computing and Intelligence Systems, pp. 523 – 525.

10. Constantin Musca , Ana Ion , Catalin Leordeanu & Valentin Cristea 2013, 'Secure Access to Cloud Resources, Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 554-558.

11. Crago, S, Dunn, K, Eads, P, Hochstein, L, Kang, D-I & Kang, M 2011, 'Heterogeneous cloud computing', In: 2011 IEEE International Conference on Cluster Computing, USA, pp. 378-385.

12. Jinghe Huo, Shifeng Shang & Zeng Zhang 2013, 'ACRUM: An Adaptive Cloud Resource Utilization Model', Proceedings of the Fourth International Conference on Software Engineering and Service Science, IEEE, pp. 275-278.

Corresponding Author

Ghanshyam Shivcharan Nikhade*

Research Scholar, Department of Computer Science, Sardar Patel University Balaghat M.P.