iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49757

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Security Challenges in Cloud Computing

Anjali M.S[1], Ananya Harshan[2], Claijo Kurian V[3]
[1,2]*B.C.A. Students,* [3]*Assistant professor, Department of Computer Application, SNGIST Arts & Science College, North Paravur, Kerala, India*

Abstract: ***The most technological trend in the IT world is cloud computing, and because of its youth, both its users and its manufacturers have certain concerns. Looking over its literature, we can observe that the primary issues are trust, privacy, and security. That makes a significant barrier for users to use. Hence, to determine whether cloud computing would be accepted, we decided to assess various issues, including security. In this article, the security paradigm was the central issue, focusing on privacy safeguards and the need for trustworthiness to implement cloud computing. As a by-product, we have suggested radical innovations for enhancing security, reducing risks, improving trust, and protecting consumers, which are crucial for the adoption of cloud computing.***

Keywords: Security, trust, privacy, authentication and validation, data recovery, and backup

I. INTRODUCTION

By improving services and economic outcomes that can improve scalability, agility, and cooperation, cloud computing is an essential instrument that may drastically reduce costs. Great companies and IT corporations in industrialized countries can greatly benefit from this technology, but these opportunities are not without risk because security is one of the major issues in this area. All aspects of cloud computing, such as handling private data on the internet, can experience issues if security measures are implemented incorrectly. To put it another way, utilizing lax security measures and practices and paying little regard to privacy when using cloud computing could lead to a major disaster. It may be said that when it comes to adopting cloud computing, security is the key factor. If the developers of this technology can overcome or at least lower this huge barrier, cloud computing will be the bleeding edge of IT, and adoption will be facilitated. Security is therefore crucial from the service provider's standpoint for safeguarding the internet and its resources and promoting trust in them. The key issues with cloud computing are security, trust, maintaining privacy, and how to encourage trust while adopting and sharing useful software and hardware in a situation where we don't know who will be managing our information. A little research about privacy and trust when using cloud computing has been published in the literature. There is a lot of research addressing cloud computing-related technological issues as well. In this section, we examine security in the context of faith and confidentiality within modern cloud computing, noting that reputation and anonymity are one of the primary hurdles to adoption. In addition, we reviewed previous studies in this field, looking for flaws and making recommendations.

II. SECURITY CHALLENGES IN CLOUD COMPUTING

A. Security

Cloud security concerns are a significant obstacle to widespread implementation. Potential threats may be categorized as vulnerable metadata, data partitioning, anonymity, bug penetration, rehabilitation, liability, malicious internal users, administration dashboard encryption, user authorization, and interpretations. To increase client confidence in cloud computing technology, there are several difficulties and concerns that might result in a loss of security that must be taken into consideration. The researcher has categorized the security threats that may influence cloud service providers or their subscribers as insider threats, hostile outsider cyberattacks, information leakage, issues with multi-tenancy, diminished oversight, and network congestion. The monitoring program for cloud infrastructure must be utilized to safeguard cloud virtual infrastructure. External intrusions, unscrupulous internal users, ubiquitous connectivity, diminished authority, and service disruption are among the sorts of acts of aggression that must be dealt with first and foremost. Farazi Sabhai et al. outline the well-known Gartner seven vulnerabilities. Profound security issues, such as data leakage and DoS (Denial of Service) assaults, are addressed. Cloud security solutions include security controls, occurrence countermeasures, and responses. Zhidong et al.'s for the Trusted Computing Environment solves cloud computing security concerns (TCP). In cloud technology, TCP offers authorization, anonymity, and reliability. TCP is implemented as a cloud computing infrastructure in authorized cloud computing systems, guaranteeing trustworthiness and confidentiality.

The components included in the proposed model include verification, performance authentication protocols, data integrity, and user activity monitoring. In this, security concerns, deployment, and service paradigms for cloud computing are discussed. The seven security concerns about cloud computing identified by Gartner are described. Privilege user access, regulatory compliance, data location and segregation, recovery, investigative support, and long-term sustainability are among these problems. Security, cost, invoicing, Service Level Agreements (SLAs), deciding what to move to the cloud, and cloud interoperability is just a few of the challenges connected with cloud computing. Carrying out a study on the market to understand current innovation, academic and industry research projects, and cloud computing challenges. There is also a breakdown of Gartner's seven security issues. Security processes such as centralized data, incident response, password assurance testing, and secure software development are all explained. Surianarayanan et al. discuss cloud computing security risks. The key areas of concern are the four levels of the network; system, virtual machine, and application security. The three types of cloud security rules and practices are pre-migration, in-operation, and termination. Many security control mechanisms are available to address security problems at these four levels. Concerns about policy, software, and hardware security. Security rules between a cloud service provider and a cloud client must consider components such as internal risks, access control, and system portability. The two types of security that must be addressed in order to build a safe cloud are software security, which includes virtualization software, encryption, and host operating systems, and physical security, which includes backups, firewalls, and server locations. The difficulties and concerns associated with cloud computing are investigated and addressed. The use of multi-tenancy techniques provides security. The cloud computing model tiers' dependencies are outlined. The functionality and security of a higher layer are dependent on lower ones in this technique. This dependency complicates the issue of cloud security. Cloud security approaches include managing access and identity, vulnerability assessment, strong authentication, reliable development of software lifespan, and strong aptitude and efficiency.

B. Trust

Trust is just keeping your word. It is founded on the guarantee that a promised action would unquestionably be carried out and kept. But it is obvious that our trust will be negatively impacted if we receive little or unnecessary information about our demands from the system. As a consequence, confidence is established when human requirements are fulfilled and all services are provided. The explanations below may help to comprehend the concept of established trust between two parties participating in a transaction. When an entity A feels certain that an entity B will perform exactly as expected and necessary, such a relationship is said to be one of trust. From another perspective, it is possible to say that having control over our data demonstrates our faith in the system. For instance, we have trust in ATMs because we know we can control our money and they will give us the precise amount we want. In contrast to when we use an ATM to make a deposit, after we have given the machine our money, we no longer have control over it. The user likewise feels the same way about their cloud-based data. Hence, trust is developed as a relational protocol between cloud service providers and consumers through time and is crucial to collaboration. As a result, trust starts off small and grows over time. Trust is seen as over when it first begins. As cloud computing is a new technology and its participants do not have considerable and complete knowledge of one another, this degree of trust is known as primary trust. It is important to note that various organizations place varying values on trust depending on the data they store in cloud systems. Cloud computing's perceived value will gain from the trust. When data and application governance are outsourced and entrusted to third parties outside the owner's strict control, the deployment method selected has a substantial influence on trust in a cloud environment. According to Hoffman et al.survey, 95% of customers do not provide personal information to websites. 63% of them indicated they suppressed personal information because they didn't trust the people collecting the information. Trust, therefore, appears to have an effect on how innovations are accepted. Moreover, trust raises the likelihood that the consumer will receive the anticipated advantages, according to Geffen et al.

C. Privacy

Four categories may be used to characterize privacy, which is a fundamental human right:

1) Physical privacy: This emphasizes everyone's inalienable right to their bodies, notwithstanding statutory limitations.
2) Interpersonal privacy: apart from legal restraints, it provides message, phone, and morse code secrecy.
3) Environmental anonymity: Except in exceptional circumstances, it is illegal to enter a person's home against their will.
4) Informational privacy: It means that (1) all individuals have the capacity to respect their personal matters, subject to legal restraints. (2) their private lives are protected in terms of the documentation and sharing of private data as stipulated in the law, and (3) it provides for the requirements relating to the inspection of published private data, the use of published private data, and the modification of this information as permitted by law.

Personal data, commonly referred to as " privacy-sensitive information", is an essential component of informational privacy. (1) "Any information that might be used to identify or locate an individual (for example, name and address) or information that can be linked with other information to identify an individual" is deemed personal data. (for example, credit card number and postal code,Internet protocol (IP) address), as well as sensitive information such as confidential health information or financial information.", (2) Sensitive information, defined as "information on religion or race, health, sexual orientation, or any information deemed private," (3) Usage data: information on activities, such as recently visited websites and prior product consumption; and (4) unique device IDs, which include any extra data that may be explicitly connected to a user device, such as IP addresses and distinctive hardware identifiers. Cloud computing security should comply with numerous national standards and legislation. These laws and guidelines were originally intended to protect information that could be used to identify a specific person.

D. Authentication and Validation

Authentication is a simple task where one party grants access rights to the system. If the username and password match the system, it returns a value indicating that permission is granted**.** Authentication in the cloud uses credentials to provide authorization to users through various context-sensitive information to access cloud services. With key authentication considerations, the Authorization and Validation Service is a vehicle and platform for managing what a user needs to access based on contextual decisions on constraints associated with the user's profile and role. provide. Authentication is considered a major concern in cloud computing. Users have an important responsibility to authenticate with their organization's devices to access cloud services hosted outside the perimeter of a managed firewall. Authentication puts tremendous pressure on users to manage their credentials stored in the Active Directory database and in the cloud. " Further, "Reference [notes that user credential authentication and validation require a great deal of effort by both IT administrators and users to manage themselves. Data saved in the cloud can only be accessed by authorized users, according to the authentication process of multifactor authentication online banking systems in the cloud. Various factors, including id, passcode, random list, and biometric fingerprinting, are utilized to authenticate users. Encrypting random numbers is done using the user's biometric fingerprint. But, throughout this procedure, an encrypted, unpredictable number is delivered to the registered mobile number via an open susceptible channel, opening the door to a variety of assaults. Moreover, the validation of biometric fingerprint samples necessitates additional computational resources. Data security is significantly ensured via validation. Attacks can be decreased with the aid of a verification component that provides the assurance that customers can approach information and data. There are several limitations to the validation of cloud users using private key access. Most modern cloud focused businesses protect their sensitive data using a simple client name and password associated with the user account, enabling client authentication and preventing unauthorized users.

E. Data Recovery and Backup

Users are responsible for being aware of basic backup and recovery mechanisms to protect their data in the cloud. "Reference states that users sometimes ignore basic recovery and backup strategies. The Reference further explains that neglecting these aspects can cause irreparable damage to data stored in the cloud." The duration and time required to recover from cloud and outages should be highlighted and factored into the service level agreement.

The Service Provider (SP) should also provide clear backup mechanisms for data recovery in the cloud. The consequences of not returning data on time have a huge financial and organizational impact on the user who has invested in the technology. As highlighted in the literature, the consequences of data recovery and backup uncertainty raise compliance and management issues. Restoring and saving data in cloud services has been one of the main problems in adopting other cloud services. Little has been done in the literature to increase user awareness of data recovery and cloud backup. The purpose of this article is to propose viable mechanisms to address these issues. The data security of cloud services is distinctive since they provide data service operations as services. The fact that user data is kept on a cloud server and that downloading and uploading both need the use of a network raises the possibility of data leakage during transmission. Cloud computing is built on a decentralized network, computer servers are contracted, and user information is kept in a network node. Information is saved with a semi-trusted third party. Theoretically, an attacker can use a certain node and a specific way to get access to nearby nodes,as mentioned above. Cloud storage has sparked a lot of interest from businesses, academia, and even governments in the development of cloud computing and its derived technologies. Its main function is to manage and store resources on a cloud platform so that users may instantly access information online. International IT behemoths like Microsoft, Google, and Amazon, as well as local firms like Baidu, Ali, and Tencent, have conducted extensive research on cloud storage and provide comparable cloud storage systems.

Redundancy of user data raises the demand for distant bandwidth, puts more storage strain on the cloud storage server, and slows down network transmission. In order to decrease the substantial quantity of duplicated data in cloud storage servers and conserve as much storage space and network traffic as possible, data duplication technology has increasingly gained popularity as a study area. It's also crucial to back up and restore their current data. It is taken into consideration by the cloud storage platform.

III. CONCLUSION

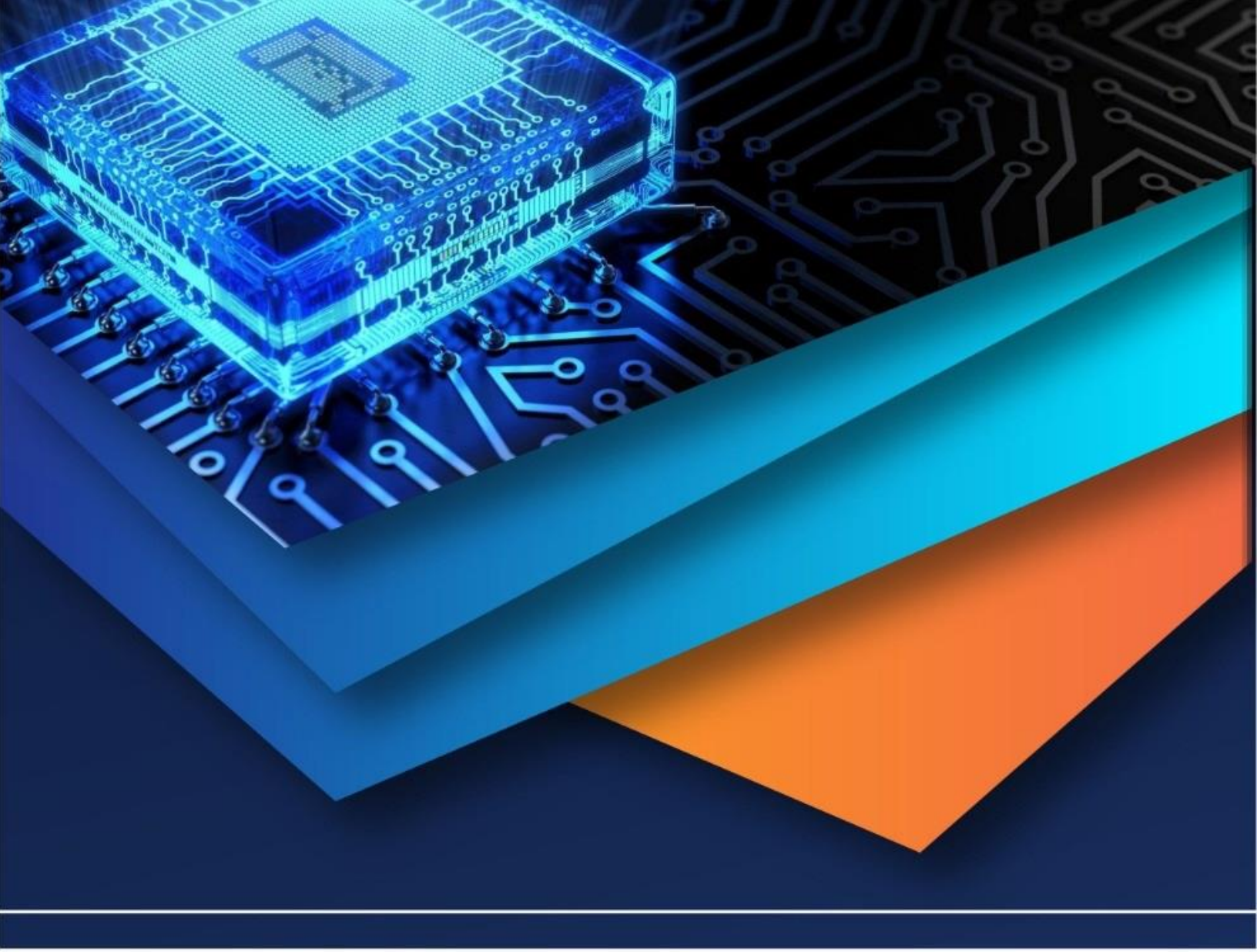
In this review article, we have offered a complete study of the security issues relating to cloud computing. Cloud computing is a form of technology that provides remote services to manage, access, and preserve data through the Internet rather than storing it on servers or local discs. Images, music, video, papers, and other types of data can all be utilized in this situation. Cloud computing undoubtedly offers a number of advantages, but there are some security issues as well. Data privacy and data security are the two main issues with cloud computing. Consumers detest not being able to access their cloud-based data. Many are worried about the security of personal data since it is kept on the cloud. Consumers also want to know if, given the size of the cloud, they will have access to all of their personal data. They also inquire as to whether their data is shared with third parties. The user should also think about whether they would be able to retrieve their data in the event that something were to happen to it. The question of whether the cloud service provider would alert customers if their information is hacked worries consumers. Using cloud computing is hampered by a lack of confidence and an uneasy sense. In this article, a summary of cloud computing, its many security characteristics, and the important factors affecting cloud security was provided. Cloud service providers and consumers alike need to be confident that their cloud is 100 percent safe. Cloud services are increasingly being used by many enterprises, but their use is still constrained by important security and protection issues.

IV. ACKNOWLEDGEMENT

We would like to express our sincere thanks and gratitude to all the professionals and guide teachers for their valuable support and guidance in our research work.

REFERENCES

[1] M. Monsef, N. Gidado, ―Trust and privacy concern in the Cloud‖, 2011 European Cup, IT Security for the Next Generation, 2011, p.1-15.
[2] D. Zissis, D. Lekkas, ―Addressing cloud computing security issues‖, Future Generation Computer Systems, Volume 28, Issue 3, March 2012, P. 583–592.
[3] S. Pearson, A. Charlesworth, ‖Accountability as a way Forward for Privacy Protection in the Cloud‖, Computing, Vol.5931, Springer, p.131-144, 2009.
[4] Fei Hu, MeikangQiu, Jiayin Li, Travis Grant, Draw Tylor, Seth Mccaleb, Lee Butler, Richard Hamner, ―A Review on Cloud Computing: Design Challenges in Architecture and Security‖, Journal of Computing and Information Technology, Vol.19, p.25-55. 2011.
[5] Miika Komu, Mohit Sethi, Ramasivakarthik Mallavarapu, Heikki Oirola and Rasib Khan, Sasu Tarkoma "Secure Networking for Virtual Machines in the Cloud", Cluster Computing Workshops (CLUSTER WORKSHOPS), IEEE International Conference, Beijing, 24-28 Sept. 2012, pp 88 – 96, Print ISBN: 978-1-4673-2893-7, DOI: 10.1109/ClusterW.2012.29.
[6] Tomohisa Egawa, Naoki Nishimura, Kenichi Kourai "Dependable and Secure Remote Management in IaaS Clouds", IEEE International Conference on Cloud Computing Technology and Science, ISSN: 9781-4673-4510-1.
[7] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 3rd International Conference on Communication Software and Networks(ICCSN), 27-29 May 2011, pp 245-249, Print ISBN: 978161284-485-5, DOI: 10.1109/ICCSN.2011.6014715
[8] Zhidong Shen, Qiang Tong " The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, Dalian, (ICSPS), 5-7 July 2010, Vol 2, pp 1115, Print ISBN: 978-1-4244-6892-8, DOI: 10.1109/ICSPS.2010.5555234.
[9] Kuyoro S. O., Ibikunle F. & Awodele O., "Cloud Computing Security Issues and Challenges", 24-28 May 2010, pp 344-349, print ISBN: 978-1-4244-7763-0.
[10] Traian Andrei, "Cloud Computing Challenges and Related Security Issues", May 2012.
[11] Suba Surianarayanan, T. Santhanam, "Security Issues and Control Mechanisms in Cloud", International Conference, 2012, pp 74-76, ISBN: 97 8-1-4673-4416-6 /12.
[12] Eystein Mathisen, "Security Challenges and Solutions in Cloud Computing", International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 31 May -3 June 2011, Daejeon, Korea, pp 208-212, ISBN: 978-1-4577-0872-5.
[13] Somesh P. Badhel, Prof. Vikrant Chole, "A Review on Data Backup Techniques for Cloud Computing", International Journal of Computer Science and Mobile Computing (IJCSMC), Volume: 03, Issue: 12 | December 2014.
[14] https://thesai.org/Downloads/Volume12No7/Paper_92-A_Systematic_Literature_Review_of_the_Types_of_Authentication.pdf (Accessed on 20 February 2023)
[15] https://onlinelibrary.wiley.com/ "VMBackup: an efficient framework for online virtual machine image backup and recovery," Concurrency and Computation: Practice and Experience, vol. 28.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY