**LITERATURE REVIEW-**

**UPI FRAUD DETECTION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sl. No. | Title, Year, Author | Methodology | Pros | Cons |
| 1. | S. Sharma et al., "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions," 2023 | - Supervised Machine Learning  - Logistic Regression and Random Forest algorithms for fraud detection  - Features engineered from transaction data | High fraud detection accuracy  - Customizable for different scenarios  - Fast processing for large datasets  - Easy to interpret the results  - Handles structured data well | - Dependence on labeled data  - Data imbalance may affect performance  - Poor handling of unstructured data |
| 2. | P. Kumar et al., "UPI-Based Financial Fraud Detection Using Deep Learning Approach," 2023 | - Deep Neural Networks  - Multi-layer perceptron with ReLU activation functions  - Utilizes transaction metadata and user behavior patterns | - Effective at detecting complex fraud patterns  - Handles unstructured data  - Adapts to evolving tactics  - High scalability for large datasets | - High computational requirements  - Requires extensive data preprocessing  - Risk of overfitting with insufficient data |
| 3. | K. Dubey et al., "AI-Driven Secure UPI Transactions Using Federated Learning," 2023 | - Federated Learning  - Data remains decentralized for privacy preservation  - Collaborative model training across multiple devices | - Preserves data privacy  - Eliminates the need for raw data sharing  - Reduces risk of data breaches  - Decentralized approach ensures flexibility | - Complex coordination of models  - High latency in updates  - Requires robust infrastructure for implementation |
| 4. | A. Patel et al., "Fraud Fighters: AI and ML Revolutionizing UPI Security," 2023 | - AI/ML Security Frameworks  - Real-time fraud detection with anomaly detection algorithms  - Adaptive learning for new fraud patterns | - Real-time fraud detection  - Scalable and robust  - Reduces human intervention  - Improves response time to dynamic threats | - Costly to implement  - Ethical concerns with AI use  - Challenges in interpreting complex AI decisions |
| 5. | R. Menon et al., "Blockchain-Based Secure Frameworks for UPI," 2023 | - Blockchain Integration  - Uses smart contracts for transaction validation  - Cryptographic techniques ensure data integrity | - Prevents tampering  - Ensures traceability  - Provides transparency and accountability  - Audit trail for compliance | - High implementation cost  - Scalability challenges with high transaction volumes  - Higher latency in processing blockchain transactions |
| 6. | M. Chaudhary et al., "Hybrid Models for UPI Fraud Detection," 2022 | - Hybrid AI models combining machine learning and rule-based systems  - Statistical techniques for anomaly detection combined with ML for predictions | -Combines strengths of statistical and machine learning models  - Reduces false negatives  - Adapts to new fraud types easily  - Flexible rule-updating | - Higher computational cost compared to standalone models  - Complexity in managing hybrid frameworks  - Requires continuous updating of rules |
| 7. | B. Singh et al., "Real-Time Fraud Detection in UPI Transactions Using Ensemble Learning," 2021 | - Ensemble Learning methods (Random Forest + Gradient Boosting)  - Real-time feature extraction from transactional data | - High accuracy through ensemble methods  - Robust to noise and outliers in data  - Handles both structured and semi-structured data  - Faster processing with optimized algorithms | - Dependence on high-quality data  - Higher computational complexity  - Requires tuning of hyperparameters for optimal results |