Analysis on Cloud Security

SNEHA SACHDEVA[1], OMRAJ SHARMA[2]
[1, 2] *Student, Maharaja Agrasen Institute Of Technology*

Abstract- In the current scenario, cloud computing is a rapidly developing technology that is widely used worldwide. Since a lot of information about people and businesses is stored in the cloud, it's important to make sure the cloud environment is safe. It is important to develop a solution in such a way that users can access their cloud storage with the given unique credentials and protect the cloud infrastructure from thefts and misgauge. Cloud security entails securing cloud environments against unauthorized use/access, distributed denial of service attacks, hackers, malware, and other risks. This paper will shed light on data security issues such as Authorization and authentication of users, data confidentiality, data encryption, non-repudiation, and availability, which are the most important considerations for cloud security. Additionally, the difficulties associated with various forms of cloud security are discussed in this paper.

I. INTRODUCTION

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers, data storage, development tools, and networking capabilities hosted at a remote data center managed by a cloud services provider. Cloud Computing provides various benefits like lower IT costs, and easy and efficient scalability [1]. It eliminates the need for enterprises to procure, configure, or manage resources themselves, and they only pay for what they use. Security in cloud computing is crucial to any company looking to keep its applications and data protected from bad actors. Maintaining a strong cloud security posture will help organizations achieve the widely recognized benefits of cloud computing [2]. Cloud security ensures your data and applications are readily available to authorized users. Authorization is an important identity service to avoid unauthorized access to cloud resources. Authentication is a key mechanism for information security that establish proof of identity to get access to the information in the system. Cloud encryption is the process of transforming data from its original plain text format to an unreadable format, such as ciphertext before it is transferred to and stored in the cloud.

II. LITERATURE REVIEW

Srinivas, Venkata, and Moiz give a superb understanding of the essential ideas of distributed computing. This paper examines several important ideas by providing examples of cloud computing-based applications and the ways in which they can help the developing world benefit from this new technology.Security concerns, according to Chen and Zhao, are one of the primary reasons why large businesses would still not move their data to the cloud. Creators have given the extraordinary examinations on information security and security insurance issues connected with the cloud.Tie Hong and Jiang-Chun Ren, give a detailed analysis of the security of the current open-source cloud platform, highlighting the fact that each cloud platform has its own implementation and the security implementation mechanisms are not disclosed.K. Surya, M.Nivedithaa, S.ema, C. Valliyammai discusses the main issues concerned with the cloud which are security, compliance, freedom, long term viability. The authors have given deep insights into various requirements to ensure security in the cloud which are authorizing and authenticating users, data confidentiality, availability, etc.Ahmed Albugmi, Mandini O. Alassafi, Robert Walters, and Gary Wills discussed the details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats[3].Steven Mathew, Sarita Gulia, Varinder Singh, and Vivek Dev highlighted the numerous benefits of cloud computing, deployment models, and cloud services. This paper examines several challenges and technical issues faced in cloud computing.

III. SAFETY MECHANISMS

There are several system safety methods. Access control, encryption technology, third-party audit, trusted computing, and other features are frequently utilised in modern computer systems[4]. In this paper, we will only cover the fundamentals of access control and encryption technologies.

A. Access Control

Access control has a broad meaning that includes authentication and authorisation. Authentication is the process of determining if a user has access to a system. Authentication is another issue to address in the networking environment. It includes security protocols like as SSL, IPsec, and Kerberos, among others.

What authorization the users have to fix the problem. Normal users, for example, cannot normally access the entire resource, but the administrator can. Authentication is a binary decision, whereas authorisation is a definition of which access is granted.We often think of access control policy as a matrix, with columns representing different users and rows representing different resources needing accessneed to be accessed[5]. If the value is 1, the identified user may access the service; alternatively, it really can.

B. Encryption Technology

Encryption serves a typical security technology function.

Encryption technology is always evolving, from simple substitution encryption to complicated public-key systems. There are three types of encryption technology: symmetric key cryptography, public-key cryptography, and hash function. Symmetric key means that the encryption key is the same as the decryption key. The usual symmetric key systems extensively utilised in modern civilization are DES and AES. Public-key systems, such as RSA, employ the public key to encrypt data and the private key to decode security data.Hash functions are commonly employed in message digesting. Attribute-Base Encryption (ABE) [6] is a new method that includes access control within the ciphertext. ABE is a kind of public key encryption algorithm. ABE creates the access control tree using the access control matrix and incorporates it into the ciphertext, allowing users who fulfil the access control tree to decode it. As far as implementation approaches go, ABE is separated into Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE).

IV. SAFETY ANALYSIS

Each open source cloud platform has its own mechanism for implementing security. There are currently no criteria for evaluating them. However, we may see them in popular security configurations such as Virtual Machine (VM) security, Virtual Machine Monitor (VMM), and so on[7]. However, we will not be able to determine who is more secure than everyone else. According to Luis M. Vaquero, the security domain is divided into three sections: machine virtualization domain, network virtualization domain, and physical domain. Kandukuri B R believes that security can be classified into five levels: server access security, internet access security, database access security, data privacy security, and programme access security. This study focuses on virtual security and network security.

A. Virtualization Security

We will mostly examine the security of VM images, VMM, and instances, therefore instance security is dependent on image security. [14] Unlike traditional servers, virtual machines are vulnerable even when they are turned off. [2]Several hazards to VM and VMM exist throughout their lifespan, including storage, deployment, and runtime. Cryptographic, VM introspection, access control, reducing privileged VM control instructions, and other technologies are used to safeguard this[8].

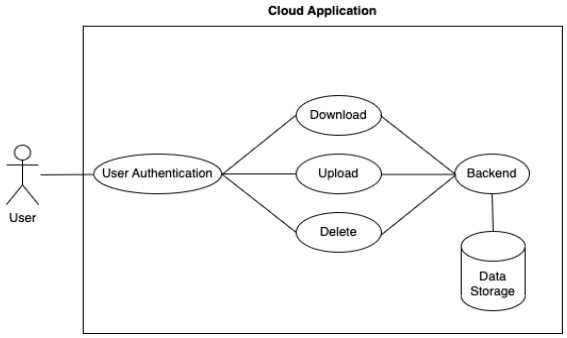
Eucalyptus uses password authentication to ensure the security of pictures; however, you can disable password-based authentication as well as the account's rights.Eucalyptus also suggests creating an unprivileged user account. Use sudo to gain access to privileged commands if necessary. Which is to say, mostly Eucalyptus An access control method to ensure the security of instances and images on trusted hosts or networks. Eucalyptus requires a private key and an X.509 certificate before you can bundle a running instance[9]. Eucalyptus recommends that users turn down any unneeded services and ports on

the image.CloudStack users are also separated into groups to manage unwanted access. In addition to these access control strategies, CloudStack supports SSH keys for cloud infrastructure login. Every cloud end user has SSH keys, which ensure that one user cannot access the instance of another user.Glance is the name of the OpenStack Image project. You can obtain a trustworthy image via booting media from a trusted source or a trusted third-party. When considering the danger of QEMU fills in virtual hardware, OpenStack recommends employing obligatory access constraints[10], such as sVirt and SELinux, to improve the security of virtualization layers.

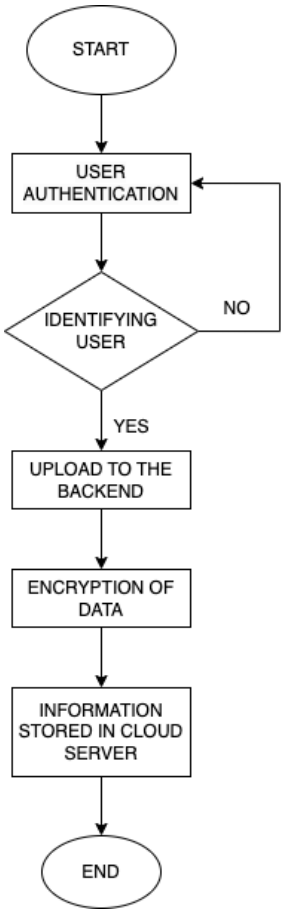
B. Network Security

Data transfer via the network should prevent sensitive messages from being leaked. For security, powerful network traffic encryption techniques such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) are used. To combat the shared network danger, we can use network traffic control, hierarchical isolation, LANs, and L2/L3 tunnelling. In the instance of Eucalyptus, advocate managed mode as the optimal networking method for secure installations, and make security groups available[11]. A VLAN tag is used to impose a security group that controls incoming traffic to instances and isolates them through Layer 2.This guards against eavesdropping and hijacking by other security groups.Eucalyptus receives data through Query or SOAP interfaces. and message exchange[12,13] as well as having an imposed time stamp to avoid replay attacks. To ensure message integrity and non-repudiation, Eucalyptus mandates that all user requests be signed and their content be correctly hashed. When it comes to message confidentiality and server authenticity[14], Eucalyptus always uses SSL/TSL protocols for communication. CloudStack uses security groups to filter incoming and outgoing VM traffic based on its rules, known as ingress and egress rules [15]. Those rules, which serve a security function, can restrict network traffic communication with the VMs. Guest VMs in CloudStack can connect with one another through a private LAN.

V. USE CASE DIAGRAM



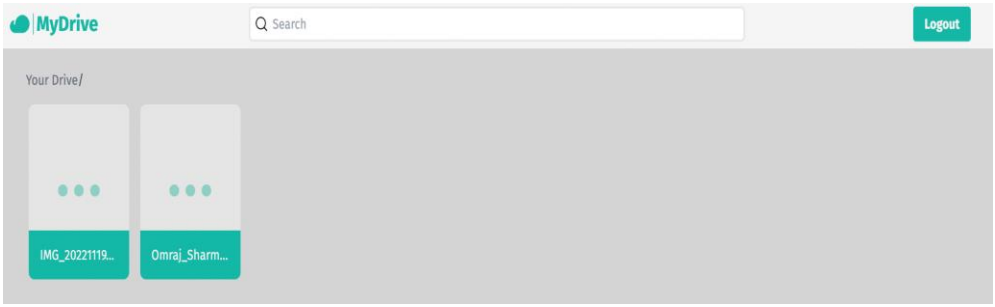
VI. FLOWCHART

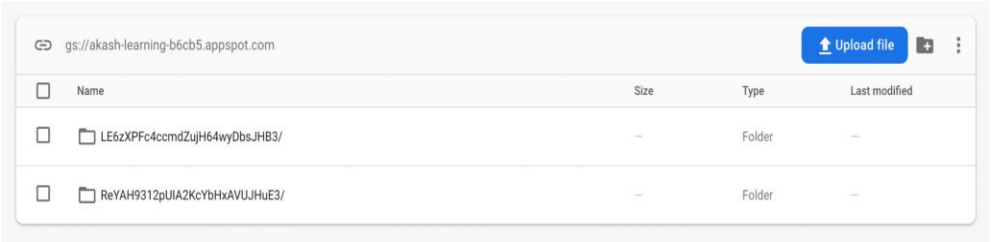


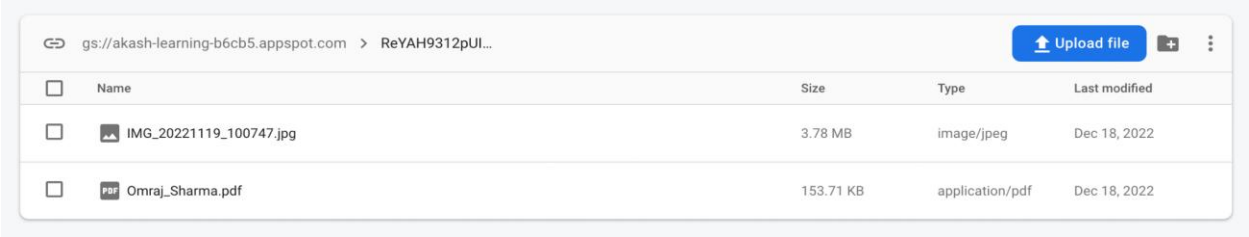
VII. RESULT

Authenticated users have secure and safe access to their storage via backend data encryption using the 256-bit Advance Encryption Standard. Users have a platform that centrally manages all applications, devices and data to ensure everything is protected. A

cloud security layer that ensures user authentication and provides easy access to cloud storage services is built.







CONCLUSION

According to a study by Oracle and KPMG, 72% of participating organizations now view the cloud as more secure than what they can deliver on-premises themselves. However, data breaches also occur, 5250 confirmed data breaches occurred because of no mention of cloud security service provider. Thus, Cloud security's ability to guard company's data, preventing leaks and data thefts will have a critical role in company's growth. In case of any accidental cyber threat, cloud security will ensure the valuable data is safe. This will enable the industry to move technology at a rapid pace and provide consumers a better experience.

REFERENCES

[1] Dubey A, Wagle D. Delivering software as a service[J]. The McKinsey Quarterly, 2007, 6(2007): 2007.

[2] Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem[C]//the proc. of the 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia. 2010.

[3] Vaquero L M, Rodero-Merino L, Caceres J, et al. A break in the clouds: towards a cloud definition [J]. ACM SIGCOMM Computer Communication Review, 2008, 39(1): 50-55.

[4] G ens F. New idc it cloud services survey: top benefits and challenges[J]. IDC exchange, 2009.

[5] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. of ACM CCS 2006. Alexandria, VA, USA (OctoberNovember 2006)

[6] Endo P T, Gonçalves G E, Kelner J, et al. A survey on open-source cloud computing solutions[C]//Brazilian Symposium on Computer Networks and Distributed Systems. 2010.

[7] Milojicic D, Wolski R. Eucalyptus: Delivering a private cloud[J]. Computer, 2011, 44(4): 0102-104.

[8] Nurmi D, Wolski R, Grzegorczyk C, et al. The eucalyptus opensource cloud-computing system[C]//Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on. IEEE, 2009: 124-131.

[9] Kandukuri B R, Paturi V R, Rakshit A. Cloud security issues[C]//Services Computing, 2009. SCC'09. IEEE International Conference on. IEEE, 2009: 517-520.

[10] Sefraoui O, Aissaoui M, Eleuldj M. Comparison of multiple IaaS Cloud platform solutions[C]//Proceedings of the 7th WSEAS International Conference on Computer Engineering and Applications,(Milan-CEA'13), ISBN. 2013: 978-1.

[11] Pepple K. Deploying OpenStack[M]. O'Reilly Media, Inc., 2011.

[12] Vaquero L M, Rodero-Merino L, Morán D. Locking the sky: a survey on IaaS cloud security[J]. Computing, 2011, 91(1): 93-118.

[13] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing[J]. Journal of Network and Computer Applications, 2011, 34(1): 1-11.

[14] Eucalyptus Admin Guide 3.4.2 URL: https://www.eucalyptus.com/docs/eucalyptus/3.4/admin-guide-3 .4.2.pdf

[15] CloudStack Admin Guide 4.1.1 URL:http://cloudstack.apache.org/docs/en-US/Apache_CloudStack/4. 1.1/html/Admin_Guide/index.html

[16] OpenStack Securtiy Guide URL: http://docs.openstack.org/securityguide/security-guide.pdf

[17] Peng J, Zhang X, Lei Z, et al. Comparison of several cloud computing platforms[C]//Information Science and Engineering (ISISE), 2009 Second International Symposium on. IEEE, 2009: 23-27.

[18] Microsoft URL: www.azure.microsoft.com

[19] Amazon URL : http://aws.amazon.com/

[20] Google URL: https://appengine.google.com

[21] Singh P, Singh V P, Pachauri G. Critical Analysis of Cloud Computing Using OpenStack[J]. 2014.