Multidisciplinary Review Journal

Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 4, 2020

Review Article

SURVEY ON DATA SECURITY ISSUES RELATED TO MULTI-USER ENVIRONMENT IN CLOUD COMPUTING

V. Devi Satya Sri[1], Srikanth Vemuru[2]

[1]Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
[2]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Received: 13.12.2019 *Revised: 25.01.2020* *Accepted: 23.02.2020*

Abstract
Usage of Multi-user Environment services leaves traces of the client data on different servers (passwords, keys etc.). Since, most of the cloud servers use virtualization technology, it is difficult to find the co-resident virtual machine attacks in the private and public cloud systems. This was the great risk for the client accessing the multi-user environment services, with the leakage of their confidential information. So several memory reconstruction mechanisms are their by examine those mechanisms and develop a mechanism to only authorized person can access the confidential data. This paper introduces an overview of cloud data replication issues, data security issues and cloud attacks in the multi-user cloud computing environment. Hence, It is necessary to decrease the server maintenance cost by migrating the cloud user's sensitive data in a secured framework for future reference.

Keywords: Security, Customer, Provider, Multi-User Environment, Data Remainance.

DOI: http://dx.doi.org/10.31838/jcr.07.04.30

INTRODUCTION

Storage outsourcing is progressively more increasing in educational and industrial sectors for its simple sharing, ease and high availability and accessibility. So many organizations like Google, Microsoft and amazon gives their very own distributed storage benefits in that where clients transfer their data to the servers, getting to them from different gadgets and offer them with others. In distributed computing, you need not stress over IT framework, since you need not claim one [1]. Utilizing cloud is a superb method to decrease the business cost and make it progressively gainful. Distributed computing presents IT on request. despite the fact that distributed storage administrations are generally embraced, their still stays a few security issues and protection issues. Conventional strategies are not relevant well for the multi-client cloud condition.

Researchers proposed powerful systematic techniques for single-client situations, the issue in multi-client condition has not been explored adequately. A practical multi-user cloud storage system needs the high security and privacy for clients and vendors. Putting away Data in the multi-client condition like cloud is extremely simple and less compelling, however dealing with the information in the distributed storage is troublesome assignment to perform. A portion of the significant difficulties multi-client cloud condition face today is respectability reviewing, confirmation, get to controlling issues, Network issues, erasing the information in a safe method to maintain a strategic distance from security blemishes. Cloud is used by huge number of clients simultaneously and the number records transferred in cloud is likewise high.

The rest of the paper is sorted out as fallows section 2 clarifies some related work and section 3 clarifies Security issues, Threats and attacks in multi-user environment and section 4 covers proposed counter measures and solutions to mitigate the issues in multi-user environment and finally section 4 fallows conclusion and future scope.

RELATED WORK

In order to overcome the security issues related to multi-user environment, various approaches have been proposed in the literature. Each work tend to cover a particular issue related to multi-user environment. Thus this section summarizes some of these proposals.

Jelciana et al. [3] It explians the various information issues and security in distributed model in muti-user condition and design a strategy to defeat the issues and information security issues in four classes initial one is CIA related security issues(confidentiality, respectability and accessibility) and second one as AAC related security issues (Authentication and Access Control) and third one as Broken Authentication Session and Access and the final one are Other data related security issues.

EI Balmany chawki[4] Investigates security issues inside in Infrastructure As A Service model segments for sake of cloud service provider and client security practices and the CSA top 12 dangers and its impact on Infrastructure As A Service model was explained but it does not propose any security technique to overcome the issues.

Zhiqiang Lin[5] TO advance the field of cloud computing propose virtual machine introspection for producing cloud based applications allows one device in a virtual machine to monitor the another device but this concept needs as many as hosting providers.

SYH-YUAN TAN [6] He said that Yang et al's. Doesn't appropriately accomplish encryption one wayness for the collusion attack and key only attack .In key only attack attacker can pretend to be original user to the attribute authorities to forge user attribute secret key with the knowledge of public parameters only and in the client arrangement assault malicious clients can conspire by sharing keys unauthorizedly to decode the cipher content to plain content. In order to solve these issues syh-yuan tan suggested pairing based proof of knowledge protocol for lacking of authentication mechanism in the key issuing protocol, then again, the collusion attack is overwhelmed by to embrace the safe decoding farmula from Lewko and waters.

Juvanna [7] To enhance the distributed storage and make the distributed storage progressively effective they propose the safe review work in distributed storage to decrease the duplication information in distributed storage and furthermore clarifies the safe evaluating, deduplication, and secure document erasure in the cloud and proposed a system to reduce the time of audit and increase the reliability of duplication process and secure data deletion by clustering of data and data remanance.

Shalini[8] Showing two secure frameworks seccloud and seccloud+ for getting the data integrity and deduplication in cloud. By comparing to previous works this approach is used to greatly reduce the data uploading and audit phases by seccloud concept and seccloud+ is designed to provide users data always encrypted before uploading and provides integrity auditing and secure deduplication on encrypted data. Introduces auditing entity with maintenance of map-reduce cloud in seccloud and similarly seccloud+ provides file confidentiality. But these process takes lot of time for auditing because to figure all the exponentiation s for every challenge block and coefficient for every column of S. correspondingly the number of blocks increases the auditor time increases.

SECURITY ISSUES RELATED TO CLOUD MULTI-USER ENVIRONMENT

Data Breach

Security of the data moving from data center to another data center, the risk of malicious, accidental and intentional information break is high in this, secret or ensured information is seen, discharged or taken by unauthorized individual. Data Breach through fiber optic Networks:- Until US Security Forces discovered the illegal fibre device in telco verizons optical network placed at mutual company the data transfer through fibre optic cables are very safe. [9]

Shared Technology related Issues

To achieve the high end scalability the increased leverage of resources gives the attackers a single point of attack. Controls to ensure that one user cannot interface with the security of another user and also this failure can be used by an attacker to gain access from one organizations resource to another organizations assets or data.

Denial of Service

The extent of this attack can effect all the cloud users. The main aim of this attack is the services assigned to the authorized users such as memory, disk space, processor power, network bandwidth are make unavailable to the authorized user. Vulnerabilities within insecure interfaces and APIs, unlimited allocation resources causes the DOS attack, at that time authorized user unable to access the service. Intrusion Detection System (IDS) is the most used popular method to solve this type of attacks [10].

Distributed Denial of Service

A distributed denial-of-service attack is a malicious attempt to disrupt normal traffic in a network. It is an advanced version of DOS in terms of denying the important services running on server by flooding the targeted system with large number of packets for that the target server cant handle the service.

Malicious insider

Insider threat has become a serious threat in cloud environment. The malicious insider attack is one of the old employee or current employee in the organization who is intentionally access the unauthorized services through their old credentials this effects the confidentiality and security of the data[4].

Account or service hijacking

Account or service hijacking exists I cloud computing where attacker takes over the control of users account. Can be performed through weak credentials, phishing, fraud and using social engineering. Loosing access to privileged account results loss of service. The attackers can do malicious activities which may effect data privacy and confidentiality, data manipulation and even data deleted and may redirect any transaction. This attack effects all the layers of the cloud computing [4].

Cyber-Attack

One of biggest advantages of cloud are access resources and services through the internet by anyone in anywhere and anytime, so this advantage attracts cyber criminals they perform their cyber-attack activities on the basis of cloud services.So thus cloud resources are the attractive ground for cyber attackers due to the huge resource available in centralized manner. So thus huge cloud resources under the disposal of cyber attackers rises threats to the cloud environment.

Insecure Interfaces, APIs, and Browser Vulnerabilities

To allow customers to interact, manage and extract information from cloud services APIs are used by the cloud service providers and software developers these are the only asset outside of the trusted boundary with a IP address so these are the first one to attract the attackers due to this interfaces and APIs use an unknown access. Browser based attacks and Insecure interface or APIs causes a significant risk for cloud computing.[4]

Data Remanance

Residual representation of a data even after the deletion performs. Any sensitive data is protected from unauthorized access and distribution but also safely erased at the end of the use. Attackers may be able to retrieve the residual data from servers. The data remanance is the major threat for sensitive data in cloud the cloud providers doesn't widely concentrate on the secure data deletion due to huge cost and time[2].

Data leakage and Data loss with no backup

This occurs when the data is handled not correctly in data while storing, transferring or processing. Data ownership losses by operational failure etc causes data loss.An accident may lead to permanent deletion of data without providing any backup facility to retrieve again.

Human errors

Many cloud security failures are caused by customer faults. Abusive use:-The cloud users use their trail period of cloud services to launch Zombie or DDOS attacks.

Advanced persistent threats

To compromising the confidentiality, integrity and availability the attackers not only use targeted cloud environment but use public cloud services to conduct their attacks. The attackers build a processing framework from which they smuggled information and intellectual property.

Insufficient Identity, Credentials and Access Management

The need user access and control identification is high in cloud due to its nature. Existing solutions are not sufficient for access management need to develop better access control and identity management.

Network availability and Data Latency

The cloud services operated through the internet only without the internet we doesn't access the cloud and data latency increases because longer time intervals for data transfer and other network related activities the distance from sources are very large.

Man in the Middle attacks

In this the attacker inject false information between the source and destination, this attack mainly occurs Saas phase.

Domain Name Server(DNS) attacks

The Domain name server provides easy remembering of IP addresses for this the attacker may perform attack and routed to malicious cloud by migrating one IP address to another IP address.

CAPTCHA Breaking

Completely Automated Public Turing test to tell Computers and Humans Apart and also called Human interactive proofs(HIP) can protect privacy.

By using advanced machine learning and AI techniques attackers trained their system After that they can run it on a target system or web server, and launch coordinated DDOS or spam posting attacks on websites where that CAPTCHA service is in use[11].

DATA MIGRATION AND SECURITY ISSUES IN MULTI-USER CLOUD COMPUTING ENVIRONMENT

Liang et. al, [12] implemented a data protection and replication model in the cloud computing environment. In this work, they considered static or limited cloud data and services to implement a secured replication model. As the future work, they have suggested dynamic data survivability, security, data replication and data partition techniques to protect data against unauthorized access.

Mokadem et. al, [13] proposed a new data replication strategy in cloud data centres. In this model, data cost and replication strategy are improved on various cloud resources. As the future work, they have suggested to implement replication strategy for real-time multi-cloud data centres.

Gustavo et. al, [14] implemented a replication and monitoring of resources in Aurora instances. In this work, they have implemented a new replication strategy to monitor and manage cloud instances and resources for efficient cost optimization. In the future work, they have suggested the monitoring of multiple remote data centres with resource sharing.

Agnieszka et. al, [15] developed two models to provide security to cloud users. In the first model, they provided scoring method to schedule tasks in cloud environment. In the second model, a cryptographic model is designed to provide security to each task. In the future work, they have suggested to implement new schedulers in amazon AWS servers.

Jinxia et. al, [16] implemented a novel multi-copy provable data possession scheme for integrity verification of replication data in cloud computing environment. This model is limited to small datasets. As the future work, they have suggested to expand this model on large data sets.

Rauthan et. al, [17] developed a new encryption model on cloud user's data. They implemented this model on the sql operations in cloud environment.

Zhou et. al, [18] implemented an advanced secured deduplication model using access control scheme in cloud computing.

Figure 1, describes the overview of multi-user secured data migration and recovery model on dynamic cloud computing environment. In this framework, initially, different users are represented as U(1)....U(n). Each user's task is given to physical machine for task execution. Since, physical machine contains k number of virtual machines. Each user's application is scheduling to kth virtual machine (VM). Each VM executed data analysis model to perform operations on the user's data. In the data migration phase, each user's application data is migrated to VMs for future reference. Here, each VM is shared with other resources. Hence, a security layer is required to preserve the privacy of the data analysis and application data. Propose framework to overcome different security issues related to multi user environment in Cloud by considering the issues like Data remanance, Access control and authentication, key agreement and encryption.

To perform data classification to make the procedure simple and also effective

In this process Clustering of data is performed data is classified to manage efficiently and easily. By using machine learning algorithm makes clustering more easy and effective for huge volume of information. Once the data is created identify the sensitive data, classify the data, define policies and create access methods for different types of data.

Authentication and access control permissions

Authentication and access control permissions is a security function that protects shared resources against unauthorized accesses.All the access control rights are stored in access control list (ACL) but in multi-user environment the access control list is very large and it be difficult so the authentication and access control permissions made totally depends on client view rather than cloud service provider priority is given to the client.

Key agreement

Keep the key at safe place, i.e. outside the cloud where data is stored.

Encryption

Strongly encrypt the data. Throughout the data life cycle it is in encrypted form only.

Multi-user Data replication and Application storage framework

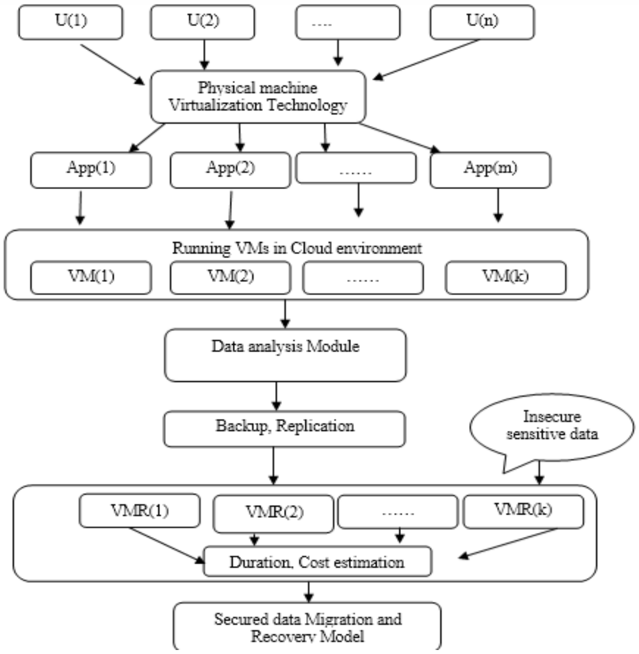

Figure 1: Overview of secured data migration and recovery model on dynamic cloud computing environment

CONCLUSION

The usage of cloud computing is rapidly increasing for its well benefits for customers but security and privacy issues are identified and increased rapidly for its multi-user environment. This paper addressed challenges and issues of multi-user environment in cloud and also some counter measures and solutions to mitigate security issues in multi-user environment. In spite of several security issues cloud computing is becoming a huge attractive.

REFERENCES

1. P. Mell and T. Grance. "The NIST Definition of Cloud Computing. NIST Special Publication 800-145 (Draft)", Retrieved September 10, 2011.
2. Khalid Aissaoui, Hafsa Ait idar, Hicham Belhadaoui, Mounir RIFI, Survey on Data Remananece in Cloud Computing Environment, 2017 IEEE.
3. P. Ravi kumar, P. Herbert, P. jelciana. "Exploring Data Security Issues and Solutions in Cloud Computing", Elsevier ICSCC 2017, 7-8.
4. EI Balamany chawky, Asimi Ahmed, Tbatou Zakariae "Iaas Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors", ELSEVIER BDNT 2018.
5. Zhiqiang lin,"To Advance the Field of Cloud Computing",2016
6. Mikal Rekdal, Aravind Pai, Ravi Choudhari, Muddukrishna Badamane Sathyanarayana. "Applications of Co-Crystals in Pharmaceutical Drugs." *Systematic Reviews in Pharmacy* 9.1 (2018), 55-57. Print. doi:10.5530/srp.2018.1.11
7. Syh-Yuan Tan. "Cmment on 'Improving privacy and security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing'", IEEE Volume 4, 2016.
8. N. Dinesh and I. Juvanna "Dynamic Auditing and Deduplication with Secure Data Deletion in Cloud" Springer Nature Singapore Pte Ltd, 2017.
9. N. Shalini, P.D. Chidhambara Rao "Secure Auditing and Deduplication Data in Cloud", ISSN 2321-8665, Vol. 04, Issue.09, July-2016.
10. Jessica T., "connecting Data Centers over Public Networks", IPEXPO.ONLINE, April20, 2011.
11. K. Vieira, A. Schulter, C.B. Westphall, and C. M. Westphall, "Intrusion detection techniques for grid and cloud computing environment:, IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43,2010. DOI:10.1109/MITP.2009.89.
12. Catalin Cimpanu for Zero Day "New Machine Learning Algorithm breaks text CAPTCHAS easier than ever" December 18, 2018.
13. Liang Luoa, Liudong Xingb, Gregory Levitina, Collaborative Autonomic Computing Laboratory, School of Computer Science, University of Electronic Science and Technology of China University of Massachusetts, Dartmouth, MA 02747, USA
14. Riad Mokadem, Abdelkader Hameurlain A Data Replication Strategy with Tenant Performance and Provider Economic Profit Guarantees in Cloud Data Center.
15. Gustavo B. Heimovski, Rogerio C. Turchetti, Juliano A. Wickboldt, Lisandro Z. Granville, Elias P. Duarte Jr FT-Aurora: A Highly Available IaaS Cloud Manager Based on Replication
16. Agnieszka Jakóbika, Daniel Grzonkaa, Francesco Palmieri Non-deterministic security driven meta scheduler for distributed cloud organizations.
17. Jinxia Wei, Mingxu Yi, Lingwei SongEfficient Integrity Verification of Replicated Data in Cloud Computing System
18. J.S. Rauthan, K.S. Vaisla VRS-DB: Preserve confidentiality of users' data using encryption approach
19. Lei Zhou, Anmin Fu, Shui Yu, Mang Su, Boyu Kuang Data integrity verification of the outsourced big data in the cloud environment: A survey
20. Osken, A., Yaylaci, S., Aydin, E., Kocayigit, I., Cakar, M.A., Tamer, A., Gündüz, H.Slow ventricular response atrial fibrillation related to mad honey poisoning(2012) Journal of Cardiovascular Disease Research, 3 (3), pp. 245-247. DOI: 10.4103/0975-3583.98904