A Comprehensive Review on Attribute-Based Encryption Techniques for Securing Healthcare Data in Cloud Environments

P.Karthik
Research Scholar, Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh, India

Dr. D.Latha
Associate Professor, Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh, India

Abstract

With the rapid growth of cloud-based healthcare systems, ensuring data confidentiality, access control, and patient privacy has become a major research priority. Attribute-Based Encryption (ABE) has emerged as a flexible and fine-grained cryptographic solution that enables secure data sharing based on user attributes. This paper reviews seven recent research contributions focusing on various ABE schemes—including Ciphertext-Policy (CP-ABE), Key-Policy (KP-ABE), and traceable or verifiable extensions—applied to secure Electronic Health Records (EHR) and medical data in cloud settings. The reviewed studies highlight improvements in policy expression, revocation, outsourced decryption, and computational efficiency. The paper concludes that modern ABE variants offer a promising trade-off between strong security and practical performance, making them suitable for next-generation healthcare data protection. This paper is an extended continuation of our previous review work published in 2023, focusing on recent developments in Attribute-Based Encryption (ABE) techniques (2023–2025) for securing healthcare data in cloud environments.[1]

Keywords

Cloud Security, Attribute-Based Encryption, Electronic Health Records, Access Control, Healthcare Data Privacy.