Chapter 7
Blockchain-Based Security for Cloud Data Storage

Mamoon M. Saeed
https://orcid.org/0000-0002-6081-2559
University of Modern Sciences, Yemen

Zeinab E. Ahmed
https://orcid.org/0000-0002-6144-8533
University of Gezira, Sudan

Rania A. Mokhtar
https://orcid.org/0000-0001-9221-4214
Sudan University of Science and Technology, Sudan

Rashid A. Saeed
https://orcid.org/0000-0002-9872-081X
Sudan University of Science and Technology, Sudan

ABSTRACT

Blockchain technology has shown promise to improve security across several industries, including cloud data storage. The integration of blockchain technology with safe cloud data storage solutions is examined in this chapter. Data integrity, secrecy, and authentication in cloud storage systems can be greatly enhanced by utilizing the decentralized and immutable nature of blockchain. Important ideas about cloud data security are covered, including distributed consensus, smart contracts, and cryptographic hashing. The chapter also explores the difficulties, advantages, and potential avenues for future research in applying blockchain technology to improve cloud data storage security.

DOI: 10.4018/979-8-3693-9984-2.ch007

1. INTRODUCTION

The combination of blockchain technology and cloud data storage is a shining example of innovation in the ever-evolving field of data protection and storage, with the potential to revolutionize how businesses safeguard and handle their priceless information assets. This chapter delves deeply into the transformative potential of this combination in strengthening data security settings by thoroughly examining the synergies between blockchain and cloud storage. The traditional ideas of data security are being redefined as contemporary businesses struggle with the exponential development of data quantities and the necessity of protecting sensitive information against a changing threat landscape.

A key component of contemporary data management systems, cloud storage solutions provide cost-effectiveness, scalability, and flexibility. However, typical cloud storage models' centralized structure has highlighted weaknesses such as data breaches, illegal access, and the possibility of data tampering (Idrus et al., 2023). Given this, blockchain technology stands out as a disruptive force that provides an immutable, transparent, and decentralized architecture for cloud data security.

Blockchain has the potential to completely transform data security paradigms by utilizing distributed consensus mechanisms, smart contracts, and cryptographic approaches to guarantee data integrity, confidentiality, and auditability in cloud storage ecosystems. This academic collection's chapters are carefully written to negotiate the complex relationships between blockchain technology and the security of cloud data storage. This chapter explores the subtleties of blockchain-based security mechanisms designed to handle the particular difficulties presented by cloud storage systems through a combination of theoretical discussion, real-world case studies, and practical insights. This will help them move toward a future in which data security is not only a compliance requirement but also a strategic imperative that is woven into the very fabric of organizational resilience and trust (M. M. A. Saeed et al., 2024).

This chapter investigates how blockchain technology might improve cloud data storage systems' security protocols. Exploring their integration seeks to clarify how blockchain properties like immutability, decentralization, and cryptographic hashing might strengthen data integrity, secrecy, and authentication in cloud storage systems. The chapter provides an in-depth examination of blockchain-based security solutions to shed light on the advantages, difficulties, and potential applications of blockchain technology to protect cloud data.