YOUNG RESEARCHER
ISSN: 2277-7911Impact Factor: 5.077 (SJIF 2021)
Peer-Reviewed, Refereed, Indexed Journal
Volume - 12, Issue - II, Apr-May-June 2023

AN EXAMINATION OF THE SAFETY OF CLOUD COMPUTING

Mrs. Varsha Mangesh Kiranpure[1] & Dr. Shabnam Sharma[2]

[1]*Ph.D. Research Scholar, Department of Computer Science and Engineering, Shri J.J.T. University, Rajasthan, India*

[2]*Professor & Research Guide, Department of Computer Science and Engineering, Shri J.J.T. University, Rajasthan, India*

Corresponding Author : Mrs. Varsha Mangesh Kiranpure

DOI - 10.5281/zenodo.10039353

ABSTRACT:

The term "cloud computing" refers to a kind of technology that stores data and applications via the use of a centralised distant server that is connected to the internet. Users are able to save money and save expenses by employing cloud computing since they no longer have to invest in their own computer gear and software. However, cloud computing is still plagued by a number of security problems, including concerns about users' privacy, the possibility of data loss or theft, and so on. Users are worried about a number of security risks with cloud services, including confidentiality, integrity, availability, privacy, and threats. This article discusses a selection of the problems and the available remedies for them.

Keywords: Cloud computing, Security.

INTRODUCTION:

The current trend in computing is known as cloud computing, and it involves delivering a flexible facility or services via the use of the cloud. Cloud computing is a kind of on-demand computing service that provides users with the ability to store and access their data through the internet [1]. Cloud computing may be defined as the combination of technology, the availability of storage space, and a hosting platform, all of which can be located on the internet [2-4]. In terms of marketing, it offers services without the end user having any awareness about the actual location at which the services are being offered and the configuration of those services. It gives you a platform in the cloud that you can use to expand your capacity and capabilities without having to worry about investing in new infrastructure, training new IT employees, or licencing new software. It provides consumers and companies the ability to access their data whenever and wherever they want and does not need the installation of any software; however, accessing it does require an internet connection. The primary aims of cloud computing [3] include scalability, cost-effective computing infrastructures that are available on demand, and high quality service levels. The use of cloud computing does, however, raise a number of concerns with regard to data security. These concerns include privacy breaches, data loss, and data theft. Although there are a large number of businesses in the current market that develop and offer cloud computing services and commodities, the vast majority of those businesses are still unaware of the implications of storing, processing, and accessing data in a location that is enormously shared and virtualized [4]. As a consequence of this, users are unable to understand how the service provider monitors their information or, more importantly, where their information is stored. As a consequence of this, a great number of questions, such as "Why do I want to trust the third party? ", will arise. and "Does the site provide a safe environment for the storage of the data information?" As a consequence of this, there are some customers who are unwilling to use cloud services despite the fact that doing so would bring them a great deal of benefit. When in fact, security is the most significant challenge that cloud-based developers have neglected to include into their products and services. As the cloud computing sector of the information technology (IT) business continues to see explosive growth, the importance of the security challenges cloud providers and clients confront has grown. In addition, despite the availability of very inexpensive technologies that are capable of managing security concerns, there are still some developers who are unable to provide the highest possible level of security in their offerings. This results in the cloud services being provided suffering from a few different vulnerabilities, such as the fact that it is simple for it to be attacked by attackers who want to obtain a free computing service, the fact that information can be stolen from cloud users, and the fact that the infrastructure can be penetrated through cloud connections. There are a few factors that have been taken into consideration, one of which is that the corporation would lose control over the data since it hosts its assets by employing outsourced security management provided by a third party [5]. Another problem is that there are no security assurances included in the Service Level Agreements (SLAs) that are made between customers and service providers [6]. As a result, cloud service providers are obligated to guarantee the safety of their infrastructures and to safeguard the data and applications of their customers. Customers are obligated to verify the security measures used by service providers to safeguard their data.

LITERATURE REVIEW:

Type of services:

Each of the cloud services is supported by its own service provider. Service providers are businesses that make available to individuals or businesses some aspects of cloud computing [7]. The concept of cloud computing may be broken down into three distinct layers. Infrastructure as a Service (IaaS) is the first layer that allows users to borrow the process, capacity, and various other essential computing assets in order to install and run arbitrary software programmes, such as operating systems and applications. Users can borrow these resources from the service provider. The Platform as a Service (PaaS) layer is the second layer, and it provides users with a platform on which they may develop and execute their applications. The third tier of the cloud service paradigm is known as software as a service (SaaS for short). It is a fully functional piece of software that can be accessed and used in a variety of ways, including via a web browser on a variety of different devices. When compared to the conventional service, it is simpler to use since the customer does not need to download and install anything on their own computer. The models for deploying clouds have branched out into many distinct forms, including public, private, hybrid, and community clouds respectively. A public cloud is a cloud that is owned by an entity that provides cloud services and is made available to the general public. Any subscriber is able to access data stored in a public cloud. It operates on a pay-per-use approach and offers a lower level of security when compared to other cloud services. A private cloud is a cloud service that is used by a single company and may either be hosted inside or externally. Users are allowed to share and utilise the virtual application and resources that are offered. Because it is founded on the idea of functionality found inside an intranet, it is more secure. The term "hybrid cloud" refers to a cloud that is created by combining two or more cloud types, such as public cloud and private cloud, in such a way that they are connected and advertise the advantages of several deployment strategies. The data and applications stored in hybrid clouds may be controlled more securely, and they are accessible to a wider variety of users. Because of its open design, it can connect with a variety of different management systems. Community cloud is a kind of cloud computing that is shared among a small number of companies and is often hosted off-site.

Technologies:

Because cloud computing is comprised of many different technologies, including virtualizations, databases, transactions, networks, load balancing, operating systems, resource scheduling, memory management, and concurrency control, it raises a great deal of problems about data safety [8]. The cloud computing environment presents a number of challenges to the security of the aforementioned technologies and systems. For instance, cloud computing has given rise to a significant number of new security challenges, most of which relate virtualization. Additionally, networks need to be maintained safe in order for cloud-based systems to be able to communicate with one another. In addition, the process of mapping the physical machines to the virtual machines must be carried out in a safe manner. Aside from that, data security places a strong emphasis on data encryption, and it also makes certain that appropriate standards are implemented for data sharing. In addition, memory management and resource allocation algorithms need to be in a safe state, and methodologies for data mining need to be appropriate to the identification of malware in cloud environments. Clients, data centres, and distributed servers make up the many parts that make up cloud computing. Mobile devices, thin clients, and thick clients are the three categories that fall under the umbrella term "client." Thin clients are the most common kind of client because they are inexpensive, have fewer potential vulnerabilities, and have a lower risk of failing or losing data. The components of a data centre are known as servers, and they are responsible for storing both data and software. Cloud providers benefit from more choices and security flexibility because to distributed servers. The security threats model consists of two different sorts of categories, which are external threats and internal risks. DoS attacks, DDoS attacks, port scanning, IP spoofing, DNS poisoning, phishing attacks, and packet sniffing are all examples of external threats. When a user is subjected to an internal attack, the attacker poses as an authorised user in order to get access to the user's resources. In addition to this, there are nine different kinds of dangers associated with cloud computing. These dangers include alterations to the business model, improper use of cloud computing, malicious insiders, insecure API interfaces, multi-tenancy environments, data theft, service hijacking, risk profiling, and identity theft. End-to-end encryption and a trust management system are potential solutions to the problem of changes to the delivery of IT services. Abuse of cloud computing may be prevented by the use of appropriate validation and verification, as well as strengthened authentication. The problem of unsecured API interfaces may be remedied by putting in place an appropriate security model and access control mechanism. To mitigate the danger posed by a dishonest employee on the inside, openness and control are necessary. In IaaS, SLA patching is an essential component for assisting with shared technological problems. A loss of control over the data should be minimised by ensuring the data's integrity, backing up the data, and other such safeguards. Theft of identity, service hijacking, and risk profiling are all problems that may be overcome with the implementation of security rules, monitoring and alerting systems, and robust authentication, in that order.

Cloud Security Architecture:

The cloud security architecture will only be able to successfully protect the cloud services from danger if and only if the appropriate preventative measures are carried out in the appropriate locations. Cloud security controls serve as a protective barrier against the shortcomings of cloud computing and cut down on the damage caused by attacks. In a roundabout way, this restriction contributes to the reduction of assaults on cloud computing. Controls may be broken down into four categories: preventative controls, detective controls, corrective controls, and deterrent controls. The use of security controls in cloud services results in an increased degree of data protection. In addition, while discussing the safety of data, there are a few security standards that need to be taken into consideration in order to avoid any kind of assault on cloud computing services. Control over data accessing by various parties is required as a security need in cloud computing. This is done to limit the likelihood that the data would be misused in any way. Security requirements include data availability, data confidentiality, data privacy, and data integrity. The term "availability" refers to the condition in which users have access to the infrastructure, software, and data at any time and from any location [9]. Users are granted the ability to access the cloud in order to get data, services, or infrastructure while they are connected to the internet. A strategy known as redundancy is used in cloud computing since that environment holds several copies of data that is identical to one another [10]. It speeds up the searching process and brings the system closer to full functionality. Following that, maintaining one's privacy and keeping one's secrets is essential [11]. The information pertaining to the user shall never be divulged to any unapproved third party. The data retrieval system is only accessible to those who have been given proper authorization. Encryption of the data should be applied as soon as possible in order to improve the level of secrecy. Homomorphic Cryptography carried out on a text that was previously encrypted [12]. The data that is being kept in the cloud may be stored at any place in the globe, but it is required to comply with the privacy and confidentiality rules of the nation in where the server is physically situated.

METHODS:

According to [13], security concerns have grown more essential in cloud computing as more and more individuals have their sensitive data stored in the cloud due to the fact that it can be accessed easily from almost any location and at any time of the day or night. As a result, a cloud service provider has to ensure that the information of their customers is safe and protected from any threats, such as the theft of information or the loss of information, both of which may result in devastating financial losses. Data security concerns, privacy issues, application security issues, threat security difficulties, and threat security issues were some of the security issues and challenges highlighted by cloud computing. Theft of data is by far the most prevalent kind of breach in cloud computing security. Concerns have been raised about the level of data security provided by cloud computing services, particularly in relation to sensitive data. Any anyone who has access to the Internet may get any data that is stored in a cloud at any time. This is despite the fact that material stored in a cloud may be shared, private, or sensitive. As a consequence of this, a large number of users as well as the providers of cloud services have access to these data and are also able to change them. Therefore, with cloud computing, it is necessary to take measures to ensure the integrity of the data. In cloud computing, where there must be two user levels—the cloud service provider level and the customer level—the fact that certain cloud service providers don't have their own servers contributes to the security problems that might arise. This is not simply the reason why data can be stolen. While service providers are responsible for ensuring that all servers are protected from any external hazards, customers are responsible for being aware of any instances of data loss or interference that may occur. For reasons relating to customers' right to privacy, cloud service providers are obligated to protect their customers' personally identifiable information and data from being accessed by other users, customers, and cloud service providers. The user who accesses the data stored in the cloud must be authenticated to ensure that they are among the proper individuals, and only authorised users may get the correct admission to the data [14]. The cloud service provider must also be verified. When it comes to application problems, it is the responsibility of the cloud service provider to monitor and maintain the application. This is done to ensure that the application is safe and does not contain any malicious code that could compromise, modify, or steal your data that is stored in the cloud. This means that service providers should have full access to their servers, since this would assist prevent any unauthorised users from uploading an infected programme into the cloud, which would have a negative impact on the cloud service as well as the data of consumers. There are nine threats that should be concerned in order to prevent the threat issues from occurring, which include information breaches, information loss, account capturing, uncertain APIs, Denial of Service, malicious insiders, mishandling of cloud service, inadequately due diligence, and shared technologies issue [15]. These threats include information breaches, information loss, account capturing, uncertain APIs, Denial of Service, and malicious insiders. The failure of the hardware was the primary factor that led to the loss of information, while human error was the secondary one. According to 16], some security concerns include privacy, availability, confidentiality, and integrity. Attacks are another concern. The security of sensitive data is still an open question since it is possible for it to get corrupted after being uploaded to the cloud. It is possible for unanticipated incidents to take place, such as a loss of control over IT services and insider threats or assaults. A few of the most important aspects of security in SaaS, PaaS, and IaaS are taken into consideration. These aspects include data security, data confidentiality, authentication, authorization, and others. When it comes to PaaS, cloud providers are responsible for the extent of security below the application level. There is a risk of hackers doing extensive black box testing as they attack the system. IaaS will use virtual computers in order to store applications and sensitive data in a cloud environment. There are many different types of security breaches that might occur, such as denial of service (DoS) attacks, authentication breaches, side channel breaches, man-in-the-middle cryptography assaults, and network security breaches.

According to [17], there are seven different kinds of assaults, and they are as follows: a zombie attack, a service injection attack, a virtualization attack, a man-in-the-middle attack, a metadata spoofing attack, a phishing attack, and a backdoor channel attack. The zombie assault disrupts both the availability and the behaviour of the cloud. Enhanced authentication, authorisation, and IDS/IPS protection are potential solutions to the problem. An attack that involves service injection may be fought against by utilising service integrity checking and maintaining a high level of isolation between VMs. Virtualization attacks may be carried out by using VM Escape and rootkits in hypervisors. Handling virtualization may be accomplished with the assistance of IDS, IPS, and firewall. The data sent between two parties may be accessed via a man-in-the-middle attack. It is advisable to protect against the attack by testing both the SSL settings and the data transmission. The Web Services Description Language (WSDL) file of the service is often modified or changed when a spoofing attack is carried out. Customers should maintain a kind of information that is encrypted in order to circumvent it. Strong authentication helps protect against phishing and other forms of attack that use backdoors.

According to the information presented in [18], deterrent controls are the measures that assist in lowering the number of assaults made against cloud computing. The attacker will get a warning from the deterrent controls, informing them that they will be held responsible for the repercussions if they continue with their assault. This option will lower the danger level, and it will also display a warning message to the potential attacker on the fence. The controls that are referred to as preventive controls are the controls that lessen the vulnerability of the system by fortifying it against an occurrence that may occur in the case that the control is unable to totally eradicate the vulnerability. Strong authentication is one of the strategies that may be used to limit the likelihood of an attacker gaining unauthorised access to sensitive data while simultaneously ensuring that users are positively recognised. This approach is one of many that can be used. The third kind of control is the detective controls, which are designed to respond appropriately when an event happens. The detective controls will identify and respond to the assaults, and then they will alert the preventive controls or corrective controls so that they may take the right actions to fix the problem. At the moment, intrusion detection and prevention mechanisms are put into place in order to identify assaults that have been made against the cloud system. Last but not least, we have corrective controls, which are controls that take over actions to limit the harm and impact that an event has on the system. Restoring the system backup is one of the steps that must be completed in order to implement remedial measures once an event has occurred. The efficiency with which the cloud system's architecture and security are protected will be impacted as a result of these measures.

The security implications of cloud computing are a topic that has received attention from a number of academics and are a source of worry. The discussion is on the many use case situations and associated needs that may possibly occur in the cloud computing architecture. The customers, developers, and security engineers are all involved in the consideration of use cases [19]. According to a different piece of study conducted by ENISA, the vulnerabilities and repercussions are the hazards that are associated with the adoption of cloud computing [20], and this causes consumers a great deal of anxiety. The study report looks at a variety of different potential threats to security. The "Top Threats to Cloud Computing" are reviewed and best practises are offered by cloud providers, customers, and security vendors [21], which are similar efforts to those of the CSA.

DISCUSSIONS:

Users of cloud computing are given the ability to choose the data and applications to which they have access inside the cloud. Cloud storage is made available to users, allowing them to save information and make use of the available computer resources. This, in turn, helps businesses and entrepreneurs reduce the costs associated with the purchase of hardware and other equipment. The use of cloud computing allows for flexibility to be provided on demand across a network. It is not dependent on either location or hardware, and resources may be used simultaneously by a large number of users. In addition, it offers consumers maintenance, dependability, and security. How do you choose cloud service providers? Users are afforded the ease of acquiring the same software on all of their devices at the same time thanks to SaaS. In the SaaS arrangement, it has the least amount of power. PaaS provides its subscribers with access to the underlying components and the ability to run programmes via the use of the internet. Users are able to outsource their storage and resources when using IaaS. In order to increase the level of security offered by cloud computing, a number of different approaches and best practises have been investigated. To begin, a cloud service provider has to routinely assess the invulnerability of their cloud service. Additionally, the cloud ought to be consistently maintained and updated in order to restrict the obtainable access point and to reduce the risk that might allow a hacker to attack your business. Second, the customer should always choose a reputable cloud service provider, such as Google, Microsoft, or IBM. The user should give careful consideration before selecting a cloud service since different cloud service providers have different strategies for managing the data and information stored in the cloud. In addition to that, all of the information that is stored in the cloud has to have a strong encryption applied to it in order to increase the level of data security. The information stored in the cloud is inaccessible to anybody who does not have permission to see it; thus, the supplier of cloud services must ensure that the user has access to the data they are storing. Aside from that, the user is responsible for making contact with the service provider before using it, and the user should have a clear understanding of the security state of the data stored on the cloud. The data of the user should always be backed up by the cloud service provider in order to ensure that in the event that accidental data loss occurs, the provider will be able to immediately restore the user's data. Users who save their data in the cloud must verify themselves not just with a login and password but also by providing digital data. Using a single login to access a multitude of apps and services while also providing robust authentication is what single sign-on, or SSO, does for users. Virtual Private Networks (VPNs), Virtual Local Area Network (VLAN) Segmentation, Authentication, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS) are some of the security defences that may be added (IDS). Within the network architecture, active/active clustering, dynamic server load balancing, and ISP load balancing are some of the ways that availability in the cloud may be achieved. Tools for data loss prevention (DLP), also known as data privacy, and cloud service providers (CSP), also known as data integrity, are both options that may be used. Isolating and analysing the activity of other network segments is how Virtual Machine Protection does its tasks.

CONCLUSION:

In the realm of technology, cloud computing is rapidly gaining in popularity. People are inclined to keep their data on the cloud since it is easy for them to access their data whenever they want and wherever they are as long as they have internet connectivity. However, concerns about privacy and safety are increasingly becoming a burden for service providers. Both the cloud service provider and the client should make sure that the cloud they use is safe from any outside threats and that no other parties may use the cloud without permission in order to have a robust and mutual understanding between the two of them. It is essential for service providers to investigate further defensive strategies in order to cut down on the number of security problems that occur. There is a significant gap between the practise of cloud security and the research that is conducted on it. The cause of this gap is because the research makes assumptions that ignore several very important distinctions between virtual machine security and real cloud security. Research ought to be the vehicle for bridging these disparities. One layer of the framework may be able to assist in the development of a solution to monitor the administration of cloud software, while another framework layer may be able to assist in the resolution of the problem of private processing for an individual customer's application. In order to provide integrated security, it is necessary to provide integration as well as conjunction with other security controls located on various tiers. The security of cloud computing should be able to adapt to changing conditions by responding to the requirements of many stakeholders. It is recommended that multi-tenancy protection be provided, with the user being permitted to examine only his or her own security settings.

REFERENCES:

[1]. Griffith E. (2015). What is cloud computing? [Online]. Available: http://sea.pcmag.com/networking-communicationssoftware/2919/feature/what-is-cloud-computing

[2]. Lamba, Harjit Singh, and Gurdev Singh. "Cloud Computing Future Framework for e-management of NGO's." arXiv preprint arXiv:1107.3217 (2011).

[3]. Singh, Gurdev, Shanu Sood, and Amit Sharma. "CM-measurement facets for cloud performance." International Journal of Computer Applications 23, no. 3 (2011): 37-42.

[4]. Schaper, Joachim. "Cloud Services." In Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on, pp. 91-91. IEEE, 2010.

[5]. Mathkunti, Nivedita M. "Cloud Computing: Security Issues." International Journal of Computer and Communication Engineering 3, no. 4 (2014): 259.

[6]. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[7]. Ashraf, Imran. "An overview of service models of cloud computing." International Journal of Multidisciplinary and Current Research 2, no. 1 (2014): 779-783.

[8]. Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security Issues for Cloud Computing." International Journal of Information Security and Privacy 4, no. 2 (2010): 36-48.

[9]. Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. "A survey on security issues and solutions at different layers of Cloud computing." The journal of supercomputing 63, no. 2 (2013): 561-592.

[10]. Singh, Saurabh, Young-Sik Jeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions." Journal of Network and Computer Applications 75 (2016): 200-222.

[11]. Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." arXiv preprint arXiv:1609.01107 (2016).

[12]. Arora, Rachna, Anshu Parashar, and Cloud Computing Is

Transforming. "Secure user data in cloud computing using encryption algorithms." International journal of engineering research and applications 3, no. 4 (2013): 1922-1926.

[13]. An, Y. Z., Z. F. Zaaba, and N. F. Samsudin. "Reviews on security issues and challenges in cloud computing." In IOP Conference Series: Materials Science and Engineering, vol. 160, no. 1, p. 012106. IOP Publishing, 2016.

[14]. Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." Optimizing information security and advancing privacy assurance: new technologies: new technologies 150 (2012).

[15]. Kandias, Miltiadis, Nikos Virvilis, and Dimitris Gritzalis. "The insider threat in cloud computing." In International Workshop on Critical Information Infrastructures Security, pp. 93-103. Springer, Berlin, Heidelberg, 2011.

[16]. Basishtha, S., Boruah, S. “Cloud computing and its security aspects.” International Journal of Research in Engineering and Technology. (2013): vol 2(2), 62-67.

[17]. Kashif Munir and Sellapan Palaniappan. “Security threats/attacks present in cloud environment.” International Journal of Computer Science and Network Security, (2012): 12(12), 107.

[18]. Mahesh B. “Data Security and Security Controls in Cloud Computing.” International Journal of Advances in Electronics and Computer Science, (2016): 11-13.

[19]. Inukollu, Venkata Narasimha, Sailaja Arsi, and Srinivasa Rao Ravuri. "Security issues associated with big data in cloud computing." International Journal of Network Security & Its Applications 6, no. 3 (2014): 45.

[20]. Stojmenovic, Ivan, and Sheng Wen. "The fog computing paradigm: Scenarios and security issues." In Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on, pp. 1-8. IEEE, 2014.

[21]. Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications 6, no. 1 (2014): 25.

[22]. Zanoon, N. “Toward Cloud Computing: Security and Performance”. International Journal on Cloud Computing: Services and Architecture, (2015): 5(5/6), 17-26