Chapter 9
Data Storage and Transmission Security in the Cloud:
The Artificial Intelligence (AI) Edge

Ankita Nayak
KIIT University, India

Atmika Patnaik
King's College, India

Ipseeta Satpathy
KIIT University, India

B. C. M. Patnaik
KIIT University, India

ABSTRACT

Cloud computing has profoundly changed the face of data management for enterprises, providing increased scalability, ease of access, and cost savings. Nonetheless, this change has highlighted the crucial need for strengthened security measures to protect sensitive data from the ever-changing spectrum of cyber threats. Following the cloud's rise as a storehouse for large datasets, the quest for sophisticated security solutions has gained traction. This motivation has resulted in the incorporation of artificial intelligence (AI) into the cloud security architecture. As cloud storage becomes increasingly popular, organizations are becoming more concerned about data security. Sensitive data is transmitted, ranging from messages and images to financial and health information. As technology advances, there is a growing threat to customer data in the cloud, making greater cloud security more important than ever. This study aims to give a comprehensive insight into the role of AI in data storage and transmission security in the cloud.

DOI: 10.4018/979-8-3693-1431-9.ch009

1. INTRODUCTION

We live in the big data age, with organizations producing, collecting, and storing huge amounts of data on a daily basis, ranging from extremely sensitive business or personal customer data is being replaced with less sensitive data, such as behavioral and analytics for marketing. Aside from the growing amount of data that businesses must be able to collect, handle, and analyze, organizations are embracing cloud services. The traditional network barrier is fast eroding, and security teams are realizing that enterprises must reevaluate existing and past methods of cloud data security. With data and apps no longer living in your data center and more workers working far away from a physical office than ever before, Organizations must figure out how to safeguard data and control access to it as it moves across and through various contexts (Ganne, 2022). The three main pillars of data are Data confidentiality, integrity, and availability. These three broad pillars, sometimes known as the CIA triad, define the basic ideas that constitute the foundation of a robust, successful security infrastructure—or any organization's security program. Any type of attack, vulnerability, or other security issue will almost certainly break one (or more) of these principles. This is why security experts employ this approach to assess possible threats to an organization's data assets. Cloud data security safeguards data stored in the cloud (at rest) or going in and out of the cloud (in motion) from security risks such as unauthorized use, fraud, and manipulation. There is usage of physical security, technical instruments, access management and controls, and organizational regulations. Securing cloud data entails developing ways to safeguard important digital assets and information from potential security breaches, inadvertent errors, and hazards posed by personnel inside an organization. This entails using technological tools, established standards, and operational approaches to protect data confidentiality while allowing authorized access in cloud-based environments. The benefits of cloud computing include a variety of benefits such as the ability to retrieve data from any internet-connected device, lowering the risk of data loss during outages or events, and boosting scalability and agility. At the same time, many organizations are still hesitant to shift sensitive data to the cloud because they are unsure of their security alternatives and how to fulfill legal requirements. (Kumar,2019; Wagh,2020). Cloud security, also known as cloud computing security, is a collection of security precautions designed to protect cloud-based apps, infrastructure, and data. User and device identification, data and resource access control, and data privacy are among the precautions. They also help with regulatory data accuracy. Cloud security is applied in cloud settings to protect a company's data against DDoS attacks, viruses, hackers, and unauthorized access or consumption. There are three main types of cloud environments as mentioned in figure 1 below (Agarwal,2019);