D3-CIS6913-Deliverable3

Taiwo Onitiju

October 6, 2024

1 Abstract:

This review critiques the paper "Scams and solutions in cryptocurrencies—a survey analyzing existing machine learning models". I looked at how the authors aimed to explore the use of machine learning in fraud detection, providing a broad overview of present models as well as their effectiveness against various popular scams such as rug pulls and Ponzi schemes. My critique is structured into unique sections that reflect the paper: an introduction that discusses the research's importance, a literature review that examines existing studies and methods mentioned in the paper while offering areas that were not thoroughly flushed out, as well as an evaluation of the contribution of the study. My critique further looks into the research design, data analysis, future research, and ethical considerations.

While the paper's strengths are acknowledged, observation of ethical implications regarding data privacy and data bias are also pointed out. Gaps including a lack of discussion on dataset quality and social engineering tactics are noted while enhancements to the research design to grow insight into model performance are offered. Overall, my review served to highlight the efforts made by the paper in advancing machine learning use in battling cryptocurrency fraud while also offering ways of improvement to make future research less daunting.

2 Introduction:

My selection of the research paper "Scams and solutions in cryptocurrencies—a survey analyzing existing machine learning models", I wanted to explore further the area of using machine learning in scam/fraud detection, a field that is currently growing due to the increasing issues of cybercrime such as the 2021 loss of over 1 billion dollars to crypto scams like rug pulls, money laundering, Ponzi scheme, etc. as outline in the paper [2]. This article seemed compelling simply from the title alone as it is sure to offer a comprehensive look at existing machine learning models meant to battle against scams which alone deems it a useful means for researchers.

This critique will be sectioned into several parts. First, I will access the literature review to observe how well the author(s) parse their research. Secondly, I will lay out the contributions of the study, detailing its significance and implications for the field. Next will be an assessment of the research design and the data analysis approach taken by the author(s) for example the performance of the various machine learning models such as Neural networks, Random Forest, etc. [1]. Lastly,

future research that could improve upon the findings as well as address possible gaps would then be followed before concluding by looking at possible ethical implications of the research.

3 Literature Review:

The overall paper is well structured and diverse. It properly mentions various crypto scams such as popular pump-and-dump schemes, initial coin offerings, rug pulls, etc. while offering a brief overview of each scam [1]. It also offers techniques for detection to combat them for example, it mentions the effectiveness of using supervised learning algorithms like Random Forest and Stochastic gradient for detecting Ponzi schemes while achieving an F1 score of 93 and 96 percent respectively [1]. Information looking into previous research as well gaps that were present that this paper aims to address is also present. Nevertheless, this paper could gain from a discussion of the quality of the various datasets used in the previous studies mentioned as well as a more in-depth discussion of the limits of the present machine learning models. I would also point out the lack of a deep analysis of the role of social engineering tactics that accompany many scams. Social engineering plays a major role in the effectiveness of fraudulent schemes but the paper lacks adequate discussion concerning the machine learning models. By exploring this further, critical insight could be gained for developing more efficient systems.

4 Contributions of Study :

The paper clearly explains the contribution of the study as it points out through its analysis on the effectiveness of machine learning models for scam detection [1]. While the contributions are clearly explained, there is a lack of examples that show how these findings could affect practical field application as well as emphasizing their relevance in advancing the area of fraud detection in cryptocurrencies. For instance, in my previous example of how the best-performing models were used for Ponzi scheme detection[1], it failed to dive deep into how this discernment can be applied to real-world fraud detection strategies.

5 Research Design:

The research design is well-defined. It provides a clear view of the evaluation metrics by its use of accuracy and F1 score [1] as well as model selection by grouping based on scam types. A proposed improvement would be an explanation of the research for the selected methodologies, discussing the pros and cons of choosing one method over its contemporaries. Addressing potential concerns such as a dependence on a specific dataset such as the paper's repeated use of the Elliptic dataset for money laundering [1] would further improve the paper's quality.

6 Data Analysis:

The data analysis provides a well-laid-out comparison of various machine learning algorithms that is reinforced by quantitative measures as well as graphs and tables of the result for example, a graph showing the accuracy comparison of fake wallets and accounts [1] which serve to enhance clarity. It also showcases their performance in detecting various scams, for example, the Random forest algorithm achieving a great accuracy of 99.51 percent for detecting fake wallets[1]. However, while the data is solid, it could be better improved by offering a discussion on why certain models outperform others and proposing what could be done to improve upon them. Overall, the data presentation is potent, a more inquisitive approach to the results obtained would strengthen the paper.

7 Future Research Direction:

While the paper identifies potential future research paths such as its suggestion for adaptive detection techniques [1], it lacks pointing out precise topics and offering questions for exploration. As an example, it mentioned the importance of further developing machine learning models for different scam types [1], offering a plan of action or methods to aid development for possible future research in the field would reinforce the groundwork for other researchers.

8 Ethical Considerations:

A commendation I would offer this paper is its emphasis on responsible and safe technology use [1]. However, it could be more detailed by exploring more precise ethical dilemmas and obstacles for example data privacy concerns that are an ever-present issue, or biases in training data that could lead to less than fair results. While it does offer improvements to the machine learning models [1], if the source of the data being provided is skewered, accurate detection cannot be attained, as such offering recommendations to address these ethical concerns would only add value to the paper.

9 Conclusion:

The paper's conclusion properly sums up the findings especially when it highlights the evolution of machine learning models and how efficient they have become at detecting various types of scams [1] as well as a performance analysis of various best-performing models. The author(s) also states areas for future research such as the importance of exploring other detection techniques that focus on other scam avenues like social media posts, and phishing links [1]. However, research into those areas could easily deviate from the crypto space. Rather, going over the overall implications for the shareholders in the crypto space in addition to minor elements of social engineering tactics would also add value.

References

[1] L. Krishnan, I. Vakilinia, S. Reddivari, and S. Ahuja, "Scams and solutions in cryptocurrencies—a survey analyzing existing machine learning models," *Information*, vol. 14, p. 171, 03 2023.

[2] F. T. Commission, "Data spotlight: Reports show scammers cashing in on crypto craze," 2022, accessed: 2022-12-21. [Online]. Available: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

[1] [2]