Elliptic Curve Cryptography and Machine Learning for Secure E-Commerce Transactions

1. Introduction

In today's worldwide environment, e-commerce has fundamentally transformed how people conduct business. Customers now have unprecedented access and convenience because to the proliferation of online platforms that allows them to explore and purchase a wide range of goods and services from the comfort of their own homes. This shift in consumer behavior has altered traditional marketplaces, providing customers with more options and allowing them to make informed purchasing decisions. E-commerce, often known as electronic commerce, refers to the process of buying and selling goods and services online. E-commerce platforms offer various advantages, including a faster purchasing procedure, reduced costs, and more freedom for customers, the ability to compare items and prices, faster response to market and customer demands, and additional payment choices. The increasing load has rendered digital transactions more vulnerable to fraud, giving criminals a profitable avenue to generate money. For both enterprises and individuals, digital transactions pose a significant barrier to secure financial and commercial interactions. Credit card fraud and compromised account information are two common e-commerce security threats.

Many factors contribute to these security issues. Keeping private data unencrypted in any database is the most difficult. Because insiders are responsible for the bulk of bridges, security concerns continue even when sensitive data is encrypted. Because of the Internet's scattered and dynamic nature, anti-fraud measures are required to ensure the integrity of online transactions. Existing transaction fraud detection approaches seek for aberrant user behavior and have gaps that limit their usefulness in dealing with potential security issues. Another major issue discovered in present transaction fraud detection systems is inadequate process control throughout the transaction. Credit card fraud and unauthorized account access are both e-commerce security concerns. A variety of variables contribute to security concerns with online transactions. The first concern is the storage of private data in any database without encryption.

The second issue is that insiders are accountable for the majority of data breaches, even when personal information is stored encrypted. As financial transactions become more sophisticated and complex, there is a greater need for enhanced procedures to avoid risks and fraud. Predetermined criteria and prior patterns have long been the foundation of fraud detection systems in the financial sector. Despite their relative efficacy, these technologies may be unable to keep up with scammers' constantly shifting techniques. The quick development of new types of fraud often outpaces traditional methods. If risk assessment methods rely on static data and are unable to correctly predict prospective financial threats, organizations may also be exposed to potential risks. In order to overcome these constraints, we suggest a secure e-commerce transaction system based on machine learning and elliptic curve cryptography.

1.1 Research aim & scope

The primary goal of this project is to improve e-commerce transaction security by combining machine learning methods with elliptic curve cryptography (ECC). This framework is intended to offer strong, effective, and flexible e-commerce transaction security that guarantees data integrity, confidentiality, and defense against online threats.

1.2 Research objectives

The fundamental goal of this study is to develop an elliptic curve cryptography solution for machine learning-based e-commerce transactions in order to increase the effectiveness of privacy-preserving and secure online transactions. The primary goal of this research is described below,

- To use data preprocessing to address unbalancing concerns and enhances the quality of e-commerce transaction data.
- To discover more precise fraud patterns by extracting the behavior pattern from transaction records.
- To choose the most crucial characteristics by using cutting-edge feature selection methods that raises the effectiveness and precision of fraud detection.

- To increase the security of online transactions by implementing an improved cryptographic encryption system that ensures data integrity and secrecy.
- To create a machine learning-based fraud detection model that optimizes feature selection and hyperparameters to increase classification accuracy and decrease false positives.

2. Problem statement

2.1 Specific problem statement

Reference 1

Title: "An Improved LSTM-Based Failure Classification Model for Financial Companies Using Natural Language Processing"

Concept

In this paper, provide an ideal LSTM model. Machine learning techniques are used to categorize the error content in statistics data in order to determine the error condition of the current failed transaction. They gathered 11,865 replies from different financial institutions and suppliers to compile a dataset, which they then classified using an LSTM classification model.

Problem defined

- Nevertheless, the quality of the data and the accuracy of the annotations have a significant impact on the model's efficacy. An unbalanced sample distribution in the payment information detection task can lead to decreased forecasting accuracy for models with fewer variables and the requirement for specific strategies to correct the imbalance in the data. Inaccurate annotations or noise in the training dataset can also affect the model's accuracy.

Solution

- In order to overcome this constraint, we suggest using the "Synthetic Minority Over-sapling technique (SMOTE) algorithm" in conjunction with Z-score normalization to balance and normalize the data distribution.

Reference 2

Title: "A Multi-perspective Fraud Detection Method for Multi-Participant E-commerce Transactions."

Concept

This paper proposes a novel fraud detection method that combines machine learning and process mining models to follow user behavior in real-time. They begin by developing a process model that incorporates user behavior detection for the B2C e-commerce platform. Second, a method for analyzing anomalies to extract important features from event logs is explained. The collected features are then fed into a classification model that employs "Support Vector Machines (SVM)" to detect fraudulent behavior.

Problem defined

- Nevertheless, the accuracy of fraud detection is impacted by the research's limitations in feature extraction of fraudulent activity patterns.

Solution

- By using a Convolutional Autoencoder (CAE) method for feature extraction in conjunction with Deep Feature Synthesis (DFS), it enhances detection accuracy by extracting significant behavior patterns.

Reference 3

Title: "Online Payment Fraud Detection Model Using Machine Learning Techniques"

Concept

This work presents a novel "ResNeXt-embedded Gated Recurrent Unit (GRU) model (RXT)" for real-time financial fraud detection. The technique aims to increase security

against online threats in wireless communication settings, manage massive volumes of data from financial transactions, and lessen data imbalance. The model seeks to greatly increase fraud detection accuracy and computing performance over current approaches by utilizing deep learning and optimization techniques.

Problem defined

- Despite the fact that "Principal Component Analysis (PCA)" is a helpful technique for feature selection, its linear structure may lead to the incorrect elimination of certain crucial traits. This linear feature is a drawback that might have an impact on the model's overall performance.

Solution

- To overcome this constraint, the most pertinent and significant characteristics are chosen using the Information Gain approach in conjunction with Oppositional Cat Swarm Optimization.

Reference 4

Title: "Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain"

Concept

This work suggests safe transaction architecture suitable for MEC-enabled e-commerce consortium blockchain in order to enhance the security of user privacy data and transaction data while guaranteeing system transaction processing performance. To prevent user privacy information from leaking, the model protects transaction data and user privacy data using the lightweight Paillier encryption technique. Additionally, it presents the Shamir secret sharing protocol to maximize the security of the leader election phase and improve the anti-Byzantine failure capabilities of the Raft consensus method.

Problem defined

- Nevertheless, as the lightweight Paillier encryption method employed in this work is still less effective, a more secure and effective privacy protection technique is required to guarantee the security and privacy of MEC e-commerce transactions.

Solution

- To improve the security and effectiveness of safe online transactions, the **Evo-Hybrid ElGamal–ECC–IDEA Cryptosystem** algorithm is a very powerful encryption technique.

Reference 5

Title: "E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining"

Concept

The study's goals are to identify e-commerce fraud, employ big data mining (BDM) to mitigate the financial risks of e-commerce companies, look into more effective solutions utilizing "information fusion technology (IFT)," and create an e-commerce "fraud detection model (FDM)" based on "IFT (computer technology (CT), artificial intelligence (AI), and data mining (DM)." Meanwhile, BDM technology, "logistic regression model (LRM), support vector machine (SVM)," and the proposed IFT-based FDM are used to extensively investigate e-commerce fraud problems.

Problem defined

- Nevertheless, considering the diversity of e-commerce fraud, all aspects of technology must be improved in order to reliably detect fraudulent users and confirm the effectiveness of the model.

Solution

- To get over this limitation, we provide **BBO-Boosted Regression Model (BBO-BRM)**, which combines Brown-Bear Optimization (BBO), Logistic Regression, and Gradient Boosting to increase fraud detection accuracy. Logistic regression

produces a trustworthy classification model, whereas gradient boosting improves prediction performance. By fine-tuning the features and optimizing our model parameters greedily, BBO enables us to raise the probability of fraud detection across a range of commodity finds in the e-commerce industry.

2.2 Overall problem statement

It is still difficult to achieve data quality, feature extraction, model accuracy, and security in modern e-commerce fraud detection. Although a lot of models depend on accurately labeled data, their effectiveness is compromised by things like uneven distributions, noisy data, and inaccurate labels.

- **Data Integrity and Noisy Concerns:** Present-day fraud detection techniques rely on the quality of data and the tags that go along with it. The model's capabilities are diminished by issues including imbalanced data distribution, noisy data, and improper tagging. Conventional methods like cost-sensitive learning and oversampling are useful, but they frequently encourage biased or overfitting predictions. Improving fraud detection performance requires addressing such data challenges.
- **Feature Extraction Limitations in Fraud Detection:** Several studies utilize pre-established rules, as well as manual feature selection, to identify fraudulent patterns. The challenges of adapting to changing fraud strategies result in obsolescence, and therefore, less than effective fraud detection. The limited ability to develop complicated behavior features further diminishes the ability to detect fraud, but demonstrates the need for fraud detection systems that can automatically and adaptively extract features.
- **PCA Constraints in Features Selection:** The PCA is often used as a method to minimize dimensionality in fraud detection. PCA's use of linear transformations, which lose the capacity to describe important nonlinear characteristics, is a drawback. Consequently, the model's ability to identify intricate fraudulent activity may deteriorate. Therefore, further methods are needed in the feature selection process to enhance the nonlinear feature selection.

- **MEC E-Commerce's Security and Privacy Issues:** Although lightweight Paillier encryption, a variation of Paillier encryption, has been used to secure privacy in MEC-based e-commerce transactions, it is not the best option for real-time transaction facilitation due to its performance issues. We concluded that a more complex encryption technique was needed to boost security and computing efficiency given the increased expectation of security.
- **Accuracy and Verification of Fraud Detection Models challenges:** Due to the complexity and diversity of fraud, it is difficult to verify these models. Current procedures might be misused or misclassified and find it difficult to adapt to the new fraud pattern. To improve the accuracy and reliability of fraud detection, more resilience and flexibility are necessary.

3. Proposed methodology

This study combines machine learning (ML)-based fraud detection with elliptic curve cryptography (ECC) to improve the security and accuracy of e-commerce transactions. Data collection and preprocessing, feature extraction, feature selection, safe transaction encryption, and ML-based fraud detection are the five main phases of the suggested technique.

- Transaction Data Preparation
- Transaction Pattern Analysis
- Optimal Attribute Selection
- ECC-Based Secure Encryption
- ML-based Fraud Classification

A. Transaction Data Preparation

In this study, we first create a reliable fraud detection system using the "E-Commerce dataset". The preprocessing stage is essential for enhancing data quality, resolving class imbalance, and lowering noise in order to guarantee optimal model performance.

- **Insufficient significance:** Missing data affects how reliable fraud detection methods are. Consequently, we employ suitable imputation techniques to

eliminate incomplete records and fill in missing values that could lead to dataset inconsistencies.

- **Embedding classified factors:** We must use encoding techniques since the e-commerce data contains categorical properties including transaction types, payment types, and client geographies. Categorical data can be converted into a machine-readable format using label encoding.
- **Data standardization:** To guarantee that numerical characteristics are constant and that scale variations don't affect the model's performance, we apply Z-score normalization. This kind of numerical column normalization standardizes all features and improves the model's capacity to learn.
- **Balanced classes allocation:** To improve the effectiveness of algorithms used to identify fraud, the "Synthetic Minority Over-Sampling Technique (SMOTE)" is used to create synthetic samples of cases in the minority class.

B. Transaction Pattern Analysis

In order to identify legitimate behavioural patterns for identifying fraud in e-commerce transactions, we carry out the feature-extraction stage after the data has been pre-processed. In order to enhance abstract features, this study will integrate **Deep Feature Synthesis with Convolutional Autoencoder** (**DeepSynth-CAE**). In order to determine the relationships between those transactional qualities, DeepSynth automatically creates features from low-level transactional attributes retroactively. These features are then utilized to find pertinent trends observed in fraudulent circumstances. While learning hidden representations that enable the detection process to distinguish between authentic and fraudulent transactions, CAE simultaneously reduces dimensions without losing crucial information. Together, the retrieved characteristics improve the overall accuracy and resilience of the fraud detection model by being more organized and informative.

C. Optimal Attribute Selection

Following feature extraction, we clean and optimize the dataset for fraud detection by doing feature selection. In this study, we assess each feature's utility based on its capacity to

distinguish between transactions that are fraudulent and those that are not using the Information Gain method (IGT). We suggest an **Oppositional Cat Swarm Optimization (OCSO)** algorithm to improve the performance of the Information Gain technique-based feature selection. With the help of exploration and exploitation of cat swam optimization, the proposed approach finds the most relevant feature.

D. ECC-Based Secure Encryption

In order to improve the encryption scheme's efficiency and raise the transaction system's overall performance and security, we present a hybrid **Evo-Hybrid ElGamal–ECC–IDEA Cryptosystem** method in this study. Using evolutionary optimization, ElGamal encryption, and Elliptic Curve Cryptography (ECC), a low latency key is generated. The International Data Encryption Algorithm (IDEA) is a symmetric key block cipher that is extremely resistant to differential and linear cryptanalysis. This algorithm is used as part of the entire encryption system to improve security; that is, it protects transaction data from more powerful cryptographic attacks. In addition to genetically improving key selection, we can also genetically optimize the key-selection process by defining and then selecting the optimum key parameters. In this scenario, genetic optimization will be geared toward decreasing the encryption period and optimizing efficiency.

E. ML-based Fraud Classification

Finally, we have presented **BBO-Boosted Regression Model (BBO-BRM)**, a unique machine learning-based fraud detection system that integrates **Brown-Bear Optimization (BBO), Logistic Regression,** and **Gradient Boosting** to improve the model's overall efficiency and detection performance. Gradient Boosting is an ensemble technique that effectively detects tiny signs of fraud in a large number of e-commerce transactions by iteratively building weak classifiers. A dependable classification model that guarantees resilience and interpretability in the decision-making process is logistic regression. In order for the model to reduce computational resources and reflect evolving fraud behaviors, BBO must be introduced for the optimization of both feature selection and hyperparameters. The **BBO-Boosted Regression Model (BBO-BRM)** method's hybrid techniques increase fraud

detection accuracy over false positives and establish a methodical foundation for protecting online transactions against fraud and theft. The following displays the proposed method's performance metrics:

- Number of epochs vs. Accuracy (%)
- Number of epochs vs. Precision (%)
- Number of epochs vs. Recall (%)
- Number of epochs vs. F1-score (%)
- False positive rate (FPR) vs. True positive rate (TPR)

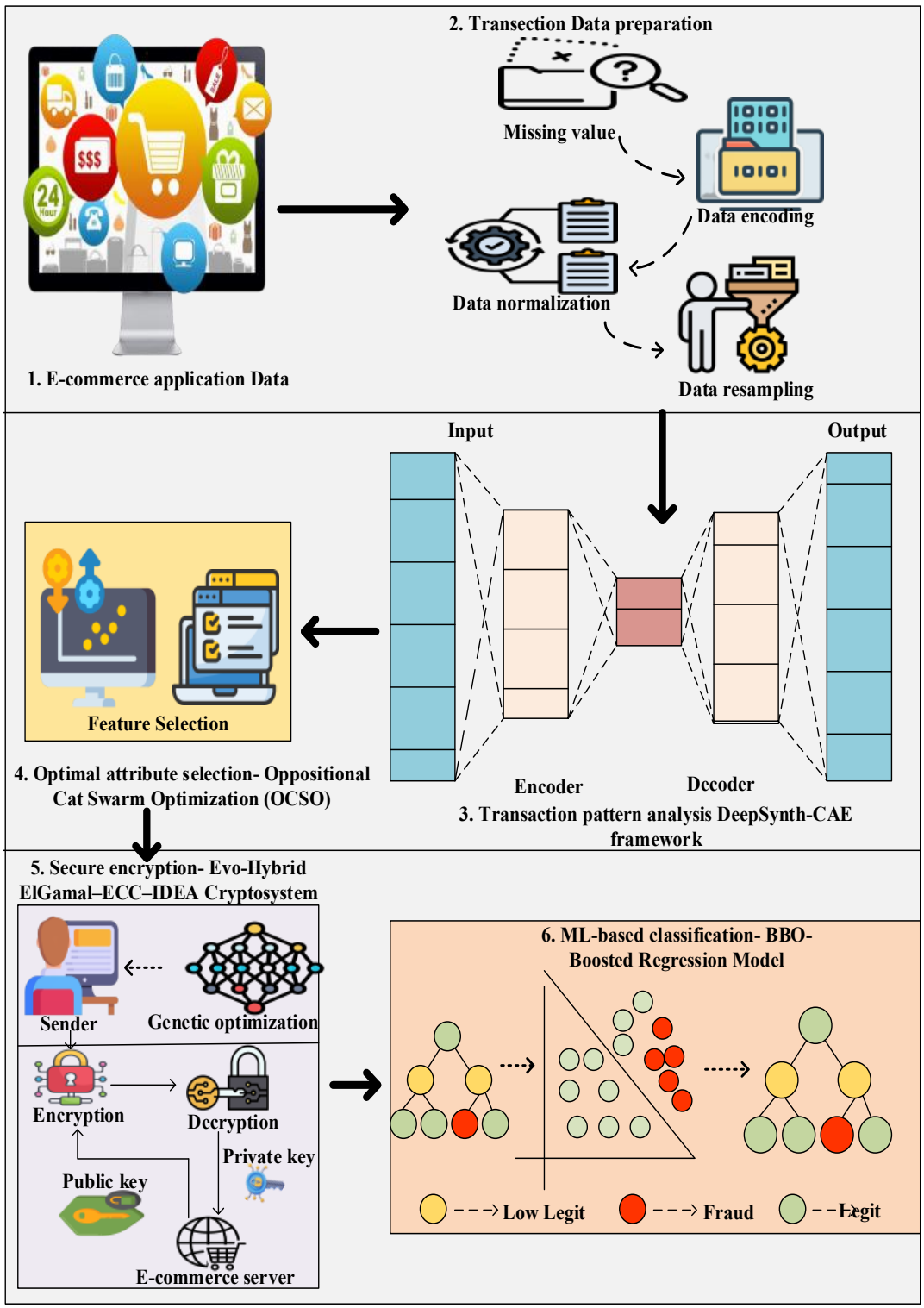

Fig.1 Overall architecture of the proposed method

Research highlights

- We used SMOTE and Z-score normalization to standardize the numerical features in order to attain class distribution balance and ensure high consistency with the model results.
- Relevant high-level features are extracted using **Deep Feature Synthesis and Convolutional Autoencoder (DeepSynth-CAE)**, which successfully captures intricate fraud patterns.
- To reduce model complexity and increase efficiency, just the most important elements are chosen using Information Gain and Oppositional Cat Swarm Optimization (OCSO).
- The use of **Evo-Hybrid ElGamal–ECC–IDEA** Cryptosystem strengthens secure transaction encryption to preserve data confidentiality, integrity, and resilience to cyber-attacks.
- The **BBO-Boosted Regression Model (BBO-BRM)** is the fraud detection method that maximizes classification accuracy while reducing false positives.

Reference 6

Title: "Applying Detection Leakage on Hybrid Cryptography to Secure Transaction Information in E-Commerce Apps"

Concept

The security of online transactions is crucial as electronic commerce grows rapidly, particularly to protect critical business data. They offer a hybrid cryptographic protocol that combines "Data Leakage Detection (DLD)" and "Fernet (FER) algorithm, ElGamal (ELG) encryption" to assist allay this worry. In contrast to other techniques, the FER algorithm's AES-128 encryption and HMAC authentication provide symmetrical, quick, and safe encryption of transaction data. ElGamal encryption guarantees that encryption keys are shielded from unwanted access while enabling a safe public-key cryptographic key exchange.

Limitation

- The proposed hybrid cryptographic protocol would require a significant amount of processing power, making it inappropriate for low-power devices or resource-constrained systems and limiting its potential for scalability in decentralized or edge-based e-commerce environments.

Reference 7

Title: "E-commerce payment model using blockchain."

Concept

This article proposes a simple payment architecture that uses basic cryptographic features like public key, private key and digital signature to eliminate the need for transaction intermediaries like public key certificates and PG. This method allows for the processing of e-commerce payments without requiring the registration of additional public keys, private keys, or public key certificates. By ensuring the nonrepudiation and integrity of electronic payments, the use of a digital signature not only eliminates expenses for intermediaries like PG but also reduces the overall cost of operating e-commerce services.

Limitation

- Nevertheless, using blockchains can result in excessive congestion and processing time.

Reference 8

Title: "ARS-Chain: A Blockchain-Based Anonymous Reputation-Sharing Framework for E-Commerce Platforms"

Concept

Describe ARS-Chain, a novel and safe blockchain-based system for anonymous reputation-sharing on e-commerce websites. Linkable ring signatures (LRS), a cutting-edge method to provide user anonymity in the face of trust uncertainty, are used to construct ARS-Chain. Crucially, LRS provides an extra functionality to support a higher level of anonymity by dynamically adding numerous rings based on a user's purchase list.

Limitation

- Anonymous reputation systems have important ethical and social implications. They may promote more honest and open communication in social situations, but they may also lead to abuse and a lack of accountability.

Reference 9

Title: "Secure Goods Storage and Anti-Theft Approach using Ethereum Blockchain."

Concept

This study offers a reliable system that creates a safe, decentralized method of tracking goods and preventing theft using the Ethereum blockchain, "IPFS (Interplanetary File System)," and contemporary cryptography techniques. When the buyer completes the transaction, they will be required to provide the unique IDs and pertinent information they received in the email. By using cryptographic techniques to encrypt sensitive data and linking distinct IDs to the acquired goods, the system protects user privacy while maintaining unchangeable transaction records.

Limitation

- The suggested blockchain-based payment approach might have issues with transaction volume scalability. Due to limited transaction throughput and network congestion, blockchain, particularly public blockchains, may have slower transaction times.

Reference 10

Title: "PBTMS: A Blockchain-Based Privacy-Preserving System for Reliable and Efficient E-Commerce"

Concept

In this work, we present a blockchain-based privacy protection system called PBTMS that use hybrid encryption, zero-knowledge proofs, and Pedersen commitments as fundamental building blocks to guarantee robust privacy protection for transaction data and

user information. Consensus protocols and blockchain technology are used by PBTMS to enable distributed storage, which reduces the risk of rogue nodes and eliminates single points of failure, resulting in safe, dependable, and effective e-commerce transactions. Additionally, the technique significantly lowers blockchain-related overheads including processing time, gas consumption, and storage costs by combining off-chain computation with on-chain storage.

Limitation

- Despite the apparent improvements in transaction validation and privacy protection, PBTMS still has a number of shortcomings. In high-concurrency circumstances, the consensus technique may experience throughput issues, particularly as the number of nodes increases.

Reference 11

Title: "Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach"

Concept

In order to facilitate inter-organizational collaboration and create a robust Machine Learning (ML) algorithm for e-commerce fraud detection, this study proposes a "blockchain and smart contract-based strategy." The proposed method of data privacy protection makes use of blockchain technology. When a smart contract is implemented in the network, the system is fully automated. An ML model is progressively enhanced using collaborative data provided by blockchain-connected businesses. To encourage the companies, they have put in place an incentive structure that adjusts to the level of work required to update a model. The difficulty of updating the ML technique determines the incentives offered to firms. A removal criterion has been introduced for efficiently mining the block.

Limitation

- The effort to improve a model's presentation is positively correlated with the reward calculated by the incentive mechanism. Models that are more difficult to

upgrade will receive larger incentives under the suggested approach. Since genuine data is more likely to impact the model's performance, the true data provider is heavily rewarded.

Reference 12

Title: "A Novel Ensemble Belief Rule-Based Model for Online Payment Fraud Detection."

Concept

In order to solve credit fraud detection, this study proposes a novel ensemble "BRB (belief rule base)" model that combines the BRB technique with an ensemble learning framework. When compared to traditional machine learning methods, the proposed model has the advantage of excellent interpretability. Furthermore, compared to standard BRB models, the ensemble structure enables better performance when managing extremely unbalanced categorization assignments.

Limitation

- The vast amount of real-time card-use data in real-world applications presents issues that need further research, even though the experiments' enormous dataset size shows the potential of the suggested technique in this field.

Reference

1. Chen, Y., Feng, L., Zhao, Q., Tian, L., & Yang, L. (2024). ARS-Chain: A Blockchain-Based Anonymous Reputation-Sharing Framework for E-Commerce Platforms. *Mathematics*, *12*(10), 1480.
2. Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *13*(3), 1673-1685.
3. Yang, F., Hu, G., & Zhu, H. (2025). A Novel Ensemble Belief Rule-Based Model for Online Payment Fraud Detection. *Applied Sciences*, *15*(3), 1555.
4. Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. N., & Rahman, R. M. (2022). Blockchain and machine learning for fraud detection: A

privacy-preserving and adaptive incentive based approach. *IEEE Access*, *10*, 87115-87134.

5. Li, G., Wu, H., Wu, J., & Li, Z. (2024). Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain. *Journal of Cloud Computing*, *13*(1), 97.
6. Wang, Z., Kim, S., & Joe, I. (2023). An Improved LSTM-Based Failure Classification Model for Financial Companies Using Natural Language Processing. *Applied Sciences*, *13*(13), 7884.
7. Li, J. (2022). E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining. *Computational Intelligence and Neuroscience*, *2022*(1), 8783783.
8. Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *Ieee Access*, *11*, 137188-137203.
9. Zhang, R., Li, Y., & Fang, L. (2025). PBTMS: A Blockchain-Based Privacy-Preserving System for Reliable and Efficient E-Commerce. *Electronics*, *14*(6), 1177.
10. Amasala, L., & Ponnuru, M. (2024). Secure goods storage and anti-theft approach using ethereum blockchain. *Procedia Computer Science*, *233*, 1-11.
11. Yu, W., Wang, Y., Liu, L., An, Y., Yuan, B., & Panneerselvam, J. (2023). A multiperspective fraud detection method for multiparticipant e-commerce transactions. *IEEE Transactions on Computational Social Systems*, *11*(2), 1564-1576.
12. Al-Zubaidie, M., & Shyaa, G. S. (2023). Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps. *Future Internet*, *15*(8), 262.