Chapter 7
Data Controlling and Security Issues in Cloud: A Step Towards Serverless

Anisha Kumari
National Institute of Technology, Rourkela, India

Manoj Kumar Patra
National Institute of Technology, Rourkela, India

Bibhudatta Sahoo
National Institute of Technology, Rourkela, India

ABSTRACT

Cloud computing has been the most demanding technology in the last decade, which several organizations have widely adopted. Most enterprise applications and data are migrated to the public or hybrid cloud due to the ease of access and infrastructure facilities provided by the cloud provider. One significant issue in the cloud environment is the security and data controlling mechanism, which needs to be focused on for better service quality. Users usually hesitate to use public cloud services due to privacy and security concerns about the personal data they want to process online. Unlike standard cloud computing notions, serverless computing does not expose the infrastructure or platforms on which the services operate to the end-user. Clients only have to worry about the application's business logic, and the service provider usually takes care of everything, including configuration, infrastructure provision, servers, etc. In this chapter, the authors have discussed several cloud computing issues regarding data security and data controlling mechanisms.

INTRODUCTION

Computer hardware and software advancements have made cloud computing a major topic in business and academia. Several factors have led to cloud computing, including conventional computer technol-

DOI: 10.4018/978-1-6684-8306-0.ch007

ogy, communication technologies, and business practices (Hashizume, Rosado, Fernandez-Medina, & Fernandez, 2013). It is built on the network and features a consumer-oriented service structure. Scalability and dependability are critical characteristics of a cloud computing system (Gong, Liu, Zhang, Chen, & Gong, 2010; Stieninger & Nedbal, 2014). The location of the computing resource in the cloud computing system is hidden from both the developer and the end user. In a cloud computing system, the customers are allowed to access the application, and their data from any location in the world (Rashid & Chaturvedi, n.d.). Many customers may utilize cloud computing resources at the same time. When the workload increases, the cloud system's capacity may be raised by adding additional hardware to manage it. As a service, cloud resources are made available on a pay-per-use basis. Significantly large quantity of commodity-grade servers are often used to create highly scalable and dependable on-demand services in the cloud systems (Y. C. Lee & Zomaya, 2012). It is possible to raise or reduce the number of resources available to users in a cloud system depending on their needs. The resource can be computing, storage, and other specification services. It has been observed by several information technology sector organizations that cloud computing has a significant influence on the social benefits of IT advancements in the near future (Kuiper, Van Dam, Reiter, & Janssen, 2014). Data centers constructed on servers using various levels of virtualization technology presently make up the vast majority of cloud computing infrastructure (Kumari, Sahoo, Behera, Misra, & Sharma, 2021). It's possible to use the services from anywhere globally, and the cloud serves as a central hub for all of your computing requirements. Using cloud computing has revolutionized the way software is developed. It's possible to store data in the cloud, making it accessible to the user at any time and from any location. Most of the data is saved on a personal computer or similar device. Cloud computing may provide data security without requiring the user to take further steps to safeguard their information. The safety of data kept in the cloud is thus a prerequisite for the use of cloud computing (Deshpande, Sharma, & Peddoju, 2019; Wang, 2011). Cloud computing platforms including Google, IBM, Microsoft, Amazon, VMware, and EMC are offered by a wide range of enterprises (Dikaiakos, Katsaros, Mehra, Pallis, & Vakali,2009). The user's private data is at risk in the cloud computing system; thus, the data must not be deleted or stolen. When hackers know that the user's information is stored on a cloud system, they may pay greater attention to accessing it. When a hacker knows that the user's data is stored on a cloud system, they may pay greater attention to accessing it. Protecting this new system requires a higher level of attention than previously required. The data is kept in the cloud by the business. Those who are not employees of the firm may access the data. The organization must have assurance in cloud computing to keep confidential information in the cloud. Regardless of whether a firewall protects the cloud system, governance and security are essential to cloud computing (Krutz & Vines, 2010). As cloud computing progresses, securing the system is a major concern. Conventional security measures cannot fully protect the cloud system. Cloud computing may rise to a wide range of new security issues with no limits and mobility. These include data privacy, user data security protection, cloud platform reliability, and management of cloud computing.

Serverless computing frees application developers from the burden of maintaining infrastructure (Baldini et al., 2017). The cloud service provider provisioned, scaled, and managed the infrastructure to execute the code using serverless applications. There are several benefits of serverless computing over conventional server-based, or cloud-based technology (Li, Lin, Wang, Ye, & Xu, 2022; Shafiei, Khonsari, & Mousavi, 2019). Serverless architectures appeal to many developers because of their lower costs, increased scalability, and increased adaptability (Castro, Ishakian, Muthusamy, & Slominski, 2019). Developers do not have to worry about procuring, deploying, or maintaining back-end servers with serverless architectures. On the other hand, serverless computing isn't a one-size-fits-all solution for every