Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

Protecting Cloud Information for Government Oversight Audits Using a Zero-Knowledge Protocol

Devesh Pratap Singh[1], Surendra Shukla[2], Rajesh Upadhyay[3]

[1]Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[2]Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[3]School of Management, Graphic Era Hill University, Dehradun, Uttarakhand India, 248002

ABSTRACT

The innovative paradigm of cloud computing as a service has made it one of the most well-known buzzwords in the IT industry. It claims to reduce operating and support expenses while enhancing adaptability, scalability, and dependability. Many would-be cloud customers are wary of making a wholesale switch to the platform because of safety concerns that have yet to be adequately addressed. In this research, we adopt a framework for security subsystems from cloud service providers and use it to examine the most pressing security concerns in cloud computing today. We discuss the strengths and weaknesses of the solutions that have been presented by other scholars. While much progress has been achieved, there is still a lot of work to do to ensure the safety of cloud computing. If cloud computing is going to overcome its security barriers and gain general use, then it has to become a lot better at dealing with consistency, multi-tenancy, and federation security challenges

Keywords: .

INTRODUCTION

One of the most cutting-edge discussions in the field of information technology is cloud computing. The landscape of computing has been altered by its resource model, and the promises of better adaptability, higher consistency, huge scalability, and lower prices have captivated enterprises and consumers alike.

It's a novel approach to making available computer resources that makes use of the tools already in use. At its core, cloud computing relies on a datacenter that implements virtualization in order to compartmentalise hosted instances of software or services. Cloud customers may lease computing resources from the datacenter for a cost that varies with the specific datacenter services required by the user. You may learn the fundamentals of cloud computing by reading the NIST definition [1].

In this study, "the cloud" will refer to the company responsible for managing the datacenter. A

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

cloud service provider is a company that stores data and software in the cloud (CSP). Last but not least, those who make use of cloud services are known as cloud customers or cloud users.

NIST identifies three distinct cloud computing service models. When using SaaS, a cloud service provider enables a cloud user to install software on the provider's cloud platform. When a cloud service provider (CSP) offers platform as a service (PaaS), it enables its customers to build and deploy applications on the CSP's cloud platform using the CSP's own set of development tools, runtime environments, and other services .

When using IaaS, a cloud service provider effectively creates a virtual computer for the cloud user. Cloud users may install and operate any programme that is compatible with the operating system running on the virtual machine, which can include processing, storage, networks, etc.

computing: public, private, hybrid, and community clouds. In a private cloud, just one company's worth of customers are given access to the cloud's resources (e.g., business units). Its location, whether on or off premises, and its ownership, management, and operation may vary.

Community cloud - The cloud infrastructure is made available to a select group of users from affiliated businesses who all have similar needs

In a public cloud, users have access to a shared cloud computing environment that is available to the public at large. A private company, university, or government agency (or a mix of these) may own and run the facility. It is housed physically in the location of the cloud service provider.

The flexibility to pay for just the computer power you need is a major selling point of the cloud. Businesses and other organisations that need substantial processing capacity may now do so without making a sizable upfront investment in the requisite information technology infrastructure thanks to the advent of the cloud computing paradigm. Massive scalability and enhanced flexibility at a relatively constant price are two additional benefits of cloud computing. [2].

Though cloud computing has numerous benefits, many corporations are still reluctant to switch from their current information technology infrastructure to the cloud. More than 87 percent of respondents in a 2009 survey by the IDC IT group on cloud computing services said they were likely to use such services.

When asked what was stopping them from using the cloud, respondents consistently mentioned security concerns [3]. More widespread usage of cloud computing would need investigation of security concerns and the incorporation of solutions that have been presented.

SCHEME FOR ANALYZING SECURITY IN THE CLOUD

Beginning in the 1980s, governments all over the globe began establishing programmes with the goal of defining the criteria for assessing the efficacy of security features integrated into computer systems. The Common Criteria was established in 1996 as a collaborative effort between the United States, Europe, and Canada. In 1999, the International Organization for Standardization ratified the

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

Common Criteria document, paving the path for universal product security solution acceptance [4].

However, the Common Criteria are most useful as a measure of a product's security features . To better manage the criteria, cloud service providers have reorganised them into five distinct security categories. We have utilised this methodology to analyse the security flaws in cloud computing and the effectiveness of offered fixes.

IBM has identified five functional security subsystems, which are as follows:

Subsystems of the Security Architecture

a. Audit and Compliance: This section deals with the necessities of evidence for an IT setting, including data gathering, analysis, and archiving. Records of events and situations occurring during system operation are collected, analysed, reported on, archived, and retrieved by the system.

b. Access Control: This component manages the identity, authentication, and authorization procedures required to gain access to resources inside a computer solution, thereby enforcing security regulations. When discussing cloud computing, it is important to see these techniques through the lens of a federated access control system.

c. Flow Control: This component controls how data moves through and around a system, enforcing security regulations and making sure data is kept private and undamaged

d. Identity and Credential Management: This subsystem is responsible for the creation and management of identity and permission objects that represent access rights information across networks and across the other subsystems, platforms, and processes in a computing solution Credential objects may need to be created and kept in accordance with legal requirements.
Subsystem e, "Solution Integrity," ensures that a computer solution will function as expected.

DEEPENING OUR UNDERSTANDING OF THE PROBLEMS AND POSSIBLE SOLUTIONS WITHIN CLOUD COMPUTING SECURITY

Evaluation and Acceptance

Compliance with current IT rules and regulations and the separation of compliance obligations are both complicated by cloud computing.

Any business using IT solutions is now expected to have built-in auditing procedures in order to comply with regulations drafted for cyber security. With cloud computing, however, businesses rely on external service providers. The audit duty of an outsourced service provider is not already accounted for in the rules that are now in place [5]. Contracts and service-level agreements (SLAs) between a company and a cloud provider should make it clear who is responsible for conducting audits to ensure regulatory compliance. An organisation creates security policies and executes them with the right infrastructure in order to meet audit rules. A company's internal rules may stipulate stricter standards than those mandated by law. If there is a discrepancy between what the CSP offers in terms of auditing and what is necessary for compliance, it is the responsibility of the client using the cloud services to close the gap.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

The CSA mandates that a Right to Audit provision, which covers audit rights as necessary by the cloud consumer to guarantee compliance with legislation and organization-specific security policies , be included in the SLA between the cloud consumer and provider.

Despite the CSA outlining a basic method for including lawyers, no actual APIs or frameworks for integrating various audit systems have been developed. Neither the CSP nor the end user of a cloud service is bound by any particular standards or models that delineate the division of labour.

Managing who is allowed in and who is not One of the most challenging problems in cloud computing security is admission management. The dispersed nature of cloud computing is one of the key distinctions between it and more conventional computing models. Therefore, with cloud computing, it is important to think about access management from a federated perspective, where a single identity and access management solution is used across numerous cloud services, and even different CSPs.

The responsibilities of admissions officers may be broken down into the following categories:
It is possible for a company to employ the cloud services of numerous CSPs, and to do so in order to supplement its own, perhaps non-cloud-based, infrastructure. An organization's internal apps may utilise one set of identity and credential providers while other cloud services may use a different one. Organizational credentials must be merged or integrated with cloud service credentials. According to the CSA, open standards are preferred since they allow for a more complete evaluation of the security of the approach followed by both CSPs and customers. The needs of an organisation, such a business, will be different from those of an individual cloud user in terms of their user profile and their access control policy.

As soon as authentication is complete, CSP-level authorization of resources may begin. Authorization techniques familiar from on-premises infrastructures may be employed in the cloud. - on In order to function as one, a federation requires at least two separate entities to establish common rules and regulations [6]. Federations make it possible for a variety of unrelated oganisations to be handled consistently. With federated sign-on, businesses may verify the identities of their cloud service users via their preferred identity provider, a crucial component of cloud computing.

One potential headache for businesses that utilise numerous cloud services is needing to authenticate several times in the same session. According to the Cloud Computing Use Cases Discussion Group, a federated identity system is the best way to avoid the hassle of having to sign in more than once. In a federated identity system, users would be able to sign in once to access services from a variety of different CSPs thanks to a central, trusted authority [7].

Regulation of Flow C. As most CSP-consumer contacts occur via the Internet, an insecure and unpredictable channel, regulating the flow of information is crucial. Data security throughout the CSP's data lifecycle of generation, storage, usage, sharing, archiving, and destruction is another aspect of flow control.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

The sheer nature of a cloud means that its underlying architecture is dynamic and must support modification as needed to accommodate its many users. It becomes difficult and needs adaptations of procedures employed in more static contexts today to secure the flow of data between cloud service consumers and providers, as well as between the different components inside a CSP. It is possible to break down flow regulation into its component parts, which are as follows:

There is an absolute need to encrypt credentials in transit, since most cloud services are accessible through the Internet, an insecure domain. Since the information travels between countless, disparate components through network domains with unknown security and these network domains are shared with other organisations of unknown reputability, encryption and secure communication are essential even within the cloud provider's internal network. Multiple layers of the networking architecture should have controls implemented. Shipping is an example of an application layer For optimal data security, lifecycle security Throughout its existence, from creation to deletion, data travels through a series of stages that are monitored by the data security lifecycle. There are a total of six stages to it. For further explanations of these stages. Data may be modified immediately after it is produced during the build process. Loss of data control due to incorrect classification or unauthorised access rights changes. As a precaution against incorrect data categorization, the CSA recommends that businesses use data labelling and classification strategies such user tagging of data . Data must be safeguarded from unwanted access, alteration by network intruders, and leaking during the storage phase since the total security of CSP systems is unknown. Whenever data from several users is stored in the same area, there is an increased potential for security issues, hence safeguards must be included in a cloud environment to mitigate this risk.

The Cloud Security Alliance (CSA) recommends the cloud customer add a condition in the SLA mandating early warning of instances in which storage may be seized or data may be subpoenaed to avoid legal concerns based on the physical location of data.

Phase of Usage and Sharing: Confidentiality of sensitive data must be safeguarded throughout the use phase, which includes transmission between CSP and consumer and data processing. The CSP has an obligation to guarantee the accuracy and consistency of shared data across numerous users or organisations. The CSP should safeguard all of its customers against any hostile actions taken by any of the other customers that use the cloud service .

Similar to the storage phase, the recording phase requires that data be secured against intruders and harmful co-tenants of the cloud infrastructure. Data backup and recovery strategies also need to be in place to stop data from being accidentally deleted or lost. The CSA recommends utilising at-rest encryption, or having the CSP encrypt the data before storage [5], for data in a live production database. To reduce the risk of a hostile CSP or co-tenant gaining access to archived material, it is recommended that cloud consumers encrypt such data locally before transmitting it to the CSP. The destruction phase presents the most difficult problems in terms of data permanence. Erasing information, making it unrecoverable, and, if necessary, physically disposing of it are all necessary steps in the process of data destruction . Disk wiping, physical data destruction techniques like degaussing, and crypto-shredding are only some of the methods recommended by the CSA to be

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

employed by CSPs to guarantee the total destruction of data .

D. Proof of who you are (management) The ability to design an identity provider that receives a user's credentials (a user ID and password, a certificate, etc.) and provides a signed security token that identifies that user is an important part of cloud computing's identity and credential management. Despite the fact that the service provider has no knowledge of the user, they may nonetheless offer the user the necessary access by using the token issued by the identity provider [7].

Different cloud services from different cloud providers may be used by the same company. All of these services need to work together to handle identities, despite the fact that they may use a wide variety of identity objects and identity management systems. Also, identities in an organization's IT system are often provisioned and deprovisioned manually and rarely. Provisioning and deprovisioning of identities must be dynamic in cloud computing because access to services changes more quickly than in a traditional IT application. With federated identity management, a company can quickly control who has access to which cloud services by using a centralised database. Within its own IT infrastructure, a business may keep track of how its many applications utilise various identities by maintaining a mapping of master identity objects to those identities. Customers using the cloud should update or expand such identity data repositories so that they include cloud-based apps and procedures [8] . As it stands, CSPs are the ones that provide bespoke connections for the exchange of IAM and ACS objects. The capabilities offered by CSPs are still insufficient for corporate users. Connectors built specifically for individual cloud services add complexity to administration and are not dynamic, scalable, or expandable. IBM Research – China recommends a brokered trust approach, in which a third-party broker server is utilised to create the trust with a user of a cloud service. The CSP may have faith in the broker because of the commercial agreement between the two parties The broker then acts as an agent for the CSP to develop confidence with other parties, such as enterprises employing cloud services. Next, the companies may use their internal identity federation services to authenticate with the cloud provider by passing over the necessary credentials [9]. This method lessens the burden on the CSP of developing credibility with several customers. This shifts the burden of complexity on the trust broker, allowing for a wider variety of federated identity systems to be supported. If numerous CSPs use the same trust broker, consumers only need to build trust once, even if they want to use many distinct services.

The integrity of the solution, letter E Solution integrity in the context of cloud computing is the capacity of a cloud provider to guarantee the accurate and dependable functioning of a cloud system in order to fulfil its legal responsibilities, such as service level agreements (SLAs), and technical standards to which it complies. Though they manage the solutions, cloud service providers must nonetheless account to their clients and any applicable authorities in the case of a breach or other problem. The cloud user must have access to sufficient data and insight into the cloud service provider's infrastructure so that they may fulfil reporting obligations to both government agencies and their own consumers. The Cloud Security Alliance (CSA) recommends that clients make it clear to their cloud service providers what kinds of occurrences are considered critical and what kinds are considered incidents . A cloud user can see a data breach as a catastrophic occurrence, but an intrusion detection notice as only something that has to be looked at. One of the worst things that

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

can happen to a CSP is for the cloud system to fail and cause an interruption in service. In April 2011, for instance, several well-known websites that relied on Amazon's EC2 service fell down along with it. The disruption was devastating for Amazon Web Services. To avoid widespread disruptions, it is essential that CSPs segregate service zones and have quick failure recovery procedures. If a cloud client has a high fault tolerance, the CSA advises that they check the cloud provider's disaster recovery and business continuity strategies.

Conclusions and Further Research

The concept of cloud computing evolved from previous methods used by computers. This means that established security measures may be implemented locally inside certain cloud computing services. Existing security methods are not sufficient to handle cloud security concerns on their own due to the unique characteristics of cloud computing, such as resource pooling and multitenancy, quick elasticity, wide network access, and on-demand self-service.

Since cloud service providers already exist, it's safe to say that the cloud paradigm has graduated from theory to practise. But existing cloud providers have given very exclusive techniques to cope with security challenges. Multiple suppliers and customers must work together to carry out a single business operation. Furthermore, the emphasis of security needs to move towards developing approaches to allow federation of security services that are employed today if cloud computing is to be deployed on a large scale and really deliver on its promised advantages of elasticity, scalability, flexibility, and economies of scale.

Cloud users should be able to quickly and easily activate and deactivate services from different CSPs via the federation. The combination of cloud computing security with traditional quality-of-service concerns and distributed computing difficulties in a network-wide scope where cloud (storage) systems are implemented in a distributed fashion will provide interesting research topics. Users who are tenants on the same physical infrastructure must have their data, computation, management, and auditing capabilities logically isolated at the component level, across architectural levels, and across providers as a result of multitenancy.

REFERENCES

1. Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128-135.
2. Subha, T., & Jayashri, S. (2017, January). Efficient privacy preserving integrity checking model for cloud data storage security. In 2016 Eighth International Conference on Advanced Computing (ICoAC) (pp. 55-60). IEEE.
3. Sarkar, M. K., & Kumar, S. (2016, October). A framework to ensure data storage security in cloud computing. In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 1-4). IEEE.
4. Kaur, M., & Singh, H. (2015). A review of cloud computing security issues. International Journal of Advances in Engineering & Technology, 8(3), 397.
5. Rani, K., & Sagar, R. K. (2017, August). Enhanced data storage security in cloud environment using encryption, compression and splitting technique. In 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) (pp. 1-5). IEEE.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/31

6. Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., & Buyya, R. (2016). Ensuring security and privacy preservation for cloud data services. ACM Computing Surveys (CSUR), 49(1), 1-39.
7. Zhe, D., Qinghong, W., Naizheng, S., & Yuhan, Z. (2017, May). Study on data security policy based on cloud storage. In 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) (pp. 145-149). IEEE
8. Sahaya Stalin Jose, G., & Seldev Christopher, C. (2019). Secure cloud data storage approach in e-learning systems. Cluster Computing, 22(5), 12857-12862.
9. Swathi, R., & Subha, T. (2017, February). Enhancing data storage security in Cloud using Certificateless public auditing. In 2017 2nd International Conference on Computing and Communications Technologies (ICCCT) (pp. 348-352). IEEE.