E-Commerce Fraud Detection Based on Machine Learning

Revathi M#1,Satheesh P#2,RatheeshKumar S#3,ShibiRaj C#4,Sivasakthi M#5

*#1AssistantProfessor,DepartmentofComputerScienceandEngineering,SriShakthiInstituteofEngineeringandTechnology, India.**Email**:mrevathicse@siet.ac.in*

*#2Student,DepartmentofComputerScienceandEngineering,SriShakthiInstituteofEngineeringandTechnology,India. **Email**:pandiyansatheesh21cse@srishakthi.ac.in*

*#3Student,DepartmentofComputerScienceandEngineering,SriShakthiInstituteofEngineeringandTechnology,India. **Email**:saravanakumarratheeshkumar21cse@srishakthi.ac.in*

*#4Student,DepartmentofComputerScienceandEngineering,SriShakthiInstituteofEngineeringandTechnology,India. **Email**:cristophershibiraj21cse@srishakthi.ac.in*

*#5Student,DepartmentofComputerScienceandEngineering,SriShakthiInstituteofEngineeringandTechnology,India. **Email**:murugansivashakthi21cse@srishakthi.ac.in*

ABSTRACT

The rapid expansion of the e-commerce industry, particularly during the COVID-19 pandemic, has led to a significant rise in digital fraud and financial losses. Ensuring a secure e-commerce environment now demands effective cybersecurity and fraud prevention systems. However, research into fraud detection faces challenges due to limited availability of real-world datasets. Recent advancements in artificial intelligence (AI), machine learning (ML), and cloud computing have renewed interest in this area, but existing literature often lacks depth in evaluating ML algorithms specifically within e-commerce platforms like eBay and Facebook. Many reviews offer generalized insights but fail to capture how these techniques apply uniquely to digital marketplaces. To address this gap, our study adopts the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology for a structured literature review. We aim to assess how ML and data mining techniques are applied to detect fraud in e-commerce. Analyzing 101 relevant publications from the past decade, our review identifies key trends, research opportunities, and the growing use of artificial neural networks in this field. These findings offer valuable insights to researchers and industry professionals seeking to implement effective fraud detection systems and highlight future research directions in combating e-commerce fraud.

*Keywords**: e-commerce fraud, machine learning, artificial intelligence, data mining, fraud detection systems, PRISMA methodology, systematic literature review, cybersecurity, digital marketplaces, artificial neural networks.***

I. INTRODUCTION

The rapid expansion of e-commerce platforms has created significant opportunities for online business transactions. However, it has also given rise to a parallel increase in fraudulent activities, posing threats to both merchants and consumers. To address this growing concern, we present a fraud detection system that leverages machine learning techniques to accurately identify suspicious transactions. Developed using Python for the backend and HTML, CSS, and JavaScript for the frontend, the system is deployed using the Flask web framework to ensure a responsive and user-friendly interface.

The system utilizes two robust machine learning models—XGBoost Classifier and Stacking Classifier—to classify transactions as fraudulent or legitimate. These models were chosen for their high performance, scalability, and ability to generalize well on unseen data. The Stacking Classifier achieves a train accuracy of 100% and test accuracy of 99%, while the XGBoost model delivers a train accuracy of 96% and test accuracy of 95%. These metrics demonstrate the effectiveness of the system in distinguishing between normal and malicious activities with minimal false positives.

A synthetic dataset containing 23,634 transaction records was generated using Python’s Faker library. This dataset was designed to simulate real-world transaction behaviors, incorporating 16 key features such as Transaction ID, Customer ID, Transaction Amount, Payment Method, and a binary indicator for fraudulent activity. The data was then preprocessed through various steps including data cleaning, normalization, handling of missing values, and feature selection. Nine relevant attributes were retained for model training to reduce noise and improve learning accuracy.

The project is structured into several modules, starting from data collection to real-time fraud prediction. The data collection module acquires transaction data, followed by preprocessing and feature extraction to prepare the dataset. The training and evaluation modules focus on fitting the models and analyzing their performance using metrics like accuracy, precision, recall, and F1-score. Confusion matrices are also generated to visualize the classification results and to highlight the distinction between true positives and false positives.

Both models are trained using an 80:20 split for training and testing. XGBoost, being an optimized gradient boosting framework, excels in handling missing data and large datasets efficiently. The Stacking Classifier combines Random Forest and Decision Tree as base learners with Logistic Regression as a meta-learner, allowing it to capture complex patterns in data through ensemble learning. Once trained, the models are saved using Python's pickle module, enabling real-time predictions during deployment.

The final output of the system allows users to input new transaction data through the web interface. The prediction module processes the input and classifies it as either fraudulent or legitimate. The evaluation module compares the performance of both models and ensures the system maintains high accuracy even under dynamic inputs. Overall, this project highlights the importance and effectiveness of machine learning in securing e-commerce platforms and mitigating the risks associated with online fraud.

II. LITERATURE SURVEY

1) Increasing cybercrime since thepandemic: Concerns for psychiatry

AUTHORS: S. Monteith, M. Bauer, M. Alda, J. Geddes, P. C.Whybrow, and T. Glenn

Since the pandemic, the daily activities of many people occur at home. People connect to the Internet for work, school, shopping, entertainment, and doctor visits, including psychiatrists. Concurrently, cybercrime has surged worldwide. This narrative review examines the changing use of technology, societal impacts of the pandemic, how cybercrime is evolving, individual vulnerabilities to cybercrime, and special concerns for those with mental illness.

Human factors are a central component of cybersecurity as individual behaviors, personality traits, online activities, and attitudes to technology impact vulnerability. Mental illness may increase vulnerability to cybercrime. The risks of cybercrime should be recognized as victims experience long-term psychological and financial consequences. Patients with mental illness may not be aware of the dangers of cybercrime, of risky online behaviors, or the measures to mitigate risk.

Technology provides powerful tools for psychiatry but technology must be used with the appropriate safety measures. Psychiatrists should be aware of the potential aftermath of cybercrime on mental health, and the increased patient risk since the pandemic, including from online mental health services. As a first step to increase patient awareness of cybercrime, psychiatrists should provide a recommended list of trusted sources that educate consumers on cybersecurity.

2) Detecting problematic transactions in a consumer-toconsumere-commerce network

AUTHORS:S. Kodate, R. Chiba, S. Kimura, and N. Masuda

Providers of online marketplaces are constantly combatting against problematic transactions, such as selling illegal items and posting fictive items, exercised by some of their users. A typical approach to detect fraud activity has been to analyze registered user profiles, user's behavior, and texts attached to individual transactions and the user. However, this traditional approach may be limited because malicious users can easily conceal their information. Given this background, network indices have been exploited for detecting frauds in various online transaction platforms. In the present study, we analyzed networks of users of an online consumer-to-consumer marketplace in which a seller and the corresponding buyer of a transaction are connected by a directed edge. We constructed egocentric networks of each of several hundreds of fraudulent users and those of a similar number of normal users. We calculated eight local network indices based on up to connectivity between the neighbors of the focal node. Based on the present descriptive analysis of these network indices, we fed twelve features that we constructed from the eight network indices to random forest classifiers with the aim of distinguishing between normal users and fraudulent users engaged in each one of the four types of problematic transactions. We found that the classifier accurately distinguished the fraudulent users from normal users and that the classification performance did not depend on the type of problematic transaction.

3) The application of data mining techniques in financialfraud detection: A classification framework and anacademic review of literature

AUTHORS:E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun

This paper presents a review of — and classification scheme for — the literature on the application of data mining techniques for the detection of financial fraud. Although financial fraud detection (FFD) is an emerging topic of great importance, a comprehensive literature review of the subject has yet to be carried out. This paper thus represents the first systematic, identifiable and comprehensive academic literature review of the data mining techniques that have been applied to FFD. 49 journal articles on the subject published between 1997 and 2008 was analyzed and classified into four categories of financial fraud (bank fraud, insurance fraud, securities and commodities fraud, and other related financial fraud) and six classes of data mining techniques (classification, regression, clustering, prediction, outlier detection, and visualization). The findings of this review clearly show that data mining techniques have been applied most extensively to the detection of insurance fraud, although corporate fraud and credit card fraud have also attracted a great deal of attention in recent years. In contrast, we find a distinct lack of research on mortgage fraud, money laundering, and securities and commodities fraud. The main data mining techniques used for FFD are logistic models, neural networks, the Bayesian belief network, and decision trees, all of which provide primary solutions to the problems inherent in the detection and classification of fraudulent data. This paper also addresses the gaps between FFD and the needs of the industry to encourage additional research on neglected topics, and concludes with several suggestions for further FFD research.

4) Frauddetection system: A survey

AUTHORS:A. Abdallah, M. A. Maarof, and A. Zainal

The increment of computer technology use and the continued growth of companies have enabled most financial transactions to be performed through the electronic commerce systems, such as using the credit card system, telecommunication system, healthcare insurance system, etc. Unfortunately, these systems are used by both legitimate users and fraudsters. In addition, fraudsters utilized different approaches to breach the electronic commerce systems. Fraud prevention systems (FPSs) are insufficient to provide adequate security to the electronic commerce systems. However, the collaboration of FDSs with FPSs might be effective to secure electronic commerce systems. Nevertheless, there are issues and challenges that hinder the performance of FDSs, such as concept drift, supports real time detection, skewed distribution, large amount of data etc. This survey paper aims to provide a systematic and comprehensive overview of these issues and challenges that obstruct the performance of FDSs. We have selected five electronic commerce systems; which are credit card, telecommunication, healthcare insurance, automobile insurance and online auction. The prevalent fraud types in those E-commerce systems are introduced closely. Further, state-of-the-art FDSs approaches in selected E-commerce systems are systematically introduced. Then a brief discussion on potential research trends in the near future and conclusion are presented.

5) Acomprehensive survey of data mining-based frauddetection research

AUTHORS:C. Phua, V. Lee, K. Smith, and R. Gayler

This survey paper categorises, compares, and summarisesfromalmost all published technical and review articles in automatedfraud detection within the last 10 years. It defines the professionalfraudster, formalises the main types and subtypes of known fraud,and presents the nature of data evidence collected within affectedindustries. Within the business context of mining the data toachieve higher cost savings, this research presents methods andtechniques together with their problems. Compared to all relatedreviews on fraud detection, this survey covers much moretechnical articles and is the only one, to the best of ourknowledge, which proposes alternative data and solutions fromrelated domains

III.PROPOSEDMETHODOLOGY

The proposed methodology for e-commerce fraud detection using machine learning involves a multi-stage pipeline that begins with data acquisition and preprocessing, followed by feature selection, model training, evaluation, and finally, deployment. The approach focuses on leveraging historical transactional data to build predictive models capable of classifying transactions as either fraudulent or legitimate in real time. This system is designed to continuously adapt to new patterns of fraudulent behavior by retraining models with fresh data.

The first step is data collection and preprocessing. A comprehensive dataset containing transaction attributes such as transaction amount, time, location, device type, and user behavior patterns is gathered. The raw data often contains missing values, duplicates, and imbalanced class distributions, which are common in fraud detection tasks. Preprocessing includes handling missing values through imputation, removing redundant entries, and applying normalization techniques. Given the highly imbalanced nature of fraud datasets (where fraudulent transactions are rare), resampling methods such as SMOTE (Synthetic Minority Over-sampling Technique) are used to balance the dataset and improve model performance.

Next, the process of feature engineering and selection is applied. Feature engineering involves transforming raw data into meaningful features that can enhance the predictive power of the model. This includes creating new features such as average transaction frequency per user, transaction velocity, and unusual location indicators. Feature selection techniques like correlation analysis, mutual information, and recursive feature elimination are used to reduce dimensionality, remove irrelevant variables, and improve computational efficiency while preserving the most predictive features.

In the model training phase, various supervised learning algorithms are tested to find the most accurate and robust classifier. Algorithms such as Logistic Regression, Decision Trees, Random Forest, Gradient Boosting, and Support Vector Machines are implemented and compared. Cross-validation techniques are employed to evaluate model generalization and avoid overfitting. The models are trained on the labeled dataset, where the target variable indicates whether a transaction is fraudulent or not. Hyperparameter tuning using grid search or random search is performed to optimize model performance.

Once models are trained, they are evaluated using performance metrics such as precision, recall, F1-score, and area under the ROC curve (AUC-ROC). These metrics are crucial, especially in fraud detection, where false negatives (missed frauds) can be more costly than false positives. The best-performing model is selected for deployment. In production, the model is integrated with the e-commerce platform to perform real-time transaction scoring, flagging potentially fraudulent activity for further investigation or automated blocking.

The final step involves model monitoring and retraining. Fraud patterns evolve rapidly, so the deployed model must be continuously monitored for performance degradation. New labeled data from recent transactions are collected, and the model is retrained at regular intervals to ensure adaptability. Feedback loops are incorporated where flagged transactions verified by investigators are fed back into the training data, thereby improving future predictions. This end-to-end methodology ensures a proactive, data-driven approach to mitigating fraud in e-commerce environments.

III. SYSTEMIMPLEMENTATION

1. Technology Stack and Frameworks

The system was developed using a combination of front-end and back-end technologies to ensure a seamless and interactive user experience. The front-end was designed using HTML, CSS, and JavaScript to create an intuitive and responsive interface. The back-end logic and model integration were implemented using Python, with the Flask framework acting as the middleware that connects the user interface with the machine learning models. Flask was chosen for its lightweight structure and ease of deployment in small to medium-scale applications, making it suitable for real-time fraud detection.

2. Dataset Integration and Preprocessing

The dataset used comprises 23,634 synthetic records, generated using Python's Faker library and supplemented with realistic transaction behavior and fraudulent activity patterns. The system imports this dataset from a local directory and begins by preprocessing the data. This step involves cleaning (removing duplicates and null values), converting categorical values using one-hot encoding, and scaling numerical values. Additionally, only 9 out of the original 16 features were selected for training based on relevance, using feature importance ranking techniques. This ensures that the machine learning models are trained only on the most impactful attributes, improving their performance and reducing computational complexity.

3. Model Training and Serialization

The core component of the system is the machine learning model training module. Two classifiers were implemented: the XGBoost Classifier and a Stacking Classifier. The XGBoost model was trained due to its strong performance on tabular data and its ability to handle imbalanced datasets and missing values efficiently. The Stacking Classifier was created using RandomForest and DecisionTree as base estimators and Logistic Regression as the final estimator. After training and evaluating the models, they were serialized using Python's pickle library and saved as .pklfiles. This allowed for efficient loading and reuse during prediction without the need to retrain the model each time.

4. Real-Time Prediction Module

Once the models are trained and saved, the prediction module is used to classify new transactions. Through the web interface, users can input transaction data (either manually or through a CSV upload), which is then processed and passed to the selected model. The model returns a binary output—0 for legitimate and 1 for fraudulent transactions. The system provides immediate feedback to the user, making it suitable for integration into live e-commerce transaction workflows. This real-time classification helps prevent fraudulent activities before they are completed.

5. Model Evaluation and Visualization

To assess and monitor the performance of the deployed models, a model evaluation module is included. It calculates key performance metrics such as accuracy, precision, recall, and F1-score using the test set. Confusion matrices are also generated and visualized using Seaborn's heatmap for better interpretability. For instance, the Stacking Classifier achieved 100% training accuracy and 99% test accuracy, while the XGBoost model achieved 96% training and 95% test accuracy. These metrics are crucial in validating the reliability of the system in real-world scenarios.

6. Deployment and User Interface

The final implementation step involves hosting the entire application through Flask, enabling it to run on a local or cloud server. Users interact with the system via a web interface, where they can test the fraud detection models with sample inputs. The interface is minimalistic but functional, showing predictions, uploading functionality, and model evaluation summaries. The modular design of the system allows for easy updates, such as retraining the model with new data or integrating more sophisticated classifiers in the futur

IV.ADVANTAGES

1. **High Accuracy in Fraud Detection:** The proposed system leverages advanced machine learning models, including the Stacking Classifier and XGB Classifier, which have demonstrated high accuracy in detecting fraudulent transactions. With train and test accuracy scores of 100% and 99% for the Stacking Classifier and 96% and 95% for the XGB Classifier, the system is highly effective in identifying fraudulent activities with minimal false positives and false negatives.

2. **Robust Synthetic Dataset:** The use of a synthetic dataset generated with Python's Faker library and custom logic ensures that the system is trained on a wide range of realistic transaction scenarios. This enables the models to generalize well and detect fraud even in cases that differ slightly from the training data, enhancing the system's robustness.

3. **Scalability and Adaptability:** Designed with scalability in mind, the proposed system can be adapted to various e-commerce platforms regardless of their size or transaction volume. Its architecture allows for easy integration into existing systems, making it suitable for both small businesses and large enterprises.
4. **Real-Time Fraud Detection:** The system is built to operate in real-time, providing immediate analysis and classification of transactions. This allows for prompt identification of fraudulent activities, enabling e-commerce platforms to take swift action to prevent financial losses and protect customers.

5. **Comprehensive Feature Set:** The dataset used in the system includes 16 carefully selected features that capture essential details of each transaction, such as Transaction Amount, Payment Method, and Customer Location. This comprehensive feature set allows the models to analyze multiple dimensions of a transaction, improving the accuracy and reliability of fraud detection.

6. **Enhanced Security and Trust:** By providing an effective tool for detecting fraudulent transactions, the proposed system enhances the overall security of e-commerce platforms. This not only helps prevent financial losses but also builds trust with customers, as they can be assured that their transactions are being monitored for fraudulent activity.

7. **User-Friendly Interface:** The system's frontend, developed using HTML, CSS, and JavaScript, ensures a user-friendly interface that is easy to navigate. This makes it accessible to a wide range of users, from technical staff to non-technical administrators, ensuring that the system can be effectively utilized across different roles within an organization.

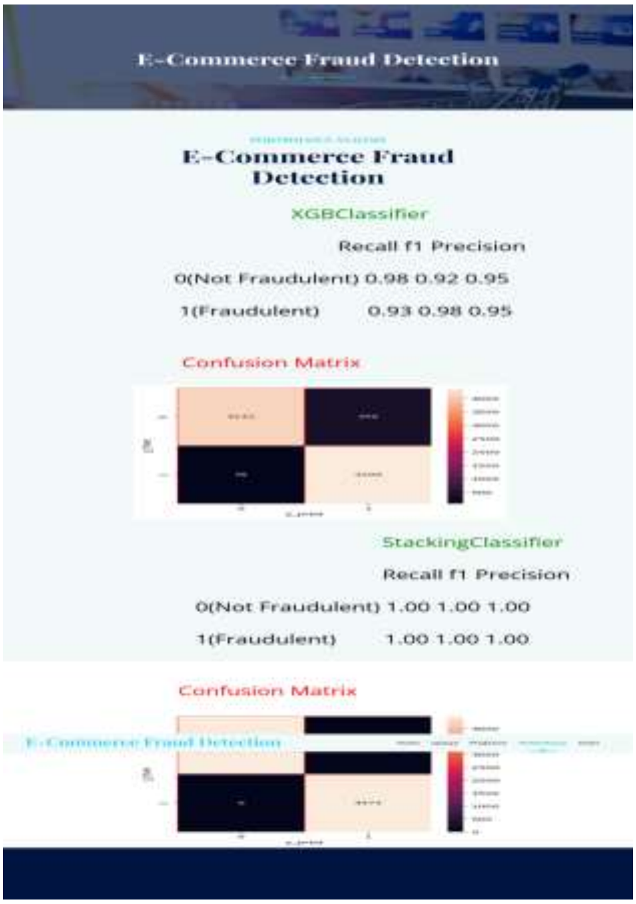
8. **Flexible Integration:** Utilizing the Flask web framework, the system is designed for flexible integration with various e-commerce platforms and back-end systems. This allows businesses to incorporate the fraud detection system into their existing workflows with minimal disruption.

9. **Customizable and Extendable:** The system's architecture is designed to be customizable and extendable, allowing for future enhancements and the addition of new features as needed. This ensures that the system can evolve in response to emerging fraud patterns and technological advancements

VI .RESULTS AND ANALYSIS

The proposed e-commerce fraud detection system effectively addresses the rising threat of digital fraud by integrating advanced machine learning techniques, specifically XGBoost and a Stacking Classifier, achieving high accuracy (up to 99% test accuracy). The use of a synthetic yet realistic dataset ensures broad generalization across transaction types, enhancing detection robustness. Key strengths include real-time prediction, modular architecture for scalability, and a user-friendly interface. The system's performance evaluation, using precision, recall, and F1-score, confirms its reliability in minimizing false positives and negatives. Literature insights reveal that while machine learning is widely applied in financial fraud detection, its specific application in e-commerce remains underexplored. This study bridges that gap through a systematic PRISMA-based review, identifying the dominance of neural networks and ensemble methods in current trends. Overall, the system demonstrates strong potential for practical deployment in digital marketplaces and highlights critical areas for future research and improvement in fraud prevention methodologies.

In addition to high accuracy and real-time performance, the system's modular design enables easy updates and integration with various e-commerce platforms, making it suitable for businesses of all sizes. The incorporation of ensemble learning through the Stacking Classifier allows for better pattern recognition and reduces overfitting. The use of a synthetic dataset with diverse transaction features ensures comprehensive model training, while the Flask-based deployment ensures responsiveness and accessibility. The PRISMA-based literature review identifies research gaps and emphasizes the growing importance of AI and ML in fraud detection. This work not only delivers a practical solution but also advances academic understanding in field.



E-Commerce Fraud Detection

E-Commerce Fraud Detection

XGBClassifier

```
                     Recall f1 Precision
0(Not Fraudulent) 0.98 0.92 0.95
1(Fraudulent)       0.93 0.98 0.95
```

Confusion Matrix

StackingClassifier

```
                     Recall f1 Precision
0(Not Fraudulent) 1.00 1.00 1.00
1(Fraudulent)       1.00 1.00 1.00
```

Confusion Matrix

.

E-Commerce Fraud Detection

E-Commerce Fraud Detection

E-Commerce Fraud Detection

E-Commerce Fraud

VII .CONCLUSION

The "E-Commerce Fraud Detection Based on Machine Learning" project successfully addresses the critical need for effective fraud detection mechanisms in the rapidly growing e-commerce sector. By employing advanced machine learning models like the Stacking Classifier and XGB Classifier, the system achieves high accuracy in identifying fraudulent transactions, significantly reducing the risk of financial losses and enhancing the security of online transactions.

The use of a synthetic dataset, carefully designed to mimic real-world transaction scenarios, enables the system to generalize well across different types of fraud, ensuring its applicability in diverse e-commerce environments. The integration of this system into a user-friendly web interface, built using HTML, CSS, JavaScript, and the Flask framework, ensures that it can be easily utilized by businesses of varying sizes and technical capabilities.

Overall, the project demonstrates the power and potential of machine learning in combating e-commerce fraud, providing a robust and scalable solution that enhances the trust and reliability of online marketplaces. By offering real-time detection and a comprehensive analysis of transaction data, the system stands as a valuable tool in the ongoing effort to safeguard digital commerce.

VIII. REFERENCES

[1].Ray, S. (2022). Fraud Detection in E-Commerce Using Machine Learning. BOHR International Journal of Advances in Management Research, 1(1).

[2]. Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P. V., &Polireddi, N. S. A. (2024). Effective Fraud Detection in E-Commerce: Leveraging Machine Learning and Big Data Analytics. Measurement: Sensors, 33, 101138.

[3]. Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P. V., &Polireddi, N. S. A. (2024). Effective Fraud Detection in E-Commerce: Leveraging Machine Learning and Big Data Analytics. ResearchGate.

[4]. Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P. V., &Polireddi, N. S. A. (2024). Effective Fraud Detection in E-Commerce: Leveraging Machine Learning and Big Data Analytics.

[5].Li, X., Peng, Y., Sun, X., Duan, Y., Fang, Z., & Tang, T. (2025). Unsupervised Detection of Fraudulent Transactions in E-Commerce Using Contrastive Learning. arXiv.

[6]. Cytron, R., Ferrante, J., Rosen, B. K., Wegman, M. N., &Zadeck, F. K. (1991). Efficiently computing static single assignment form and the control dependence graph. ACM Transactions on Programming Languages and Systems (TOPLAS), 13(4), 451–490.

[7]. Suganuma, T., Yasue, T., & Komatsu, H. (2002). Design and evaluation of dynamic optimizations for a Java Just-In-Time compiler. ACM SIGPLAN Notices, 37(5), 304–315.

[8]. Chow, F., Chan, S., Kennedy, K., Liu, S.-M., Lo, R., & Tu, P. (1997). A new algorithm for partial redundancy elimination based on SSA form. ACM SIGPLAN Notices, 32(5), 273–286.

[9]. Chaitin, G. J., Auslander, M. A., Chandra, A. K., Cocke, J., Hopkins, M. E., & Markstein, P. W. (1981). Register allocation via coloring. Computing Research Repository (CoRR), cs/0101001.

[10]. Davidson, J. W., & Fraser, C. W. (1984). Code selection through object code optimization. ACM Transactions on Programming Languages and Systems (TOPLAS), 6(4), 505–526.