International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 6 ǁ 2022 ǁ PP. 165-170

A Study on Cloud Computing Security: Concerns, Strategies and Best Practices

Sandhya D S, Chandrika M,
Department of MCA, Department of MCA,
Dayananda Sagar College of Engineering Dayananda Sagar College of Engineering

Abstract- *Cloud computing is a technology that allows users to access a variety of services quickly and on-demand through a common pool of programmable computer resources. This technology increases issues regarding the flow of data and control into the control sphere of a third party. This article addresses cloud security challenges and security standards. A potentia1 cloud architecture is proposed, as well as cloud security best practices.*

Keywords - *cloud computing; security; access control; patterns; data encryption; cloud data security; encryption; security monitoring, consistent computing, access control;*

Date of Submission: 20-05-2022 Date of acceptance: 03-06-2022

I.INTRODUCTION

Cloud computing has evolved from previous network computing approaches and is based on both standing and emerging technologies. The cloud offers several service models, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [1]. The cloud's information technology infrastructure consists of infrastructure, IP-based networks, virtualization, software, and service interfaces. Cloud computing uses a variety of service models, including hybrid, community, and public cloud models. The cloud creates a new understanding of the connection between an organization and its information, thereby embracing the presence of third-party cloud providers. This has created many security challenges in various data management scenarios. [2]. Cloud security is primarily concerned with safety and assurance. According to the NIST cloud model, moving from SaaS to PaaS and then back to laaS service mode allows customers or tenants to have more security control over more resources. [3]. Because this infrastructure shares resources to safeguard and process data that does not belong to them, there is a risk that data will be exposed by other nefarious cloud users. As a result, data security in the cloud is more important than it is in conventional computing paradigms. This study presents a paradigm for cloud-based unified security architecture. Section 1 outlines the relevant cloud security work and related concerns. Cloud security requirements are identified and compiled as security policies in Section II. Imaginary cloud protection structure is proposed in segment III.

The final section examines recommended practices for cloud service providers, customers, and tenants.

II. CLOUD SECURITY CONCERNS AND RELATED WORK

The National Institute of Standards and Technology (NIST) defines cloud computing as an information technology (IT) architecture that offers suitable, on- demand network access to a shared pool of configurable resources that may be controlled and released at any time with negligible administrative efforts or serviceprovider intervention.

A data center and redundant network connections link to the cloud system at the back end, allowing a person to establish a cloud system with a limited amount of resources.

As a result, a system created this way poses a number of real and perceived security threats, which is one of the reasons why cloud computing has yet to gain widespread acceptance among corporations and organizations.

- Many cloud designs do not integrate on-demand access and self-service in the cloud services paradigm.
- The cause for this is inadequacies in design and operations that do not meet the time sphere needs of cloud computing. As a result, Security must be considered when designing cloud infrastructure. By addressing cloud security problems, they may be included in the scheme of secure cloud architecture, either by verifying them or disputing them with reimbursing mechanisms. Some of the key problems for cloud computing are:
- Network Availability: The value of cloud computing can only be achieved if network connectivity and bandwidth are adequate.
- Cloud provider viability: The viability and commitment of new cloud providers should be reviewed.
- Disaster Recovery and Business Continuity: A good disaster recovery strategy in the event of a cataclysmic outage.
- Transparency: Establish trust in the cloud provider's security promises without disclosing specific security policies.
- Loss of physical control: There are a number of issues that come with losing physical control, including the fact that data may not stay with the same system in public and community clouds (data privacy), and that user and organization data may mix with other data (data control).

Authorized and governing compliance: Using public clouds to handle data that is subject to permitted or controlling compliance is challenging and impractical. To meet the demands of regulated markets, providers must create and certify clouds.

III. CLOUD ARCHITECTURE SECURITY REQUIREMENTS

- There are several models that may be used to create a safe Software Development Life Cycle (SDLC).
- These can be used as templates for different security systems, operations, and cloud security.
- Customers care about identity and access management, data loss prevention, online security, e-mail security, security assessments, intrusion management and event management, encryption, business continuity, and disaster recovery, and cloud providers must meet these security requirements.
- The benchmarking agencies' criteria are linked with cloud-specific implementation security needs. A cloud security policy is developed based on these principles

A. Security Policies and Procedures

- Physical access to amenities should be included in the policy, as should coherently access to systems and their applications.
- It is necessary to assign jobs and tasks to various individuals. In addition, the policy should provide methods for doing investigative reporting.
- All infrastructure apparatuses, including servers, switches, software settings,and network configurations, are backed up.
- Initial and ongoing testing documentation
- As a standard for encryption, agreed cryptographic procedures with essentialkey lengths should be utilized.
- Standards Justify with the acceptable password quality.

B. Requirements for Cloud Security

Following the development of a cloud security policy, the cloud security architecture is constructed on these recommendations. The security policy should guide the development of cloud security architecture. The security standards listed below are implemented to this cloud architecture.

By syncing with the same time source, Network Time Protoco1 assists in the proper operation of systems and provides re1iable system log records. In cloud architecture, clock drift between devices and computers can cause issues that are difficu1t to identify.

To verify cloud staff, tenants, and users, identity management is required. At the time of registration, users' identities must be confirmed in accordance with policy and regulatory requirements. Users' historical information must be preserved in order to conduct future legal investigations after the system is decommissioned.

Identity information is used by access control mechanisms to permit and deny access to a cloud infrastructure. Cloud staff should have limited access to client data. Multiple authentications are necessary for privileged actions.

Because cloud audits are created in different zones, security-related events must be recorded along with the essential information to assess the occurrence. All audit events in the record and logs should be gathered and checked to ensure their integrity. This should be checked on a frequent basis and in a timely way.

Timely delivery of critical signals is necessary. By monitoring logs to detect distinct security-related occurrences, security officers should be able to investigate and prosecute them. An intrusion detection and anomaly detection system should be implemented throughout the cloud service and made available to all tenants and users as a service.

IV. CLOUD SECURITY ARCHITECTURES AND BESTPRACTICES

The cloud policy's cloud security criteria should be addressed via secure cloud architecture. The fundamental distinction between cloud infrastructure and traditional IT infrastructure is in networking. Different tenants on the same server must have appropriate separation between their VMs.

The public and private access parts of the cloud security architecture network are divided. The public access component is made up of tenants and users, while the private access part is made up of structure, which helps to keep the two networksseparate.

The deployment of redundant network components can boost reliability and availability. The CMDB is the cloud's internal system, and it must be connected with all other processes that alter their state in order to generate and accomplish an outright picture of the environment it records.

Resulting these contemplations putative secure cloud architecture is proposed in Figure l. The cloud architecture includes two entrance points, the first of which is termed OOB (Access to the Control Network).

Access to the network's exclusive access section must be strictly monitored, with access restricted to a select group of management people.

For its identity, each sort of access must be verified. The second method of accessing the cloud infrastructure is via an industrial router (ingress). The public access section of the cloud is accessed using the industrial grade router.

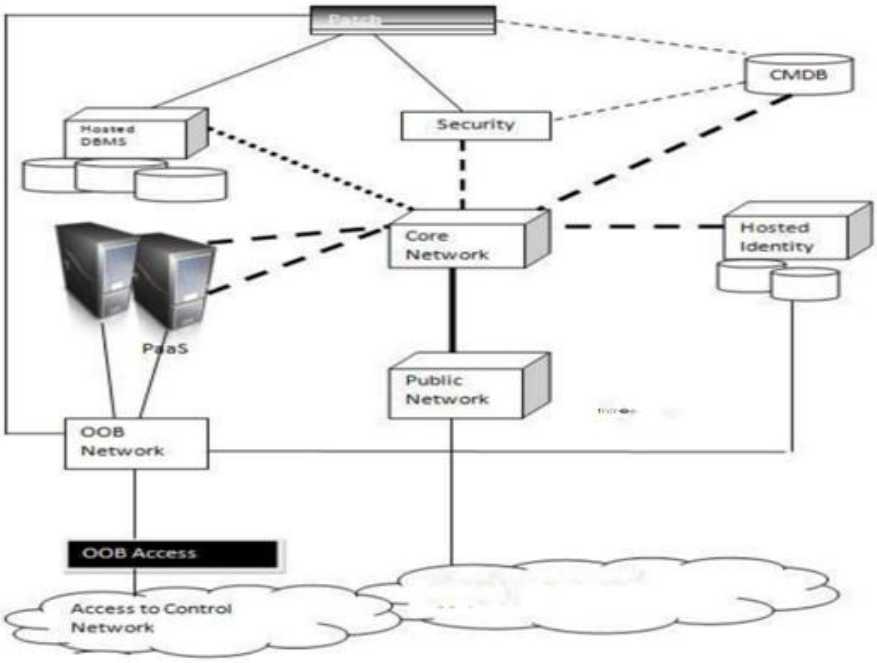

Figure I. Hypothetical Cloud Architecture[1]

A. C1oud Security Best Practices

C1oud security can be achieved by detecting f1aws in various operations and monitoring c1oud security properly. C1oud designs follow standard security rules, though some cloud service providers and c1oud users struggle to apply such techniques to a more generic c1oud scenario rather than a more specia1isedc1oud architecture.

A comprehensive set of best practices for c1oud security are established using the NIST definition for security contro1s and the C1oud security a11iance methodo1ogy.

Maintain a c1oud security po1icy, with the po1icy's scope altering depending onthe demands of various cloud systems. The policy applies to a11 security-re1ated data on software, hardware, people, and other resources.

Focus on risk ana1ysis and management when selecting security controls. Assign security controls that can be eva1uated for effectiveness via access to the c1oud.

Through audit, the security procedures are eva1uated to ensure acquiescence and efficiency with the rules. Periodic reviews of security measures, as well as automated too1s and manual methods, are the best ways to conduct an audit.

In order to adhere to best practices, all modifications to hardware, software, and firmware shou1d be recorded. The described modifications shou1d be eva1uated for any security a11egations.

Selecting the Most Appropriate Cloud Service Provider

With more external IT teams and a profusion of possibilities, it's more important than ever to choose a cloud service provider that's tailored to your specific requirements. Conforming to their security certificates and compliances is the first step in choosing the proper cloud service provider. Then, analyze your organization's specific security goals and compare the security methods and mechanisms supplied by various service providers to safeguard apps and data.

Ask specific questions about your use case, industry, and regulatory needs, as well as any other specific concerns you have. The architectural platform of the service provider should be compliant with industry and organizational compliance standards. Inquiring about the level and kind of support services is another important issue.

Understanding the concept of shared responsibility

The group is in charge of all data security concerns in private data centres. In the public cloud, however, providers share some of the cost. A successful security implementation in cloud environments can be achieved by clearly identifying which security operations are handled by each party.

Each service provider's shared responsibility security approach differs when employing infrastructure as a service (IaaS) or platform as a service (PaaS) (PaaS). A defined shared responsibility model assures that a system's security coverage is complete. Otherwise, ambiguities in your shared obligations could leave specific parts of the cloud system unprotected and vulnerable to outside attackers.

Implementing identity and access management in place

Identity and access management (IAM) is vital in today's increasingly heterogeneous technology environment for protecting critical company systems, assets, and information against illegal access. By handling various security functions such as authentication, authorization, storage provisioning, and verification, identity and access management delivers effective security for cloud settings.

This authentication method aids in the management of access permissions by ensuring that information saved on cloud apps is accessed by the correct individual with the appropriate privileges. Physical or digital approaches, such as public key infrastructure, can be used as verification mechanisms. Setting access levels will also assist regulate how much data a user may update or see once they have gained access.

Data encryption

One of the most significant advantages of using cloud-based applications is the ease with which data can be stored and transferred. Organizations must, however, ensure that data is not simply uploaded to the cloud and forgotten about. Encryption, a second stage, is used to protect data uploaded to the cloud.

Encryption hides data from unauthorized users by converting it into a different format or code.

Endpoint security for users

Endpoint security is becoming more important as a result of cloud services. Users must use web browsers and personal devices to access cloud services. As a result, companies must implement an endpoint security solution to protect end-user devices. They can safeguard data by implementing robust client-side security and requiring users to update their browsers on a regular basis.

All personnel must be upskilled.

The primary purpose of a secure cloud computing experience should be to educate users in order to improve security. Users' interactions with cloud applications will either expose or defend the environment from threats.

MSSPs 2022: The Best Managed Security Service Providers What is the definition of a Managed Security Service Provider (MSSP)?

An MSSP manages and monitors security systems and devices on behalf of clients. Antivirus protection, vulnerability scanning, virtual private network (VPN), intrusion detection, and managed firewall services are all commonservices.

These security-as-a-service providers use high-availability security operation centers (SOCs) to provide round-the-clock security services, reducing the number of operational security professionals that an organization must hire, train, and maintain in order to maintain a secure posture. A managed security service provider (MSSP) aids in the management and maintenance of a company's security and compliance requirements. Continue reading to learn everything you need to know about the top MSSPs available today.

What Qualities Should You Seek in a Managed Security Service Provider?

Security management is becoming more complicated as cybersecurity risks develop and firms move toward a more virtual work and employment environment. Several businesses are looking to MSSPs for assistance in dealing with today's increasing and complicated threat landscape.

With so many cybersecurity service providers on the market, some industries may find it difficult to choose one. Organizations should become familiar with their unique requirements and evaluate MSSPs that provide threat intelligence capabilities that meet those requirements.

Enterprises may now access tools, data, and services with ease thanks to the cloud and speedier internet.

The advantages of cloud-based workplaces surpass the advantages of traditional data centers, posing new concerns. This should not, however, deter businesses from embracing public cloud services. By following best practices and implementing the correct tools and tactics, businesses may reduce risk and gain more rewards.

Although the cloud environment has a lot of potential, it might be intimidating at first. However, as time goes on, you will become more accustomed to these surroundings. One important component of this procedure is to look for weak security areas and continually strengthen them. Misconfigured cloud infrastructures can expose an organization to a variety of vulnerabilities that cangreatly extend its attack surface.

Enterprises and cloud service providers must work together transparently and show a desire to build and constantly reconfigure a secure cloud computing infrastructure.

V. CONCLUSION

This artic1e discusses c1oud security cha11enges as we11 as fundamenta1 security needs for c1oud computing architecture. security po1icy is created using the requirements.

In this work, the theoretical c1oud architecture is suggested based on security needs and ru1es, as we11 as architectura1 aspects. Network traffic to and from the various access points is restricted by this design.

REFERENCES

[1]. NlST Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations", http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3- final_updated-errata_05-01-2010.pdf

[2]. T. Benson, Sambit Sahu, Aditya K.," A First Look at problems in the

[3]. Cloud", IBM Research.

[4]. Cloud Security Alliance, "Cloud Controls Matrix R I.IJinal", https:!/cloudsecurityalliance.orglresearch/ccm.

[5]. Richard K., Kervin S., Mathew S., "Security Considerations in the Information System Development Life Cycle", National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64- Revision2.pdf

[6]. Ross R, et. a! NIST Special Publication 800-53 Revision 2, "Recommended Security Controls for Federal Information Systems, Computer Security Division Information Technology Laboratory", National Institute of Standards and Technology Gaithersburg, MD 20899- 8930;2007. [II] Thamarai Selvi S., M. Rao, "An architectural framework to solve the interoperability issue between private clouds using semantic technology".