IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CHALLENGES IN CLOUD SECURITY A REVIEW

[1]Rohit Kapoor

[1]Research Scholar

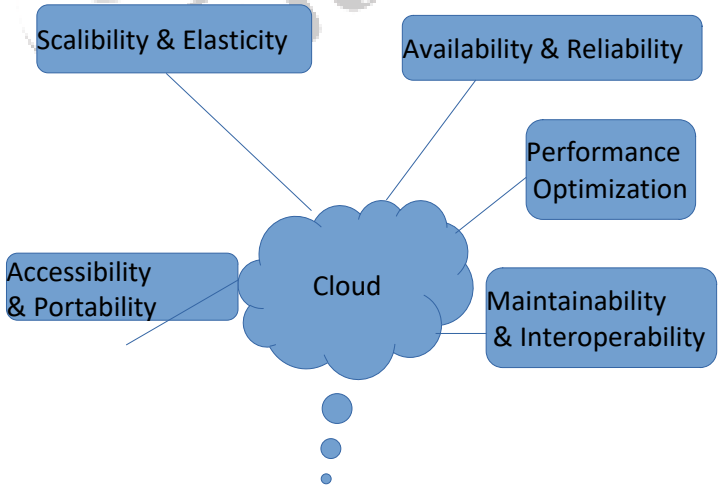
1Maharishi University of Information Technology, Lucknow

Abstract: - Cloud computing provides a mechanism that offers on demand, elasticity, measured services at reduced cost, which attracts the organization & users to utilize the cloud environment without investing much on hardware & maintenance. One major concern regarding cloud environment is that, user is availing cloud services to store the data that is managed by third party, which brings threat to user. As the resources & services are available on shareable basis that can be accessed remotely it brings in an account the problems that need to be addressed for data security which includes confidentiality, integrity, authentication, multi-tenancy & key management. This paper highlights the different types of issues related to data security in cloud computing environment & discusses the various solutions available for above problems.

Keyword: Authentication, Key Management, Multitenancy

INTRODUCTION:-

Cloud Computing environment is in demand due to various types of benefits it offers, which includes on demand services, easily scalable of computing resources in a cost effective manner. The technology provides an effective centralized computing environment which allows renting of resources (including server, storage, services & applications) according to needs and budget requirements of consumers. Cloud computing has changed the era where the application, resources can be accessed in a virtual manner in a pay as you go basis which reduces the cost of investments by the client in buying hardware/applications.



Cloud Characteristics & Properties:-

There are various advantages of using cloud computing environment on the basis of enterprise & end user perspective's :-

- Reduced Initial Investment

- Reduced Capital expenditure
- Improved resource utilization
- Reduced local computing & storage power

On the basis of the underlying key features we can differentiate between traditional & cloud computing environment.

Key Parameters	Traditional	Cloud Computing
Time	Long establishment time is required	Business ready type approach
Software	Local installation required	No local installation
Hardware	Requires powerful hardware	Requires basics hardware
Computing power	Can be accessed through desktop	Can be accessed through smart devices

Comparison of Traditional Vs Cloud Computing Environment

Due to the fact that cloud services are easily available on shareable basis there is requirement to address the factors associated, so that risk regarding data can be minimized. This paper highlights the various types of risks involved in cloud computing environment & analyzes the present techniques that provide security to the data.

Cloud Service Model:-

- SaaS (Service as Service):- It provides a facility where hosting of software is done on cloud environment rather than downloading & installing the software on client machine which helps to minimize the overhead of space at client side.
- IaaS (Infrastructure as service):- It provides a way in which computing resources along with devices having storage capabilities is available as pay on use basis. In this type of services client have full control on operating system, storage & deployed application but no control on cloud infrastructure. Microsoft Azure, Amazon web service, Rackspace are some of commonly known examples of IaaS.
- PaaS (Platform as a service):- PaaS also known as cloudware is a variation of Saas. In Paas it is quite difficult to switch to other service provider because provider cannot interact with each other. Here Client has full control on deployed environment as well as application hosting environment but have no control over infrastructure. AWS elastic benstalk , Window Azure, Openshit are commonly known examples of PaaS.

As cloud environment offers services using network, also there is sharing of various types of resources including storage medium & computing.

LITERATURE REVIEW:-

[1] **Ashwani Phadke, Devashree Jadhav, This** paper discusses the usefulness of cloud computing environment. It focuses on various types of security issues and attacks in cloud environment. The possible outcomes are reviewed in this paper. It also discusses the security model with cryptographic algorithm to maintain the integrity of data in cloud.

[4] Amal Matrok Aljohani, reviews the concept of cloud computing and discusses various type of issues occurred in cloud computing environment. Some common security risks are discussed in the paper. Various types of breaches are explained. The paper concludes that the level of security must be upgraded to protect the data from breach.

[5]Ramgovind S, Eloff MM, Smith E, suggested an overall security perceptive of cloud computing with the aim to highlight the security concern which should be properly addressed & managed to realize the full potential of cloud computing.

Ni Zhang, Di Liu, Yun Yong Zhang discusses the cloud security impact in perspective to customers &

industry. The paper then suggested the technical solution to the security problems.

Ahmed Albugmi, suggested the security aspects of data in cloud environment. It enhances the data protection and reduces the risk & threat involved in computing. It also discusses the different states of data & addresses them with the help of various techniques which are effective for data encryption during data at rest & transit.

Author	Challenges/ Threats	Proposed Solutions
[1] Ashwani Phadke, Devashree Jadhav	Accountability Trust Data location Data Stealing	Cryptography
[4] Amal Matrok Aljohani	Integrity Confidentiality Availability Data Sanitization	Idea about location of data Data center security policy Backup your data
Ni Zhang, Di Liu, Yun Yong Zhang	Data Leaks Data Compromise Data Wiping	Identity & access management Virtualization • Access Control • Virtual machine monitor • Virtual firewall
Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan	Data Segregations Data Location Data Privacy Data Availability Data Transmission	Suggested that multi-tenancy architecture can be used to minimizes the impact of security issues
M B Benjula Anbu Malar & Dr.J.Prabhu	Data Breach Cloud Abuse Insecure API Loss of Data	Prefer appropriate cloud provider Complete analysis of network traffic Integration of authentication & encrypted communication Confirm the integrity of data running time period

SECURITY ASPECTS IN CLOUD ENVIRONMENT

The three major factors considering data includes confidentiality, integrity & availability which is commonly referred as CIA triad

- **Confidentiality: -** It means protecting data from unauthorized access i.e only intended user is allowed to access the required information during data exchange process. Higher level of confidentiality is required for sensitive data. It can be achieved by data encryption. Data leakage due to human or due to hardware directly affects the confidentiality. Data confidentiality can be hampered depending upon geographical location where the client data resides. As in many cases data is moved from physical boundary of country where there is a

different set of law enforced which introduces a threat to the confidentiality.

- **Integrity: -** It is a concept that averts the data from being updated or deleted. It assures that data is consistent & hasn't being tempered during its life cycle. It is applicable when the data is in moving form.
- **Availability: -** It ensures that user have easy access to the required data, software & hardware when they need them. Data is of no use if is not available when it is required. Availability is majorly affected by denial of service attack. In order to avoid availability problem we should prefer redundancy path, fail over strategies. Majority of cloud service providers ensures 99.9% availability for their servers but it is not revealed that it is for single server or for multiple servers.

Authorization, authentication and non-repudiation1 are other important aspects in respects to the persons who access the data.

- Authorization: - It represents that a person has an authority to perform the desired operation on data or not. For security measures there should be appropriate authentication mechanism to test the identity of client.
- **Non Repudiation: -** It ensures that user cannot refuse or decline the performed task.
- **Accountability: -** Accountability refers to responsibility or how efficiently resources are being managed to meet the required outcome. As data is outsourced to other parities in cloud based environment so user has no control over data rather than they rely on Cloud service provider for data security. Accountability is a serious matter of concern which must be taken into consideration because of following reasons.
  - ✓ Irregular machines deliver incorrect computational result
  - ✓ valuable data may be stolen due to virus attack
  - ✓ Performance of the service offered to customer is degraded if resource are not efficiently utilized

- **Privacy: -** It is a concept in which user have to control over which information need to be disclosed. In other words it ensures that only authorized user have access to the data. As in cloud environment data resides at multiple server ie locations which increases the risk of confidentiality & privacy breaches.

- **Trust: -** Trust signifies the extent of confidence in something. Trust mainly whirls around confidence & assurance that the data, service, people will act in anticipated ways. Trust can be classified in many ways
  - ✓ Human to Human
  - ✓ Human to machine
  - ✓ Machine to Machine
  - ✓ Machine to Human

- **Data Leaks: -** Client is having concern about their data security from two perspectives one from cloud service providers end & another from unauthorized users access. As in multi-tenant environment where clients share resources with other clients, a logical separation is mandatory between them to avoid data leaks.

- **Data Compromise: -** Data can be compromised in various scenarios. Data authenticity can be comprised whenever a client whether govt or private resides there data in Cloud Service provider data center.

POSSIBLE SOLUTIONS

As we have noticed that data security is a major concern that needs to be addressed in cloud environment. There are various methods to address the issues for Confidentiality, Integrity & Availability

- ✓ Data encryption strategies can be applied to data at rest as well as data during transit. Cryptography & steganography are methods that can be utilized to address confidentiality where the first approach help us to encrypt the data so that it is not recognizable by third party (ie apart from sender and receiver) & second approach hides the valuable information so that its presence is not recognized by human eye.
- ✓ Data integrity can be verified by Third party auditing
- ✓ Encryption key should not be stored with encrypted data
- ✓ IDS create a shield which prevents the system from new kind of attacks suspected on a virtual machine. Intrusion detection system can enhance the security of cloud by examining the network traffic for an unusual activity & convey alerts when it finds such an event.
- ✓ Log inspection is responsible for collecting & examines various that of events that include operating system & application log.

There are methods that addresses authentication and access control

- ✓ Single sign on policy may be used which allows user to have a single sign in into application via providing credentials only once & you will be automatically authenticated to related applications. For example the concept is used in google as we sign into google service we are automatically signed or authenticated to google apps, YouTube , google playstore etc. In the same ways office 365 also supports single sign on policy.
- ✓ To get better data protection and to have proper access control on cloud environment, Intrusion Detection System and firewalls can be applied.
- ✓ Some implicit methods should be applied for data protection like RSA cryptosystem

CONCLUSION:-

- ✓ The paper gives a generalized view on the issues encountered in cloud computing environment & provides suitable countermeasures for them. It exhibits two major problems encountered in cloud computing environment which includes data security & privacy. Various approaches like Firewalls, intrusion detection system, log monitoring is used but these approaches are having limitation with regards to data security. So to overcome these limitations steganographic based approaches are a better solution, which makes data hard to figure out with human vision. Various authentication mechanisms like biometric authentication, digitial signature can be used for authenticating the user identity to handle privacy issues. Integration of biometric & steganography will take the security of cloud to next level.
- ✓ So in future work we are looking forward to integrate the concepts of biometric authentication & image steganography to make a more secure system.

REFERENCES:-

[1] Ashwani Phadke, Devashree Jadhav "Cloud Computing an Overview of architectures, security threats & their solutions" International Journal of Science and Research (IJSR) Volume 6 Issue 4, April 2017, 394 - 403

[2] Kunal Chadha, Anvita Bajpai "Security Aspects of Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 40– No.8, February 2012

[3] Amit Sanghi, Sunita Chaudhary and Meenu Dave "Enhance the Data Security in Cloud Computing by Text Steganography" Springer Nature Singapore Pte Ltd. 2018

[4] Amal Matrok Aljohani " Cloud Computing Security issues & data privacy" International Journal of Science and Research (IJSR), Volume 9 Issue 5, May 2020, 1472 - 1477

[5] Ramgovind S, Eloff MM, Smith E "The management of security in cloud computing" (2010) Information Security for South Africa. doi:10.1109/issa.2010.5588290

[6] Zhang, N., Liu, D., & Zhang, Y. "A Research on Cloud Computing Security" Zhang, N., Liu, D., & Zhang, Y. (2013) International Conference on Information Technology and Applications. doi:10.1109/ita.2013.91

[7] Ahmed Albugmi, Madini O. Alassafi & Robert Walters, Gary Wills (2016) "Data Security in Cloud Computation" 2016 Fifth International Conference on Future Communication Technologies (FGCT)

[8] Yoshita Sharma, Himanshu Gupta & Sunil Kumar Khatr "Security Model for enhancement of data privacy in cloud computing" IEEE 10.1109/AICAI.2019.8701398

[9] M B Benjula Anbu Malar & Dr.J.Prabhu "AN ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)

[10] Jahangeer Qadiree, & Mohd Ilyas Maqbool "Solutions of Cloud Computing Security Issues" International Journal of Computer Science Trends and Technology (IJCS T) – Volume 4 Issue 2, Mar - Apr 2016

[11] Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan "CLOUD COMPUTING: STUDY OF SECURITY ISSUES AND RESEARCH CHALLENGES" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4,April 2018, ISSN: 2278 – 1323

[12] Shital A.Hande, Prof. Sunil B. Mane "An Analysis on Data Accountability and Security in Cloud" 2015 International Conference on Industrial Instrumentation and Control (ICIC)

[13] Raniyah Wazirali " Steganographic Authentication in cloud storage for mitigation of security risk" (2017). Steganographic Authentication in Cloud Storage for Mitigation of Security Risks. 2017 25th International Conference on Systems Engineering (ICSEng).