Chapter 6
Cloud Security Protocols for Protecting Carbon Monitoring Systems

Pawan Kumar Goel
https://orcid.org/0000-0003-3601-102X
Raj Kumar Goel Institute of Technology, India

Satya Prakash Yadav
https://orcid.org/0000-0002-2634-5600
Madan Mohan Malaviya University of Technology, Gorakhpur, India

ABSTRACT

Carbon monitoring systems are crucial for mitigating climate change and promoting environmental sustainability. To protect their integrity and security, cloud security protocols are essential. Challenges in ensuring data privacy, reliability, and availability include data breaches, unauthorized access, and system vulnerabilities. A novel security framework based on advanced encryption techniques and distributed trust models is proposed for cloud-based carbon monitoring systems. This approach is the first to integrate such a comprehensive solution for this domain. Results show significant improvements in data protection, reducing cyberattack risk while maintaining efficiency. The proposed framework offers higher security with minimal impact on system performance, making it an innovative contribution to cloud security for environmental monitoring.

DOI: 10.4018/979-8-3373-2091-5.ch006

INTRODUCTION

The increasing severity of climate change has necessitated the deployment of robust carbon monitoring systems to track greenhouse gas (GHG) emissions and evaluate environmental policies. These systems play a pivotal role in supporting sustainability initiatives and regulatory frameworks, as they provide real-time data on carbon footprints from various sources, including industries, transportation, and energy sectors (Smith et al., 2023). Governments and environmental agencies worldwide rely on these monitoring mechanisms to develop strategies that mitigate climate change by reducing emissions and promoting carbon sequestration (Wang & Li, 2022). The integration of advanced technologies such as the Internet of Things (IoT), big data analytics, and artificial intelligence (AI) has further enhanced the efficiency and accuracy of carbon monitoring systems (Brown et al., 2024). However, as these systems increasingly depend on cloud computing for data storage, processing, and sharing, their security becomes a critical concern (Zhang et al., 2023).

Cloud computing has revolutionized carbon monitoring by enabling large-scale data aggregation, real-time analytics, and seamless information exchange among stakeholders. The scalability and computational power of cloud-based platforms make them ideal for processing vast amounts of environmental data (Gupta et al., 2023). However, these benefits come with significant security challenges, including data breaches, unauthorized access, and cyberattacks targeting sensitive environmental information (Nguyen et al., 2022). Without adequate security measures, malicious actors can manipulate carbon data, leading to inaccurate emissions reporting and potential environmental policy failures (Patel & Singh, 2023). Therefore, it is essential to establish stringent cloud security protocols that ensure data confidentiality, integrity, and availability in carbon monitoring systems (Lee et al., 2024).

Cloud security protocols are essential for protecting carbon monitoring systems, which are critical for tracking and managing greenhouse gas emissions. These systems often handle sensitive environmental data, and their integrity, confidentiality, and availability must be safeguarded. Below are key cloud security protocols and best practices tailored for protecting carbon monitoring systems:

1.1. Data Encryption

- In Transit: Use TLS (Transport Layer Security) or SSL (Secure Sockets Layer) to encrypt data transmitted between the carbon monitoring system and cloud services.
- At Rest: Implement AES (Advanced Encryption Standard) or similar encryption protocols to protect stored data in cloud databases or storage systems.