

## **CLOUD COMPUTING AND ITS VARIABLE TECHNIQUES IN OBTAINING DATA SECURITY PARAMETER**

<sup>1</sup>Sd Parveen, Assistant Professor, CSE, parveensyed.sd@gmail.com  
Swarna Bharathi institute of science and technology,  
Khammam

<sup>2</sup>B.Sowjanya, Assistant Professor, CSE(AIML), sowjib.194@gmail.com  
Swarna Bharathi institute of science and technology,  
Khammam

<sup>3</sup>Ameena nasreen, Assistant Professor, CSE(AIML), amena.nasreen.md@gmail.com  
Swarna Bharathi institute of science and technology,  
Khammam

### **ABSTRACT:**

Cloud computing is an emerging technology paradigm that migrates current technological and computing concepts into utility-like solutions similar to electricity and water systems. The main aim of this research is to understand the security threats and identify the appropriate security techniques used to mitigate them in Cloud Computing. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. Keywords: Cloud Computing, Security, Techniques & Challenges.

### **INTRODUCTION:**

Cloud computing provides a centralized pool of configurable computing resources and computing outsourcing mechanisms that enable different computing services to different people in a way similar to utility-based systems such as electricity, water, and sewage. Cloud computing separated the application from the operating system and hardware via middleware. Therefore, for cloud computing, if the operating system or hardware does not work, the application services do not stop. There is no doubt that cloud computing has many advantages that an organization can use. There are some basic features of

cloud computing, such as virtualization, on-demand services, fast flexibility, broad network access, resource group, measured service. Clouds bring out tremendous benefits for both individuals and enterprises. Clouds support economic savings, outsourcing mechanisms, resource sharing, any-where any-time accessibility, on-demand scalability, and service flexibility. Clouds minimize the need for user involvement by masking technical details such as software upgrades, licenses, and maintenance from its customers. Clouds could also offer better security advantages over individual server deployments. Since a cloud aggregates resources, cloud providers charter expert security personnel while typical companies could be limited with a network administrator who might not be well versed in cyber security issues. Similarly, clouds are more resilient to Distributed Denial of Service (DDoS) attacks due to the availability of resources and the elasticity of the architecture. The clouds support mobile computations where Virtual Machines (VMs) migrate from one physical machine to another. In addition to alleviating dedicated DDoS attacks, mobile computations help to avoid settings in which a single administrator has exclusive control over the computation.

**Cloud Computing Security Issues:** There are many issue related to privacy, security in cloud

computing. The security issues are concerned in cloud computing because in cloud at any time the data can outbreak the service provider and the information is deleted deliberately. Fig. 1 shows organization of data security and privacy in cloud computing environment.

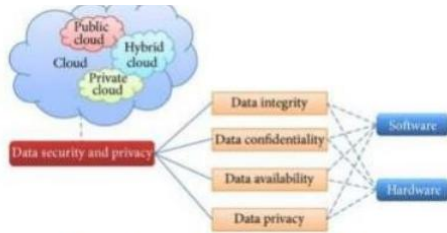


Fig 1 : Data security and privacy in cloud computing

The cloud is expected to offer features such as encryption strategies to ensure a secure data storage environment, rigorous access control, secure and stable backup of user data. However, the cloud allows users to reach computing power that exceeds their physical domain.

## LITERATURE REVIEW:

When it comes to encrypting data and outsourcing it to mobile devices with low resources in the cloud, Syam Kumar et al. (2020) suggested a safe and efficient method called the probabilistic public key cryptography algorithm. An implicit keyword search is enabled in order to retrieve encrypted data from the cloud. An effective data encryption system that does not compromise data privacy is the aim of this technique. The current research and experimental landscape around data security and cloud privacy is outlined by Shaikh Rizwana et al. (2019). When it comes to moving to the cloud, data loss prevention and privacy must be top priorities for organizations. The degree of security needed to preserve various kinds of data differs. The parameters of a suggested classification method are defined in terms of many dimensions. To facilitate safe cloud storage, Ateniese et al. (2018) introduced two PDP that are both very effective and demonstrably secure. There is little server overhead in the suggested models. These approaches aim to minimize client-server connection, processing on the server, and file block visits. Concerning data availability in a geo-distributed edge cloud system constructed with commodity resources, Jonathan et al. (2017) put forth a model. A node's dependability is assessed using the reliability factor

concept. Considering the reliability factor, the jobs are assigned to a group of nodes that achieve a certain reliability target. Practical considerations for implementing the solutions proposed by KekeGai et al. (2017) in the cloud center on issues related to big data sets. A dynamic data encryption (D2ES) method was created to enhance the efficiency of privacy protection. When it comes to encrypting data packets with varying time restrictions, the DED technique is most useful for supporting the D2ES paradigm. Maximizing privacy protection with runtime-specific, selective encryption techniques is the primary goal of this approach.

## 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.

### **CLOUD DEPLOYMENT MODELS:**

The deployment models depict the manner through which the cloud is being used or accessed by the users. The four types of cloud deployment models as identified by NIST is depicted.

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

**Private Cloud:** Private clouds are data centers which are owned by a single company that provides flexible and scalable services to the customers of that particular company. Private cloud does not offer these services to external customers. Here, the customer has some control over their data. Example: Any corporate IT environment today could be considered a private cloud.

**Community Model:** A community cloud model is a multi-tenant platform which allows several companies to work on a same platform when their requirements and concerns are the same. Example: Environments such as a U.S. federal agency cloud with stringent security requirements, or a health and medical cloud with regulatory and policy requirements for privacy matters.

**Public Cloud:** Public clouds are mainly owned and operated by companies that offer rapid access over a public network to affordable computing resources. In public cloud, the whole computing infrastructure is located on the premises of a cloud computing company that offers the cloud service. In public cloud services, users need not purchase the hardware, software or supporting

infrastructure. These infrastructure related components are owned and managed by providers. But the user has no control over the infrastructure. Example: Amazon Elastic Compute Cloud (EC2), International Business Machine (IBM's) Blue Cloud, Sun Cloud, and Google AppEngine.

**Hybrid Model:** A hybrid model is where some applications or servers, based on business needs, run some operations in a public cloud infrastructure like Microsoft Azure or Amazon Web Services (AWS). After moving some operations to public cloud, the organization may want to maintain their own data center for some legacy applications, and use a private cloud for storing the data.

### **DATA AVAILABILITY:**

**Secure redundancy** – One of the most widely used methods to ensure data availability has been through the redundancy concept. Along with providing redundancy, security is encapsulated in to it. The entire details regarding the redundant copies and their storage are secured using a secret sharing algorithm. The main objective has been to guarantee data availability in a secure manner. The proposed model is also able to protect the redundant copies of the data from various attacks.

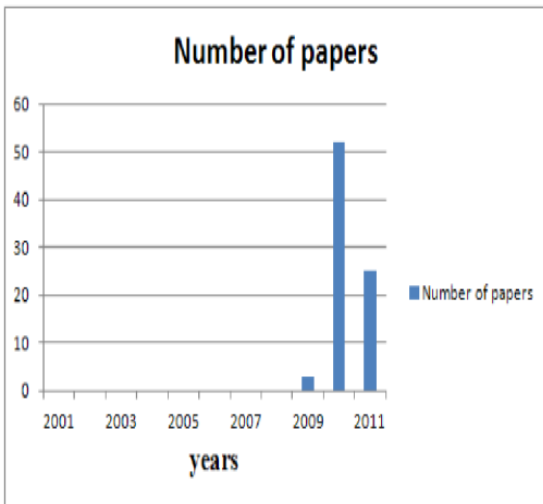
**CompWare** – To optimize the memory space used for a user, and to ensure data availability, the concept of compression is used in the CompWare model. After encrypting the data for security, it is stored as the first copy. The encrypted data is compressed using a lossless technique and stored as a second copy. To compress and de compress the data a middle ware component CompWare is used. The component does the compression after certain authentication parameters are met. The compressed second copy can be stored in another cloud storage. Data can be retrieved from one cloud storage when the other cloud storage fails. Depending on the criticality of the data, number of copies can be made.

### **RESULTS AND ANALYSIS:**

The Reporting review consist the results from SLR and Survey. In this we have reported the identified security challenges and mitigation techniques from SLR also given information about survey participants and explained the

analyzed results from the survey.

**SLR Results:** In recent years, the huge amount of research has been done in the area of Cloud Computing. In the process of SLR, we have extracted 69 papers relevant to meet the goals of the research from the large number of papers published since the year 2001. This section covers the results and analysis of the papers that were extracted in the process of SLR.



In the past years, research is followed the distributed computing and mainly focused on service like grid computing. From the last decade, there is a rapid increase in research on new paradigm Cloud Computing which is the next generation computing.



Figure: List of Compromised attributes

### Identified Mitigation Techniques:

From the analysis, we have identified 34 security techniques during the SLR. The detailed description of these techniques is presented in Appendix B. The summary include Identity based authentication, RSA algorithm, Dynamic

Intrusion detection system, Multi tenancy based access control model, TLS Handshake, Public key homomorphic, Third party auditor, probabilistic sampling technique, Diffie – Hellman key exchange, Private face recognition, MACs, Data coloring and water marking, A novel Cloud dependability model, KP-ABE, RBAC, ARVTM, Security assertion markup language, TPM, Proof of retrievability, Fair MPNR protocol, Sobol sequence, Redundant array of independent Net storages, Hadoop distributed file system, self cleansing intrusion tolerance, searchable symmetric encryption, Provable data possession, Privacy manager, Time bound ticket based mutual authentication scheme, Security Access Control Service, The Service Level Agreement, Intrusion detection system.

The above mentioned mitigation techniques have strong impact on the Performance, Security, Efficiency, QoS, Privacy and Access control of Cloud Computing. The defined mitigation techniques somehow improve the overall services in Cloud Computing environment. The result is shown in figure 6.3.

### Impact of Mitigation Techniques

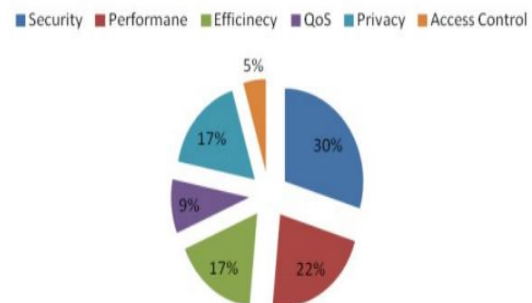


Figure: Impact of mitigation techniques

### CONCLUSION:

The identification of security challenges and mitigation techniques in Cloud Computing is challenged by considering the large number of services. Most of the responses from survey, noted that Cloud Computing will place dominant and expandable information transactions. Because it offers many flexible services, provides easy, individualized and instant access control to the services and information where they are for the users. In the process of identification from the research methods SLR and Survey, we have identified satisfactorily number of challenges and mitigation techniques in current and future Cloud Computing. The identification of security

challenges and mitigation techniques in large number of services of Cloud Computing is a very challenging task. In the process of identification from research methods (SLR and Survey), we had identified a satisfactory number of challenges and mitigation techniques which are being used at present and also in future Cloud Computing.

#### 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.