Data Analytics and Artificial Intelligence
Vol: 1(3), 2021
REST Publisher
ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/daai/

Securing the Skies: Navigating Cloud Computing Landscape and Security Challenges

G. Amalredge
St. Joseph's College of Arts and Science for Women, Hosur, Tamil Nadu, India.
Corresponding Author Email: g.amalredge@gmail.com

Abstract

With the ability to rely on outside providers for data processing, storage, and public access, the cloud has emerged as a successful computing model for individuals and businesses. The components, service models, deployment methods, and security ideas of cloud computing are summarized in this survey. Numerous security concerns related to cloud computing are currently receiving a lot of attention. These concerns include identity management, data protection, network security, virtualization security, and application integrity. Although several methods are recommended for cloud computing data safety, there are still many unanswered questions. This paper provides an overview of the cloud computing framework and addresses security concerns about data processing, storage, and management.

Keywords: Cloud Computing, Virtualization, Cloud Security, Service Model, Deployment Model

1. Introduction

A widely spread and varied observable fact is cloud computing. Large volumes of data can be stored by users on cloud storage platforms for later use. Access to dynamically provide virtualized IT resources at anytime, from any location. The machines do not have to be in the same physical place to participate in cloud computing. The process of managing, processing, and storing data via an internet-hosted system that includes distant servers as opposed to a local server or personal computer. The majority of cloud service providers save customer data in plaintext; if necessary, users must employ encryption techniques to protect their data. Every time the data is to be processed, it must be decrypted. The data is kept on the public cloud of Amazon Web Services (AWS) using DynamoDB. In a public cloud, user computing is done on encrypted data. Results can be downloaded to a client computer when needed. Users' data is never kept unencrypted on a public cloud in this situation. The US National Institute of Standards and Technology (NIST) defined cloud computing (Mell & Grance, 2011). A shared pool of reconfigurable computing resources (such as a network, servers, storage, applications, and services) that can be quickly provisioned and released with little management work or service provider interaction is what they define as cloud computing (Mell & Grance, 2009). A ground-breaking technique that is transforming enterprise software and hardware design and procurement is cloud computing. Cloud computing offers a plethora of advantages to its users, including free services, elastic resource allocation, internet-based accessibility, and more. Small and large businesses are adopting cloud computing to grow their clientele and form partnerships with other businesses. Prominent companies that have made investments in cloud computing include Google, Amazon, Cisco, IBM, Sun, Dell, and HP. They also offer a variety of cloud-based products to people and organizations. Regarding the many services offered, cloud computing comes in a variety of forms and models. Thus, cloud computing encompasses communal, hybrid, private, and public clouds. Two categories are typically used to categorize cloud computing: geographic location and service offerings. The following Figure. 1 shows a diagrammatic explanation of cloud computing (Khorshed, Ali, & Wasimi, 2012):

Copyright@2021REST Publisher

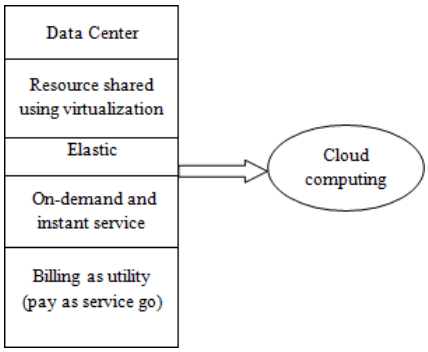

FIGURE 1. Schematic Definition of Cloud Computing

With this technology, customers outsource their data to a cloud provider-run server located outside of their building (Zhou & Huang, 2012). Furthermore, a client can use the internet to visualize, access, and manage memory, processor, bandwidth, and storage (Kumar & Lu, 2010). Cloud computing offers very effective availability and retrieval of data. Resource optimization is becoming more and more delicate for cloud providers.

I. Characteristics Of Cloud Computing

A. On-demand Self Service

The first is on-demand self-service, in which a service user gets the resources they require without assistance from a human and without having to communicate with the cloud provider. Without having to communicate directly with each service provider, a customer can independently provision computer resources, such as server time and network storage, as needed automatically.

B. Broad Network Access

Broad network access, or the ability to access resources from any location using a standard mechanism via thin or thick client platforms such as desktop computer, laptop, or mobile phone, is the second attribute.

C. Resource Pooling

Resource pooling is another feature; this means that resources are combined so that multiple tenants can share them. Resources are dynamically allotted to a consumer in the multi-tenant model, and once the consumer uses them up, they can be transferred to another one to meet high resource demand. Customers are unaware of the location of the resources they are allotted, even if they are assigned on demand. They occasionally have a high-level abstraction of the place, like the nation, state, or data center. The resources that are allocated include storage, processing, memory, and networks. In summary, distinct physical and virtual resources are dynamically assigned and reassigned in response to customer demand, and the provider's computing resources are pooled to serve multiple consumers through the use of a multi-tenant model.

D. Rapid Elasticity

Another feature of cloud computing is rapid elasticity, which allows resources to be dynamically expanded when needed and lowered when not. It is possible to elastically provision and release capacities, and in some situations, they can scale quickly both inward and outward in response to demand. The capabilities that are available for provisioning frequently seem limitless to the user and can be used in any amount at any time.

E. Measured Service

Measured service to determine the amount used. To bill the customer, the cloud provider also has to know how much the user has utilized. By employing metering at a level of abstraction appropriate for the type of service (e.g., storage, processing, bandwidth, and active user accounts), cloud systems automatically regulate and optimize resource utilization. Transparency is ensured for both the service provider and the user by the ability to track, manage, and report on resource utilization.

Copyright@2021REST Publisher

II. Framework Of Cloud Computing

The following Figure.2 shows the framework of cloud computing, which consists of service models available in the cloud, deployed models of the cloud, basic components of the cloud and the security concepts in the cloud.

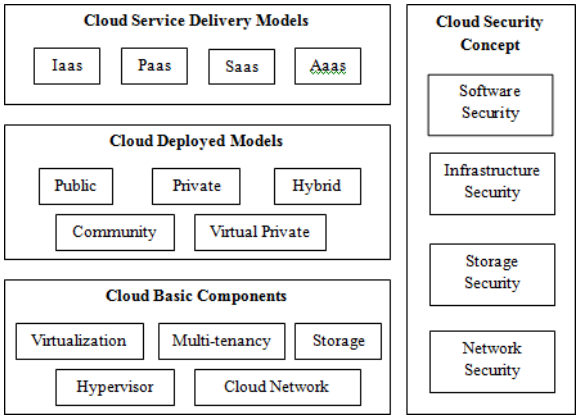

FIGURE 2. Cloud Computing Framework

III. Service Models

Four models are available. The features that each of the models offers to the customer vary (Mell & Grance, 2011). It may be an infrastructure, platform, or piece of software.

A. Software as a Service (SaaS)

It is an assortment of services for remote computing (Fan, Haolong, & Hussain, 2015). The clients can use the software on the cloud infrastructure for their application by using the software and cloud infrastructure provided by the cloud service provider. Without the involvement of the client, the cloud service provider is the only one in charge of managing the underlying physical environment. Using a web browser, the client can use this software as a thin client.

B. Platform as a Service (PaaS)

It is a component of the service model middleware and provides services as development tools (Sun, Dawei, & Chang, 2011). While the infrastructure is managed by the cloud service provider, this service differs from SaaS in that users can install their software. The cloud service provider controls and restricts the physical settings, but each user has power over the application settings.

C. Infrastructure as a Service (IaaS)

This service is at the bottom of the hierarchy (Madjid, Kashif, & Kifayat, 2013). It is possible to provision computing resources like networks and processing storage. Any operating system can be installed and used by the IaaS client. The operating system allows the clients to launch their applications. The ability to allocate virtual or physical resources flexibly contributes to the infrastructure's abstract provision. Additionally, it offers infrastructure provisioning and scalability without requiring significant financial or temporal investments.

D. Anything as a Service (AaaS)

It's a catch-all term for X as a service that incorporates several elements. As a service, X might be anything or anything. In cloud land, this service becomes interchangeable. Using Monitor as a Service (MaaS), Data as a Service (DaaS), Communication as a Service (CaaS), Security as a Service (SecaaS), and Routing as a Service (RaaS), cloud systems can support enormous resources to specific, personal, and granular requirements (Ali, Mazhar, & Khan, 2015).

IV. Deployment Model

In general, cloud computing relies on individual devices or local servers sharing resources. As a result, it can take advantage of resource sharing to achieve consistency. The deployed model explains the nature and function of the cloud. These are the models that have been put in the cloud: In 2014, Aguiar, Zhang, and Blanton (El-Etriby, Mohamed, and Abdelkader, 2012) (Gul and others, 2011) (Smith, Eloff, and Ramgovind, 2011)

Copyright@2021REST Publisher

A. Private Cloud :

Cloud infrastructure is supplied by the cloud provider to a single organization with numerous clients. They are the only ones who may use this infrastructure for their needs. Stated differently, private cloud computing refers to cloud computing that runs and is managed inside an organization's data center. Because the infrastructure in private clouds is owned and run by the same company, it is much simpler to determine the relationship between the customer and the provider. Security threats are therefore simpler to identify.

B. Public Cloud :

This model is different from the preceding one in that it is not private or reserved for the community; rather, it is available to the general public. To meet their demands, the public can have access to a public cloud. A solid service level agreement (SLA) between the provider and the client to uphold confidence is a true representation of cloud hosting. This raises several problems because we have no idea who owns the resources or where they are located, making it more difficult to defend them against harm.

C. Community Cloud:

Many organizations that create a community and share a common objective, security requirements, compliance considerations, or policy can access cloud infrastructure from the cloud provider. A specific feature has been created for the community model's exclusive use in the cloud infrastructure of the organizations, which addresses shared consumer concerns. It may be located on or off campus, and it is either owned, administered by a third party, or driven by a combination of them. Multiple organizations share and manage a community cloud.

D. Hybrid Cloud :

More than one deployment model (public, community, or private) is included in this model. Combining those models can create the cloud infrastructure. Data that travels from a data center to a private or public cloud, or the other way around, is referred to as hybrid data. Technology that is standardized and reliable surrounds the data and application. With a hybrid cloud, you may benefit from several cloud deployment options. If you access the entities through the internet, it is more planned and secure than a public cloud.

E. Virtual Private Cloud :

It is a virtual private network (VPN) that uses less resources and is a semi-private cloud. It is a necessary pool of shared resources that may be customized and allocated inside the cloud upbringing.

V. Cloud Computing Basic Components

These components consist of a wide range of services that we can use all over the internet.

A. *Virtualization* :

It is essential to the cloud's deployment. Multiple consumers can access physical resources in the cloud thanks to a strategic component (Subashini, Kavitha, & Veeraruna, 2011). For the framework to use the resources across several execution environments, it constructs a virtual occurrence of the operating system, servers, network resources, and storage devices.

B. *Multi-tenancy* :

In a multi-tenant environment, different users or customers may not be affiliated with the same company, but they may share resources or functions in an execution environment without viewing or sharing each other's data. Multi-tenancy yields optimal hardware and data storage mechanism utilization.

C. *Storage* :

It is a component that is made available over a network so that users may access the data and is hazily maintained, managed, and backed up.

D. *Hypervisor* :

One essential component of virtualization is the virtual machine manager or monitor. It permits the operation of several virtual computers on a single physical host. It oversees and controls the different operating systems that are installed on a single physical system.

E. *Network* :

It is capable of running many reliable data centers. There are hundreds or thousands of servers in a typical data center. An internet connection is necessary for the cloud to effectively build and administer the storage, much as it is for a virtual private network that lets users safely access files, printers, apps, and other devices.

VI. Cloud Security Concept

Copyright@2021REST Publisher

Security considerations should take precedence when transferring data to cloud services. Cloud computing poses numerous security risks, including insider threats, loss of governance, unsecured incomplete data, and infection of critical documents. Additionally any unlawful applications found within a company. Hence, creating a cloud application security architecture that offers control, visibility, and correction is an extremely difficult task. The primary security problems associated with cloud computing are briefly introduced in the following section:

A. *Software Security* :

The fundamental concepts of software security are provided by the engineering software department, which ensures that the programme operates properly even in the face of harsh actions. One of the main and most important issues in creating a cloud environment is software security. It has security issues, such as implementation errors, buffer overflows, flawed designs, broken error-handling promises, and more.

B. *Infrastructure Security* :

Proving the reliability of the cloud's virtual physical infrastructure is one of the most frequent and basic issues. For the organization to confirm that the primary infrastructure satisfies business needs for security, the third party's certification is insufficient.

C. *Storage Security* :

With a cloud storage system, the data is saved on the cloud and the end user no longer controls the data or the location of its storage. This has always been a crucial component of high-quality service. Concerns regarding malware, data sanitization, cryptography, data leaking, and snooping on data availability are related to storage security.

D. *Network Security* :

The internet is used for communication in cloud computing, and this is one of the advantages of the cloud environment. Worries about external and internal attacks related to network security. These network attacks might happen on a physical or virtual network.

VII. Cloud Security Issues And Challenges

Notwithstanding all of the benefits, the main worry in a cloud environment is security. This document aims to present the most significant security issues effectively. Some authorities on public and private clouds are also included, along with their security concerns.

The following Figure.3 shows the classification of cloud security issues:

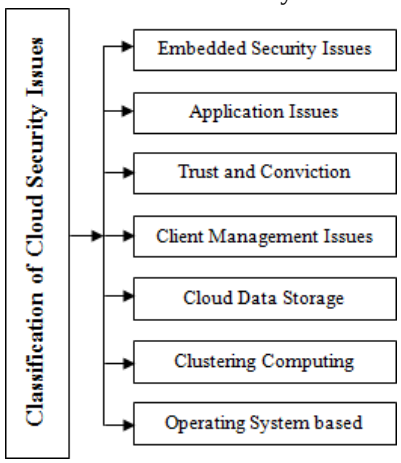

FIGURE 3. Classification of Cloud Security Issues

A. Embedded Security Issues

These days, security in cloud computing environments is a critical concern. Because of these systems' special characteristics, embedded systems security faces several difficulties. Linking an embedded device to a local network is an easy approach to debugging it. Virtualizations are the primary source of security problems for cloud computing in embedded systems (Zissis, Dimitrio, & Lekka, 2012). The following are some distinct domains where embedded systems security vulnerabilities exist:

- Virtual Machine Isolation
- Virtual Machine Monitoring

- Programmability
- Electronic Access Control System
- Simple Network Management Protocol (SNMP) Server

B. Application Issues

The most vulnerable aspect of a software application is its security. The majority of programmes feature a front end, a back end, several platform types, frameworks, and parallelism. The fact that a software application contains one million lines of computer code is its primary security vulnerability. Software is written by many programmers using various languages, and many programming languages contain flaws. The many types of application problems in cloud computing are as follows:

- User Frontend
- User backend
- Platform
- Framework
- License
- Service Availability
- Parallel Application

C. Trust and Conviction

We measured it as the degree to which one relies on the employer's experience to make a judgment that is worthy of confidence. Apart from cloud stakeholders, other aspects include storage, hardware, virtualization, web-based access, and trust-related computational techniques. (Deyan, Chen, and Zhao, 2012) The TCP principles, which are intended to protect the confidentiality and integrity of data handled by the service provider, are the next limit in security transparency. TCP's security programme determines whether or not data has been tampered with or altered. Concerns around cloud computing trust include the following:

- Humal Factor
- Forensic Value
- Reputation
- Governance
- Trusted Third party
- Lack of consumer trust

D. Client Management Issues

From a security perspective, one of the main concerns in cloud computing is client management (Attas, Batra, & Omar, 2011). The following are the security vulnerabilities associated with cloud computing client management:

- Client Experience
- Client Authentication
- Client Centric Privacy
- Service level management

E. Cloud Data Storage

One of the most crucial elements of cloud computing is data storage. With the proliferation of internet services and online applications, data security and storage across distributed computing is becoming a major concern. The following are the security concerns related to cloud storage:

- Location of the Data Warehouses
- Anonymization
- Availability
- Integrity Management
- Data Loss and Leakage
- Cryptography
- Unreliable Data
- Sanitization
- Maintenance

Copyright@2021REST Publisher

- Location protection of metadata

F. Clustering Computing

A computing system cluster is created by grouping several computers, virtual machines, and servers that are configured to be loosely or tightly coupled and function as a single unit. Implementing parallel processing applications in businesses is the primary purpose of cloud clustering (Kim & Jin-Mook, 2013). However, it increases the number of nodes per cluster for the system administrator and presents numerous challenges. The cloud computing cluster security challenges are as follows:

- Physical Cluster
- Virtual Cluster
- Multi-Cluster
- Hierarchical Cluster

G. Operating System- based Issues

Numerous virtual machines, various server types in various intra- and inter-networks, and various operating systems coexisting present numerous security difficulties when it comes to cloud computing (Artem, Volokyta, & Igor, 2012). The various security flaws and vulnerabilities in the various cloud computing operating systems are as follows:

- Desktop Operating System
- Server Operating System
- Network Operating System
- Smart Phone Operating System

2. Conclusion

One of the most promising computing models for service providers, cloud providers, and cloud consumers is the cloud computing paradigm. Cloud security is quickly becoming a top concern for all parties involved due to the quick expansion of cloud computing platforms and services. This study provided an overview of the key features of cloud computing, including deployment models, basic components of cloud computing, service delivery methodologies, and cloud security concerns. Firstly, I am happy to express my gratitude to THE LORD ALMIGHTY for providing me with the motivation to finish this thesis. I would like to express my gratitude to my family for their unwavering support during my preparation.

References

1. Aguiar, E., Zhang, Y., & Blanton, M. (2014). An overview of issues and recent developments in cloud computing and storage security. Springer , 3-33.
2. Ali, Mazhar, & Khan. (2015). Security in cloud computing: Opportunities and challenges. Inf.Sci.305 , 357-383.
3. Artem, Volokyta, & Igor. (2012). Secure Virtualization in Cloud Computing.
4. Attas, Batra, & Omar. (2011). Efficient Integrity checking technique for securing client data in Cloud computing. Intt. J. Electr. Comput. Sci. 11, 6105.
5. Chen, Zhao, & Deyan. (2012). Data security and privacy protection issues in cloud computing. Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE). I. 1, pp. 647- 651. IEEE.
6. Fan, Haolong, & Hussain. (2015). An integrated personalization framework for SaaS-based cloud services. 157-173.
7. Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. 28, 833 – 851.
8. Kim, & Jin-Mook. (2013). An Effective Resource Management for Cloud Services using Clustering Schemes.
9. Kumar, K., & Lu, Y.-H. (2010). Cloud computing for mobile users: Can offloading computation save energy? Computer , 51–56.

Copyright@2021REST Publisher

10. Mell, P., & Grance, T. (2009). The NIST Definition of Cloud Computing.
11. Subashini, Kavitha, & Veeraruna. (2011). A survey on security issues in service delivery models of cloud computing. . Netw. Comput. Appl. 34 (1) , 1-11.
12. Sun, Dawei, & Chang. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. (pp. 2852-2856).
13. Zhou, Z., & Huang, D. (2012). Efficient and secure data storage operations for mobile cloud computing. Proceedings of the 8th International Conference on Network and Service Management (pp. 37–45). International Federation for Information Processing.
14. Zissis, Dimitrio, & Lekka. (2012). Addressing cloud computing security issues. Future Gener. Comput. Syst. 28 (3), 583-592.

Copyright@2021REST Publisher