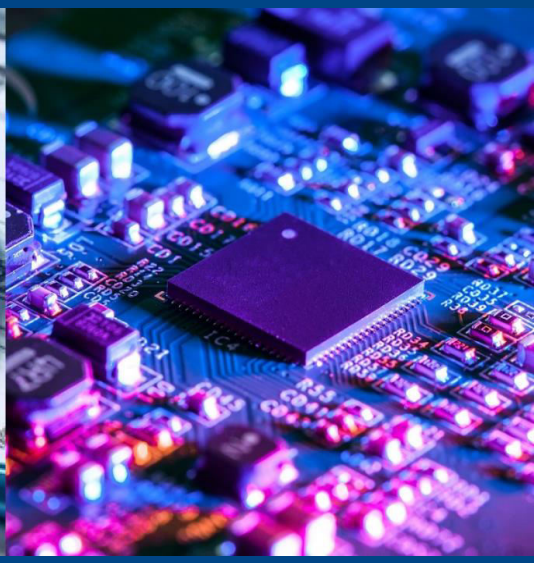
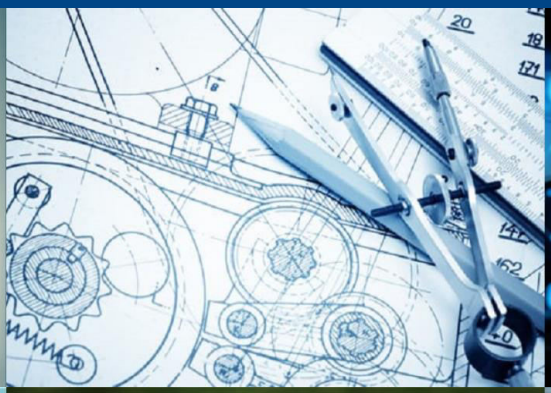
ISSN: 2582-7219

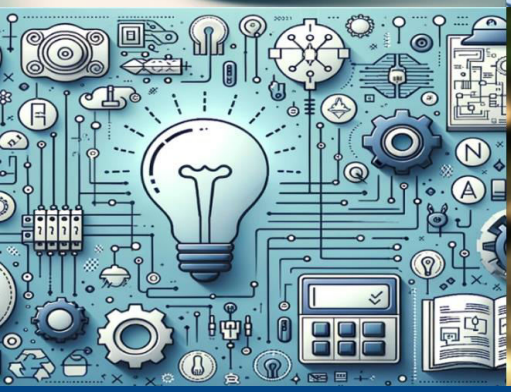




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904457

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fraud Detection and Prevention Using Machine Learning Algorithms

Sanika Dahibhate, Sneha Singh

DR. D.Y. Patil Dnyaan Prasad Global University's, School of Management & Research, Pune, India

ABSTRACT: The growth of payment systems has increased the risk of financial fraud. This includes issues like phishing, identity theft, and fake transactions. Old methods of detecting fraud are often slow and not good at handling large amounts of data. Machine Learning (ML) is a tool that helps find fraud by looking for patterns and unusual activity in real time. This study looks at how aware users are of ML-based fraud detection systems, their experiences with them, and their opinions. The results show that most users know about the risks of fraud but don't understand Machine Learning well. People generally agree that ML improves the accuracy and security of fraud detection. However, there are still concerns about data privacy, system transparency, and trust. The study concludes that Machine Learning is important for detecting fraud, but more awareness and better system reliability are needed for it to be widely accepted.

KEYWORDS: Fraud Detection, Machine Learning, Digital Payments, Cybersecurity, Artificial Intelligence, Financial Fraud.

I. INTRODUCTION

The digital revolution has changed how we do transactions. Systems like UPI, mobile banking, and online payments are now a part of everyday life. However, this convenience has also led to more digital fraud cases. Financial fraud refers to activities that aim to gain money through deception. These include phishing attacks, credit card fraud, identity theft, and online scams. Studies show that fraud is a growing problem, affecting both individuals and organizations, with increasing financial losses every year. Traditional fraud detection systems use rule-based methods, which are often inefficient and unable to detect complex fraud patterns. Machine Learning offers a more advanced approach by analyzing large datasets and identifying unusual transaction patterns. This enables real-time detection and prevention of fraud. This research focuses on understanding user awareness of fraud and evaluating the effectiveness of Machine Learning in fraud detection based on survey responses.

Objective:

1. To understand how aware users are of digital fraud in online payment systems.
2. To look into users' experiences and how often they face financial fraud.
3. To check how people use digital payment methods like UPI and mobile banking.
4. To assess how well users know about Machine Learning in fraud detection.

II. LITERATURE REVIEW

Murat Golyeri et al. (2023), This research looks at using machine learning classifiers to detect e-commerce fraud. The study compares models like Decision Trees, SVM, and Random Forest. It highlights the importance of choosing the right features and preparing data properly. The findings show that methods using multiple models work best for spotting fraud patterns.

Adi Saputra (2019), This study discusses using machine learning to stop e-commerce fraud.
The researcher looks at different algorithms, including Logistic Regression and Naive Bayes, for detecting fraud. It concludes that using machine learning can lower the chance of fraud in online payments. The study also explains how transaction history plays a key role.

G. Jaculine Priya & S. Saradha (2021), The authors review different machine learning algorithms used for fraud detection. They talk about both supervised and unsupervised learning, such as neural networks and clustering techniques.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

They point out some challenges, like dealing with imbalanced datasets and getting too many false alarms. They also stress the need for real-time fraud detection systems.

Rabah Y.R. Abdaljawad et al. (2023), This study analyses financial fraud using machine learning. The performance of different algorithms is tested based on how well they work and how accurate they are. The importance of good data and proper feature engineering for building a strong fraud detection model is highlighted. The study finds that machine learning can help predict fraud.

Kamal Upreti et al. (2023), The paper provides a review of using machine learning for predicting and detecting fraud. Models are developed to find patterns of fraud. The use of big data and advanced analytics is seen as an important part of improving fraud detection.

III. RESEARCH METHODOLOGY

Research Design: Descriptive research methodologies used
Data Collection: Primary data (questionnaire) & Secondary data (research papers and journals)
Sample Size: The 40 respondents were people who use payment systems, including students, professionals, and general users.
Sampling Method: Convenience sampling
Tools Used: Excel data analysis, Percentage method and Graphical representation (Pie charts)
Variables Studied: Awareness of digital fraud, Experience of fraud, Usage of payments, Trust in systems, Awareness of Machine Learning, Effectiveness of Machine Learning, Importance of real-time detection.

Data Analysis and Interpretation:
Based on the survey responses:

Graph1

Interpretation: The pie chart shows that 100% of the 42 respondents are aware of digital fraud in online transactions. Every single person answered "Yes", with no "No" responses.

Graph2

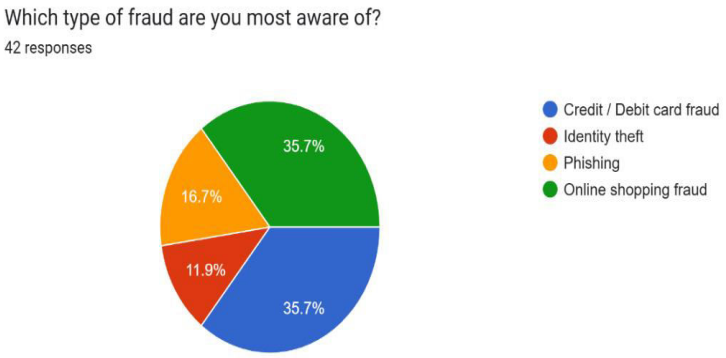
Interpretation: Out of 42 respondents, the majority (76.2%) have never experienced online fraud. However, 19% (8 people) said they have been victims, while a small group (4.8%) are unsure if they have faced any fraud.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

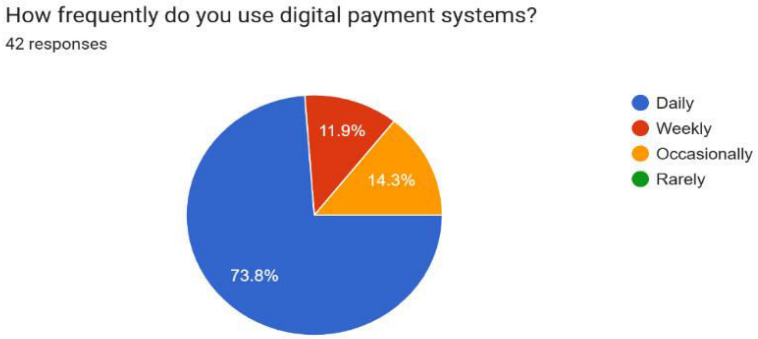
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Graph3



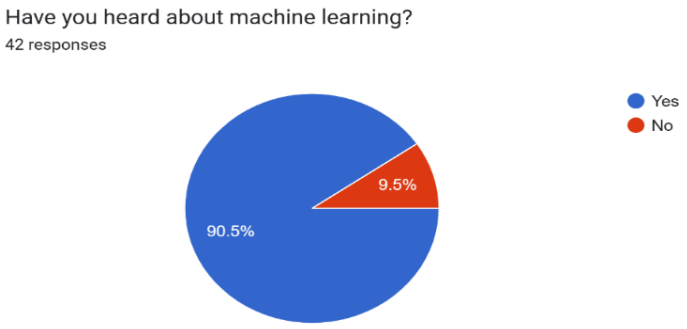
Interpretation: The chart shows that awareness is mainly focused on direct financial threats. Online Shopping Fraud and Credit/Debit Card Fraud each account for 35.7% of responses. Phishing and Identity Theft are less commonly known, with 16.7% and 11.9% respectively. While people are alert to immediate transaction risks, they need more information about data-related threats like identity theft.

Graph4



Interpretation: The chart reveals that digital payment systems are a regular part of daily life for the 42 respondents. Over 73.8% use them every day. A combined 26.2% use these systems less often, either weekly or occasionally. No one said they used them rarely.

Graph5



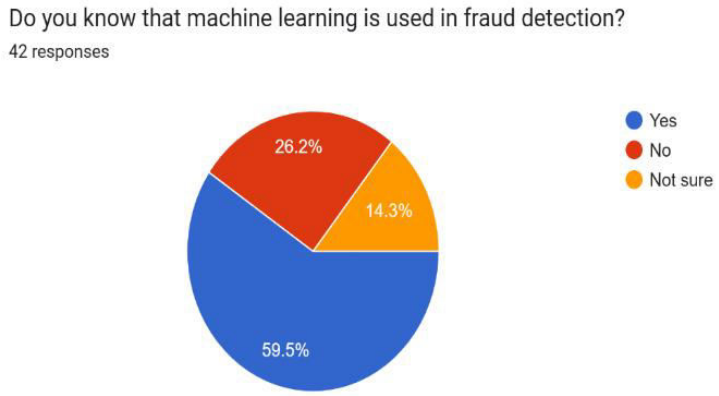
Interpretation: The chart indicates that most of the 42 respondents (90.5%, or 38 people) have heard of Machine Learning. Only a small portion, 9.5%, said they had no knowledge of the term.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

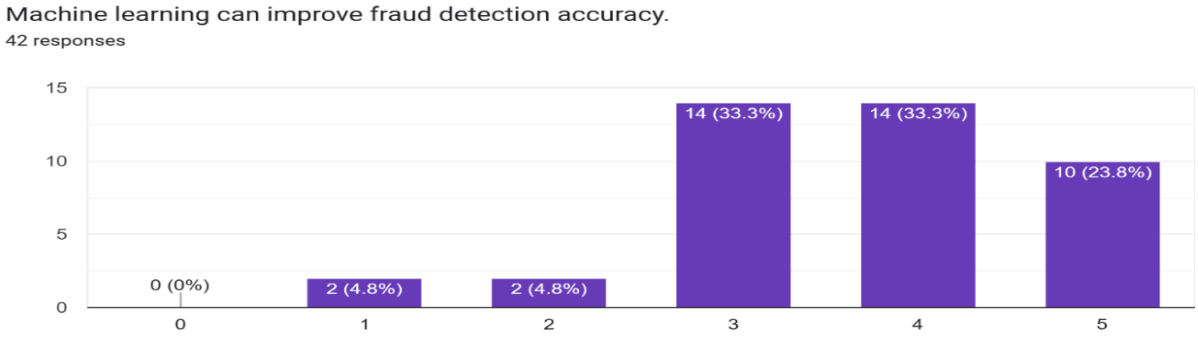
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Graph6



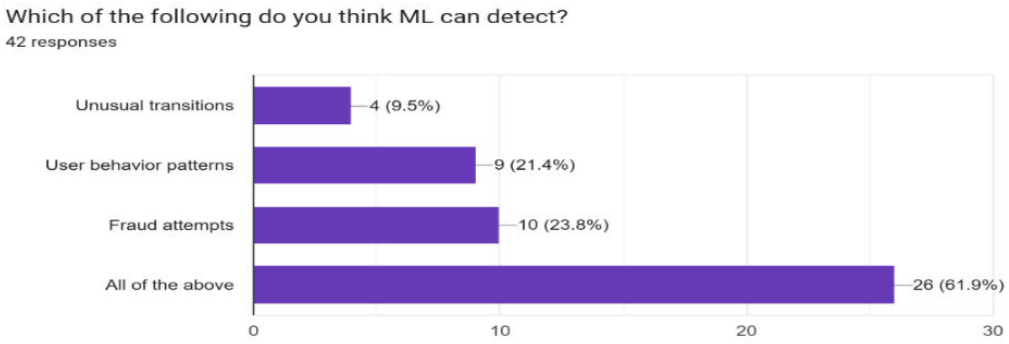
Interpretation: 59.5% of respondents are aware that Machine Learning is used for fraud detection. 26.2% are unaware, and 14.3% are unsure.

Graph7



Interpretation: Responses are heavily skewed toward the higher end of the scale, with 90.4% of participants rating Machine Learning's ability to improve accuracy at a 3, 4, or 5.

Graph8



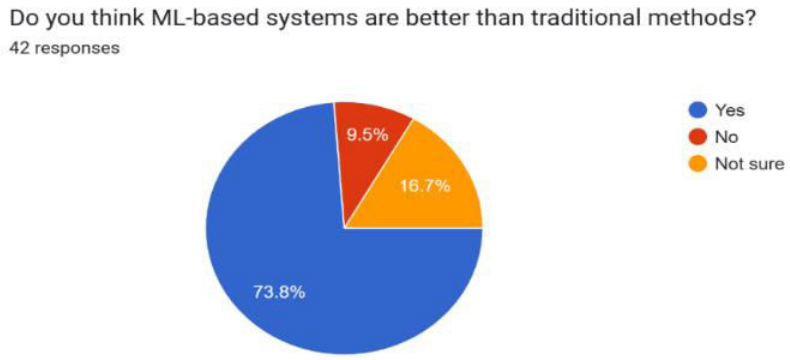
Interpretation: 61.9% of respondents believe Machine Learning can detect all mentioned factors, such as unusual transactions, behavior patterns, and fraud attempts.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

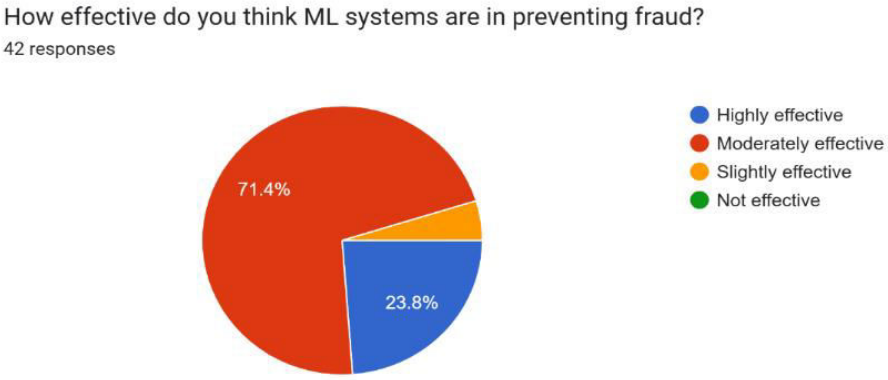
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Graph9



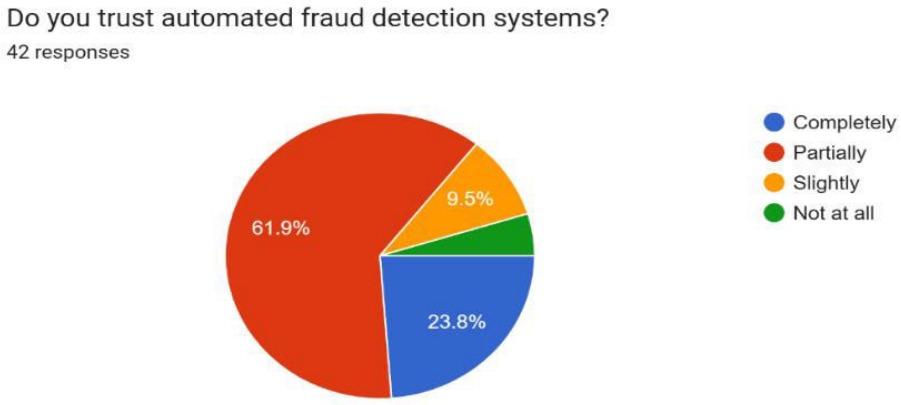
Interpretation: Nearly 74% of respondents think Machine Learning-based systems are better than traditional methods. Only 9.5% disagree.

Graph10



Interpretation: 71.4% view Machine Learning as "moderately effective" and 23.8% as "highly effective."

Graph11



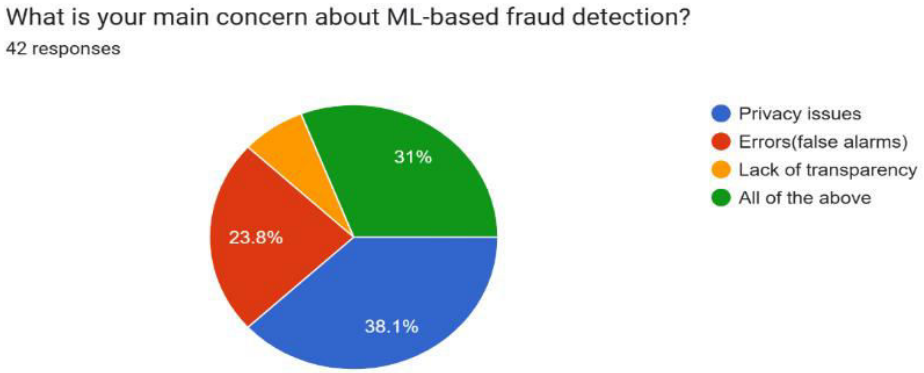
Interpretation: Most users (61.9%) only "partially" trust automated fraud detection. Only 23.8% trust it completely.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

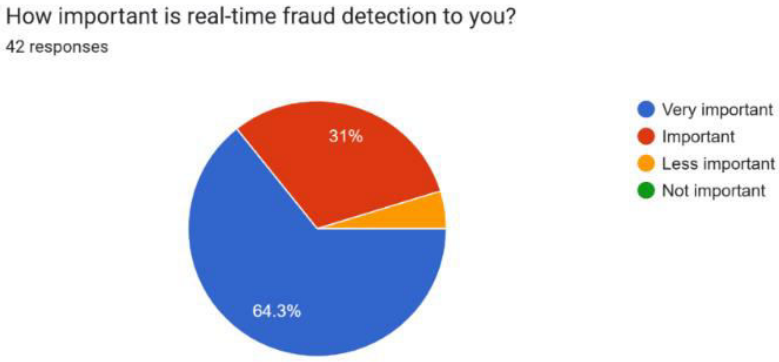
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Graph12



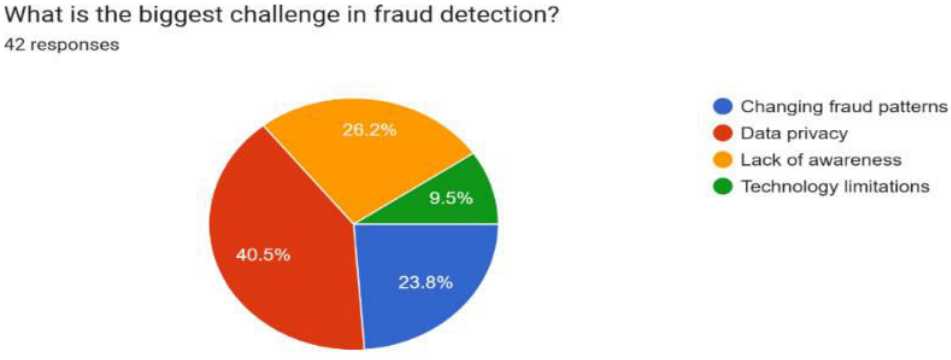
Interpretation: Privacy issues (38.1%) and "All of the above" (31%) are the main concerns, followed by fears of false alarms.

Graph13



Interpretation: An overwhelming 90.5% of respondents consider real-time fraud detection "Very important." The rest (9.5%) see it as "Important."

Graph14



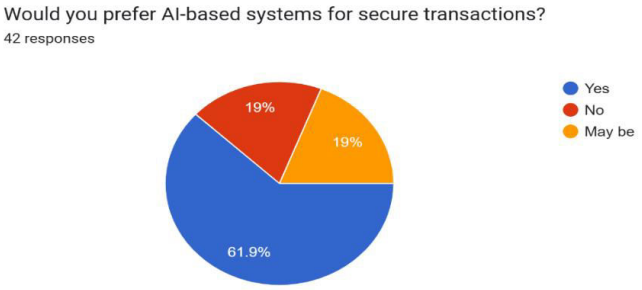
Interpretation: 64.3% of participants think Machine Learning can reduce the overall rate of fraud. 26.2% are unsure, and 9.5% are skeptical.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Graph15



Interpretation: The chart shows that 76.2% of the 42 respondents believe Machine Learning is effective in identifying new and evolving fraud patterns. 16.7% are unsure, and 7.1% don't think it's effective.

IV. RESULTS AND FINDINGS

High level of awareness regarding digital fraud – all respondents know about digital fraud threats., Limited personal involvement – most of the respondents (76.2%) do not have any such experience, but some have had it., Regular usage of digital payments – most respondents use digital payment systems almost daily, exposing themselves to possible threats. Positive attitude towards machine learning – the majority of respondents agree that ML increases accuracy and speed of fraud detection., Partial trust of users – limited trust due to privacy concerns, lack of transparency, and possibility of mistakes.

V. CONCLUSION

The study provides the following conclusions:
Users have awareness of digital fraud but lack a deep technical understanding.
A significant number of respondents have experienced fraud, indicating risks.
Digital payment systems are widely used, increasing exposure to fraud., Machine Learning is seen as an advanced solution.
Users believe Machine Learning improves the accuracy and speed of fraud detection.
Real-time detection is an important feature expected by users.
Trust in Machine Learning systems is moderate due to concerns about privacy and transparency.
Existing fraud detection systems are not fully sufficient.
Users demand security, instant alerts, and improved systems.
Organizations should invest more in AI/Machine Learning technologies and user awareness programs.
Overall, Machine Learning has potential in fraud detection, but its success depends on user trust, system transparency, and continuous technological improvement.

REFERENCES

1. [Financial Fraud Detection Based on Machine Learning] (https://www.mdpi.com/1850374)
2. [Fraud. Machine Learning in Auditing]
(https://journal.midpublisher.com/index.php/esrj/article/view/229)
3. [Introduction to Machine Learning for Fraud Detection]
(https://www.mdpi.com/2076-3417/15/21/11787)
4. [Unsupervised Learning in Fraud Detection]
(https://e-journal.unair.ac.id/jraba/article/view/49927)
5. [Machine Learning Techniques in Credit Card Fraud Detection]
(https://journal.seisense.com/jom/article/view/770)
6. RBI Reports on Digital Payment Security
7. Journals on Financial Technology (FinTech)
8. Primary Data collected through Survey (Excel Responses)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com