SECURITY PARAMETERS IN CLOUD COMPUTING

Mr.K.Janardhan[1]., Mr.J.Sravani[2]
1,2 Assistant Professor, Department Of CSE.,
(✉kondar15@gmail.Com, ✉jsravani6566@gmail.Com)
1,2 Malla Reddy College Of Engineering For Women., Maisammaguda., Medchal., Ts, India

ABSTRACT:

The term "cloud computing" refers to a relatively new computing paradigm that transforms traditional IT and computer solutions into more conventional utilities such as public water and power. Understanding the security dangers and determining the proper security measures utilized to minimize them in Cloud Computing is the primary goal of this study. One of the biggest problems with Cloud Computing is how to keep user data safe while it's being stored and processed.

INTRODUCTION:

Akin to utility-based systems like those used for delivering electricity, water, and sewage, cloud computing makes it possible to access a shared pool of configurable computing resources and computing outsourcing mechanisms that make it possible to deliver a variety of computing services to a wide range of end users. Due to the use of middleware, cloud computing may operate independently of the user's computer's operating system and hardware. Consequently, with cloud computing, application services continue regardless of the functionality of the underlying operating system or hardware. Organizations may unquestionably benefit from cloud computing various features. Cloud computing is characterized by a number of defining characteristics, including but not limited to: virtualization; on-demand services; rapid adaptability; widespread network access; resource groups; and metered service. The cloud has several advantages for businesses and consumers alike. In addition to cost savings, outsourcing methods, resource sharing, accessibility 24/7, scalability on demand, and service versatility, clouds also provide other advantages. By hiding the complexity of things like software updates, licensing, and maintenance from end users, clouds save the time and effort required on their part. A further potential benefit of cloud computing is increased safety in comparison to locally hosted server setups. Unlike conventional businesses, which may only have access to a network administrator who isn't well knowledgeable in cyber security concerns, cloud providers may afford to hire skilled security experts due to the pooling of resources. For the same reasons that they are more resistant to other types of assaults, clouds are able to withstand Distributed Denial of Service (Dodos) attacks better than traditional data centres. As a kind of mobile computing, the cloud enables Virtual Machines

(VMs) to move from one physical system to another. Mobile computations assist prevent circumstances where a single administrator has sole control over the calculation, which may be particularly problematic during focused Dodos assaults. Concerns about Cloud Computing Safety: In cloud computing, there are a lot of concerns about data privacy and security. Cloud computing raises security concerns since any service provider may accidentally or intentionally erase data at any moment. Secure and private data storage in the cloud is shown in Fig. 1.

Figure 1: Cloud computing commitment to data privacy and security it is predicted that the cloud would include security features including encryption techniques, strict access control, and reliable backups for user data. However, consumers are now able to access computational power that is otherwise out of their grasp thanks to the cloud.

LITERATURE REVIEW:

With the probabilistic public key cryptography algorithm, Syam Kumar et al. (2020) have presented a safe and efficient method of securing personal information while it is stored in the cloud and accessed by mobile devices with low resources. Files that have been encrypted in the cloud may be retrieved with the use of an implicit keyword search. For this method, data efficiency is prioritized above data privacy. Data security and cloud privacy is an active topic of experimentation and study, as described by Sheikh Rizwana et al. (2019). Concerns about data loss and privacy must be given top priority by businesses considering a shift to the cloud. When it comes to security, not all data is created equal. We offer a classification method in which the parameters are established using many criteria. Two very efficient and provably secure PDP for safe cloud storage have been proposed by Agenise et al. (2018). The suggested models have been determined to have little server overhead. These models are optimized to decrease the number of times a file block is accessed, the amount of server-side processing required, and the amount of data sent between clients and servers. In order to address data availability concerns in a commodity-based, geographically dispersed edge cloud system, Jonathan et al. (2017) suggested a model. To ascertain a node's trustworthiness, the idea of dependability factor is used. Tasks are assigned to a group of nodes that together achieve a predetermined dependability target. KekeGai et al. (2017) considers the feasibility of implementing solutions for challenges involving massive data sets in the cloud. A dynamic data encryption (D2ES) strategy was created to improve the efficiency of privacy protection. The D2ES model, designed for the encryption of dynamically alternative data packets under varying time restrictions, is the primary model supported by the DED algorithm. The primary goal of this strategy is to provide the highest possible level of privacy protection while still meeting the necessary runtime constraints.

SERVICE MODELS OF CLOUD COMPUTING:

1. **Software as a Service (SaaS):** IaaS is a model, where the cloud provider hosts the infrastructure components traditionally present in the on-premises data center. The components include servers, storage, networking hardware, and the virtualization or hypervisor layer. The IaaS provider offers a range of services to the users to use those infrastructure components. The users can access these resources and services through a wide area network (WAN), such as the internet. These services are increasingly policy-driven, enabling IaaS users to implement greater levels of automation and orchestration for important infrastructure tasks

2. **Platform as a Service (PaaS):** PaaS is a cloud computing model, where a third-party provider delivers hardware and software tools. These tools are needed for the application development by the users and are provided over the internet. PaaS frees its users from the burden of having to install an in-house hardware or software component needed to run a new application.

3. **Infrastructure as a Service (IaaS):** SaaS is a software distribution model where a third-party provider hosts applications and makes them available to customers over the Internet. SaaS removes the need for organizations

to install software on their own computers or in their own data centers. It eliminates the software licensing, installation and support of the needed software. This service also eradicates the expense of hardware acquisition, provisioning, and maintenance of these software and applications.

NEED FOR DATA SECURITY AND DATA AVAILABILITY:

In recent years, there has been a rise in the number of people using cloud computing for data storage. Through the internet and cloud computing, users all over the world are linked together. The proliferation of users and the degree to which they are linked together has raised the possibility of leaks and assaults occurring by accident. On addition, the user's data that is stored in the cloud is located somewhere else than at their physical location. When information leaves a secure area, it may no longer be protected by the precautions put in place by the CSP or the user. Because of this, businesses or individual users of cloud storage need to take precautions beyond what is supplied by providers to ensure the safety of their data. As a result of using cloud storage, the user's data is no longer their own. This means the user has to have confidence that his information will be restored.

DATA SECURITY:

The cloud provider's data might be attacked from inside or outside in a variety of ways. As a result, measures must be taken to protect user information from such threats. Any of the third party, user, or Cloud Service Provider might take responsibility for data security (CSP). The third party uses a Third Party Auditor (TPA) to check the data at regular intervals to ensure its accuracy. The user must take many safety measures to ensure the data remains intact if he or she is responsible for doing integrity checks. The user's actions include encrypting the information and putting away the encrypted version. Similarly, the CSP or server does certain checks to ensure the truthfulness of the information.

DATA AVAILABILITY:

The notion of redundancy has been extensively employed to increase the likelihood of data availability, and it may be implemented safely. Security is baked in with the redundancy it provides. Information about the redundant copies and where they are kept is encrypted using a secret sharing method. The primary focus has been on ensuring the safety of data availability. The suggested approach can also safeguard the backups from a wide range of threats. Software for Personal Computers - Compare the Compare paradigm employs the idea of compression to minimize the memory space needed by a user and guarantee data availability. Information is encrypted for safety purposes and then saved as the original. A second duplicate of the encrypted data is compressed without compromising its integrity. Compare is a middleware component used for data compression and decompression. After strict authentication criteria are fulfilled, the component compresses the data. A second, compressed copy may be kept in yet another cloud service. Even if one cloud service fails, data may be accessed from another. The quantity of copies created should reflect the importance of the information being copied.

RESULTS AND ANALYSIS:

Reviewing the SLR and Survey findings makes up the Reporting review. Here, we detail the security issues discovered by SLR and the countermeasures put in place to deal with them. We also provide details on the people who took the survey and the methods used to evaluate their responses. Findings from the SLR: An enormous amount of study has been devoted to Cloud Computing in recent years. Using SLR, we narrowed the field down to 69 articles out of the thousands that have been published in the field since 2001 that were deemed most relevant to the research's aims. This section discusses the SLR process's extracted articles and its subsequent analysis. Recently, researchers have been focusing their attention on distributed computing services like grid computing. There has been a dramatic uptick in study of the emerging computing paradigm known as Cloud Computing during the last decade.

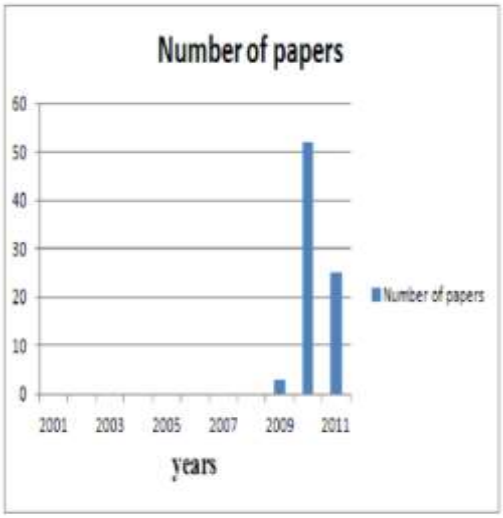

Figure: Number of papers published in year wise

Based on our research, we've found 43 distinct security issues that arose during the SLR. Appendix A provides a more in-depth explanation of these difficulties. The problems that have been found are WS- security, Tampering, repudiation, information disclosure, denial of service, elevation of privilege, IP spoofing, wrapping, injection, phishing, and spoofing. Safety against harm, Wireless LAN protection, Using a frontal assault strategy, To launch a second round of attacks, Attacks such as "Man in the Middle," "Reflection," and "Interleaving" The ability to strike at the right time, Managing data storage resources in a dynamic manner, Keep an eye on the clientele, Inability to trust, Poor Service Level Agreements, low trustworthiness, Auditing, Away from the public eye, Invasion of TCP/IP, As a kind of social engineering, To rummage through garbage cans, Guessing a password, The Trojans, Completeness, Pull the plug on the assault, Fairness, Information disclosure, Computer network assault, Service denial, Security for data and networks, data isolation, data backups, data integrity, and data manipulation are all important.

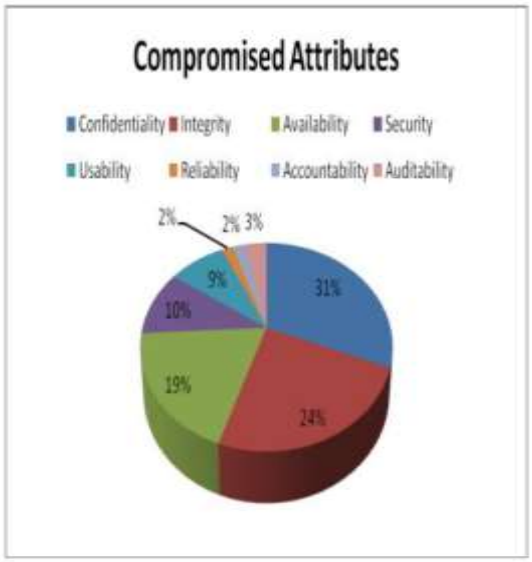

Figure: List of Compromised attributes

Identified Mitigation Techniques:

Thirty-four different SLR-era security measures were uncovered during our research. In Appendix B, we give the specifics of these methods. Some of the topics covered in this synopsis include identity-based authentication, the RSA algorithm, and the dynamic intrusion detection system. TLS Handshake, Public key homomorphism, Third-party auditor, Probabilistic Sampling Method, Duffle-Hellman Key Exchange, and Multi-Tenant Access Control Model. Hidden cameras, facial recognition software, and MACs. Colour coding and watermarking of data, Innovating a new framework for Cloud reliability, Using methods like KP-ABE, RBAC, and ARVTM Proof of irretrievability, Trusted Platform Module, and Security Assertion Mark-up Language Cobol sequence,

fair MPNR procedure, Handout distributed file system, self-cleaning intrusion tolerance, searchable symmetric encryption, and a redundant cluster of separate online data repositories. Access Control Service, Provable Data Possession, Privacy Manager, Time-Bound Tickets for Mutual Authentication, an Intrusion Detection System with SLA. The aforementioned countermeasures have significant effects on Cloud Computing scalability, reliability, availability, privacy, and user control. The identified mitigation strategies enhance Cloud Computing service delivery in a fundamental way. Pictured here in Figure 6.3 is the end outcome.

Figure: Impact of mitigation techniques

CONCLUSION:

The sheer variety of services available in the cloud complicates the task of identifying threats and developing countermeasures. The majority of respondents to the study agreed that Cloud Computing will come to dominate and even grow information commerce. As a result of its adaptable nature, it allows users to exercise complete command over the services and data available to them, regardless of their current location. We have found a sufficient number of problems with Cloud Computing and ways to fix them using secondary data analysis and survey research. Security threats and countermeasures in the diverse Cloud Computing service ecosystem must be identified and evaluated with great care. We found a good number of problems and solutions to those problems that are being used now and will be utilized in the future of Cloud Computing by using two different research methodologies (SLR and Survey).

REFERENCES:

1. Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', High Capacity Optical Networks and Enabling technologies (HONET), 19-21 Dec, pp. 190-195.

2. B. lagesse. (Mar.2011) 'Challenges in Securing the Interface between the cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, 106-110.

3. Chang Lung Tsai, Uei –Chin Lin. (Aug 2010) 'Information Security issue of enterprises adopting the application of Cloud Computing', 6th International Conference on Networked Computing and Advanced Information Management (NCM), 645-649

4. Dawei Sun, Guiran Chang. (Sept.2010) 'A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques', Pervasive Computing Signal Processing and Applications, 305-310.

5. Gul I, Rehman A. (June 2011) 'Cloud Computing Security Auditing', 2nd International Conference on next Generation Information Technology (ICNIT), 143- 148

6. Jia Weiwei Zhu, Haojin Cao. (10-15 April, 2011) 'A Secure data service mechanism in mobile Cloud Computing', Computer Communications Wrokshops (INFOCOMWKSHPS), IEEE Conference 2011, 1060 - 1065.

7. Jun-Ho Lee, Min-Woo Park. (feb. 2011) 'Multi level Intrusion Detection System and Log management in Cloud Computing', Advanced Communication Technology (ICACT), 13th International Conference 2011, 552-555.

8. Lishan Kang, Xuejie Zhang. (Nov.2010) 'Identity-Based Authentication in Cloud Storage Sharing', Multimedia Information networking and Security, 851-855.

9. Mathisen, Eystein. (may 31, 2011) 'Security challenges and solutions in Cloud Computing', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference, 208-212

10. Somani U, Lakhani K. (Oct 2010) 'Implementing Digital signature with RSA Encryption algorithm to enhance the data security of Cloud in Cloud Computing', 1st International Conference on Parallel Distributed and Grid Computing , 211-216.