A Systematic Literature Review and Analysis of Information Security in Cloud Computing

Darcy S*

Editorial Office, International Journal of Innovative Research in Science Engineering and Technology, Belgium

Corresponding Author*

Darcy S

Editorial Office,

International Journal of Innovative Research in

Science Engineering and Technology, Belgium

E-mail: innovativeresearch@scienceresearchpub.org

Received December 25, 2021, Manuscript No. IJIRSET-22-52388; **Editor Assigned:** January 05, 2022, PreQC No. IJIRSET-22-52388 (PQ); **Reviewed:** January 12, 2022, QC No. IJIRSET-22-52388(QC); **Revised:** January 21, 2022, Manuscript No. IJIRSET-22-52388(R); **Published:** January 31, 2022, DOI:10.37533/ijirset.3.1.04-05

Abstract

Cloud computing is an extension of previous computing systems that incorporate both old and new technologies. Cloud computing is a network access architecture that allows users to access a shared pool of resources such as servers, storage, applications, and other services on demand. Cloud computing can be deployed and released with little to no interaction from the cloud service provider, if at all. As people become more aware of cloud services and their underlying technologies, there is a greater demand for up-to-date security standards. These changes have resulted in new security vulnerabilities, as well as security flaws whose full scope is currently unknown. Cloud computing's security challenges are tough, especially when it comes to public clouds. An organisation owns the infrastructure and computational resources. The services are sold to the general public by an outside party. The security needs of the cloud have been addressed in although there have been previous publications, it is still impossible to quantify what which requirements have been studied the most, and which have received the greatest attention? This report conducts a thorough investigation. By identifying cloud computing security, you can do a literature review. specifications derived from articles In addition to security concerns, The benefits of information security in cloud computing have also been discovered. I'm proud to have been a part of this project.

Introduction

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction," according to the official NIST definition. Virtualization or multi-tenancy is commonly promoted as an essential cloud technology in cloud computing. However, it's worth noting that virtualization isn't a must for cloud computing. This strategy is more popular because it has aided in the reduction of pricing and ease of implementation for the pay-per-use model. Cloud computing has gotten a lot of attention in recent years, and it's getting more popular as a result of lower capital and operational costs. The varied layers of controls in different service models and deployments are critical to cloud information security. Security has been identified as the key hurdle or impediment to the adoption of cloud computing technology by several studies and surveys, including that conducted by International Data Corporation (IDC). Users and cloud service providers face several security challenges as a result of the fast rise of cloud computing. This is the primary motivation for delving deeper into this topic and researching potential challenges to adoption, as well as preparing a literature review report on important issues. The focus of this research study is on public cloud deployment because this deployment approach requires extra security considerations.

The top three challenges to adopting a successful cloud strategy in enterprise differ dramatically between IT and line-of-business, according to a recent poll by International Data Group (IDG) enterprise.Concerns about security are raised by 66% of IT professionals, and 42% of cloud-based initiatives are eventually brought back in-house due to security concerns (65%). According to a 2011 survey by International Data Corporation (IDC), 47% of IT executives were concerned about security vulnerabilities in cloud computing. Security and privacy were mentioned as a key impediment to cloud adoption by 76% of respondents in Cisco's Cloud Watch 2011 study for the United Kingdom (research done by loud house). Various governments, IT businesses, and relevant ministries have conducted research on cloud computing security technology in order to improve cloud computing security standards. Data privacy protection, trusted access control, cloud resource access control, retrieve and process of cypher text, confirmation of existence and usability of data, and trusted cloud computing are six components of existing security technology. Data can be turned into cypher text to improve data security, but this may result in the loss of numerous features when data is converted into cypher text.

Cloud Computing Classification

Multi-tenancy, huge scalability, elasticity, pay as you go, and self-provisioning of resources are the main characteristics of cloud computing. The cloud services model.

There are three types of computer systems:

- IaaS (infrastructure as a Service) enables the use of virtualized infrastructure. Internet storage, computer infrastructure environment
- PaaS (Platform as a Service) (hardware, servers, and networking components; form as a service) is a platform for developing applications
- SaaS (Software as a Service) allows users to access internet applications. Applications and software that the service hosts providers

Data security is a major concern with the public cloud deployment strategy. In the SaaS delivery model, on the other hand, the client is reliant on the service provider for adequate security measures. To protect numerous users from seeing each other's data and gain consumers' trust, the supplier must employ some stringent security procedures. Recent evaluations on cloud computing security vulnerabilities are offered, although these assessments are restricted and do not focus on a detailed examination of data security issues. Neither of them conducts a thorough literature review. By using a systematic literature review process, we were able to focus our research on data security issues in more depth.

Information Security in Cloud Computing

The chosen literature will now be assessed against the NIST and CSA recommendations common concerns. This review of the literature will also assist us in identifying areas that have received more attention than others and that require more investigation. This will aid us in making recommendations for future research and work.

Data handling

It's worth noting that prospective cloud service users might be concerned about the security of storing and processing sensitive data. The following states expose data.

Resting data

Data at rest refers to any data stored in computer storage, and it refers to data stored in CSP storage in this case. Since data is saved on the cloud provider's storage, he has more control over it than the client. As a result, it should be assured that CSP maintains conventional security measures and that the service provider's data centre is certified for at least the client's industry type.

Data on the move

Data in motion refers to data that is moved from a stored state to a different location in the same or different form. Data in motion can also refer to data that is in the process of being saved but is not yet complete. Accessing a website with a username and password is also ancillary data in motion.

Data breach

To demonstrate the scope of the threat, CSA cited a research study that showed how a virtual machine may collect secret cryptographic keys used by other VMs on the same server using side-channel timing information. If a multitenant cloud service database isn't correctly constructed, a single defect in one client's application could let an attacker to access not only that client's data, but also the data of all other clients in different ways:

Hijacking of service traffic

If an attacker obtains your credentials, he or she can listen in on your operations and transactions, change data, return modified or misleading information, and redirect your clients to untrustworthy websites. The attacker may use your account or services instances as a new basis. They may then use the strength of your reputation to launch additional attacks.

Insecure APIs and interfaces

For cloud provisioning, management, orchestration, and monitoring, system administrators rely on interfaces and Application Program Interface (API). Organizations and third parties have been known to build on these interfaces, adding add-on services to make system administration easier. Weak interfaces and APIs can expose a company to security concerns such as confidentiality, integrity, availability, and accountability.

Denial of service (DoS) assault

DoS has been a major threat for years, but it becomes more potential threats for CSP and CSU both. It is possible that a malicious user will take all the possible resources which has been hired by client on cloud and the system cannot satisfy any request from other legitimate users due to resources being unavailable. DoS outages can cost service providers, customers and prove pricey to customers who are billed based on compute cycles, bandwidth and disk space consumed.

In today's high-bandwidth era, with enhanced security mechanisms enabled by CSP, an attacker may not be able to completely disable a service, but he might still cause it to use a significant amount of processing time and bandwidth. CSUs are charged on a pay-per-use basis for resources such as compute cycles, storage, and bandwidth, among others. In such instances, CSU will be forced to shut down, and you will be compelled to do so yourself.

Insider attacks by nefarious insiders

Insiders who obtain access to a network, system, or data for malevolent reasons can be current or former employees, contractors, or outsourced third parties. These threats are common in all three Cloud Computing service models: IaaS, PaaS, and SaaS. The system is still vulnerable to hostile insider assaults, even if encryption is used and the keys are not retained with the CSU and are only exposed when data is used.

What methods have been utilized to promote data security in cloud computing?

Encryption

The results suggest that encryption (45%) was the most popular method for ensuring data security in the cloud. It proposes a digital signature scheme based on the RSA algorithm to ensure cloud data security. The "hashing algorithm" was employed by the software to crush down the data documents into a few lines. These lines are known as the message digests, and the digital signature is created by software encrypting the message digest with his private key. The software will decrypt the digital signature into a message digest using its own private key and the sender's public key.

If proposed a location-based encryption approach that relied on the user's location and geographic location. In this case, a geo encryption method was deployed on the cloud and on the user's PC, and the data was labelled with the company's name or the names of the people who work there. When data is needed, similar labels will be searched for and retrieved in the cloud, together with the information that corresponds to the label. To ensure the anonymity of data kept in the cloud, proposes a solution that combines digital signatures and Diffie Hellman key exchange with the Advanced Encryption Standard encryption algorithm. Because it provides authentication, data security, and verification all at once, this technique is referred to as a three-way mechanism.

Guidelines

According to the findings of our analysis, 21% of studies employ guidelines to maintain data security in the cloud. Guidelines for data security in the cloud are offered by establishing a new cloud system design method that includes three features: separation of software and infrastructure service providers, hiding information about data owners, and data obfuscation. To secure data security in cloud architecture, the agents technique is introduced. For data security, three agents were used: file agent, authentication agent, and key managing agent.

Framework

The framework approach accounts for 14% of the total results. In, a framework called TrustCloud is presented, in which a data-centric and detective strategy is proposed to improve data security, with the goal of encouraging the adoption of file-centric and data-centric logging mechanisms to improve data security and confidentiality in cloud computing. By constructing a multi-tenant system, a framework is created. Presentation layer, business logic layer, and data access layer are the three layers in which the produced solution is divided. These levels ensure that user data is kept safe.

Conclusion

Cloud computing is gaining popularity due to its low cost and a variety of other benefits to its customers. Simultaneously, if security concerns are adequately addressed, its adoption may be accelerated.

Traditional security techniques may not be effective in cloud environments due to the complexity of the architecture, which is made up of a variety of complicated technologies.

In order to meet cloud architecture, new security techniques must be developed. On the basis of three prominent cloud computing service models, a security study was conducted.

Cite this article: Darcy S. A Systematic Literature Review and Analysis of Information Security in Cloud Computing. Int J Inn Res Sci Eng Tech, 2022, 3(1), 004-005.