iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4355

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

A Conceptual Analysis and Review on Cloud Computing Data Security: Challenges and its Solutions

Saima Safa[1], Safdar Tanweer[2], Syed Sibtain Khalid[3]
[1]*Student,* [2,3]*Jamia Hamdard, New Delhi*

Abstract: ***Cloud computing is one of the most developing technology in computing. It gives so much benefit to users. But still it has many different security issues and challenges. In this paper we explore some major issues and challenges of cloud computing in multi-tenant environment, and prefer some useful techniques and methods to overcome the challenges and issues in cloud. As we know that now a days business fully depends upon cloud, cloud uses in any business directly or indirectly and if any data threat or leakage has happened, that will affect the business on daily basis. Leakage of data or threats of data can break the trust of cloud users that is why it is very important that cloud companies give special attention on the cloud security issues. So here I am discussing some suggestion on the basis of review to avoid data security issues in cloud computing.***
Keywords: Cloud Computing, Data security, confidentiality, Key management

I. INTRODUCTION

In recent years cloud computing becomes more popular. As a business model Cloud computing is developed mainly from grid computing and distributed processing etc. famous companies like Google, Microsoft, IBM, Amazon, Rack space have provided cloud services on the Internet[1]. We can be considered cloud computing as a new computing technique which provides services on demand network. Nowadays cloud computing data security is very important. If security measure does not provide properly then data security will be in high risk into the cloud. There are lots of security issues in the cloud computing. But we can find out the solution by identifying about that challenges and issues. In this paper we discuss about those challenges and issues and their solutions. Here Fig.1 shows the bar chart of security issues and challenges in the cloud computing.

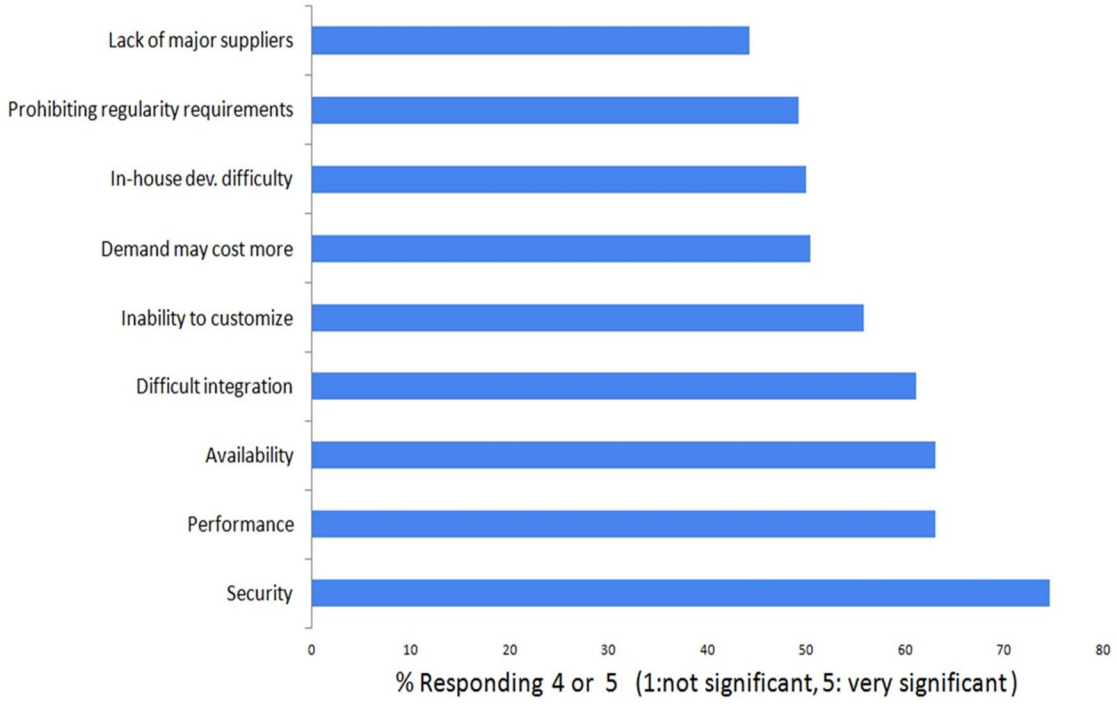


Fig1.Challenges in cloud computing (adapted from [10])

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

II. LITERATURE SERVEY

Popovi and Hocenski gave some useful discussion about the issues and challenges of data security which is a very big problem for the service providers during cloud engineering[2]. Behl explores the cloud computing security issues. He discussed some approaches related to security issue in cloud environment, which is beneficial for security of cloud infrastructure and applications[3]. Sabahi gave a discussion on the data security issues, availability and reliability, Sabahi gave an achievable solution to reduce the security issues in cloud computing[4]. Wentao Liu proposed some systems related to cloud computing and examine cloud computing security issues and its strategies[5]. Mathisen ,E discussed about some keys related to security issues in cloud computing[6].

III. DATA SECURITY ISSUES AND CHALLENGES

As we know that there are lots of data security issues in the cloud computing. which effects badly on business and any organizations. Now a days data security issue is very challenging for every organization and business, Data loss or data leakage are two main factors which effects business and organizations verily badly.so the prevention of that challenges is most important. Here we explore some major issues and challenges of data security in cloud computing and then we use some techniques and methods for prevention of data security issues.

The challenges of security in cloud computing environment can be categorized into network level, user authentication level, data level and generic issues

A. Network Level

The challenges that can be categorized under a network level deal with network protocols and network security, such as distributed data distributed nodes, Internode communication.

B. Authentication Level

The challenges that can be categorized under user authentication level deals with encryption /decryption techniques, Authentication methods such as administrative rights for nodes, authentication of applications and nodes, and logging and monitoring.

C. Data Level

The challenges that can be divided into data level deals with data integrity and availability such as data protection and distributed data.

D. Generic Types

The challenges that can be classified under general level are traditional security tools, and use of different technologies.
Nowadays Cloud computing is very developing technology which is used everywhere, we can say that the whole world depends upon the cloud, It gives a lot of benefits of users, but it faces so many challenges and security issues, In this paper data security techniques and methods are provided to reduce the issues and challenges in cloud computing. Cloud computing security issues can be enhanced in coming times. For the safety of data advance encryption technique can be used for secure data access. The key allocation to the users can be managed in such a way to provide the access only to the authorised user.

E. Locality

Data locality refers to the location of data at different regions in cloud computing. User should know about their data location, but at the time of movement of data to different geographic location laws governing on that data becomes change, because of this changes compliance and data security issues come out in cloud computing [1].
e.g. European union data centre cannot share its citizen profile, so when cloud data stored any individual information its should not shared outside EUROPE, and this will followed by FACEBOOK, DROPBOX etc..

F. Data Confidentiality

Data confidentiality is used for users to keep their private or confidential data in the cloud. Authentication and access control strategies are applied to protect data confidentiality [7].
With using MFA feature in each application data can be more secure because user name and password is not enough to secure application Adding the MFA, it give higher level of security, because it prompt to proof WHO you are and WHAT you HAVE

G. Integrity

Data integrity refers to prevention of data from unauthorized access, and modification. Integrity means that maintaining the consistency, reliability, and trustworthiness of data in cloud computing. To preserve the data integrity data should not be changed in transit and steps should be taken to confirm that data cannot be access by third person or unauthorized person. To protect the data from unauthorized access ACID properties should be used for every transaction in cloud computing [7].

Data packet should transfer over SSL or TLS encrypted methods, and it ensure that there is no CIPHER in network transmission.

All the codes behind running any application in cloud safely attested and tested through different code verifier, so that it can assure data transmission and INTEGRITY get maintained.

H. Data Breaches

Data breaches is one of the most important data security issues, as we know that larger data keep on the cloud, so it may be a possibility of malicious attack on the data in cloud.it may be quite possible that breaches can happen due to insider attack[8].

I. Malware Injection

Malware injection is also a security issue in cloud computing.in this process code or scripts can be inserted into cloud services, which acts like SAAS service model and runs on cloud server. after the execution of injection cloud begins operating with it, attackers can spy and steal the information's. According to some report's malware injection is major issue in cloud computing [8].

J. Data Loss

Data loss is the biggest problem in cloud. several big organizations like SONY, SAMSUNG, Google Amazon have suffered data loss, data loss can happen due to malicious attacks on cloud services, or if data erase by the sevice provider un-intentionally, then data loss also happen. you can prevent of data loss by reviewing provider's backup process [8].

Data loss can be prevented by multiple process

1) Running CRONE JOB in operating systems to get incremental backup
2) Running Full Backup process to get timely manner
3) If data loss happened then run the RESTORE process again through CRONE JOB in every operating system
4) Each data packets / FULL BACKUP should require every FORTNIGHTLY
5) Incremental backup / restore data can be ENCRYPT / De-Crypted

IV. SOLUTIONS & TECHNIQUE USED

Encryption is one of the best methods to protect useful information and data in cloud computing. Homomorphic encryption is a type of encryption system suggested by Rivest et al. homomorphic operation is a system which implement operations on encrypted data beyond the knowing of private key(beyond decryption). Only client has secret key. After decrypting the result, we will see, it is same as the raw data [9].

Hybrid technique is recommended for data confidentiality and integrity. Which uses for the key sharing and authentication techniques. By using the utilizing powerful key sharing and authentication process, connection becomes more secure and useful between the user and cloud service provider. RSA public key algorithm is used for the purpose of secure distribution of keys [11]. A three-layered data security technique is recommended.

First layer for the authenticity of the cloud user either by one factor or by two factor authentications; Second layer is used for encryption of the user's data. and the Third layer recovers data vastly by using the decryption process. Data concealment can be used to maintain the data confidentiality in the cloud.

Delettre et al proposed a data concealment concept. Basically this concept is used for Data base security. Data concealment involves merging real data with the usual fake data to invalidate the real data volume. Although the user can recognize and isolate the real data from false data. This technique raise the overall size of real data. But increase the security for the private data. The main purpose of Data concealment is to make the real data secure from destructive users and attackers [12].

A. Although cloud computing can add multiple access points using VDI (Virtual Desktop Infrastructure), and that has to be access by Fine Grained authorized access points.

V. ADVANTAGES

1) with using VDI each individual no need to login into whole systems, VDI have special authorization access of datacentre, that can be shared by multiple accounts, e.g. in single data centre if MS Windows 10 installed and shared by 100 accounts of that domain, so company can save 100 of Thousand in license cost as well as all updates and patches will be done by single deployment process.

2) Cloud systems will be well managed by using central identity management solution assigned each individual Role which is specific to application and it will support multi-tenancy which can be managed by layers of Business Roles i.e. Tenant Admin, Business user, Client Admin

3) each business role attached by individual systems or IT rules e.g. IT Manager will be associated with multiple access of different applications IT manager can manage multiple applications based on their FINE GRAINED AUTHORIZATION Identities and role correlate with each other depends on individual's ROLE BASED ACCESS CONTROL

4) Each application will follow Single Sign on or CDSSO using HEADE

5) Each application can share multiple authentication systems and share access token info as well as ID TOKEN details, so that when next application try to get access no need to do RELOGIN, because of ACCESS TOKEN already available in HEADE

6) Cloud systems or application can be well managed and followed by multiple compliances i.e. FEDERAL, SOX, HIPPA etc

7) Each organization follow different compliances, i.e. password policy for HIPAA is different than SOX, and each Account creation policies for FEDERAL is different than HIPPA i.e. for Health Care as well Role assignment policies , entitlement assignment is differ in different DOMAIN i.e. ORGANIZATION

8) Cloud computing managing PAAS Services to build central DBMS using virtual address i.e. Azure SQL services or MONGO DB, or NOSQL etc.

9) If customer want to buy individual MSSQL server using VMWARE or individual H/W based MS RDBMS the cost will be 10 Times higher than Cloud based PAAS services, so Microsoft or Amazon have their own DB PAAS services, so that single deployment process can update or PATCH with latest version of binaries as well as customer will save lots of money using this CLOUD BASED PAAS Services

VI. CONCLUSION AND FUTURE WORK

Nowadays Cloud computing is very developing technology which is used everywhere, we can say that the whole world depends upon the cloud, It gives a lot of benefits of users, but it faces so many challenges and security issues, In this paper data security techniques and methods are provided to reduce the issues and challenges in cloud computing. Cloud computing is managing central product management systems that uses multiple services i.e. IaaS, Paas and SaaS, which uses multiple technologies i.e. Central IAM solution, SSO and RBAC model as well as Fine grained authorization. In future, cloud computing security can be improve.so in future work, cloud computing can be developed some advance encryption techniques, also some advance key management techniques which can be used to allot the key to authorized users. By this way cloud computing can more secure in future.

REFERENCES

[1] www.sciencedirect.com R. Velumadhava Raoa,*, K. Selvamanib,*2014.Data security challenges and its solutions in cloud computing..International conference on Intelligent Computing Communication & Covergance(ICCC-2014)Conference organized by Interscience Institute of Management and Technology Bhubaneshwar,Odisha,INDIA.

[2] Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges, in: MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.p.344-349

[3] Akhil Bhel, Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congresson, Mumbai, 2011.p.217-222.

[4] Farzad Sabahi. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks(ICCSN), May 2011.p.245-249.

[5] Wentao Liu. Research on Cloud Computing Security Problem and Strategy, in: 2nd International Conference on Consumer Electronics Communications and Networks (CECNet), April 2012.p.1216-1219.

[6] Eystein Mathisen. Security Challenges and Solutions in Cloud Computing, in: International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 2011.p.208-212.

[7] https://journals.sagepub.com/doi/full/10.1155/2014/190903 Yunchuan Sun,,Junsheng Zhang,Yongping xiong,Guangyu zhu,,First published july 16,2014,|Data Security and Privacy in Cloud Computing |Review article. https://doi.org /10.1155/2014/190903

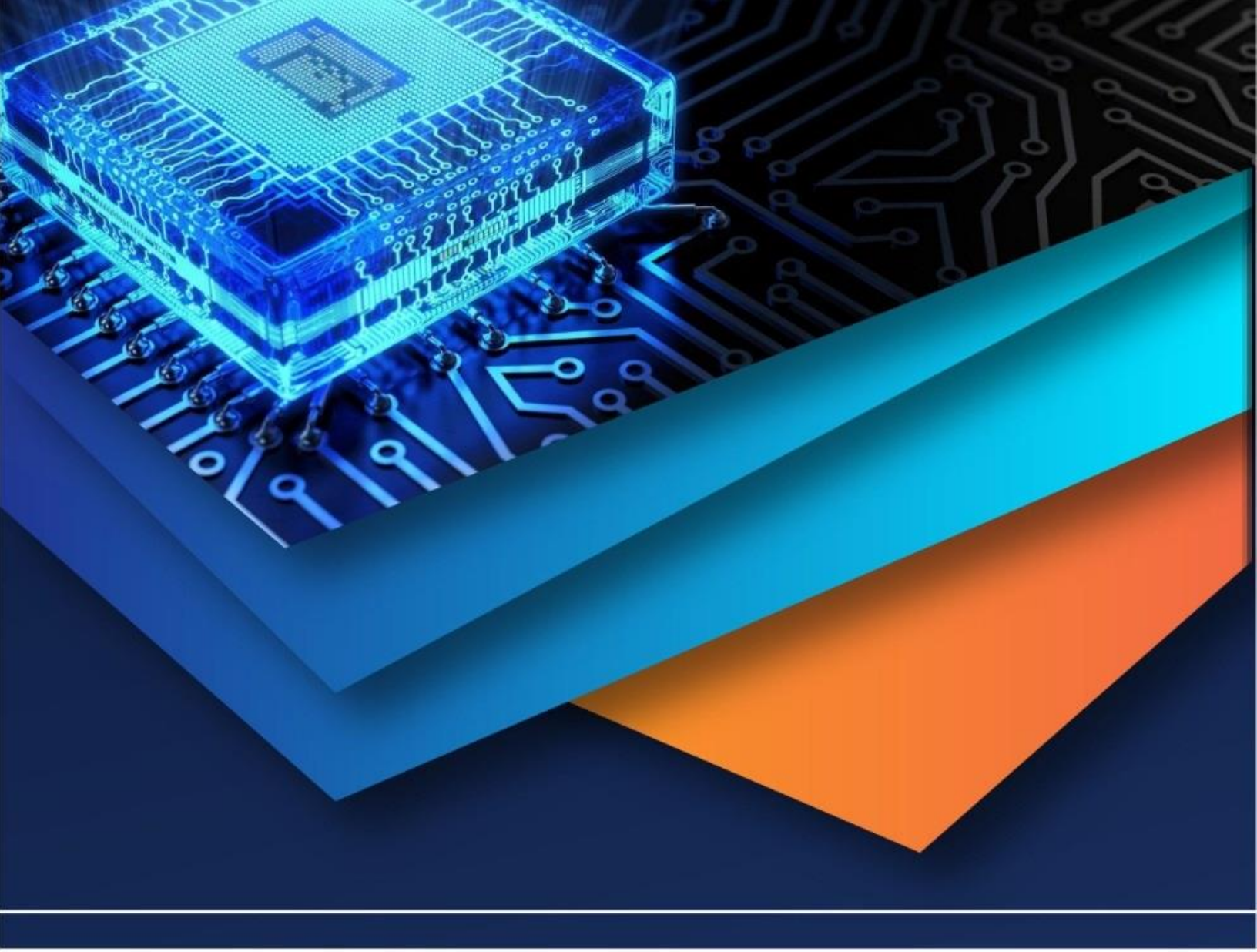
[8] https://www.incapsula.com/blog/top-10-cloud-security-concerns.html

[9] https://arxiv.org/pdf/1409.0829 1Maha TEBAA, 2Said EL HAJII 1Laboratory of Mathematics, Computer and Applications, University Mohammed V–Agdal, Faculty of Science, Rabat-Morocco,Mohammed V–Agdal, Faculty of Science, Rabat-Morocco,.Secure Cloud Computing through Homomorphic Encryption elhajji@fsr.ac.ma

[10] Available on file.scrip.org. Osama Harfoushi[1], Bader Alfawwaz[2], Nazeeh A. Ghatasheh[3], Ruba Obiedat[1], Mua'ad M. Abu-Faraj[4.] Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review

[11] www.ijsr.net .Pooja Bharadwaj1, Shivani Mankotia issue on 8 august 2016 : Cloud Computing Security and RSA Algorithm International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391 Licensed Under Creative Commons Attribution CC BY Up in the Air:

[12] Available on Google Scholar. Biedermann, S., Katzenbeisser, S. POSTER:2013, on Computer & Communications Security event-based isolation of critical data in the cloud Proceedings of the ACM SIGSAC Conference.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY