Chapter 15
Predictive Analysis-Based AI-Driven Data Security Authentication and Authorization for Medical Warehousing Mechanisms

G. A. Senthil
https://orcid.org/0000-0001-7442-5499
Agni College of Technology, India

R. Prabha
Sri Sairam Institute of Technology, India

ABSTRACT

Maintaining data security is important for several reasons, as it shields patients, first and foremost, from fraud, identity theft, and prejudice due to their medical history. This paper presents a comprehensive framework for enhancing data security authentication and authorization within medical warehousing mechanisms in the context of e-commerce, leveraging predictive analysis, artificial intelligence (AI), and blockchain technology. In an era where the integrity and confidentiality of medical data are paramount, the proposed framework integrates advanced predictive analysis models and AI-driven authentication mechanisms with the immutable nature of blockchain to ensure robust security measures. The proposed solution presents an innovative approach to enhance data security authentication and authorization within medical warehousing mechanisms, leveraging predictive analysis and AI algorithms within the context of e-commerce-enabled blockchain. Specifically, the study focuses on employing Naive Bayes, LSTM, and XGBoost for predictive analysis

DOI: 10.4018/979-8-3693-5718-7.ch015

to fortify security measures.

1. INTRODUCTION

Due to the delicate nature of the data held, called Protected Health Information (PHI), privacy protection in medical warehousing is crucial. This includes medical history, prescriptions, diagnosis, and treatment data. Robust data security procedures are necessary to protect PHI from loss, abuse, and unauthorized access. Patients may seek care honestly and freely without anxiety about exploitation because they understand that confidentiality is maintained when their information is protected. Second, it's critical to preserve patient and healthcare provider trust (Singh, A. K et.al., 2024). This confidence can be damaged by a data breach, which may discourage people from seeking critical medical attention or disclosing important information. Adhering to rules like HIPAA is more than about staying out of legal problems; it's also about maintaining moral principles and safeguarding the rights of patients. PHI security breaches can have a negative financial and reputational impact on the firm by entailing significant penalties and legal ramifications. Healthcare firms suffer large financial losses as a result of data breaches.

This study presents a novel approach to strengthening the integrity of medical data repositories inside a blockchain architecture supporting e-commerce. The system creates robust permission, authentication, and data protection by utilizing blockchain technology and artificial intelligence (AI). Predictive analytics, in which AI systems examine user activity and access patterns to anticipate and counteract possible security attacks, is a crucial component of this strategy. Additionally, AI-driven authentication techniques like voice or facial recognition enhance standard password systems for an increasingly secure login procedure. By using blockchain technology, medical data is stored in an unchangeable manner, protecting data integrity and improving traceability. Unauthorized data manipulation is discouraged by decentralized ledger systems, strengthening patient confidentiality and privacy. Autonomous smart contracts enable authorization management. Smart contracts, self-governing programs integrated into the blockchain that allow for exact authority over access to information based on specified criteria and user responsibilities, make authorization management easier. The advantages of this strategy include improved patient privacy through impermeable information retention on the blockchain, as well as increased data security made possible by AI-driven threat detection and sophisticated authentication procedures. Smart contract-managed authorization processes that are streamlined add to the growing confidence in e-commerce transactions containing medical data. In general, the goal of this research is to address the growing need for strong data security in medical warehousing, particularly in

Key Performance Indicators for the Organized Farm Products Retailing in India

Rajwinder Singh, Ajit Pal Singhand Bhimaraya A. Metri (2017). *Business Analytics and Cyber Security Management in Organizations (pp. 256-269).*
www.irma-international.org/chapter/key-performance-indicators-for-the-organized-farm-products-retailing-in-india/171852