COMPARISON OF THREATS AND MEASURES FOR CLOUD SECURITY POLICIES

Parikshit V Mulay
Department of MCA
Surana College, Kengeri
parikshitvmulay@gmail.com

Gayathri V B
Department of MCA
Surana College, Kengeri
vallika.gaye@gmail.com

K Keerthi Yadav
Department of MCA
Surana College, Kengeri
yadavkeerthi2000@gmail.com

Chandan Hegde
Assistant professor
Department of MCA
Surana College, Kengeri

***Abstract*—Cloud computing has certainly been useful upgrades to information technology. The growing popularity of cloud computing has led to many questions about the infrastructure, software and network security. The risk related to cloud safety precautions is one of the most significant safety risks. The document examines safety policies and illustrates the methods and solutions implemented to safeguard them. In recent years, there have been plenty of developments in the area of cloud security, as well as many improvements to privacy laws. The security of data in cloud computing is covered in this paper. This is an analysis of security issues connected to cloud data and associated topics. Worldwide protection techniques and strategies are employed to guarantee the highest level of data protection by lowering risks and threats. Similar to this, using virtualization for cloud computing may put data at danger when a guest OS is run atop a hypervisor without knowledge of the guest OS's dependability and potential security flaw. The study is based on all the levels of services like SaaS, PaaS, IaaS.**

***Index Terms*—Cloud Computing, Service models, Security principles, Security challenges, Security Threats, Security Policies.**

I. Introduction

Cloud computing will be crucial in the Internet of Services and computer infrastructure. In the cloud computing environment, both programmers and resource are given to the Internet as Service only on demand. Security and privacy are important concerns with cloud data adoption. Cloud security refers to comprehensive range of rules, tools, and controls used to safeguard the data, applications and the cloud computing infrastructure. Cloud computing network concerns fall into two broad categories : security issues faced by cloud providers and security issues faced by their customers. It is proposed to create a data security architecture for cloud computing networks. The privacy will be utilised to examine the tangible and intangible risks. Some difficulties in data security includes data privacy, data protection and data availability and so on. The many security challenges includes data loss, data threats and severe attacks from outsiders. Chen and Zhao used cloud security methodologies and data segregation to examine and describe difficulties in the cloud computing environment related to data privacy and security

A. Services of Cloud Computing

Cloud computing services are divided into three classes, according to the abstraction level of capability provided and the service model of providers namely: Infrastructure as a Service (IaaS), Software as a Service(SaaS), Platform as a Service(PaaS). The abstraction level is viewed as the layered architecture in which services of higher level can be build from services of underlying layer[4]

- **Infrastructure as a Service (IaaS)** : IaaS provides virtualized computing resources over the internet, including computing resources over the internet, including virtual machines, storage networks and operating systems. In IaaS the end users are provided direct access to machine resources allowing them willingly utilise their resources[4]. Popular IaaS providers include Amazon Web Services (AWS)EC2, Microsoft Azure Virtual Machines, Rack Space and IBM Computing on demand.
- **Platform as a Service (PaaS)** : PaaS offers a platform and environment for developing, testing and deploying applications[5]. In this model, end users develop, test and uploads applications using tools and libraries hosted by CSP. As an illustration of PaaS, consider Google App Engine which provides users with scalable environment for the deployment and testing of java or python web apps. Examples of PaaS providers is Google App Engine.
- **Software as a Service (SaaS)** : SaaS offers subscription-based software delivery over the internet. Thin client or web browsers can be user by users to access the apps, doing away with need for local installation[6]. Examples of SaaS popular applications include Customer Relationship Management(CRM) system like Salesforce, collaboration tools like Google Workspace and Microsoft365 and project management tools like Asana and Trello.

In addition to these service models, there are various specialized services and technologies, including: Storage as a Service, Database as a Service, Serverless Computing, Big Data and Analytics and Internet of Things(IoT).

B. Cloud Delivery Models

They define how cloud services are made available to customers by cloud delivery models. There are three primary models for Cloud Delivery Models :

- **Public Cloud** : With the public cloud concept, external cloud service providers supply cloud services over the internet. These service providers make services available to the general public or a large number of customers in addition to managing and owning the infrastructure. Few examples of are Amazon Web Services(AWS), Microsoft Azure and Google Cloud Platform(GCP).

- **Private Cloud** : Cloud services that are exclusive for single business or other entity are referred to as private cloud. The infrastructure may be hosted internally or externally by a service provider. They provide more protection, control and customisation than public clouds. Private cloud deployments can be handled internally by the IT department of the company or externally by managed service providers[12]
- **Hybrid Cloud** : This cloud combines private and public cloud computing infrastructures. It enables businesses to manage and integrate workloads across several cloud platforms, both on and off premises. Strong management and connection between the various cloud environments are necessary for hybrid cloud architectures.
- **Community Cloud** : This cloud infrastructure is intended to be used by numerous organisations within a single, mutually beneficial community. Here, all users have unrestricted access to data and apps. A variety of other cloud deployment strategies are being created in response to various consumer needs. Example is a virtual private cloud[13]

II. LITERATURE REVIEW

Gartner (Jay Heiser, 2009) defines cloud computing as "a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies" [1] Moiz, Venkata, and Srinivas offer a clear understanding of cloud computing's fundamental ideas. In this paper, a number of essential ideas are explored by using instances of Applications that can be created with cloud computing, as well as how they can aid the developing world, are discussed. Nabil Giwali put up a solution-based strategy known as the Data Centric Security strategy in 2013. This method seeks to provide security at the data level, so along the course of their existence in cloud environments, the data are self-protecting. With this method, it is only the data owner's responsibility to establish and oversee data privacy and security safeguards. This suggested solution makes us of both symmetric and encryption methods and is based on the Chinese Remainder Theorem (CRT). The proposed strategy is shown to be very effective in this study since it eliminates the need for several encryptions of the data file and does not necessitate the use of complicated key derivation techniques[9] The three main categories of Cloud Computing are application, storage and connectivity. Each section has a distinct function and provides various goods to companies all around the world. Software as a Service (SaaS) had been used to describe the services themselves. Cloud-creating architecture was developed to help computer users who are pressed for time solve problems with hardware, software and resource availability. A simple and effective solution for daily computing is offered by cloud computing. The main issue with Cloud Computing are cloud security and properly implementing the cloud over a network, according to International Journal of Computer. Users can improve the data security of Cloud Computing by using various encrypting techniques, such as Data Encryption Standard(DES)[11] According to Shaikh and Modak, Data Security in the Cloud is always a top priority from the perspectives of both consumers and CSPs. They also discussed some of the most pressing security vulnerabilities in the cloud, according to a thorough analytical assessment produced by CSA. It is suggested to use a model with different data security parameters. These parameters are given certain numerical weights and the customers can use them as a guide for choosing CSP[11] Where Data Sanitization is the process of concealing sensitive information in a test and development of databases by overwriting it with realistic-looking but fictious data of a similar type. An effort has been made to offer solutions that will improve the cloud's current capabilities while hiding the display of sensitive data, helping both cloud users and cloud providers by enhancing business intelligence.[12]

III. SECURITY CHALLENGES

Cloud computing improvements two influential concerns that is security and the other one is privacy. The virtual environment in the cloud delivers customers to access technology that exceeds that locked their physical world. Cloud also provides various benefits, including versatility, flexibility, cost savings and improved communications.

- **Losing control over data** : Outsourcing indicates a major reduction of data control. The Amazon Storage Service APIs provides bucket and object level access controls, with basics enabling only authenticated access.
- **IP Spoofing** : The production of TCP/IP packets using another person's IP address. The hacker gets illegal access to a computer and sends messages to a system with an IP address that indicates communications is from a trusted host.
- **Packet Sniffing** : The process of listening to a raw network devices for packets of interest. when two virtual instances owned by the same user and hosted on the same physical host are unable to listen to each other's information.
- **Instance Isolation** : This ensures that different situations are running on the same physical machine that are isolated from each other.
- **Data Sanitization** : It is the process of removing sensitive data from a storage device. AWS procedures includes procedure of removing data that are not exposed to unauthorized individuals. The storage area is then made available only for write operations and the date that are overwritten by newly stored data.

IV. SECURITY PRINCIPLES FOR CLOUD COMPUTING

The International Standards Organization(ISO) establishes information security concerns that can also be uses as guide in relation to the major security requirements for cloud computing for an efficient and safe technology. The following defines them :

- **Integrity** : Integrity refers to ensuring that data is not altered or modified while it is being stored or transferred and that only users with permission can update, modify, copy or delete data. Implementing security controls like digital signatures and checksums.
- **Confidentiality** : Data privacy implies protecting user information and restricting access to privileged parties. It is essential to protect data both when being stored and being transmitted, data should be secured against unauthorised access.
- **Availability** : Availability refers to the assurance that the user may always access the data he request or the service, wherever it may be. High data and application availability must be guaranteed via cloud services[15]
- **Authorization** : A user's request for specific information must be authorised in order for them to gain access to it. Based on entity roles, responsibilities and permissions, access privileges are managed and granted.
- **Authentication** : Before granting access to data, authentication ensures the user's identity and this is accomplished by applying specific protections to their profiles. It helps to prevent unauthorised access and protect sensitive data by ensuring only authorised people are given access.
- **Network security** : Advanced network security procedure are needed in cloud environments. To safeguard against unauthorised access, malware and network-based attacks, this involves setting firewalls, prevention systems and secure network segmentation[16]

V. SECURITY POLICIES IN CLOUD COMPUTING

The set of guidelines and procedures for safeguarding data and other information properties against security risks, human error, and other security threats are defined by cloud security policies. Here, only authorised people have access to your data and applications. Even though cloud service providers (CSPs) typically create cloud security policies, businesses using the cloud also have the option to do so. Example : Data backup and recovery, Data Encryption. Cloud security policies stipulates that :

- Data kinds that can and cannot be moved to the cloud.
- How the teams manage the risks associated with each data type.
- Who makes the choice to move workloads to the cloud?
- Who has permission to view or move the data?

A. CREATING A CLOUD SECURITY POLICY

Creating a cloud security policy for an organization involves considering specific requirements and challenges unique to the specific sector. Here's an example of how to create a cloud security policy for an educational organization:

- **Policy Scope and Objectives** : Define the policy's purview in detail, mentioning the cloud services and environments it covers inside the educational organisation. List the policy's main goals, such as safeguarding student information, assuring continuous service, and adhering to any relevant laws like FERPA (Family Educational Rights and Privacy Act).
- **Data Classification and Protection** : Find out what category educational data in the cloud falls under, including student records, financial data, and research data. Establish rules for access controls, encryption, and data protection. Provide guidelines for handling sensitive data and the usage of suitable encryption techniques.
- **Access Control and Authentication** : Creating rules and guidelines for user access control and authentication techniques. Establish standards for multi-factor authentication, strong passwords, and frequent access reviews. To limit access to private information and systems, define user roles and permissions in accordance with the principle of least privilege.
- **Compliance with Privacy Regulations** : Address any compliance needs, such as FERPA, GDPR (General Data Protection Regulation), or other relevant privacy laws. Specify the processes to follow in order to get consent for data collection, processing, and dissemination. Make sure that data processing procedures adhere to privacy legislation and that student and staff privacy rights are respected.
- **Incident Response and Data Breach Notification** : Establish protocols for detecting, responding to, and reporting security incidents and data breaches. Define incident response procedures, including steps for containment, investigation, and communication. Specify the roles and responsibilities of incident response teams and the process for notifying affected parties and regulatory authorities in case of a data breach.
- **Data Backup and Disaster Recovery** : Address any compliance needs, such as FERPA, GDPR (General Data Protection Regulation), or other relevant privacy laws. Specify the processes to follow in order to get consent for data collection, processing, and dissemination. Make sure that data processing procedures adhere to privacy legislation and that student and staff privacy rights are respected.
- **Policy Review and Revision** : Establish a procedure for routine policy evaluation and amendment to make sure it keeps up with changing security threats, legal requirements, and educational institution requirements. Establish a schedule for periodic review, taking academic calendar milestones or regulatory revisions into consideration. Specify the people or teams in charge of reviewing policies[19]

B. Advantages of Cloud Security Policies:

- Improved Data Protection : By specifying encryption criteria, data protection measures, access controls and cloud security rules help us to protect delicate information stored in the cloud.

- Regulatory and Quality Alignment : Cloud security policies ensures that the company ensures with relevant rules and standards.
- Uniform Security practises : The company may implement regular practises across their cloud environments by establishing cloud security policies.
- Improved incident responses : These processes are included I cloud security policies, making sure that the companies have an structured planning for detecting, responding to and reducing security problems.
- Vendor management : Cloud security policies establishes rules for selecting and managing cloud service providers, so that vendors can satisfy the security objectives of the organization's.

C. Disadvantages of Cloud Security Policies

- Complexity and Resource requirements : Creating, implementing and maintaining robust cloud security rules may be time-consuming and costly. To maintain policy effectiveness, significant time and constants efforts are required.
- Potential impact on User experience : Strict security precautions are necessary for additional authentication processes or access limitations, which may impact on user experience. Balancing security with consumer ease can be difficult.
- Dynamic threat Landscape : Cloud security rules must be updated as an ongoing schedule to handle emerging security threats and vulnerabilities.
- Balancing security and Flexibility : Strict security regulations may limit the flexibility and agility of cloud services. The organizations must find a balance between security precautions and the advantages of cloud computing, such as scalability and rapid deployment.

It's a vital role to remember that the advantage and disadvantage will differ depending on the company's specific demands, the nature of its activities and the cloud environment being used. When developing and implementing cloud security policies, organization should carefully consider these factors[19]

VI. SECURITY THREATS IN CLOUD COMPUTING

In addition to the benefits that cloud computing provides, there are several security risks that prevent users from taking advantage of these benefits. Security threats that have been acknowledged and a widely accepted are defined in this section.

- **Data Loss** : Aside from malicious attacks, there are other ways that data loss might could occur. Data security breaches can occur as a result of deletion, alteration or loss of encryption key, as well as natural disasters. To protect themselves against suck risks, organisations should maintain a complete backup of their data.
- **Data Breaches** : They happen when private data is exposed to unauthorised people. It may be caused by inadequate authentication methods, flaws in cloud infrastructure or apps. Microsoft, Yahoo, Apple's, iClouds and others are businesses that have experienced this problem. Data breaches can be used for financial fraud, identity theft.
- **Service Hijacking** : This happens when an attacker obtains login credentials then their account hijacking happens. This can be accomplishes using brute-force attack, phishing scams. Once an account is compromised, the attacker has access to and control all over the data and they can also carry and utilise account for illicit activities[17]
- **Identity theft** : In the context of Cloud Computing, it poses a serious security risk. Data is processed and stored on distant servers that are owned and maintained by cloud service providers as part of cloud computing.
- **Insecure interfaces and APIs** : They are present a important safety concern in cloud computing systems. These interfaces and APIs give client applications and cloud services a way to interact and connect. Some specific threats associated with Insecure interfaces and APIs are Denial of Service attacks and API data exposure.
- **Shared technology issues** : Organisations need to be aware of the security risks brought by cloud computing's shared technologies. The shared nature of cloud resources-where numerous users share the same underlying infrastructure, platforms or software-gives rise to these hazards. Example co-tenancy dangers, data residuals[18].

Other risks are less serious than above mentioned but nevertheless present in the cloud environment include lost of governance, acquisitions of cloud providers, threats to trust, failures in isolation and data segregation.

VII. THREATS AND SOLUTIONS TO CLOUD SECURITY POLICY

- **Unauthorized Access** : Threat : Unauthorised access to sensitive data and cloud resources by attackers. Solution : Implement robust access controls based on user roles and privileges, such as multi-factor authentication (MFA), and enforce them strictly.
- **Data Breaches** : Threat : Sensitive data kept in the cloud may be accidentally or maliciously exposed. Solution : Implement strong access controls, encrypt data both in transit and at rest, monitor and audit data access often, and run security audits and vulnerability scans.
- **Insider Threats** : Threat : Negligent behaviour or unintentional errors made by authorised users inside the organisation. Solution : Implement least privilege access, observe user behaviour frequently, enforce separation of roles, run employee training and awareness campaigns, and set up incident response protocols.
- **Service and Infrastructure Vulnerabilities** : Threat : Exploiting software or infrastructure flaws in cloud service providers. Solution : Keep your software and security patches up to date, perform penetration tests and

vulnerability analyses, and choose trustworthy and secure cloud service providers.

- **Lack of Visibility and Control**: Threat : The cloud service provider's security measures are difficult to see and regulate. Solution : Give priority to cloud service providers with open security policies, exercise due diligence when choosing vendors, and create Service Level Agreements (SLAs) with specific security specifications.
- **Regulatory Compliance Violations** : Threat : Failure to adhere to all applicable laws and norms. Solution : Conduct compliance audits and assessments, review and update cloud security policies on a regular basis, and keep accurate records of security practises and controls[20]

VIII. POPULAR PRACTICES AND METHODS FOR A STRONG SECURITY POLICY

The success of cloud security policies is ensured by addressing these threats and putting into place the necessary remedies. This helps to improve the overall security posture of cloud environments. It's critical to adhere to accepted procedures and techniques that support the efficacy of the policy in order to build a solid security policy. Here are some key practices and methods to consider:

- **Risk Assessment and Management** : To find potential threats and vulnerabilities in your cloud environment, conduct a thorough risk assessment. Put risks in order of importance depending on their potential impact and propensity to arise. Create plans to efficiently manage and reduce these risks.
- **Least Privilege Principle** : Abide by the concept of least privilege, which dictates that users only be given the rights essential to carry out their job duties. Limit who has access to sensitive information and vital systems to just those who have been given permission.
- **Encryption** : Utilise encryption techniques to safeguard data while it is in transit and at rest. Before storing sensitive information in the cloud, encrypt it, and use secure encryption algorithms for sending data..
- **Multi-Factor Authentication (MFA)** : To add an additional layer of protection to user authentication, enable MFA. impose a multi-factor authentication requirement on users in order to access cloud resources, such as passwords, security tokens, or biometrics.
- **Regular Monitoring and Auditing** : Implement thorough monitoring and auditing procedures to quickly identify and address security incidents. Keep an eye out for any odd behaviour by monitoring user activity, system logs, and network traffic. Security audits should be conducted on a regular basis to spot vulnerabilities and verify compliance[19]

IX. CONCLUSION

The Internet of Services and computer infrastructure will rely heavily on cloud computing. Cloud data use raises significant security and privacy concerns. Cloud security refers to a comprehensive set of rules and methods used to protect data, apps and cloud infrastructure like Azure. As a result, it is clear that the cloud environment has a particular difficulties and risks when comparing the threats and policies for cloud security. Because of the increasing reliance on cloud services, effective cyber threats targeting sensitive data and infrastructure have increased. Organizations, on the other hand have realized the need of deploying complete security measures to successfully defend their cloud environments. Unauthorized access and data breaches are serious dangers in the cloud. To summarize, while cloud computing poses new data security dangers, firms can effectively minimize these risks using a mix of technical safeguards, operational strategies. Organizations must use multi-factor authentication, storage access controls and encryption measures to secure data in transit and at rest to mitigate these threats. In the cloud, data privacy and compliance are also key challenges.

REFERENCES

[1] Stanojevi and Shorten, 2008 2008, Vaquero et al., 2009 2009, Weiss, 2007, Whyman, 2008, Boss et al., 2009

[2] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011, pp. 3–22, 2014.

[3] Barbara. (2009, Sep.) Eucalyptus [online]. http://open.eucalyptus.com

[4] : P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory,Technical Report Version 15, 2009.

[5] Cloud computing, in Proceedings 1st International Conference on Cloud Computing

[6] (CloudCom 09), Beijing, 2009, pp. 3,27

[7] Z. L. X. C. Z. Y. J. C. Shengmei Luo, "Virtualization security for cloud computing services," in International Conference on Cloud and Service Computing, 2011.

[8] J. S. N. G. L. L. I. Meiko Jensen, "On Technical Security Issues in Cloud Computing," in IEEE International Conference on Cloud Computing, Bangalore, India., 2009

[9] Nabil Giweli (2013) Enhancing Cloud Computing Security and Privacy, 20, Jan, 2019

[10] Muijnck-Hughes Jan de (2011) Data Protection in the Cloud, 12 Jan, 2019 [Online], Available: http://www.ru.nl/ds

[11] Rajesh, S., S. Swapna, and P. Shylender Reddy. "Data as a service (daas) in cloud computing." Global Journal of Computer Science and Technology12.11-B (2012)

[12] Barbara. (2009, Sep.) Eucalyptus [online]. http://open.eucalyptus.com.

[13] IEEE/ACM International Symposium on Cluster Computing and the Grid

[14] "The Secure Migration of Data to Cloud using Data Sanitization and MAC address based AES" Hitesh Marwaha, IJRTE March 2019.

[15] M. M. E. E. S. S Ramgovind, "The Management of Security in Cloud Computing," in Information Security for South Africa (ISSA), 2010.

[16] R. Z. W. X. W. Q. A. Z. Minqi Zhou, "Security and Privacy in Cloud Computing: A Survey," in Semantics Knowledge and Grid (SKG), 2010.

[17] "Cloud Computing-ENISA-Benefits, risks, and recommendations for information security," ENISA, 2009.

[18] "CSA: Top Threats to Cloud Computing," Cloud Security Alliance, 2010.

[19] Cloud security policies https://phoenixnap.com/blog/cloud-security-policy

[20] https://www.getkisi.com/blog/7-tips-prevent-cloud-security-threats