ANALYSIS ON DATA STORAGE SECURITY CONCERNS IN A CLOUD

Dr. Rajesh Kumar

Assistant Professor in Computer Science Govt College for Girls Sec14 Gurugram

Mail Id Rajeshbeniwal78@Gmail.Com

Abstract

A paradigm shift in the design and procurement of enterprise hardware and software is taking place thanks to cloud computing. Because of the convenience they give, everyone is moving their data and applications to cloud data centres. Providers of cloud computing services are required by law to ensure that the integrity, accessibility, privacy, and confidentiality of their customers' data are never compromised. Many CSPs, on the other hand, fail to follow through on this promise. According to this research, data theft and a lack of access to cloud-based information are highlighted. Finally, we've come up with viable solutions to cloud-related issues.

Keywords:*Cloud service provider (CSP), cloud data storage, security issues, policies & protocols.*

1.INTRODUCTION

The ability to develop and acquire enterprise hardware and software on the cloud is a game-changing mechanism. Cloud computing offers a wide range of advantages to its customers, including cost-free services, scalability of resources, and ease of access over the internet. Cloud computing is becoming increasingly popular with businesses of all sizes, from small start-ups to major corporations**(Abbas et al., 2015)** In spite of the many advantages of the cloud, many users are hesitant to save their private or sensitive data there. This encompasses everything from personal health information to emails to sensitive government documents. It's possible that after data are moved to the cloud, the cloud client losesdirect control over their data sources.

By deploying firewalls and virtualization, Cloud Service Providers (CSPs) offer to protect the stored data of cloud clients. CSPs have complete control over cloud apps, hardware and client data, therefore these approaches would not provide complete data protection over the network. Prior to hosting, sensitive data should be encrypted to ensure data privacy and confidentiality from cloud service providers (CSP) **(Mell & Grance, 2009).** As cloud access patterns change, so do the communication overheads associated with encryption schemes. As a result, cloud storage and management must be done in a safe manner to protect data secrecy and privacy. This study emphasis mostly on safety flaws and privacy concerns related to client data.

2.CLOUD DATA STORAGE CONCERNS

No control is given over the data kept in cloud data centres. Any nefarious operations, such as copying, destroying, or editing, can be carried out by cloud service providers because they have complete control over the data they store. Control over the virtual computers is provided by cloud computing. There are more security risks with cloud computing in general because of this lack of control over the data. Encryption isn't perfect, but it's better than plain data when it comes to protecting stored information. There are many more ways to attack a cloud computing system because of its virtualization and multi-tenancy features. Figure 1 has a number of difficulties, which are explained in detail in the paragraphs that follow.

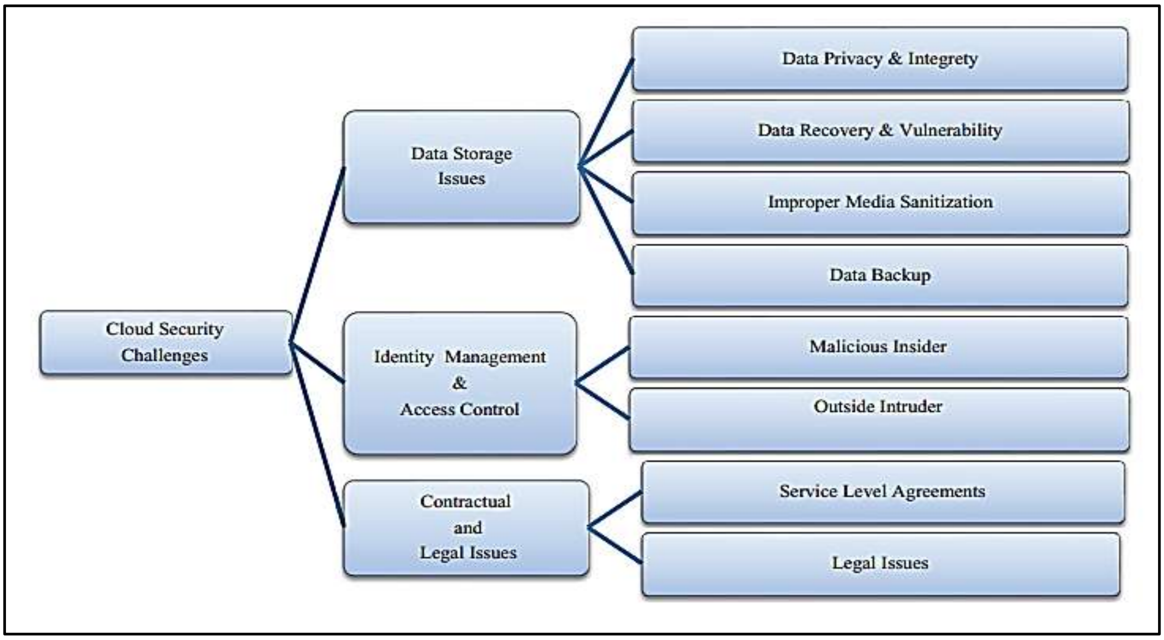
Cloud Security Challenges
Data Storage Issues
Identity Management & Access Control
Contractual and Legal Issues
Data Privacy & Integrety
Data Recovery & Vulnerability
Improper Media Sanitization
Data Backup
Malicious Insider
Outside Intruder
Service Level Agreements
Legal Issues

Figure 1: Cloud security Concerns

2.1 Cloud Storage Concerns

2.1.1 Data Privacy and Integrity

Despite the fact that cloud computing saves money and time, there are still security risks to consider. However, the cloud computing paradigm is more vulnerable to security issues than any other computing architecture we've examined so far because of its inherent flaws. The number of people using the cloud is soaring, as is the number of cloud-based applications. In these situations, cloud users are at greater risk of data loss or theft. Unauthorized access to the data of everyone who uses the cloud is possible if an attack on a data entity is successful. Consequently, cloud data lost its multi-tenant nature as a result of this integrity breach. Technical data and data storage can be lost for SaaS organisations, which are more vulnerable. When data is spread out among a large number of users, additional dangers arise. allows several users to access the same resources at the same time through virtualization. A hostile CSP and/or organisation employee can therefore start an assault. A malevolent user may be able to attack the stored data of another customer while the data of that customer is being processed. When the CSP outsources data storage to a third party, there is a second major concern**(Wang et al., 2011).** Computing in the cloud Key creation and management in cryptography do not fulfil industry requirements. Typical cryptography approaches cannot function in a general cloud computing context without standard and secure cloud key management. Because of this, the dangers of cloud computing can be reduced through the application of cryptography.

2.1.2 Data Retrieve and Liability

Because of the cloud's resource pooling and elasticity, it delivers dynamic and on-demand resource supply to customers. In the future, some of the assigned resources may be shifted to a different user. Data recovery techniques can be used by a malicious user to get access to past users' data if memory or storage resources are involved. **(Alese et al., 2013).** A total of 98 percent of Amazon machine picture files were recovered by the researchers. The security of user information could be jeopardised by the data recovery vulnerability.

2.1.3 Inappropriate Media Alteration

The storage media are cleanse and the reason

(i) A new disc may be required in the future;

(ii) The disc no longer needs to be maintained or cared for

(iii) Services are being massacred. The saved data is at severe danger if the refining is not done correctly. As an early tenant in a multi-tenant cloud, it is not possible to fine-tune.

2.1.4 Data Backup

Having a backup copy of your data is essential when disaster hits, whether by accident or intentionally. The CSP must perform backups on a regular basis to ensure the data's availability. As a precaution against tampering and unlawful access, backup data must comply to stringent security policies and procedures.

2.2 Identity Management and Access Control

Access control and identity management are intertwined with data integrity and confidentiality. To prevent unauthorised access to the stored data, keep a record of the user's identity. Since data is hosted on different platforms from its owner, it is more difficult to impose authentication and access rules in cloud computing. Many organisations in the cloud rely on authentication and authorisation policies. Complex scenarios are created over time by using various methods of identifying and authorising users. A service's IP address is dynamically assigned when it is activated or cancelled since cloud resources are charged per use. The flexibility of users to join and depart cloud resources allows for flexible, on-demand access controls. Access control and identity management are required for all of these features to work properly. Cloud resources need to have identity management in place so that users may join and leave easily. An account can be locked for an extended period of time due to denial-of-service attacks, weak credentials can be reset rapidly, and inadequate logging and monitoring capabilities exist, to name a few.

2.2.1 Malevolent Insiders

From the inside, a company's employees, contractors, and/or third-party business partners can all pose a security risk. Attempts on a cloud service provider's integrity or confidentiality endanger the privacy and integrity of its customers. There is a risk that sensitive information will be compromised in both scenarios... The bulk of the organisation is aware of this attack, which is incredibly valuable. Having insider knowledge of an organization's data storage infrastructure allows them to carry out a wide range of assaults. Because of the difficulties of guarding against this attack and the lack of a coherent response, most companies are ignoring it. Data breaches and loss of privacy are serious concerns for both the corporation and the cloud as a result of this attack. **(Khorshed et al., 2012).**

2.2.2 Intruder

"Outsider attacks" refer to attacks that originate outside of an organisation (Patel et al., 2013). The safety of user data in the cloud is a top priority. Due to a lack of authorization, service providers are unable to access data centres' physical security systems. Trust in the infrastructure provider is required to ensure total data security and privacy. We have no idea how security parameters are implemented in a virtual private cloud system because they can only be changed remotely. Keeping cloud-based sensitive data from being accessed by persons who aren't supposed to have it is a top priority for the infrastructure provider in this procedure.

2.3 Contractual and Legal Issues

When moving to the cloud, there are a slew of legal, regulatory, and contractual issues to contend with. Data centre location, legality and service level agreements all fall under this umbrella **(Andrieux et al., 2007).**

2.3.1 Service Level Agreements

Customers and cloud service providers agree to the terms and conditions of their service level agreement (SLA). The SLA should include the following: When a data breach occurs, the CSP will take remedial activities and keep its performance level at a minimum. The service level agreement (SLA) should specify the security expectations of the customer as well as any additional requirements. Because of the lack of validity of CSP's figures, contract enforcement is getting problematic. To ensure that contracts are non-negotiable and pre-defined, the CSP and user must have a cordial relationship. A hot-button issue is Sarbanes-Oxley and HIPAA rules**(Marston et al., 2011).**

2.3.2 Legal Issues

Legal concerns occur due to the fact that CSP resources are located in countries that are in conflict with each other. A legal issue will arise if the user is relocated from one jurisdiction to another. There are multiple data centres operated by CSPs, each with its own laws and regulations, which are used to store movement data. This could be a severe cloud computing problem.

3.LITERATURE SOLUTIONS

At the same time as describing the research work answers, we also provided a detailed explanation.

3.1 Data Storage Concerns Solutions

(Xiong et al., 2013) devised a time-basedre-encryption method using the ABE algorithm that would allow the group to securely share data while still allowing for access control. Users' renunciation and data security are both ensured by using this kind of data forwarding. When the time period expires, the Cloud Service Provider automatically revokes the user's access to the service (CSP). Using this method of time-based encryption, users can exchange their encryption keys with CSP in the past and have CSP produce new encryption keys on their behalf. To establish access control, the ABE protocol checks a user's attribute set instead of their ID. This system protects the confidentiality and availability of group members' data, but it does not focus on data integrity. Random sampling is used instead of re-creating the complete tree in order to reduce computational redundancy. The Computer Security Alliances (CSA) has compiled the following list of best practises to keep your data safe. Responsibility for the key's scope should be delegated to an individual or an organised body. There should be no use for shoddy encryption standards and sloppy algorithms.

3.2 Identity Management and Access Control Solutions

RB MTAC, a new solution to multi-tenant access control, has been recommended. As part of the role-based access control framework, identity management is integrated. User registration with CSP is required before they may make use of this functionality. Creating an account on the CSP portal requires a password. As soon as a user logs in using these credentials, they'll be forwarded to the role assignment module, where they'll be assigned roles inaccordance with their enrolment information. The identity module will then be returned to the cloud environment **(Yang et al., 2013).**

3.3 Contractual and Legal Issue Solutions

As a result, clients benefit greatly from the cloud computing environment, but they also put themselves at significant danger if service level agreements are not adhered to. As a means of reducing the security risks associated with cancellation or breach of a Service Level Agreement (SLA), they developed a method. This technique is based on a risk-awareness renegotiation algorithm. An algorithm that uses a risk-averse strategy to discover the most acceptable level of service meets the needs of users. This method does a complete analysis and renegotiation of services at runtime for service replacement or cancellation. Following the SLA, risk variables are re-evaluated and updated **(Hale & Gamble, 2012).**

4. CONCLUSION

On-demand access to data and application software is provided via the internet, needing no management effort from the user. In the cloud, there are no binding policies or promises that customers may rely on. Confidentiality, integrity, and availability of data will be compromised as a result of this. This study focuses on data storage security difficulties in cloud computing, which encompasses a wide variety of security concerns. Towards the end of this section, we looked at possible solutions to cloud storage's privacy and confidentiality issues.

Reference

1. Abbas, A., Bilal, K., Zhang, L., & Khan, S. U. (2015). A cloud based health insurance plan recommendation system: A user centered approach. *Future Generation Computer Systems*, *43*, 99–109.

2. Alese, B. K., Adetunmbi, A. O., & Adewale, O. S. (2013). Elliptic Curve Cryptography for Securing Cloud Computing Applications. *International Journal of Computer Applications*, *66*(23), 10–17.

3. Andrieux, A., Czajkowski, K., Dan, A., Keahey, K., Ludwig, H., Nakata, T., Pruyne, J., Rofrano, J., Tuecke, S., & Xu, M. (2007). Web services agreement specification (WS-Agreement). *Open Grid Forum*, *128*(1), 216.

4. Hale, M. L., & Gamble, R. (2012). Secagreement: Advancing security risk calculations in cloud services. *2012 IEEE Eighth World Congress on Services*, 133–140.

5. Khorshed, M. T., Ali, A. B. M. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, *28*(6), 833–851.

6. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176–189.

7. Mell, P., & Grance, T. (2009). Perspectives on cloud computing and standards. *Usa, Nist*.

8. Patel, A., Taghavi, M., Bakhtiyari, K., & Júnior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*, *36*(1), 25–41.

9. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2011). Toward secure and dependable storage services in cloud computing. *IEEE Transactions on Services Computing*, *5*(2), 220–232.

10. Xiong, J., Yao, Z., Ma, J., Liu, X., & Li, Q. (2013). A secure document self-destruction scheme with identity based encryption. *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, 239–243.

11. Yang, S.-J., Lai, P.-C., & Lin, J. (2013). Design role-based multi-tenancy access control scheme for cloud services. *2013 International Symposium on Biometrics and Security Technologies*, 273–279.