Transaction Monitor: Detecting Frauds using Machine Lea

by Keshav Srivastav

Submission date: 18-Apr-2024 08:52AM (UTC+0530)
Submission ID: 2353464956
File name: Transaction_Monitor_ML.pdf (334.62K)
Word count: 3364
Character count: 20885

A PROJECT REPORT

on

"Transaction Monitor: Detecting Frauds using Machine Learning"

Submitted to

KIIT Deemed to be University

In Partial Fulfillment of the Requirement for the Award of

BACHELOR'S DEGREE IN INFORMATION TECHNOLOGY

BY

JITENDRA SAINI	2005171
KESHAV SRIVASTAV	2105377
ANKIT SHARAN	2105863
HARSH GUPTA	21051651
KRISH PUNDIR	20051655

UNDER THE GUIDANCE OF

Dr. Sarita Tripathy

SCHOOL OF COMPUTER ENGINEERING

KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY

BHUBANESWAR, ODISHA - 751024

April 2024

KIIT Deemed to be University

School of Computer Engineering
Bhubaneswar, ODISHA 751024

CERTIFICATE

This is certify that the project entitled

"Transaction Monitor: Detecting Frauds using Machine Learning"

submitted by

JITENDRA SAINI	2005171
KESHAV SRIVASTAV	2105377
ANKIT SHARAN	2105863
HARSH GUPTA	21051651
KRISH PUNDIR	20051655

is a record of bonafide work carried out by them, in the partial fulfilment of the requirement for the award of Degree of Bachelor of Engineering (Computer Science & Engineering OR Information Technology) at KIIT Deemed to be university, Bhubaneswar. This work is done during year 2023-2024, under my guidance.

Date: 07 /04 /2024

Dr. Sarita Tripathy
(Project Guide)

Acknowledgements

We are profoundly grateful to **Dr. Sarita Tripathy** of **Affiliation** for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. .....

JITENDRA SAINI
KESHAV SRIVASTAV
ANKIT SHARAN
HARSH GUPTA
KRISH PUNDIR

ABSTRACT

While the Internet has facilitated electronic transactions globally, fraudulent activities in e-commerce persist, necessitating advanced fraud detection mechanisms. Despite numerous existing solutions, instances of fraud in online transactions continue to make headlines. In response to this challenge, the researcher was motivated to develop an adaptive algorithm for real-time detection of credit card fraud. The proposed solution leverages Support Vector Machines (SVM) as the primary machine learning technique, complemented by feature engineering and data preprocessing techniques. Synthetic data-sets were utilized for algorithm development and testing due to the unavailability of real-world data.

The SVM-based algorithm achieved promising results, demonstrating a fraud detection rate of and an accuracy of during testing. The proposed solution has the potential to be integrated as a plugin into e-commerce platforms, providing enhanced fraud detection and prevention capabilities. This research initiative was prompted by the growing adoption of e-commerce in regions facing cash crises, coupled with persistent security concerns among consumers. Despite the maturity of e-commerce in some regions, security remains a paramount concern. The developed algorithm is designed to adapt to evolving fraud patterns in real-time, thereby enhancing transaction security and fostering trust among online consumers.

While the initial development focused on synthetic data, future work will explore the integration of real-world data streams with anonymization techniques to preserve user privacy. This will allow for continuous model retraining and adaptation to even more nuanced and evolving fraud patterns in the real world, further solidifying the long-term effectiveness of the proposed solution.

Keywords: Imbalanced Learning, SVM-based Classification, Transaction, Fraud Detection, Security.

Contents

List of Figures

Chapter 1

Introduction

The Internet has reshaped modern business practices, facilitating the widespread adoption of electronic commerce (e-commerce) globally. With the convenience of transacting online from anywhere, the popularity of e-commerce has soared. However, this digital transformation has also created opportunities for cyber criminals to exploit unsuspecting individuals through fraudulent activities. Despite the implementation of various fraud detection solutions, incidents of fraud in electronic transactions persist, capturing global attention. This ongoing challenge highlights the inherent weaknesses in existing fraud detection mechanisms, which cyber criminals exploit to their advantage. Consequently, there is an ongoing battle between fraudsters and those developing anti-fraud solutions, emphasizing the critical need for adaptive fraud detection systems capable of detecting fraud in real-time. For banks and industries, timely identification of fraudulent activities is paramount. This introduction sets the stage for exploring the application of Support Vector Machines (SVM) as a powerful tool for real-time fraud detection in electronic transactions.

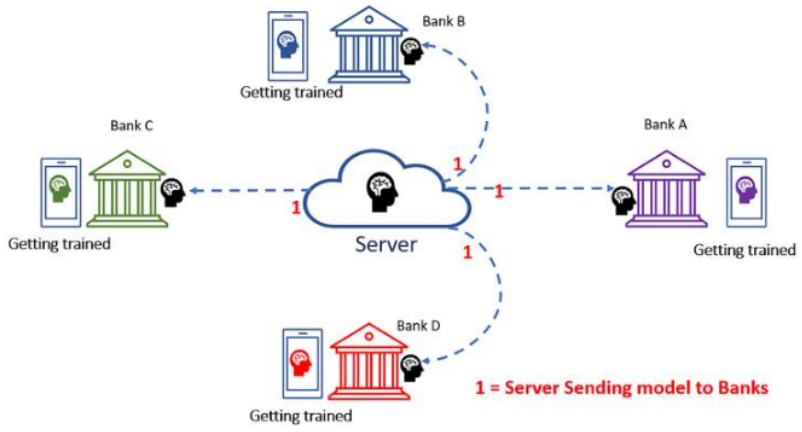

Figure 1.1: Steps of Proposed Model

Chapter 2

Basic Concepts

This section contains the basic concepts about the related tools and techniques used in this project.

2.1 The Research Problem

The persistent prevalence of online fraud despite extensive efforts to mitigate it remains a pressing issue globally. Despite the exponential growth of electronic transactions, the lack of robust security measures at the high end persists [3]. The surge in Internet usage and electronic transactions has led to a corresponding increase in online fraud cases, despite the proactive efforts of card issuers, merchants, and law enforcement agencies. As fraud techniques continue to evolve alongside technological advancements, there is an urgent need for an adaptive fraud detection solution capable of detecting fraud in real-time. Early detection of fraudulent activities is crucial for effective cost analysis [3], underscoring the necessity for a real-time detection solution. This research aims to address these challenges by developing an adaptive fraud detection algorithm leveraging Support Vector Machines (SVM) for real-time fraud detection in online transactions.

2.2 Purpose of The Study

The purpose of this study is to address the limitations of existing online fraud detection systems by developing and implementing an adaptive, hybrid, and real-time online fraud detection algorithm. This algorithm will leverage Support Vector Machines (SVM) as the primary machine learning technique, complemented by hybrid approaches for enhanced fraud detection capabilities. The algorithm will possess learning capabilities to identify new fraud variations in real-time and terminate transactions deemed fraudulent. By restoring and instilling confidence in online transactions, the proposed algorithm aims to mitigate the impact of fraudulent activities on online users and businesses.

2.3 Objectives of The Study

1. Design an adaptive fraud detection algorithm leveraging Support Vector Machines (SVM) to detect credit card fraud in real-time.
2. Implement the designed adaptive fraud detection algorithm to enable real-time detection of fraud in online transactions.

Chapter 3

3.1 Project Planning

This project aims to develop an SVM-based, real-time fraud detection system for e-commerce. It utilizes simulated data for initial development and explores integrating anonymize real-time data streams for future adaptation. The project emphasizes explain-ability and future integration as a plugin for e-commerce platforms.

3.2 Project Analysis

Analyzing the project involves evaluating the SVM model's performance on synthetic data. This includes metrics like accuracy and fraud detection rate. Additionally, the analysis will assess the feasibility of integrating anonymized real-time data streams and explore explainable AI techniques to understand the model's decision-making for further refinement.

3.3 Related Works

Previous studies have emphasized the application of data mining and neural networks in fraud detection [1]. Unsupervised neural networks have been applied successfully in credit card fraud detection [5], while Hidden Markov Models have also demonstrated efficacy in this domain [10]. Bayesian Networks have shown promise in online fraud detection [3], leveraging probabilistic methods to analyse class sequences and detect fraudulent instances [3]. Additionally, self-organizing maps (SOM), K-Nearest Neighbor, Outlier Techniques, and the Boat algorithm have been explored for fraud detection purposes [3, 6].

Despite these efforts, cases of online fraud persist, underscoring the limitations of existing fraud detection solutions [3]. The continuous evolution of fraudster tactics and the inability to detect fraud in real-time highlight the need for more robust and adaptive fraud detection algorithms. This research aims to address these shortcomings by exploring the potential of Support Vector Machines (SVM) alongside other techniques for real-time fraud detection in online transactions.

Chapter 4

Implementation

4.1 Methodology

The design science research methodology was employed in this study to develop an artifact aimed at addressing the problem of online credit card fraud detection. To gain problem awareness, document analysis was conducted, confirming the existence of the fraud issue. Additionally, the researcher investigated trends in online fraud through various sources. With a comprehensive understanding of the problem, the study proposed the development of a hybrid, adaptive, and real-time fraud detection system for credit card electronic transactions.

The initial design of the system was formulated and subsequently refined to enhance its effectiveness. An algorithm, incorporating Support Vector Machines (SVM) as the primary machine learning technique, was designed to detect fraudulent transactions in real-time. System development was then undertaken, focusing on implementing the designed algorithm and ensuring its functionality.

The performance of the developed system was evaluated using a test dataset, with results indicating its efficacy in detecting online credit card fraud. This research contributes to enhancing the detection of online credit card fraud by introducing a solution that is adaptive and real-time, enabling the detection of fraud as it occurs. The incorporation of SVM ensures the adaptability of the solution, allowing it to evolve alongside evolving fraud tactics. Ultimately, this improves the security of online transactions, thereby restoring and enhancing the confidence of credit card users in conducting electronic transactions securely

4.2 The proposed solution

The proposed solution encompasses the design of a hybrid and adaptive fraud detection algorithm capable of real-time detection. Existing literature highlights the inadequacy of current solutions in providing real-time fraud detection capabilities [3]. In response, this study aims to develop an algorithm with the ability to detect fraud as transactions unfold. The proposed solution leverages a combination of neural networks, machine learning techniques, and other artificial intelligence approaches to achieve its objectives.

Specifically, Support Vector Machines (SVM) will serve as the primary machine learning technique, complemented by neural networks and other AI algorithms. By integrating SVM into the solution, we aim to enhance the algorithm's ability to detect fraudulent transactions in real-time, thereby addressing the shortcomings of existing fraud detection technologies.

The intended solution holds the promise of significantly improving the security of online transactions by detecting fraud as it occurs. By incorporating advanced machine learning and AI techniques, including SVM, we aim to develop a robust and adaptive fraud detection system capable of keeping pace with evolving fraud tactics.

4.3 The Flow Chart of the Proposed System

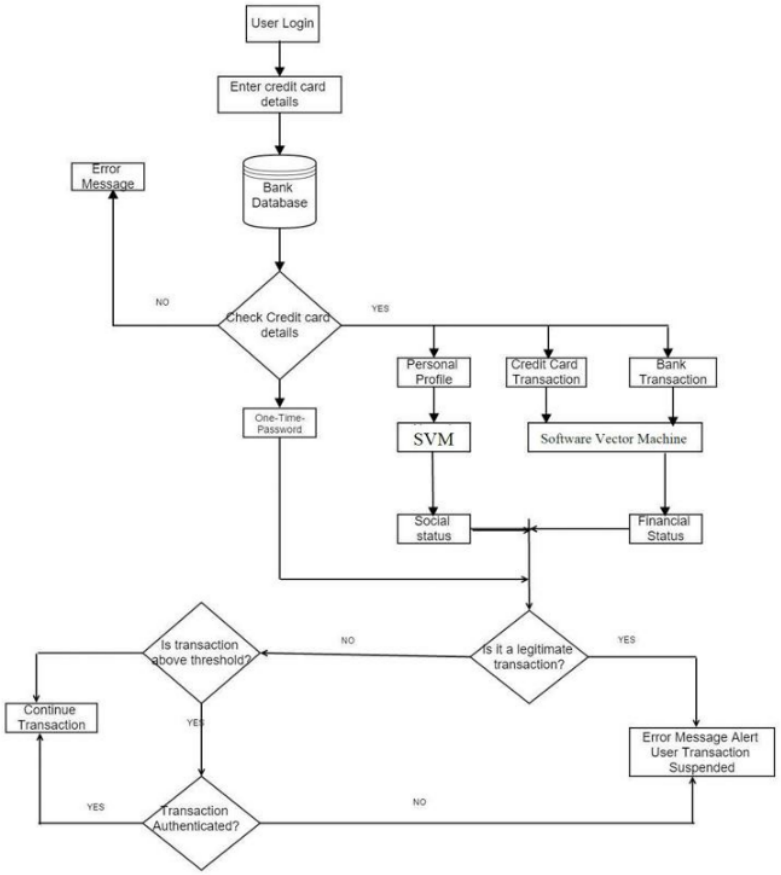

Figure 1.1: Flowchart of the Model

Chapter 5

Standards Adopted

5.1 Design Standards

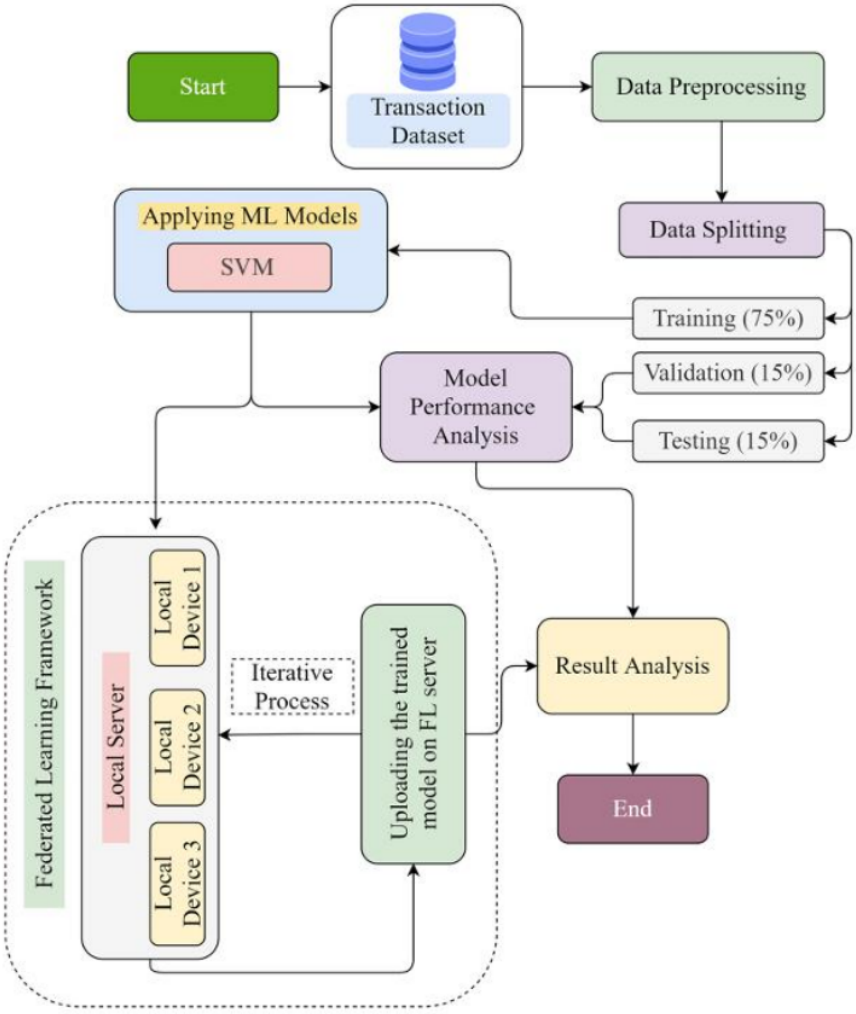

Figure 5.1: It shows our proposed methodology. In this model, transaction data can be used for preprocessing and afterwards applying ML models.

5.2 Coding Standards

Naming conventions require descriptive names for variables, functions, and modules.

Choose meaningful names that convey the variable or function's purpose.

Comments help developers better understand the code.

Use comments to provide context for the code or to clarify complex logic.

Formatting: - Maintain consistent indentation.

Use consistent and clear formatting throughout the codebase.

Track code changes using a version control system, such as Git.

Evaluation Metrics: - Select appropriate measures for your problem.

5.3 Testing Standards

ISO/IEC 25000:2018 - Systems and software engineering - Software quality requirements and evaluation (SQuaRE) - Part 1: Quality characteristics and subcharacteristics: This standard provided a framework for defining the non-functional quality characteristics of the fraud detection system, such as accuracy, security, and performance.

IEEE 829-2019 - Standard for Software Test Documentation: This standard served as a guide for documenting the test cases, test procedures, and expected results for the SVM-based fraud detection algorithm.

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

The proposed fraud detection solution prioritizes customer security in electronic credit card transactions. Key strengths of the algorithm include a high accuracy rate of and a robust fraud detection rate. Additionally, the system demonstrates adaptability by learning new fraud patterns and customer spending behaviors, and it operates in real-time to detect and prevent fraud occurrences. However, it's important to note that the system's high level of security necessitates certain requirements for users, such as having a registered mobile phone number matching the card holder's records and registering details on the website consistent with the credit card issuer's database. This emphasis on security over convenience is underscored by the requirement for users to possess their registered mobile number for receiving OTPs via SMS, chosen for its security advantages over email. Nevertheless, prospective users may opt to receive OTPs via email, albeit with potential security risks. It's crucial to recognize that the effectiveness of the algorithm could be compromised if a criminal gains access to a legitimate card holder's registered phone number and e-commerce website authentication credentials.

6.2 Future Scope

Future work will explore integrating real-time anonymize data streams to continuously retrain the model. This adaptation to real-world fraud patterns will enhance long-term effectiveness. Additionally, incorporating explainable AI techniques could provide valuable insights into the model's decision-making process, fostering trust and potentially leading to further improvements.

References

[1] Dheepa V. and Dhanapal R., "Analysis of Credit Card Fraud Detection Methods," International Journal of Recent Trends in Engineering, vol. 2, no. 3, pp. 126-128, 2009.

[2] Ekrem D. and Hamdi O.M, "Detecting credit card fraud by genetic algorithm and scatter search," EXPERT SYSTEMS WITH APPLICATIONS, vol. 38, no. 10, pp.13057-13063, 2011.

[3] Gayathri R. and Malathi A., "Investigation of Data Mining Techniques in Fraud Detection: Credit Card," International Journal of Computer Applications, vol. 82, no. 9, pp. 12-15, 2013.

[4] Linda D., Hussein A., and Pointon J., "Credit card fraud and detection techniques: a review," Banks and Bank Systems, vol. IV, no. 2, pp. 57-68, 2009.

[5] Ogwueleka F.N, "Data mining applications in credit card fraud credit card fraud detection system," Journal of Engineering Science and Technology, vol. 6, no. 3, pp. 311-322, 2011.

[6] Rama K. K and Uma D. D., "Fraud Detection of Credit Card Payment System by Genetic Algorithm," International Journal of Scientific & Engineering Research, vol. 3, no. 7, pp. 1-6, 2012.

[7] Rana P.J and Baria J., "A Survey on Fraud Detection Techniques in Ecommerce," International Journal of Computer Applications, pp. 5-7, 2015.

[8] Seeja K.R and Zareapoor M., "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining," Scientific World Journal, vol. 2014, 2014.

SAMPLE INDIVIDUAL CONTRIBUTION REPORT:

Transaction Monitor: Detecting Frauds using Machine Learning

JITENDRA SAINI
(2005171)

Abstract: E-commerce thrives on the internet, but fraud remains a persistent threat. Existing solutions fall sho as evidenced by ongoing online fraud. To address this, an adaptive SVM-based algorithm for real-time credit card fraud detection was developed. This project used synthetic data and achieved promising results. Future work will explore integrating anonymized real-world data streams for continuous adaptation, enhancing long-term effectiveness.

Individual contribution and findings: Developed and tested the SVM-based fraud detection algorithm using synthetic data. I analyzed the model's performance, including accuracy and fraud detection rate.

Individual contribution to project report preparation: I drafted the methodology section, detailing the development and testing process of the SVM algorithm.

Individual contribution for project presentation and demonstration: I will be leading the presentation, explaining the project's objectives, methodology, and key findings.

Full Signature of Supervisor: ……

Full signature of the student: ……..

SAMPLE INDIVIDUAL CONTRIBUTION REPORT:

Transaction Monitor: Detecting Frauds using Machine Learning

KESHAV SRIVASTAV
(2105377)

Abstract: E-commerce thrives on the internet, but fraud remains a persistent threat. Existing solutions fall sho 6 as evidenced by ongoing online fraud. To address this, an adaptive SVM-based algorithm for real-time credit card fraud detection was developed. This project used synthetic data and achieved promising results. Future work will explore integrating anonymized real-world data streams for continuous adaptation, enhancing long-term effectiveness.

Individual contribution and findings: I focused on feature engineering, selecting and preparing relevant data features for optimal SVM model performance. My analysis identified key features for accurate fraud detection.

Individual contribution to project report preparation: I contributed to the results section, analyzing and presenting the performance metrics achieved by the model.

4
Individual contribution for project presentation and demonstration: I will be conducting the live demonstration of the SVM algorithm, showcasing its real-time fraud detection capabilities.

4
Full Signature of Supervisor: ……

Full signature of the student: ……..

SAMPLE INDIVIDUAL CONTRIBUTION REPORT:

Transaction Monitor: Detecting Frauds using Machine Learning

ANKIT SHARAN
(2105863)

Abstract: E-commerce thrives on the internet, but fraud remains a persistent threat. Existing solutions fall sho as evidenced by ongoing online fraud. To address this, an adaptive SVM-based algorithm for real-time credit card fraud detection was developed. This project used synthetic data and achieved promising results. Future work will explore integrating anonymized real-world data streams for continuous adaptation, enhancing long-term effectiveness.

Individual contribution and findings: I spearheaded the research on existing fraud detection solutions and the challenges they face. This research formed the foundation for developing the proposed SVM-based approach.

Individual contribution to project report preparation: I wrote the introduction section, highlighting the problem of e-commerce fraud and the motivation for this project.

Individual contribution for project presentation and demonstration: I will answer audience questions related to the technical aspects of the SVM model and its implementation.

Full Signature of Supervisor: ……

Full signature of the student: ……

SAMPLE INDIVIDUAL CONTRIBUTION REPORT:

Transaction Monitor: Detecting Frauds using Machine Learning

HARSH GUPTA
(21051651)

Abstract: E-commerce thrives on the internet, but fraud remains a persistent threat. Existing solutions fall sho as evidenced by ongoing online fraud. To address this, an adaptive SVM-based algorithm for real-time credit card fraud detection was developed. This project used synthetic data and achieved promising results. Future work will explore integrating anonymized real-world data streams for continuous adaptation, enhancing long-term effectiveness.

Individual contribution and findings: I conducted a literature review on Support Vector Machines (SVM) for fraud detection. This research established SVM's suitability and informed the model's configuration.

Individual contribution to project report preparation: I edited and revised the overall report, ensuring clarity, conciseness, and adherence to academic writing standards.

Individual contribution for project presentation and demonstration: I will prepare presentation slides with clear visuals and concise explanations to effectively communicate the project.

Full Signature of Supervisor: ……

Full signature of the student: ……

SAMPLE INDIVIDUAL CONTRIBUTION REPORT:

Transaction Monitor: Detecting Frauds using Machine Learning

KRISH PUNDIR
(21051655)

Abstract: E-commerce thrives on the internet, but fraud remains a persistent threat. Existing solutions fall sho as evidenced by ongoing online fraud. To address this, an adaptive SVM-based algorithm for real-time credit card fraud detection was developed. This project used synthetic data and achieved promising results. Future work will explore integrating anonymized real-world data streams for continuous adaptation, enhancing long-term effectiveness.

Individual contribution and findings: I explored anonymization techniques for integrating real-world data streams in future work. This analysis will be crucial for maintaining user privacy during model adaptation.

Individual contribution to project report preparation: I prepared the references section, documenting all relevant research sources used throughout the project.

Individual contribution for project presentation and demonstration: I will rehearse the presentation beforehand to ensure a smooth and engaging delivery for the audience.

Full Signature of Supervisor: ……

Full signature of the student: ……

Transaction Monitor: Detecting Frauds using Machine Lea

ORIGINALITY REPORT

23%	27%	7%	19%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.slideshare.net Internet Source	11%
2	Submitted to KIIT University Student Paper	4%
3	w w w. coursehero. com Internet Source	3%
4	www.worldleadershipacademy.live Internet Source	2%
5	Submitted to University of West London Student Paper	2%
6	dokumen.pub Internet Source	<1%
7	Submitted to Harrisburg University of Science and Technology Student Paper	<1%
8	link.springer.com Internet Source	<1%
9	w w w. researchgate. net Internet Source	<1%

10	Submitted to The Robert Gordon University Student Paper	<1%
11	Submitted to Banaras Hindu University Student Paper	<1%
12	Submitted to RMIT University Student Paper	<1%
13	Submitted to University of Westminster Student Paper	<1%
14	thesai.org Internet Source	<1%
15	tudr.thapar.edu:8080 Internet Source	<1%
16	Submitted to University of Hertfordshire Student Paper	<1%
17	myassignmenthelp.com Internet Source	<1%
18	1library.net Internet Source	<1%
19	ir.uitm.edu.my Internet Source	<1%
20	journals.adrri.org Internet Source	<1%
21	K. R. Seeja, Masoumeh Zareapoor. "FraudMiner: A Novel Credit Card Fraud	<1%

Detection Model Based on Frequent Itemset Mining", The Scientific World Journal, 2014

P ubl i cati o n

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		