Mathematical Analysis of Adaptive Cryptographic Communication & Cat-Boost Based Intrusion Detection in IOV

R. Anitha Jyothi
Department of Mathematics & Statistics, VFSTR Deemed to be University, Vadlamudi, Guntur, India

P. Siva Prasad
Department of CSE, SOCI VFSTR Deemed to be University, Vadlamudi, Guntur, India

Abstract

Advanced technologies such as cloud computing, IoT, IoV, and machine learning generate massive amounts of data that require secure and efficient processing. The Internet of Vehicles (IoV) enables communication between vehicles and roadside infrastructure but remains vulnerable to attacks due to its decentralized architecture. Malicious vehicles and false data injection can significantly affect network reliability and traffic safety.

To address these challenges, this paper proposes a secure IoV communication framework based on trust management and hybrid encryption. The proposed system combines RSA for authentication and secure key exchange with AES for fast data encryption. In addition, a CatBoost-based Intrusion Detection System (IDS) is implemented using the UNSW NB15 dataset to identify malicious activities in the network. Experimental results demonstrate that the proposed model achieves an accuracy of 93.57%, providing secure, reliable, and low-latency communication for IoV environments.

Keywords

IoV, Hybrid Encryption, RSA, AES, CatBoost, Intrusion Detection System, Cybersecurity, Machine Learning.