A REVIEW ON SECURITY ISSUES IN CLOUD COMPUTING

ANCY JERO J R, *Department of Computer Science, Nesamony Memorial Christian College, Marthandam. Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli 627012, TamilNadu, India.* jeroancy96@gmail.com

DR. D.S MISBHA Department of Computer Science and Applications, Nesamony Memorial Christian College, *Marthandam. Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli 627012, TamilNadu* India.,misbhasatheesh4@gmail.com

ABSTRACT— The fact that many enterprise applications, data, and services are shifting to cloud platforms demonstrates how widespread cloud computing technology has become around the world. Security and privacy are two important concerns with cloud computing. Confidentiality, availability, and integrity are all aspects of the phrase security. Security assurance is a key motivator for cloud adoption and deployment. This study will examine major security and privacy challenges as well as potential solutions in the literature. The classification of cloud computing security issues has been investigated. In addition, it analyses many ineffective solutions found in the literature and makes recommendations for establishing a secure, adaptive cloud environment. Furthermore, Cloud Service Providers (CSPs) can solve the afore mentioned challenges to improve security and privacy.

Keywords— Cloud Computing, Security, Privacy, confidentiality, availability, integrity, Cloud Service Providers (CSPs), Framework

I.INTRODUCTION

Cloud computing is quickly becoming a household term, and it has fundamentally transformed the computing environment, communication infrastructures, and networked services [1]. Cloud Computing (CC) is a critical tool for capturing the digital computing paradigm and commercial models for both software and hardware resources [4]. Cloud services are a collection of apps and services that run on cloud infrastructures and can be accessed via a private network or the Internet. A Cloud Service Providers (CSPs) is a company that offers cloud services to customers. Cloud Computing has several important advantages, including on-demand services, charging customers only for the services they use, ease of maintenance, flexibility, and dispersed storage of services [1]. Services on demand, payment for utilized services, easy maintenance, elasticity, distributed storage of services, and so on are some of the fundamental advantages of cloud computing [3]. Service-oriented architecture, virtualization, web 2.0 and other technologies are all part of cloud computing [7].

II. CLOUD COMPUTING OF FRAMEWORK

Cloud security is a subset of computer and network security that uses privacy-enhancing technology and is overseen by a set of policy guidelines to safeguard data, software applications, and other cloud-based services [8]. Users can store data on remote servers and access it from anywhere at any time using cloud computing. Users get access to data through the "Cloud Service Provider." It is necessary to take care of the processing of data stored on remote servers. Data security in cloud computing is a serious worry these days. The data that will be stored on remote data servers is extremely vulnerable and must be controlled carefully. Data security is a major concern since different users can access data from faraway systems. "Cloud Computing" is a model for quick, on-demand access to resources and resource pooling for "Cloud Service Providers" to supply services to customers. The user can choose any resources he requires, such as servers, operating systems, RAM, and so on, and pay solely for those resources. Using virtualization techniques, cloud computing allows users to efficiently access resources. Deployment Models of Cloud.

(i) Private Cloud

Any organization or business can own a private cloud, which is less secure. For example, Window Server 'Hyper-V'. The most significant disadvantage of these setups is the high cost of equipment and utility bills [1]. It also ensures that operational and sensitive data are not accessible to third-party providers.

(ii) Public Cloud

The security threats are heightened because the public cloud is exposed to all users and organisations. The term "Service Level Agreement" (SLA) refers to the licence and trust that exists between the CSP and the customer. Identifying the location of resources in the public cloud is challenging, and the hazards of data security are larger. Example: - Google Sheets. Large companies that provide cloud services, such as Google Apps, Amazon AWS, and Microsoft Office 365, own the public cloud [6,9].

(iii) Hybrid Cloud

The term "hybrid cloud" refers to a cloud that is both public and private. When it comes to accessing data over the Internet, hybrid cloud is more secure than public cloud. For instance, consider cloud bursting for load balancing [6,9]. Due to the presence of two or more cloud providers, a hybrid cloud service can be offered by a private cloud owner forming a partnership with a public cloud owner, making it more complex [1].

III.SERVICES OF CLOUD COMPUTING

Software as a Service (SaaS) provides users with software services based on their needs. Users can use the software services if they have an internet connection and can access the services through a web browser. Platform as a Service (PaaS) refers to the services that end users require in order to solve application-level issues. Infrastructure as a Service (IaaS) is a sort of service that aims to raise a system's performance by increasing memory space or compute capacity [2]. IaaS [Infrastructure as a Service]. The bottom level of the model is IaaS. It covers with hardware, networking, servers, data centres, processors, and memory, among other things. Because some businesses cannot afford to own a server, they can instead rent one from a "Cloud Service Provider".IaaS allows physical management of aggregated resources. Storage or computational capability are used to supply services [6, 12, 13].

IV.CLOUD COMPUTING SECURITY & PRIVACY ISSUES

Cloud computing raises concerns about the security and privacy of data that is outsourced. applications and data that are outsourced to the cloud benefit from its dynamic abstraction and scalability. Have unrestricted security infrastructure and boundaries. Cloud computing infrastructure and services have lately been expedited by cloud providers such as Google, Microsoft, and Amazon to serve a larger number of users [14]. The most important cloud computing security and privacy concerns are data confidentiality, integrity, availability and privacy are all aspects of network and data security in cloud computing.

V.CONCLUSIONS

The cloud has a number of advantages, including lower costs, fewer management obligations, and more organizational efficiency. Cloud service and deployment models were examined in this article. The key security and privacy challenges in cloud computing were also recognized, and solutions were explored in this study. This study discusses the security and privacy concerns associated with cloud computing. Multiple aspects of security are studied in the literature, including data integrity, confidentiality, and availability, as well as remedies. Cloud computing is the most recent IT industry trend. It provides numerous advantages for businesses and organizations. In the future, suitable key management techniques can be utilized to distribute keys across multiple cloud service providers in order to improve data security in cloud computing.

REFERENCES

[1] Awodele, O., A. O. Adebayo, and O. O. Tayo. "Security and privacy issues in cloud computing." *Commun. Appl. Electron* 7.3 (2017).

[2] Abdulsalam, Yunusa Simpa, and Mustapha Hedabou. "Security and Privacy in Cloud Computing: Technical Review." *Future Internet* 14.1 (2021).

[3] Arjun, U., and S. Vinay. "A short review on data security and privacy issues in cloud computing." *2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*. IEEE, 2016.