IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Comprehensive Analysis of Cloud Security Risks and Mitigation Strategies

Nikhil Gola, Tanishq Parashar, Mayuri Ahuja
Department of Computer Science and Applications
Sharda School of Engineering & Technology, Sharda University, Greater Noida, India
nikhilsarthak1234@gmail.com

Abstract: *After the Covid 19 pandemic the demand for cloud has skyrocketed. With Cloud Providers giving attractive benefits to the consumers like over the network resource sharing. Particularly data storage is the most prominent feature available in cloud computing. Data owners consider cloud a safer way to store and manage data than traditional ways of storing it locally on physical systems. Even large organizations and govt. sectors are shifting to cloud environment for reliable and cheap data storage alternative. Even with so many strengths of a cloud few challenges arise in storing sensitive and non -sensitive data. Data security on cloud is a growing phenomenon which is primarily caused by intruders, hackers and attackers. Many researchers have worked on these problems and proposed various techniques and methods to ensure data security in cloud environment. In this paper, detailed study and investigation is performed on few of the research papers that is published over the period of time in this field. This literature paper gives insights about data breaches and data security challenges in cloud environments.*

Keywords: Cloud Computing, Data Security, Data Breaches

I. INTRODUCTION

Cloud Computing is a resource pool or network of remote servers hosted over the internet for storage and processing data. Cloud Computing is also called ubiquitous computing, the resources can be accessed anywhere anytime with a reliable internet connection at hand. Cloud consumers pay for the resources they use with a "Pay as you go Model".

Before talking about the security concerns, it is necessary to know about cloud architecture. Three significant actors in cloud computing are Cloud service Providers (CSPs), Cloud Brokers and Cloud Consumers. Cloud Providers are organizations that make the resources available to consumers and monitor resource provisioning. Cloud Brokers is an intermediate between cloud service providers and consumers, negotiates relationships deliver the services in an efficient way. Cloud Consumers are the end users, utilizes the resources as per need.

Some defining featured of cloud computing are on-demand provisioning, the resources are available to the consumers as per demand. Over provisioning and under provisioning is managed at the service provider's side. Elasticity is one of the highlighting features, for e.g., When a website is accessed by a ton of users during peak hours, the network traffic is managed by providers by creating more servers. On the other hand, when the website traffic is less the servers automatically scales itself back down. Another important feature is Service Level Agreements offered by cloud service providers which guarantees resources availability, capacity and efficiency.

There are three types of cloud deployment models in the industry, Private Cloud, Public Cloud and Hybrid Cloud as well as three service models of cloud computing are infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (Saas).

Deployment Models

- Private Cloud: Private cloud is also called corporate model. A single IT organization utlizes the private cloud which is dedicated to them. The servers provided by the cloud provider are owned and hosted on the company premises and maintained by the organization administrator. Companies can configuree their servers as per their demands. Private Clouds are more secure than Public Clouds.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

- Public Cloud: This type of cloud is open to the general public over the internet. Applications, servers and storage resources are provided to cloud user for free of cost or pay as per need model. Service Provider itself manages the cloud infrastructure making it hassle free for the cloud user.
- Hybrid Cloud: A hybrid cloud deployment model comprises of both the features of private and public cloud. For instance, Company A wants to secure the sensitive data then they can store it in private cloud and the insensitive data can be moved to the public cloud.

Service Models

- Infrastructure as a Service (SaaS): IaaS model delivers infrastructure such as servers, operating system and storage and network. Instead of buying and installing servers, operaing systems and setting up infrastrucutre locally. Consumers can lease the same for cheap and scalably from the cloud providers.
- Platform as a Service(PaaS): In this service model the developer is given a runtime environment for the applications developed. The developed code is directy deployed on the cloud platform which is executed, tested and managed by the service providers.
- Software as a Service(SaaS): Software as a service model offers software over the internet hosted on cloud servers. It is also known as On Demand Service available for cloud consumer accessed with thin client on a web broswer. The main advantage is SaaS is easy to maintain and cost very low for implementation.

Security Risks in Cloud

Security Challenges	Description
Data Breaches	Confidential is stolen or shared to untrusted environment. Major breaches that need to be protected are Ransomware, Malware, Phishing, Denial of Service and Password guessing.
Poor Access Management	Unauthorized access to data due to poor policies and management of technology for accessing the technology resources.
Account Hijacking	Attacker hijacks an individual or organization cloud account to perform unauthorized activity like utilizing users services.
DDoS Attack	Making the service unavailable to the end user by initiating network traffic.
Malicious Insider	Security risk within the organization by an individual.
Insecure APIs	Misuse of API keys, Attacker targeting on key access which is used to secure cloud API infrastructure.

II. LITERATURE SURVEY

Many researchers have proposed different ways to overcome security challenges.

In 2019, K Latha proposed a technique for security in data storage and distribution in multi cloud environment. A prototype was developed by the author to avoid major concerns that arise by internal or cloud hackers from accessing the critical information like medical and personal data and to safeguard data security, confidentiality and authenticity. A novel approach called block-based data security using Galois field is carried out to achieve protection of cloud data in multi cloud environment to avoid intentional or unintentional data breaches in cloud. To simulate multi cloud, Amazon Simple Storage service (S3) and drop box was utilized. The results show efficiency in data security and efficient method to hide data from attackers.

In 2019, Murtadha Arif illustrated a web client application approach for securely storing the application in cloud, it guarantees confidentiality and integrity of data that is stored in cloud database against insider attacks. Several experiments were conducted to test security of data using web applications in real time multi cloud environment. Performance is evaluated by measuring response time, start and end time of the user request for downloading and uploading the data from cloud. It has shown effective results for the proposed method by which the Insecure API problem is kept away.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

In 2020, G.Viswanath concentrated on providing algorithm for securely storing big data in multi cloud storage environment. The author developed a framework to restrict insider attacks, Tampering attacks and DDOS attacks. Various approaches like data uploading, slicing, indexing, encryption, decryption. Retrieval, merging process. Hybrid encryption algorithm, combination of Feistal algorithm and Advance Encryption Standard algorithm was implemented for encryption process and the same is used for decryption process but in reverse manner to store big data storage in cloud. The results were shown with high performance and security using simulation analysis in real time cloud environment.

In 2020, P. Blessed Prince proposed a privacy enforced model for Health care system which uses Privacy Rating (PR) based approach to provide privacy access control to data owner to achieve data privacy, high confidentiality data integrity and availability in cloud data through proper access management technique. In this model the Privacy rating is measured for both data and end user to provide access to any user requested data. The author implemented discrete mathematical modeling to overcome system overhead during access granting mechanism. The results showed that privacy rating policy is governing body for all other access control methods and well suited for control over data.

III. CONCLUSION

Cloud Computing is provisioning of resources like storage, networking, Hardware, software, servers on demand availability to consumers over the internet. Every individual utilizes the cloud technology every day in today's world. Apart from the benefits of cloud technology, it has its own issues which is hindrance for many people around. One of the major concerns that need to be addressed is data security in cloud. In particular data breaches are way up high, business, industries and organization are looking for overcoming those hindrances and protect their own data at the same time utilizes the features of emerging technology. It is therefore very much essential for researchers to concentrate more on cloud data security that will prevent hackers, intruders from getting access to sensitive data over the cloud.

Based on the study and insights obtained from various research papers, it shows many researchers have concentrated on internal hackers attack in data centers and few papers satisfy aspects like confidentiality, integrity of data in cloud environment. Better solution for data breaches is needed as data revolves around the cloud and everything has changed in pandemic situation with lot of internet users worldwide. In future, efficient algorithm for secure data storage and retrieval of data by end user for IOT based application can be addressed.

IV. ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to Ms. Himani Tyagi for her invaluable guidance, support, and encouragement throughout the development of this research work. Her expertise and constructive feedback have been instrumental in shaping the direction of this paper. I am deeply thankful for her dedication and mentorship, which inspired me to achieve this milestone..

REFERENCES

[1]. D. V. Lindberg and H. K. H. Lee, "Optimization under constraints by applying an asymmetric entropy measure," J. Comput. Graph. Statist., vol. 24, no. 2, pp. 379–393, Jun. 2015, doi: 10.1080/10618600.2014.901225.

[2]. B. Rieder, Engines of Order: A Mechanology of Algorithmic Techniques. Amsterdam, Netherlands: Amsterdam Univ. Press, 2020.

[3]. Boglaev, "A numerical method for solving nonlinear integro-differential equations of Fredholm type," J. Comput. Math., vol. 34, no. 3, pp. 262–284, May 2016, doi: 10.4208/jcm.1512-m2015-0241