

REVIEW ARTICLE

Data-Driven Detection of Online Investment Fraud: A Review of Statistical and Machine Learning Approaches

Rohini Rahul Anyapanawar^{a,*}, Parmeshwar Madhukar Patil^b^a Assistant Professor, Department of Management and Computer Science, Sangameshwar College (Autonomous), Solapur, Maharashtra, India^b Assistant Professor, Department of Statistics, Sangameshwar College (Autonomous), Solapur, Maharashtra, India

* Corresponding author

OPEN ACCESS

This article is licensed under CC BY-NC 4.0.

**ARTICLE HISTORY**

Received: 18 Sep 2026

Accepted: 04 Oct 2026

Published: 14 Oct 2026

CORRESPONDING AUTHOR

Rohini Rahul Anyapanawar, Department of Management and Computer Science, Sangameshwar College (Autonomous), Solapur, Maharashtra, India.

HOW TO CITEAnyapanawar, R. R., & Patil, P. M. (2026). Data-Driven Detection of Online Investment Fraud: A Review of Statistical and Machine Learning Approaches. *Global Journal of Advanced Science and Technology*, 1(1), 7–11.

© 2026 The Author(s).

ABSTRACT

Online investment fraud, in which victims are persuaded through websites, messaging groups or trading applications to invest in schemes that do not exist, has become one of the most damaging forms of cyber-enabled financial crime in India. Unlike card fraud, where the bank sees every transaction, investment fraud is usually carried out by the victim's own authorised payments, which makes it hard to detect with conventional controls. This review examines the statistical and machine learning approaches that have been used to detect financial fraud and considers how they apply to investment fraud. It covers rule-based systems, statistical models, supervised classifiers such as random forests and gradient boosting, unsupervised anomaly detection, and the analysis of text and payment networks. It then discusses the problems that limit these methods in practice: extreme class imbalance, changing fraud patterns, delayed and incomplete labels, and the difficulty of detecting fraud that the customer has been manipulated into authorising. The literature suggests that no single method is sufficient. Effective detection combines supervised models trained on confirmed cases, anomaly detection for new schemes, network analysis to trace mule accounts, and text analysis of advertisements and messages, all supported by human review. The review closes with priorities for research in India, including shared anonymised datasets drawn from cybercrime complaints and closer study of victims' behaviour.

Keywords: Online investment fraud; Fraud detection; Machine learning; Anomaly detection; Cybercrime; Financial technology

1. Introduction

Few crimes have grown as quickly with digital finance as investment fraud. The pattern is familiar to anyone who has read cybercrime complaints in India: a stranger adds the victim to a messaging group, shares screenshots of large trading profits, and invites them to an application or website that shows their

investment growing day by day. When the victim tries to withdraw, they are asked for fees or taxes, and eventually the contact disappears. The money has long since moved through a chain of accounts.

Fraud detection has a long history in statistics and computing. Bolton and Hand (2002) reviewed the statistical methods used against credit card, telecommunications and money-laundering fraud, and later surveys extended this work to data mining and machine learning (Ngai et al., 2011; Phua et al., 2010; West & Bhattacharya, 2016). Most of this research, however, concerns fraud committed against an account holder without their knowledge. Investment fraud is different: the victim usually makes the payments themselves, believing them to be genuine.

This review asks how well existing detection methods transfer to this setting. It describes the main families of methods, examines the practical problems that limit them, and identifies research priorities, with particular attention to India.

2. The nature of online investment fraud

Online investment fraud takes several forms: fake trading or cryptocurrency platforms, Ponzi-style schemes that pay early investors from later deposits, pump-and-dump promotions of thinly traded shares, and impersonation of real brokers or advisers. What these schemes share is persuasion. They exploit the appeal of quick gains and the reluctance to accept a loss, tendencies that prospect theory describes in general terms (Kahneman & Tversky, 1979). DeLiema et al. (2020) studied the mindsets and behaviours of investment fraud victims in the United States and found that exposure to sales pitches and willingness to consider risky opportunities distinguished victims from other investors.

From a detection point of view, three features matter. The payments are authorised by the victim, so they pass the authentication checks that stop most card fraud. The money is usually routed through accounts opened or rented for the purpose, often called mule accounts. And the scheme leaves traces outside the banking system, in advertisements, messaging groups, app stores and websites, that can be analysed before any money is lost.

3. Approaches to detection

Figure 1 groups the methods discussed in the literature into five families. In practice they are combined rather than used alone.

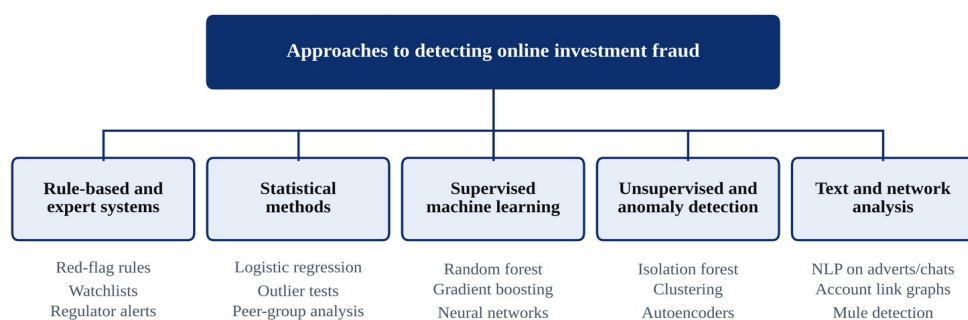


Figure 1. Families of approaches used to detect online investment fraud.

3.1 Rule-based and expert systems

The oldest approach encodes the knowledge of investigators as rules: a new account that receives many payments from unrelated individuals within a short time, transfers to beneficiaries named in regulator alerts, or payments described as trading fees. Rules are transparent and can be put in place quickly when a

new scheme is reported. Their weakness is that fraudsters learn them, and a large rule set produces many false alarms that investigators cannot follow up (Bolton & Hand, 2002).

3.2 Statistical methods

Statistical methods model what normal behaviour looks like and flag departures from it. Bolton and Hand (2002) described peer-group analysis, which compares an account with others that behaved similarly in the past, and break-point analysis, which looks for sudden changes in an account's own behaviour. Logistic regression remains widely used when confirmed fraud cases are available, because its coefficients show which factors raise the risk.

3.3 Supervised machine learning

When enough confirmed cases exist, supervised classifiers can learn the patterns that separate fraudulent from genuine activity. In their review of financial fraud detection, Ngai et al. (2011) found that logistic models, neural networks, Bayesian networks and decision trees were the most frequently used techniques. Since then, ensemble methods such as random forests and gradient boosting have become the usual choice for tabular transaction data. West and Bhattacharya (2016) note, however, that reported accuracies are hard to compare because studies use different data, different measures and often no common benchmark.

3.4 Unsupervised and anomaly detection

New schemes appear faster than labelled examples can be collected. Anomaly detection methods address this by learning what normal activity looks like and scoring how unusual each new case is, without needing fraud labels (Chandola et al., 2009). Isolation forest, which isolates unusual points with fewer random splits than normal ones, is efficient on large data and is now common in practice (Liu et al., 2008). Clustering and autoencoders are also used. The cost is a higher false-alarm rate, because unusual is not the same as fraudulent.

3.5 Text and network analysis

Investment fraud is advertised before it is paid for. Natural language processing can screen advertisements, social media posts and messages for the promises typical of fraud, such as guaranteed daily returns or pressure to act immediately. Network analysis takes the other end of the chain: by linking accounts that send money to the same beneficiaries, share devices or are opened with the same documents, it can reveal rings of mule accounts that individual transaction checks miss (Abdallah et al., 2016). Table 1 compares the five families.

Table 1. Comparison of approaches to detecting online investment fraud.

Approach	Data needed	Main strength	Main limitation
Rules and expert systems	Investigator knowledge; alerts	Transparent; quick to update	Easy to evade; many false alarms
Statistical models	Account history; some labels	Interpretable risk factors	Limited to patterns specified
Supervised machine learning	Large set of confirmed cases	High accuracy on known schemes	Weak on new schemes; needs labels
Anomaly detection	Normal activity only	Can flag new schemes	Unusual is not always fraud
Text and network analysis	Adverts, messages; payment links	Detects schemes and mule rings early	Needs data from outside the bank

Source: compiled by the authors from Bolton and Hand (2002), Ngai et al. (2011), West and Bhattacharya (2016) and Chandola et al. (2009).

4. Problems that limit detection in practice

4.1 Extreme class imbalance

Fraud is rare compared with genuine activity. A model can therefore appear accurate while missing most fraud, and evaluation must rely on measures such as precision, recall and the area under the precision–recall curve. Resampling methods and cost-sensitive learning help, but they do not remove the problem.

4.2 Changing patterns and delayed labels

Dal Pozzolo et al. (2014), drawing on a large card fraud system, showed that fraud patterns drift over time, that the true label of a transaction is often known only weeks later, and that the investigators' own choices determine which cases are labelled at all. Each of these problems is worse for investment fraud, where victims may report the loss months after the first payment, and many never report it at all.

4.3 Authorised payments

The hardest problem is that the victim wants the payment to go through. Even a correct alert may be overridden by a customer who believes the investment is genuine. Detection therefore has to be paired with intervention, such as a call from the bank or a cooling-off period for first payments to a new beneficiary, and with public awareness. Cross (2015) has shown how the blame directed at victims of online fraud discourages many of them from reporting, which in turn starves detection systems of labels. Table 2 summarises these problems and the responses suggested in the literature.

Table 2. Practical problems in investment fraud detection and suggested responses.

Problem	Effect on detection	Suggested response
Class imbalance	High accuracy but low recall	Precision–recall measures; cost-sensitive learning
Concept drift	Models age quickly	Regular retraining; drift monitoring
Delayed or missing labels	Training data incomplete and biased	Semi-supervised learning; link to complaint data
Authorised payments	Alerts overridden by victims	Human contact; delays on new beneficiaries
Fragmented data	Each bank sees only part of the chain	Secure data sharing between banks and police

5. Priorities for research in India

India has built an unusually rich source of data on cybercrime through the National Cyber Crime Reporting Portal and the 1930 helpline, which record complaints, payment details and the accounts involved. Little of this has reached researchers. We see four priorities.

1. Anonymised datasets drawn from cybercrime complaints, released under clear safeguards, would allow methods to be tested on Indian investment fraud rather than on card fraud from other countries.
2. Network methods that trace mule accounts across banks deserve more attention than further improvements to single-transaction classifiers.
3. Text classifiers for advertisements and messages need to work in Indian languages and in mixed Hindi–English and Marathi–English text, which most current tools do not handle well.
4. Detection research should be linked with studies of victims' behaviour, so that alerts and interventions are designed around how people actually make investment decisions.

6. Conclusion

The methods developed for card and payment fraud provide a strong base for detecting online investment fraud, but they cannot be transferred unchanged. Because victims authorise their own payments and report late, transaction-level classifiers see only part of the picture. The literature points towards layered systems that combine supervised models for known schemes, anomaly detection for new ones, network analysis for mule accounts and text analysis for the advertisements that start the process, with human review at the point of payment. For India, the most valuable next step is not a new algorithm but access to well-governed data from the complaints that victims are already filing.

Author contributions: R. R. Anyapanawar: conceptualisation, literature search, writing – original draft. P. M. Patil: methodology of the review, writing – review and editing.

Conflict of interest: The authors declare no conflict of interest.

Funding: This research received no external funding.

Declaration of generative AI use: During the preparation of this work the authors used an AI writing assistant (Claude, Anthropic) to help structure and draft the text. The authors reviewed, edited and verified the content and take full responsibility for this article.

References

- Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90–113. <https://doi.org/10.1016/j.jnca.2016.04.007>
- Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235–255. <https://doi.org/10.1214/ss/1042727940>
- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), Article 15. <https://doi.org/10.1145/1541880.1541882>
- Dal Pozzolo, A., Caelen, O., Le Borgne, Y.-A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, 41(10), 4915–4928. <https://doi.org/10.1016/j.eswa.2014.02.026>
- Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187–204. <https://doi.org/10.1177/0269758015571471>
- DeLiema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. *Journal of Consumer Research*, 46(5), 904–914. <https://doi.org/10.1093/jcr/ucz020>
- Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263–291. <https://doi.org/10.2307/1914185>
- Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In *Proceedings of the 8th IEEE International Conference on Data Mining* (pp. 413–422). <https://doi.org/10.1109/ICDM.2008.17>
- Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569. <https://doi.org/10.1016/j.dss.2010.08.006>
- Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv*. <https://doi.org/10.48550/arXiv.1009.6119>
- West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47–66. <https://doi.org/10.1016/j.cose.2015.09.005>