Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 12 (2023) pp: 01-04
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Cloud Computing Security Concerns

Dr. Rajendra Kumar Mahto[1]
Assistant Professor
Department Of Information Technology,
Dr Shayama Prasad Mukherjee University,
Ranchi

Urmila Kumari[2]
Research Scholar
Department Of Khortha(TRL),
DSPMU, Ranchi

Abstract
The most popular information technology trend right now is cloud computing. Many firms worldwide are drawn to it because of its noteworthy characteristics and benefits, which include scalability, inexpensive and quick access, throughput, and on-demand Iaas, Paas, and Saas grading. In addition to all the benefits and features of cloud environments, there are certain hazards and difficulties. The two greatest obstacles are security and privacy. This paper reviews many security concerns and dangers, including resource sharing, key management, encryption, trust, and secrecy. It also describes the efforts taken to address these issues.

Keywords
Cloud computing, security concerns, encryption, trust, authenticity, and confidentiality.

***R**eceived 01 Dec., 2023; **R**evised 10 Dec., 2023; **A**ccepted 12 Dec., 2023 © The author(s) 2023.*
P**ublished with open access at **www.questjournals.org

I. Introduction

Technology has advanced to the point that the IT infrastructure is entirely different. In the past, in order to carry out regular duties and store the firm's operational data, an organization needed to construct costly infrastructure. Typically, information was kept in relational databases on one or more internal servers, and clients had to request information from those computers. This was highly expensive because the company had to pay employees to install, oversee, and maintain the infrastructure.

The ideas of clusters [1] and grid computing have emerged in recent decades.

[2} created new avenues for the architecture and storage of information. Data on clusters or in the form of geographically distributed, diverse, and weakly linked grids might now be stored [3]. Similar to clusters and grids, it makes use of resource pooling and wide network access, but it differs in that it allows users to access self-services on demand [5].

Cloud security remains a major concern, despite the fact that cloud computing has undoubtedly offered many exciting services and features like flexibility, dependability, limitless storage, portability, and quick processing power [6]. The failure of cloud services, the possibility of malevolent insiders, and a lack of trust are just a few of the security issues covered in [7]. This paper reviews different security threats to Cloud Computing like trust, privacy, confidentiality, Authenticity, encryption and discusses the presented solutions to overcome these issues. Each security risk will be covered in detail in its own section, along with the workable There are four sections in this paper. The features and challenges of cloud computing are introduced in Section I. Cloud computing background work is covered in Section II. In Section III, the issues were thoroughly examined along with suggested fixes. These problems and their fixes are covered in Section IV. Finally, recommendations for further work are provided.

II. Background Work

Since cloud computing is currently the hottest technology, a lot of research has been done on it, particularly in the area of cloud security. The Cloud Security Alliance (CSA) [8] was established in December 2008 with the goal of ensuring security in cloud computing environments. As their first offering, CSA released "Security Guidance for Critical Areas of Focus in Cloud Computing" [9] to assist users in improving knowledge

of cloud computing and security requirements. Many efforts have been made to provide efficient and effective controls to provide information security in the cloud environment by the Multi-Agency Cloud Computing Forum and the Cloud Computing Interoperability Group [31].

To date, a lot of work has gone into identifying the primary cloud security vulnerabilities. According to reports, cloud computing's two main security concerns are trust and privacy [10]. The difficulties with cloud computing's security and privacy are covered in detail in [11]. Where the security issue is also addressed in [12]. It is stated that security and privacy concerns must be resolved before cloud systems can expand [13]. A framework for cloud computing and an information as set classification model were presented to assist cloud users in selecting various models and services of delivery [31].

III. Security Problems and Their Fixes

The challenges associated with cloud computing are covered in this section along with suggested fixes.

A. Trust

The primary problem facing cloud computing today is trust between customers and service providers. The customer is never certain if the service is reliable or not, or if his data is safe from hackers. The terms of the Service Level Agreement (SLA) document bind both the customer and the service provider. This is a type of an agreement between the customer and the service provider; it contains the duties of service provider and his future plans [7]. Regretfully, though, there are no SLA standards. Up until now, a lot of work has been done to address the concerns of privacy and trust in fix the cloud's security problems. In order to improve the security and interoperability of the cloud computing environment, a trust model is presented in [10]. In partnership with social media, Husky Healthcare Social Cloud [14] offers a trust-rating mechanism to secure the cloud environment. SLA StructureA trust management model for security in cloud environments is proposed in [16] using [15].

B. Keep Information Private

Preventing the disclosure of sensitive and private information is the definition of confidentiality. Since all of the data is kept in geographically dispersed locations, confidentiality becomes a significant problem. There are several ways to maintain secrecy, but encryption is the most popular one. But the cost of this method is somewhat high.

A secure cloud storage service [17] is created to protect privacy and is based on the ure and by utilizing cryptographic methods, confidentiality is attained. A novel strategy put forth by [18] protects privacy by using a P2P reputation system hierarchy. With virtualized defense, it obtains it.[19] explains how attribute-based cryptography can be used to protect security and privacy in cloud-based electronic health record systems while enabling patients to share data in a way that is adaptable, scalable, and dynamic.

C. Genuineness

Another significant problem with cloud computing is integrity. It alludes to incorrect information modification. Since the data is scattered throughout the cloud, the access control system needs to be extremely safe, and each user needs to have their identity confirmed.Digital signatures can be used to solve authentication issues, but even after gaining access to Without digital signatures, a user is unable to access and validate the data subsets.

The access control scheme introduced by [20] is a robust and decentralized mechanism that verifies the identity of cloud users without requiring the cloud to know who they are before storing any data. Information can only be decrypted by authorized users. This scheme also prevents replay attacks. Another scheme [21] presents a new environment in which users are not required to register with service providers and are free to choose their own provider. The user receives the credential information from the data owner. The identity information for each user is generated by the username and password combination, which the data owner provides to the service provider. This plan shows to be incredibly scalable.

The use of encryptionThe most popular technique for protecting data in cloud computing is encryption. But it also has a few shortcomings. For encryption, a lot of processing power is required. The encrypted data must be decrypted before a query can be executed, which lowers database performance overall. There are numerous ways to guarantee that improved encryption is offered in terms of improved security and functionality.

According to a method put forth by [22], employing multiple cryptographic techniques can increase the overall throughput as opposed to using just one. These techniques are used to encrypt data in every single cell of a cloud table. The query parameters are used whenever a user creates or runs a query. examined and

assessed in relation to the recorded data. In order to improve performance, the user decrypts the query results rather than the cloud.

A different method called "send-to-end policy based encryption"[23] uses a different policy for data encryption and decryption. Decryption keys are made available by the Trust Authority, allowing users to have fine-grained access control in public clouds. A different technique called fully homomorphic encryption[24] is a more recent development that offers the outcomes of calculations made on encrypted data as opposed to the raw data. It offers stronger encryption and increases data confidentiality.

D. Crucial administration

Encryption and decryption keys are required for encryption, and maintaining these keys poses a significant security risk in cloud environments. Keeping these Using cloud encryption keys is not a good idea. While storing a single encryption key is simple, doing so for real-time systems becomes more difficult. To store the keys locally in a protected database, this might need the creation of a second, tiny database. However, that is also a bad idea because it will defeat the purpose of moving our data to the clouds. We will require more hardware and software resources as a result, and financial concerns will also surface. The soleTwo-level encryption could be a key management solution [25]. The ability to store encryption keys in the cloud can be very useful.

E. Data Division

Splitting data could be a better option than using encryption. It is undoubtedly extremely quick when compared to encryption alone. The primary concept is to distribute the data among several non-communicable hosts. A user needs to be able to access both service providers in order to retrieve the original data whenever they need it back. It is undoubtedly a very quick technique, but it also has security problems of its own.The Multi-Cloud Database Model [7] is a data splitting technique that uses several clouds and various methods to guarantee the availability and integrity of the separated data. As a result of the data being stored and replicated across several clouds, security is significantly improved and the likelihood of an intrusion is reduced. These clouds use a secret sharing algorithm to exchange data.[26] and TMR methodology [27].

F. Multitenancy

Various resources and services are shared by various applications at various geographical locations in a cloud environment. This is done in order to address the problems of scarce resources and to achieve the primary goal of the cloud, which is cost elimination. However, issues with confidentiality arise when an organization shares its resources. To maintain confidentiality, these systems and applications need to be somewhat isolated. If not, it is exceedingly challenging to monitor the data flow, and security breaches occur [28].Both real hardware and virtual servers may be used to store data and apps in the cloud. Security concerns are present in both situations. If these are digitally saved, there are possibilities that the performance of other virtual machines may be impacted by one machine hosting a malicious application. Because of multi-core processing, there might be security risks if these are kept on actual hardware. To ensure the safety of their clients in cloud environments, cloud providers ought to utilize Intrusion Detection Systems [29]. In [29], an architecture for deploying IDS is provided. The goal of the Trusted Cloud Computing Platform (TCCP) is to increase virtual machine security [30].

IV. Discussion

Although cloud computing has brought about a number of exciting new features and services, such as portability, flexibility, dependability, limitless storage, and fast processing power, cloud security is still a major concern. The discussion included important security concerns related to cloud computing, such as trust, confidentiality, integrity, authentication, encryption, and resource sharing. their fixes.One of the primary issues raised is defining the appropriate structure for a SLA document, which helps to clarify for both customers and service providers what services the cloud is meant to offer and what they can expect from it.

Encryption is another significant problem with cloud computing, and various mechanisms have been implemented to address it, such as end-to-end policy-based encryption [23], cryptographic techniques, and others.[22] and encryption that is fully homomorphic [24].

There is also discussion of various trust management models [10], [14], [15], and [16]. The three main methods for maintaining confidentiality are described as attribute-based cryptography [19], virtualized defense [18], and secure cloud storage service [17]. The model of data splitting technique is examined as a substitute for encryption.Additionally, [7] is explained.

V. Conclusion

The various security risks associated with cloud computing are examined in this study, along with potential solutions. In this context, it can be concluded that the two most important issues are data encryption and trust, followed by authenticity and data integrity.

VI. Future Work

As a relatively new and rapidly developing field, cloud computing needs to resolve security concerns if it is to become a more and more important technological advancement in the future. Many studies are being conducted in this area to address these important problems, but there are still a lot of unanswered questions and opportunities for more research.

References

[1]. "High performance cluster computing," Buyya, Rajkumar, F'rentice, New Jersey (1999).
[2]. Foster Authors: Ian and Carl Kesselman. "The Grid 2: Blueprint for a new computing infrastructure", Elsevier, 2003.
[3]. Grid computing: what is it? Gridcafe. E- [Available Online:
[4]. ScienceCity.org (retrieved on June 18, 2014).
[5]. "A view of cloud computing," Michael Armbrust et al., Communications of the ACM 53.4 (2010), pp. 50–58.
[6]. "The NIST definition of cloud computing (draft)", NIST special publication 800.145(2011):7, Mell, Peter, and Timothy Grance.
[7]. IEEE Security and Privacy, pp. 49–55, 2011. Weis, J., and Alves-Foss, J. "Securing Database asaService".
[8]. "A Novel Method Using Redundancy Technique to Enhance Security in Cloud Computing." AlZain, M., Soh, B., Pardede, E. IEEE, 2012.
[9]. Ellen Messmer, "Cloud Security Alliance formed to promote best practices," March 31, 2009. world of computers.obtained May 02, 2014.
[10]. "Security Guidelines for Cloud Computing's Critical Areas of Focus." Alliance for Cloud Security. obtained May 02, 2014.
[11]. "Trust model to enhance security and interoperability," Li, Wenjuan, and Lingdi Ping 69–79. of cloud environment, In Cloud Computing. 2009; Springer Berlin Heidelberg.
[12]. "Trust Cloud: A framework for accountability and trust in cloud computing," by Ko, RyanKL, et al., was presented at the 2011 IEEE World Congress on Services (SERVICES).
[13]. "Privacy, security, and trust issues arising from cloud computing," by Pearson, Siani, and Azzedine Benameur, in Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. IEEE, 2010.
[14]. "Security and privacy challenges in cloud computing environments," by H. Takabi, J.B.D. Joshi, and G. Ahn, IEEE Security & Privacy, 8(6), pp. 24–31, 2010.
[15]. In the 12th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing (CCGrid), Wooten, Ryan, et al., "Design and implementation of a secure healthcare social cloud system," IEEE, 2012.
[16]. "Conceptual SLA Framework for Cloud Computing," by M. Alhamad, accepted for IEEE DEST 2010 on March 15, 20 October 2010.
[17]. Elizabeth, Tharam Dillon, Mohammed, and Alhamad Chang "Sla-based trust model for cloud computing," IEEE, 2010 13th International Conference on Network-Based Information Systems (NBiS).
[18]. "Cryptographic cloud storage," Kamara, Seny, and Kristin Lauter, Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 136-149, 2010.
[19]. "Cloud security with virtualized defense and reputation-based trust management," Hwang, Kai, Sameer Kulkareni, and Yue Hu. Dependable, Autonomic and Secure Computing, 2009. DASC'09.Eighth IEEE International Conferenceon. IEEE, 2009.
[20]. Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ACM, 2010. Narayan, Shivaramakrishnan, Martin Gagné, and Reihaneh Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure".
[21]. In the 2010 IEEE INFOCOM Proceedings, Yu, Shucheng, et al. discussed "Achieving secure, scalable, and fine-grained data access control in cloud computing."
[22]. In the International Journal of Security & Its Applications 6.2, Yassin, Ali A. et al. discussed "Efficient Password-based Two Factors Authentication in Cloud Computing". "Efficient Query Processing on Outsourced Encrypted Data in Cloud with Privacy Preservation," Purushothama B. and Amberker B. (2013).
[23]. In the 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), Pearson, Siani, et al. presented "End-to-end policy-based encryption and management of data in the cloud."
[24]. Tebaa, Maha, Abdellatif El Ghazi, and Saïd El Hajji. "Applying homomorphic encryption to the security of cloud computing," World Congress on Engineering Proceedings, Vol. 1, 2012.
[25]. "Achieving fine-grained access control for secure data sharing on cloud servers" (Wang, Guojun, Qin Liu, Jie Wu) was published in Concurrency and Computation: Practice and Experience 23.12(2011) on pages 1443–1464.
[26]. "How to share a secret," Adi Shamir, Communications of the ACM 22. 11 (1979), pp. 612-613.
[27]. The application of triple-modular redundancy to increase computer reliability was discussed by Lyons, Robert E., and Wouter Vander kulk in IBM Journal of Research and Development 6.2 (1962), pp. 200–209.