www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 440-445

e-ISSN : 2583-1062
Impact Factor : 2.205

CLOUD SECURITY

Harpreet Kaur Mavi[*1], Miss Gurmandeep Kaur[*2], Dr. Kriti[*3]

[*1]Student, Management, Chandigarh Group of Colleges, Jhanjeri, Punjab, India.

[*2]Assistant professor, Management, Chandigarh Group of Colleges, Jhanjeri, Punjab, India.

[*3]Assistant professor, Management, Chandigarh Group of Colleges, Jhanjeri, Punjab, India.

ABSTRACT

A cloud security is a set of policies, technologies, and controls designed to protect the various components of a cloud computing environment from unauthorized access and manipulation. These controls are typically used to protect the multiple services and applications part of a cloud computing environment.

Keywords: Cloud security; Cloud Computing; data security; Security as a service.

1. INTRODUCTION

Cloud computing is one of the most important information technology revolutions in our lives. The traditional business paradigm is being transformed by cloud computing. Cloud computing has become a hot topic in the information and communication technology (ICT) industry. Everyone is looking forward to the potential expansion of the latest market. NIST [1] is a government-funded R & D organization. Cloud computing is a network access technology that provides users with on-demand access to a pool of programmable computing resources. It can be delivered and made available immediately with little effort from the administrator or cloud provider (network, server, storage, apps, services, etc.). The term "cloud" existed until the late 1990s. It began offering VPN (Virtual Private Network) services at a lower cost than dedicated point-to-point data connections with the same level of service [2] Is derived from Cloud computing is revolutionizing traditional business models. Cloud computing technology can co-exist with different service and delivery approaches and other technologies and software design strategies in different topologies. Cloud computing is characterized by five key characteristics: three service models (IAAS, SAAS, PAAS) [3] and three delivery methods (public, private, hybrid) [4]. Innovative aspects of cloud computing, such as multi-tenancy [5], resource sharing [6], and remote data storage [7], tested not only existing security systems but also uncovered new security challenges. Bottom. Should perform A thorough security assessment of cloud computing results to enable governments, organizations, and individuals to manage cloud computing services without worrying about security risks. Unfortunately, operators are only making sporadic efforts to focus on cloud computing security (or cloud security). Therefore, a series of technical research on cloud security from the operator's point of view and the development and adoption of technology in the industry is required. This article examines the security challenges of cloud computing and explores possible technical solutions to these problems. The rest of this work is divided into the following sections. Section II provides a definition and scope of cloud computing security, an overview of the cloud security industry, and an analysis of the impact of cloud computing on public and private sector security.

2. DETERRENT CONTROLS

These are management approaches to ensure compliance with external regulations and limit attacks on cloud systems. Deterrents, such as fences and warning signs for assets reduce the threat level by informing potential attackers that an intrusion could be detrimental. (Some consider them as a form of preventative control.) These authorities include policies, methods, standards, policies, rules, and laws that govern an organization's security efforts. Proactive controls are designed to increase system defense against incidents by reducing, if not eliminating, vulnerabilities and preventing unauthorized access and intrusion. We can achieve this by adding software or changing the approach. It is supported via way of means of a communications infrastructure. Most organizations purchase or construct a consultant safety operations centre (SOC). An expert body of workers uses logs and SIEM software programs to reveal the organization's IT infrastructure constantly.

Corrective controls serve to lessen the outcomes of an occasion via way of means of restricting the harm. During or after a safety incident, technical, bodily, and administrative guidelines are used to repair structures or assets to their preceding condition. Corrective management can take a variety of physical and technological forms. Corrective controls encompass reissuing a right of entry to the card or repairing bodily damage. Technical leadership, which includes preventing a process and administrative management, which consists of an incident reaction plan, needs to be considered. The purpose of corrective controls is to get well and reverse any damage due to a safety breach or unlawful right of entry.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 440-445

e-ISSN : 2583-1062
Impact Factor : 2.205

3. CLOUD COMPUTING SECURITY

This section covers the definition and scope of cloud computing security, responsibilities in the cloud security sector, and dangers to both clients and operators.

A. The concept and scope of cloud security

Many operators are now sharing their cloud computing knowledge. In cloud computing, often known as cloud security, it is unavoidable for operators to confront security issues. It refers to a collection of rules, tools, and controls to safeguard data, applications, and the cloud computing infrastructure. Cloud security concerns the security of Cloud computing systems, such as privacy protection, data encryption, and resource availability in the face of a security attack. To maintain the long-term viability of the cloud computing development environment, we must ensure that all these challenges are adequately addressed and overcome. It's essential to distinguish cloud security from "cloud-based" security services that protect against traditional threats. This security service may be strengthened with cloud computing, defending against DDOS, Trojans, Viruses, and Spam more effectively than before.

B. Industry of cloud security

Should explain the composition of the cloud security sector to prevent security events to the most significant degree possible. The following are three roles played by the cloud security industry.

Cloud Vendors. Vendors who offer cloud-based services. Many cloud service providers, including Amazon [9], IBM [10], and Microsoft [11], have previously provided. Cloud computing security deployment solutions to increase. Cloud computing service platform service and the safety of user data. Most of them rely on ID verification, auditing, and data encryption.

Operators. From the operator's standpoint, there are two approaches to cloud computing security. On the one hand, companies may gain central control over the network by combining current security measures with cloud computing technologies. On the other hand, they can create cloud computing security services for their clients. Customers of several network operators have begun to receive this service.

Vendors in the security field: When traditional IT security suppliers enter the cloud computing industry, they offer cloud-based security solutions and products that may be divided into two categories. One sees the "cloud" through the eyes of the server, while the other sees it through the eyes of the client.

The former goal is to prevent security risks from reaching the client-side by stopping them on the server-side. It may also be viewed as the creation of a massive list system. The latter employs a more conventional strategy. That is, terminal clients are used as security measures.

Operators enable cloud security to provide customers with security services for these three jobs in the cloud security business. Operators collaborate with Customers and can purchase client-side and server-side security services from security vendors Side cloud security services or apps based on operator advantages and combine them with cloud vendors' ID authentication, auditing, and data encryption solutions to provide clients with end-to-end security solutions in cloud computing.

4. Security and privacy

Services that do not have an "enhanced" environment are considered "soft" targets. Data breaches, malware, and exploited vulnerabilities need to be circumvented on virtual servers and physical servers. "Data loss or breach accounts for 24.6% of cloud outages, and cloud-related malware accounts for 3.4%."

Identity management

To regulate access to information and computer resources, each company will have its identity management system. To integrate the customer's identity, Cloud providers can integrate federation or SSO technology and biometric systems into their infrastructure or provide identity management systems... For example, clouded provides cloud-based inter-company biometrics while protecting privacy. Connect the user's data to the biometric data and encrypt and store it.

Physical security

Cloud providers can integrate federation or SSO technology and biometric systems into their infrastructure or provide identity management systems. Ensure that critical supplies (such as energy) are sufficiently reliable to avoid outages from unauthorized access, interference, theft, fires, floods, and other natural disasters and ensure that critical supplies (such as energy) are sufficiently reliable to avoid outages. It is usually accomplished by providing cloud applications from data centers that have been adequately defined, developed, built, managed, monitored, and maintained.

Privacy

Providers guarantee that any sensitive data (such as credit card details) is hidden or encrypted and that only authorized users have full access to the data. Furthermore, any data that the provider gathers or creates regarding client behavior in the cloud and digital identities and credentials must be secured.

Data security

Cloud data services are related to several security risks. Traditional and non-traditional dangers are included. Traditional hazards include network eavesdropping, unlawful invasion, and denial-of-service assaults, as well as cloud computing-specific concerns, including side-channel attacks, virtualization vulnerabilities, and cloud service abuse. Personnel Protection Potential new employee security screening, security awareness and training programs, and precautions are examples of pre-employment, in-employment, and post-employment activities. Outsourced data is stored in the cloud and is not under the owner's direct control. The CIA Triad relates to secrecy, integrity, and access controllability, which may be further explained as follows. It's worth noting that many suitable security methods cover all three categories or at least some of them. Encryption, for example, protects data from illegal access and preserves its confidentiality, availability, and integrity. On the other side, backups often maintain integrity, whereas firewalls merely cover secrecy and access controllability.

Confidentiality

The property of data confidentiality is that the data contents are not made public or given to unauthorized users. Outsourced data is stored in the cloud and is not under the owner's direct control. Only authorized users should have access to sensitive data, and others, including CSPs, should be kept in the dark. Meanwhile, data owners anticipate being able to fully employ cloud data services such as data search, data calculation, and data sharing without fear of data contents being leaked to CSPs or other enemies. Confidentiality refers to how data must be kept private by the data's owner.

Encryption, for example, is a type of security measure that protects data secrecy by allowing only authorized users to access it.

Access controllability

Access controllability refers to a data owner's ability to selectively restrict access to data that has been outsourced to the cloud. Legal users can be granted access to the data by the owner, while others cannot do so without authorization. In addition, fine-grained access control to offsite data needs to be enforced. Different users should be allowed various access privileges for individual data components. In untrusted cloud settings, access permission must be handled only by the owner.

Availability is another term for access control. While it should avoid unlawful access at all costs, access for administrative and even consumer purposes should be permitted but closely controlled. Availability and access control guarantee that the appropriate permissions are issued to the right individuals.

Integrity

Data integrity entails ensuring and preserving data correctness and completeness. A data owner wants their data to be kept accurately and securely in the cloud. The data should not be tampered with unlawfully, wrongly edited, erased, or manufactured maliciously. The owner should be able to notice data corruption or loss if any undesired processes are corrupt or erase them. Furthermore, even if a section of the outsourced data is destroyed or lost, the data consumers can still retrieve it. Effective integrity security rules protect data from hostile actors and unintended changes.

Internet Vulnerabilities

To access the cloud, you'll need an internet connection and, as a result, internet protocols. As a result, it's vulnerable to various internet protocol flaws, including man-in-the-middle attacks. Furthermore, because of the firm reliance on internet connections, users would be cut off from any cloud resources if the connection breaks.

Cryptographic Weakness

Cryptography is a constantly changing science and technology. What was secure ten years ago may be considered a severe security concern by today's standards. New means of cracking encryptions will develop as technology advances, and older technologies become obsolete, as will catastrophic weaknesses in previous encryption approaches. Because the data that cloud providers often hold is so important, they must maintain their encryption up to date.

Legal issues

The law on privacy varies a lot from nation to country. When data is kept in the cloud, it might be challenging to establish whose jurisdictions the information belongs to. Transborder clouds are beautiful because the most prominent corporations operate across many nations. Other legal issues arising from the cloud's ambiguity include the distinction

in privacy regulations between information exchanged between enterprises and information shared within organizations.

Encryption

Advanced encryption methods that have been used in cloud computing have improved privacy protection. When the data is no longer needed, the keys may be simply removed using a process known as crypto shredding.

Attribute-based encryption (ABE)

Attribute-based encryption is like public-key cryptography in that it uses attributes to encrypt data. The user's ciphertext and private key depend on their characteristics (such as country of residence and subscription type). Only if the user key's qualities match the attributes of the ciphertext can a ciphertext be decrypted in such a system.

Attribute-based encryption has the advantage of attempting to address difficulties that exist in existing public-key infrastructure (PKI) and identity-based encryption (IBE) systems. ABE avoids the need to transfer keys directly, as with PKI, and to know the receiver's identity, as with IBE, by relying on characteristics ABE suffers from redistributing decryption keys, so these benefits come at a price. It is difficult to establish the identity of a user because the ABE decryption key contains only information about the access structure or user properties. As a result, criminals may deliberately expose attribute information to allow unauthorized users to impersonate access.

Ciphertext-policy ABE (CP-ABE)

A type of public-key cryptography called Ciphertext Policy ABE (CPABE) is a type of Ciphertext Policy ABE (CPABE). CPABE's encryption capabilities control the access strategy. The access structure design is the main focus of the CP study. ABE setup, encryption, KeyGen, and decryption are the four algorithms that make up the attribute-based encryption method for ciphertext policies. The setup method takes security settings and a description of the attribute universe as input and generates public parameters and a master key. The encryption algorithm takes data as input. It then encrypts it to create a ciphertext that can only be decrypted by a user with a set of attributes that satisfy the access structure. The KeyGen algorithm then takes the master key and the user's details to develop a private key. Finally, the Decrypt algorithm takes the public parameters, the ciphertext, the private key, and user attributes as input. The algorithm first checks if the users' details satisfy the access structure and then decrypts the ciphertext to return the data.

Key-policy ABE (KP-ABE)

KP-ABE, or Key-policy Attribute-Based Encryption, is a form of Attribute-Based Encryption. Like another Attribute-Based Encryption system, KP-ABE permits senders to encrypt their messages with the usage of hard and fast attributes. Private user keys, including decryption algorithms for decoding the news, are produced for each encryption, and these private user keys enable users access to specific communications to which they belong. In a KP-ABE system, the creator's tag ciphertexts, or encrypted messages, with a set of characteristics, and the user's private keys are supplied with a list of ciphertexts that the key may decrypt. A user's private keys determine which ciphertexts they may decipher. The attribute sets are used in KP-ABE to characterize the encrypted messages and the keys. The defined policy that users will have for decrypting ciphertexts is coupled with private keys. One disadvantage of KP-ABE is that the encryptor has no control over who has access to the encrypted data other than through descriptive qualities, putting the key-issuer in charge of giving and refusing user entry. As a result, various ABE systems, such as Ciphertext-Policy Attribute-Based Encryption, have been developed.

Fully homomorphic encryption (FHE)

Fully Homomorphic Encryption is a cryptosystem that permits unrestricted ciphertext computations and sum and product computations for encrypted data without decryption. Fully Homomorphic Encryption, or FHE, has another intriguing feature: it allows operations to be performed without using a secret key. Not only has FHE been related to cloud computing but also electronic voting. The evolution of cloud computing and computing technologies has significantly benefited from Fully Homomorphic Encryption. The necessity for cloud security has grown in tandem with the development of these technologies. FHE hopes to safeguard data transit and cloud computing storage with its encryption techniques. Its purpose is to be a considerably safer and more efficient form of communication.

Searchable encryption

It is an encryption technology that allows users to view encrypted data securely. SE systems are divided into two types: those that use secret-key (or symmetric-key) cryptography and those that use public-key cryptography. Symmetric-key SE often develops keyword indexes to increase search performance to answer user queries. It has the apparent problem of allowing unwanted data retrieval via multimodal access channels, circumventing the encryption process by submitting the framework to different settings inside the shared cloud environment.

Legal and contractual issues

Aside from security and compliance concerns, cloud providers and their customers will talk about accountability (for example, How are data loss or breaches, intellectual property, and out-of-service support incidents handled? (When the data and application are finally returned to the customer). Furthermore, getting data from the cloud that may be significant in a legal lawsuit is a source of concern. These issues are addressed via service-level agreements (SLA)

Public records

Documents-keeping obligations in the public sector may also be a legal concern since many agencies are required by law to store and make electronic records available in a particular manner. Legislation may regulate this, or regulation may oblige agencies to follow the norms and procedures established by a records-keeping agency. These risks must be considered by government entities that use cloud computing and storage.

4. CONCLUSION AND BEST PRACTICES

Cloud computing presents both issues and opportunities for information security. The changes may be seen in technological concepts, industrial development, and security regulation techniques. As technology evolves, users, service providers, and government authorities weigh their security expectations. Users and cloud providers each have their security concerns. Those needs can be incompatible in some way. One of the most difficult challenges we face is balancing the demands of data security and privacy protection. This balancing of needs necessitates a rethinking of our technical concepts. The industry's evolution reflects the shift in emphasis on information security from product development to service development. It is required. Must be pushed Information security products to move beyond product development to service and infrastructure development. A unified service and infrastructure platform can assist users in resolving a variety of security challenges.

The evolution of regulations and management reflects the shift in the focus of market regulators. In contrast to traditional law, which focuses on the safety of core network infrastructure, authorities are increasingly concerned about large-scale assaults in the cloud. It's worth noting that all modifications are enhancements rather than revolutions of current technological solutions. As a result, operators offer several recommended practices to address cloud security shortfalls.

1. Operators should evaluate how to transition from traditional to cloud platforms while maintaining service continuity. 2. Operators should consider addressing data security issues in their clouds, such as security transmission, security isolation, security storage, and data recovery solutions.

5. REFERENCES

[1] 1] P. Mell, T. Grace. The NIST Definition of Cloud Computing, Vol 15, 2009. http://csrc.nist.gov/groups/SNS/cloud-computing.

[2] [2] Cloud computing. http://en.wikipedia.org/wiki/Cloud_computing.

[3] [3] Security guidance for critical areas of focus in cloud security computing V3.0 http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[4] [4] Top Threats to Cloud Computing, V1.0, Cloud Security Alliance, 2010, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[5] [5] A. Sirisha, G. G. Kumari. "API access control in the cloud using the role-based access control model." 2nd International Conference on Trendz in Information Sciences & Computing, 2010, p.135-137.

[6] [6] D. W. Chadwick, M. Casenove. "Security APIs for My Private Cloud: Granting access to anyone, from anywhere." 2011 IEEE 3rd International Conference on Cloud Computing Technology and Science, 2011, p.792-798.

[7] A. Mana, A. Munoz, J. Gonzalez. “Dynamic security monitoring for Virtualized Environments in Cloud computing.” 1st International Workshop on Securing Services on the Cloud (IWSSC), 2011, p.1-6.

[8] Amazon Web Services, http://aws.amazon.com.

[9] Cloud computing security. URL :http://en.wikipedia.org/wiki/Clo ud_comput ing_security.

[10] IBM, "Implementing Gentry’s Fully-Homomorphic Encryption Scheme", http://researcher.ibm.com/

[11] Reference Architecture for Private Cloud.http://social.technet.micro soft.com/wiki/contents/articles/6

[12] Mowbray, Miranda (15 April 2009). "The Fog over the Grimpen Mire: Cloud Computing and the Law". SCRIPT-ed. 6 (1): 132–146. doi:10.2966/scrip.060109.132.

[13] Mather, Tim; Kumaraswamy, Subra; Latif, Shahed (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc. ISBN 9780596802769.

[14] Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Elsevier. ISBN 9781597495929.

[15] Ottenheimer, Davi (2012). Securing the Virtual Environment: How to Defend the Enterprise Against Attack. Wiley. ISBN 9781118155486.

[16] BS ISO/IEC 27017: "Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services." (2015)

[17] BS ISO/IEC 27018: "Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." (2014)

[18] BS ISO/IEC 27036-4: "Information technology. Security techniques. Information security for supplier relationships. Guidelines for security of cloud services" (2016)