Mediterranean Smart Cities Conference (MSCC 2024)
2-4 May, 2024, Martil, Morocco

Towards Effective Local Financial Cybercrime Detection using Machine Learning

Marouane Dirchaoui
Laboratoire de Modelisation Mathematiques et de Calculs Economiques
Hassan First University
Settat, Morocco
m.dirchaoui.doc@uhp.ac.ma

Abdallah Abarda
Laboratoire de Modelisation Mathematiques et de Calculs Economiques
Hassan First University
Settat, Morocco
abdallah.abarda@uhp.ac.ma

***Abstract*—** Financial cybercrime is a growing threat to individuals and institutions worldwide. While significant efforts have been made to detect financial cybercrime using machine learning, the local complexity of the problem remains unclear. In this study, our goal is to compare the work of researchers in detecting five different types of financial cybercrime: Social engineering, Romance fraud, Pump and dump schemes, Fake reviews, and Money laundering. Through this comparison, we aim to help researchers prioritize their efforts based on the type of financial cybercrime prevalent in their regions and the resources they have available. The focus is on understanding key characteristics such as the type of data used, funding, contribution to the scientific community through data sharing, and identification of the most effective models of the past studies done to detect the five financial cybercrimes. The results of this study provide valuable insights for the development of targeted machine learning solutions to combat financial cybercrime at the local level.

***Keywords*—**financial cybercrime, fake reviews, machine learning, money laundering, pump and dump, romance fraud, social engineering.

I. INTRODUCTION

Financial cybercrime in simple words is a financial fraud committed online. Abdallah et al. [1] defines financial fraud as an illegal behavior that results in a financial gain to either an individual or an organization from unethical and illegal ways. The digitization of many organizations, businesses, and government agencies [2] has made financial cybercrime a threat to everyone [1]. Financial cybercrime in Morocco has increased during the last three years, it is now common to hear that a family member or a person you know has been scammed online.

A lot of work has been done on financial cybercrime detection using machine learning [3], but the complexity of dealing with the problem locally is still unknown. Starting with data, it is not easy to get access to the data of all transactions that occur in an application or a bank due to privacy constraints. Also, researchers should have an idea of what financial cybercrime they want to tackle in their country.

We have made a comparison of how researchers were able to detect five types of financial cybercrime to provide researchers with insights on which type of fraud to target first if they want to address the problem of financial cybercrime using machine learning in their own country. The rest of the paper is organized as follows: In Section II, we will present the papers related to our work. Section III, we will introduce five financial cybercrimes, social engineering, romance fraud, pump and dump schemes, fake reviews and money laundering. In addition, we will present how researchers have been able to detect them using machine learning. In Section IV, we will discuss the differences between the studies that used machine learning to detect the five financial cybercrimes, focusing on key features for comparison: the data used, the funding, if they contributed their data to the scientific community, and the identification of the best performing model. In Section V, we present the conclusion.

II. RELATED WORK

Great efforts have been made by Nicholls et al. [3] to fill the knowledge gap regarding the financial cybercrime ecosystem. The researchers clarified the different fraud techniques used by cybercriminals and then analyzed the systems, algorithms, limitations, constraints, and metrics used to combat each type of fraud. In addition, they analyzed the relevant personas and stakeholders closely associated with the field, along with an exploration of open and emerging issues within the financial cybercrime landscape. Our work can be seen as an extension of this work. Although we have worked on a small scale, we have presented some of the studies that have been conducted after their work was published. In addition, we have compared different studies that have used machine learning to detect different financial cybercrimes, which will give researchers another perspective that can help them figure out which type of fraud to target first if they want to address the problem of financial cybercrime in their own country.

There have been other studies focusing on each type of financial cybercrime individually, such as social engineering [4], romance fraud [5], pump and dump schemes [6], [7], fake reviews [8], [9], [10], and money laundering [11].

III. FINANCIAL CYBERCRIMES

A. Social Engineering

The growth of social media has inspired many criminals to use social engineering techniques to gain access to user information [12]. Social engineering attacks take advantage of people's shortcomings rather than technology flaws to obtain information or access without authorization. Because these assaults rely on human error, they are more difficult to mitigate than technical methods [4].

Moroccan scammers have a unique take on social engineering, often exploiting the victim's dream of making easy money online. A recent scam involves contacting individuals on WhatsApp with foreign numbers, posing as a company offering simple online tasks like writing reviews or following accounts for payment. Lured by the promise of quick cash, victims are invited to a Telegram group filled with fake workers, and the actual victim. To build trust, the first few tasks are easy and pay small amounts (around 15dh). Then, the trap is sprung. At the third task, victims are instructed to transfer 250dh for a supposed "online operation" promising a 350dh payout. To further convince them, insiders within the group share fake screenshots "proving" they have completed the transfer and received their money. If the victim falls for it and sends the 250dh, they are promptly blocked and kicked from the group, losing their money to the scammers.

Aun et al. [13] used deep learning to detect social engineering attacks on social media. They built their data from hundreds of corporate and personal Facebook posts, the dataset contain 5000 instances and labeled with five attack classes, each class attack have 1000 instances to avoid data imbalance. The researchers used the Recurrent Neural Network Long Short Term Memory (RNN-LSTM) model to achieve high performance in detecting social engineering attacks in social media posts.

SEADer++ v2, is a tool developed by Lansley et al. [14] for detecting social engineering attacks in online environments. Leveraging natural language processing and artificial neural networks, this system analyzes online chat conversations for specific features that indicate deception. The researchers assessed their social engineering attack detection system using two datasets. The first, a real-world collection of 147-labeled attack and non-attack entries obtained from Bezuidenhout et al. [15], and a hybrid version called the compound dataset obtained from their last work Lansley et al. [16]. This compound dataset expanded the real-world data by adding 600 customer support tweets from Twitter, none of which were labeled as attacks. The researchers achieved high performance using random forests.

B. Romance Fraud

On dating websites and other online platforms, such as Facebook or Instagram, cybercriminals create fake user profiles. They interact with possible victims through these accounts, presenting themselves as enticing and attractive companions [17]. Scammers use a variety of tactics to take advantage of their victims once they establish contact. They frequently build up a fake romantic relationship over time in order to gain their targets' trust [18].

This is one of the oldest forms of financial cybercrime in Morocco. Scammers often ask for anything from internet or phone top-up cards to large sums of money. Although many people nowadays take precautions against this type of financial cybercrime, such as requesting pictures or voice messages from the scammer, these methods are not always effective. Many female scammers assume fake identities so it will be very difficult to detect them using these traditional methods, also there are many pictures online and many AI tools that generate female voices that can be used by males.

DatingSec was developed by He et al. [19] to detect malicious accounts in dating applications. The researchers collected a huge amount of data from posts and comments published on Momo, a widely used dating application. They then constructed four datasets containing 20000, 40000, 100000, and 200000 instances, respectively, with each dataset containing an equal number of malicious and legitimate users. They used long short-term memory (LSTM) neural networks and an attentive module to achieve high performance in detecting fake accounts.

Suarez-Tangil et al. [20] tried to automatically detect and eliminate romance fraud using machine learning. The study's data came from datingnmore.com, a dating service known for its rigorous screening procedures aimed at identifying and publicly disclosing romantic scammers on scamdigger.com. The dating site's screening procedure, which flags and lists profiles deemed to be scams, made it easier to identify the fake accounts. The researchers created three different classifiers: one for profile demographics using Naive Bayes, one for profile images using SVM, and one for profile descriptions using SVM. To improve the overall efficacy and robustness of the fake profiles detection, these separate classifiers were combined to form an Ensemble model. The created model was able to detect 93% of the fake profiles on online dating sites.

C. Pump and Dump Schemes

The surge in popularity of cryptocurrencies has attracted a large number of novice investors as well as experienced ones. There are currently hundreds of cryptocurrencies in a chaotic and highly unregulated marketplace of cryptocurrencies, this led to pump and dump schemes being more common than ever [21].

To explain the pump and dump scheme in simple words, a group of scammers will decide to buy a coin at the same time, which will lead to the rise of the price of that coin. Simultaneously, they will start advertising that coin on social media as the new Bitcoin. This will lead many people who are not experts to start buying this coin. When the coin reaches a predefined price, the scammers will start to sell at once, securing huge gains. However, this will lead to a decrease in the price of that coin, resulting in a big loss for the rest of the investors.

LLD is a solution developed by Bello et al. [22] to automatically detect pump and dump activities on centralized cryptocurrency exchanges without

considering post-pump data. They collected the details of pump and dump events between January 2021 and August 2022 from five groups. Since their approach is unsupervised, they only labeled 55 pumps to test their model. The authors selected only the pumps and dumps committed on Binance because they agree with La Morgia et al. [23] that the pumps on this exchange are challenging. Moreover, it is estimated that 60% of all pumps occur on Binance [24]. The authors achieved good results using the LSTM autoencoder and were able to achieve a practical near real-time detection delay while detecting pump and dump schemes.

La Morgia et al. [21] developed a pump and dump scheme detector. The researchers collected pump-and-dump schemes conducted on Binance from a set of 20 Telegram groups. Ultimately, they selected 317 confirmed events on Binance as the foundation for their analysis. The researchers obtained positive results with Random forest, and then they conducted a long-range experiment in which the detector is tested on different cryptocurrencies. The study suggests that the detector is reliable, even if it generates some false positives. The researchers believe that it is advisable for investors to refrain from investing in these instances.

D. Fake Reviews

Reviews have a powerful impact on the customer's decision to buy a product. Good reviews mean a financial gain for the company, while bad reviews can result in a financial loss [25]. Customers can freely post their reviews on social media, which has led some companies to start creating fake reviews to promote their products or services, to diminish the impact of the real bad reviews on their products, or to criticize the products of their competition [8]. Cybercriminals can do the same thing to promote a bad quality product and fool customers into buying it resulting in a financial loss for them.

According to Odeh et al. [4], most existing studies suggest that fake reviewers do not write detailed reviews about a product, which could help in identifying them. However, detecting fake reviews based on text content alone has been shown to have low accuracy [26], [27]. With the advent of Ai tools like ChatGPT or Bard, which can help write detailed reviews in a short amount of time, this is no longer a problem for fake reviewers.

To understand why fake reviews are dangerous, one recent attack in Morocco is using a combination of fake reviews and phishing techniques to scam Facebook users. A sponsored post appears to the victim, the page name and logo are the same as that of one of the established companies specializing in domestic appliances, televisions, phones, and video games in Morocco. It advertised the sale of an iPhone 14 for just 23dh (2.3$), and in the comments, the victim finds multiple fake reviews saying that they cannot believe it is true and posting a picture showing their hands holding the phone. The link on the post will direct you to a website that the fraudsters are using to take the credit card information of their victims. What makes these attacks more dangerous is that even if buying an iPhone 14 for just 2.3$ sounds impossible, the comments can convince people that it is the real deal. Note that the whole post disappears after hours, either because Facebook will stop the advertisement or because the scammer reached his goal.

Ram et al. [28] developed a method of classification to detect fake reviews. The researchers made use of Yelp, which is known for filtering reviews, to construct a real dataset of restaurant reviews. The authors reported that Logistic Regression has the highest performance in detecting fake reviews compared to KNN and Naive Bayes.

Mohawesh et al. [29] developed the first explainable fake review detection model, they used two datasets, namely Yelp NYC and Yelp ZIP, from Yelp [30]. They contain 322,167 restaurant reviews and 608,598 restaurant reviews, respectively. The researchers have used an ensemble classifier that combines three deep learning models, a convolutional neural network to handle the reviewer information, a deep neural network for the product level, and a Bidirectional-LSTM (Bi-LSTM) for the review level. They also used two explainable techniques to interpret and understand the decisions made by the model. The proposed model achieved good results in the detection of fake reviews on both datasets. In addition, the model provided reasonable explanations as to why certain reviews were classified as fake.

E. Money Laundering

Transforming dirty money obtained through criminal activity into clean money in the eyes of the law and government authorities is called money laundering [3]. Cybercriminals has been creative in the way they launder money online. Including and not limited to the use of online gambling platforms to make their money clean by removing a percentage of the money deposited and recording it as a gambling loss [31], buying in-games currency then exchanging it with real money afterwards [32], exploiting the privacy of Bitcoin for money laundering [33], [34].

In Morocco, cybercriminals has a lot of freedom. For example, you do not need to use machine learning to detect some of the money laundering attempts. You can easily type "solde PayPal" in Facebook Marketplace, and you will find many individuals trying to exchange their PayPal money for clean Moroccan money. There are other platforms to investigate, such as TikTok, which allows users to buy TikTok coins and gift them to TikTok live hosts.

Wahrstätter et al. [35] used an unsupervised approach to detect money laundering. To get their data, they collected a large amount of bitcoin blockchain data. Then, to evaluate their model, they used the publicly available GraphSense tag pack published on Github [36]. The main focus of the GraphSense tag package is on criminal marketplaces, ponzi schemes, ransomware and hacking incidents [35]. The dataset contains 86897 addresses related to cybercrime, 37470 addresses related to miners, and 834 addresses related to exchanges. The authors introduced a novel set of features to better identify potential criminal activity. Applying k-means

while using these new features proved to be very effective in detecting money laundering attempts.

Zhou et al. [37] attempted to detect money laundering accounts in Tencent QQ, a well-known Chinese online social network that provides a range of services that are connected by the virtual currency Q coin. The data used by the researchers contains 114,891 malicious accounts and 381,523 benign accounts. In order to label their data, they bought cheap virtual currency advertised on major e-commerce platforms. Then, the sellers' QQ accounts were labeled as malicious accounts. Afterward, they labeled all the accounts that logged in in the same day from the same IP as the seller as a money laundering account. The researchers achieved high accuracy in detecting money laundering accounts using SVM.

IV. Comparative Analysis of Machine Learning Applications in Financial Cybercrime Detection

In this section, we will attempt to give researchers who want to contribute to the fight against financial cybercrimes in their countries a clear idea of which financial cybercrime they should address first. To do that, we chose to compare the papers presented in this study as described in Table I. We chose the following criteria to make the comparison: Financial Cybercrime (FC): the type of financial cybercrime they are detecting. Data (D): if they collected their own data. Size of data (SD): the size of data. Labeling Data (LD): if the data was manually labeled by the researchers or was already labeled. Data Availability (DA): If the researchers made their data available. Financing (F): if the researchers received funding that helped them conduct the study. Imbalanced data (ID): if the data is imbalanced. Results (R): the results obtained. Model (M): best performing model.

TABLE I. *Summary of studies using machine learning to detect five different financial cybercrimes.*

Ref	FC	D	SD	LD	ID	DA	F	Results	M
[13]	Social engineering	Yes	5000	manually	No	No	Yes	Precision = 84% Recall = 81%	RNN-LSTM
[14]	Social engineering	Yes	1056	Already labeled	Yes	Yes	No	AUC = 89.2% Accuracy = 80,1%	Random Forest
[19]	Romance fraud	No	D1:20000 D2:40000 D3.100000 D4:200000	Already labeled	No	No	Yes	Precision = 90.5% Recall = 81.4% F1-score = 85.7% AUC = 94%	LSTM
[20]	Romance fraud	Yes	20122	Already labeled	Yes	Yes	Yes	Accuracy = 97% F1-score = 94.5% Precision = 96.2%	Ensemble model (SVM, Naïve Bayes)
[22]	Pump and dump	Yes	55	manually	-	No	Yes	Precision = 78% Recall = 83% F1-score = 80%	LSTM Autoencoder
[21]	Pump and dump	Yes	317	manually	-	Yes	No	Precision = 98.2% Recall = 91.2% F1-score = 94.5%	Random Forest
[28]	Fake reviews	Yes	-	Already labeled	-	No	-	-	Logistic regression
[29]	Fake reviews	No	D1:322167 D2:608598	Already labeled	Yes	Yes	No	D1. Precision = 96.93% Recall = 84.16% F1-Score = 90.09% AUC = 85.51% D2. Precision = 83,18% Recall = 77,86% F1-Score = 80,43% AUC = 81.49%	Ensemble model (Bi-LSTM, CNN, DNN)
[35]	Money laundering	Yes	-	Already labeled	-	Yes	No	-	K-means
[37]	Money laundering	Yes	496414	manually	Yes	No	Yes	AUC = 96.6% False Positive Rate = 0.97% Detection Rate = 94.2%	SVM

To contribute to the fight against financial cybercrime, the majority of the researchers present in this study had to build their own data. The size of data used in these studies varies between studies; if we exclude Aun et al. [13], He et al. [19], Suarez-Tangil et al. [20], Bello et al. [22], Zhou et al. [37], who received financing, the rest worked with small datasets. Other than Suarez-Tangil et al. [20], who made use of the website listing the fake accounts. Ram et al. [28], Mohawesh et al. [29], who made use of Yelp filtering reviews. Wahrstätter et al. [35] who made use of GraphSense tag pack, and Lansley et al. [14], who made use of an already labeled dataset collected in a previous research, the other researchers have struggled to label their data. La Morgia et al. [21] Found some suspicious events which they could not decide if it was a pump and

dump event or not, while Zhou et al. [37] had to contact the scammers directly and buy from them to confirm that they were really money launderers and detect their other accounts. The majority of studies had to deal with imbalanced datasets, while La Morgia et al. [21] chose not to split their data and used cross-validation. La Morgia et al. [21], Bello et al. [22] Reported that some of the scammers may be deleting the chat after their successful pump and dump scheme, which explains detecting only a small number of confirmed events. Suarez-Tangil et al. [20], La Morgia et al. [21], Mohawesh et al. [29], Zhou et al. [37] have made their data public as a contribution to the scientific community. Lansley et al. [14] Also made their data public in their previous research Lansley et al. [16]. All the researchers have reported successful results in detecting their respective financial cybercrimes, Suarez-Tangil et al. [20], Mohawesh et al. [29] chose to use an ensemble model that combines different models to focus on different characteristic of the criminals. Bello et al. [22], Wahrstätter et al. [35] used an unsupervised approach. Only Mohawesh et al. [29] used an explainable method to justify the decisions taken by their model.

Despite the enormous efforts made by researchers, there is still room for improvement. A small dataset or a limited number of confirmed fraud instances can affect the generalizability of the developed models. The introduction of new fraudulent instances, different from those learned by the model, can lead to a decrease in model performance. Furthermore, financial cybercrimes can be committed in various ways and on different platforms. For instance, models created to detect romance fraud on dating websites may not be as effective when applied to other platforms, such as Instagram. Most papers did not report their models' performance in terms of false positives and false negatives. Balancing model performance with false positive and negative rates is crucial when deploying the model in real-world scenarios. False alarms in financial cybercrimes, such as money laundering, can result in wasted time and resources investigating transactions or activities that are ultimately authentic. A high number of false positives may make the model impractical for deployment by financial organizations. On the other hand, for financial cybercrime such as pump and dumps, false positives can be flagged as suspicious events because they share the same characteristics as the fraudulent events. Investors are safer by avoiding putting their money in these events.

There is a lack of accessible datasets, mainly because they contain sensitive information about individuals or organizations. For example, in cases such as money laundering, where the data contains confidential transactions of individuals and organizations, access is often restricted to researchers and governmental entities. However, datasets related to financial cybercrimes, such as social engineering or fake reviews, may be publicly available with privacy considerations, such as anonymizing personal identifiers. Therefore, if researchers want to address any type of financial cybercrime locally, they will have to collect the data themselves. Labeling the data is another problem, as money laundering, romance fraud, and fake reviews detection require the assistance of different actors to label the data. Social engineering attacks and pump and dump schemes have less difficulty because it is easier to label it once you have access to the data. Financing has a great impact on the ability of researchers to collect a sizable amount of data, so the governments need to provide researchers with funding and access to more data to accelerate research in the area of financial cybercrime detection.

V. CONCLUSION

In conclusion, financial cybercrime poses a significant threat to individuals and organizations alike. Our primary objective was to conduct a comprehensive comparison of researchers' approaches to detecting five different types of financial cybercrime: social engineering, romance fraud, pump and dump schemes, fake reviews, and money laundering. By examining these specific types, our goal was to provide researchers with valuable insights to help them prioritize their efforts when using machine learning to combat financial cybercrime in their own country. This study did not cover all types of financial cybercrimes that exist. In future research, we aim to broaden the scope to include a more comprehensive range of financial cybercrimes. This will provide researchers with deeper insights and a broader perspective, enhancing their ability to combat financial cybercrimes effectively on a local scale.

REFERENCES

[1] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *J. Netw. Comput. Appl.*, vol. 68, pp. 90–113, Jun. 2016, doi: 10.1016/j.jnca.2016.04.007.

[2] M. Pejic-Bach, "Invited Paper: Profiling Intelligent Systems Applications in Fraud Detection and Prevention: Survey of Research Articles," in *2010 International Conference on Intelligent Systems, Modelling and Simulation*, Liverpool, United Kingdom: IEEE, Jan. 2010, pp. 80–85. doi: 10.1109/ISMS.2010.26.

[3] J. Nicholls, A. Kuppa, and N.-A. Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," *IEEE Access*, vol. 9, pp. 163965–163986, 2021, doi: 10.1109/ACCESS.2021.3134076.

[4] N. Odeh, D. Eleyan, and A. Eleyan, "A SURVEY OF SOCIAL ENGINEERING ATTACKS: DETECTION AND PREVENTION TOOLS," Sep. 2021.

[5] A. Bilz, L. A. Shepherd, and G. I. Johnson, "Tainted Love: a Systematic Literature Review of Online Romance Scam Research," *Interact. Comput.*, p. iwad048, Oct. 2023, doi: 10.1093/iwc/iwad048.

[6] M. J. Rajaei and Q. H. Mahmoud, "A Survey on Pump and Dump Detection in the Cryptocurrency Market Using Machine Learning," *Future Internet*, vol. 15, no. 8, p. 267, Aug. 2023, doi: 10.3390/fi15080267.

[7] L. P. Krishnan, I. Vakilinia, S. Reddivari, and S. Ahuja, "Scams and Solutions in Cryptocurrencies—A Survey Analyzing Existing Machine Learning Models," *Information*, vol. 14, no. 3, p. 171, Mar. 2023, doi: 10.3390/info14030171.

[8] R. Mohawesh *et al.*, "Fake Reviews Detection: A Survey," *IEEE Access*, vol. 9, pp. 65771–65802, 2021, doi: 10.1109/ACCESS.2021.3075573.

[9] M. Walther, T. Jakobi, S. J. Watson, and G. Stevens, "A systematic literature review about the consumers' side of fake review detection – Which cues do consumers use to determine the veracity of online user reviews?," *Comput. Hum. Behav. Rep.*, vol. 10, p. 100278, May 2023, doi: 10.1016/j.chbr.2023.100278.

[10] J. C. Rodrigues, J. T. Rodrigues, V. L. K. Gonsalves, A. U. Naik, P. Shetgaonkar, and S. Aswale, “Machine & Deep Learning Techniques for Detection of Fake Reviews: A Survey,” in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Vellore, India: IEEE, Feb. 2020, pp. 1–8. doi: 10.1109/ic-ETITE47903.2020.063.

[11] M. Alkhalili, M. H. Qutqut, and F. Almasalha, “Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering,” *IEEE Access*, vol. 9, pp. 18481–18496, 2021, doi: 10.1109/ACCESS.2021.3052313.

[12] A. Algarni, Y. Xu, Taizan Chan, and Yu-Chu Tian, “Social engineering in social networking sites: Affect-based model,” in *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, London, United Kingdom: IEEE, Dec. 2013, pp. 508–515. doi: 10.1109/ICITST.2013.6750253.

[13] Y. Aun, M.-L. Gan, N. Haliza Binti Abdul Wahab, and G. Hock Guan, “Social Engineering Attack Classifications on Social Media Using Deep Learning,” *Comput. Mater. Contin.*, vol. 74, no. 3, pp. 4917–4931, 2023, doi: 10.32604/cmc.2023.032373.

[14] M. Lansley, S. Kapetanakis, and N. Polatidis, “SEADer++ v2: Detecting Social Engineering Attacks using Natural Language Processing and Machine Learning,” in *2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, Novi Sad, Serbia: IEEE, Aug. 2020, pp. 1–6. doi: 10.1109/INISTA49547.2020.9194623.

[15] M. Bezuidenhout, F. Mouton, and H. S. Venter, “Social engineering attack detection model: SEADM,” in *2010 Information Security for South Africa*, Johannesburg, South Africa: IEEE, Aug. 2010, pp. 1–8. doi: 10.1109/ISSA.2010.5588500.

[16] M. Lansley, F. Mouton, S. Kapetanakis, and N. Polatidis, “SEADer++: social engineering attack detection in online environments using machine learning,” *J. Inf. Telecommun.*, vol. 4, no. 3, pp. 346–362, Jul. 2020, doi: 10.1080/24751839.2020.1747001.

[17] M. T. Whitty, “The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam,” *Br. J. Criminol.*, vol. 53, no. 4, pp. 665–684, Jul. 2013, doi: 10.1093/bjc/azt009.

[18] J. Huang, G. Stringhini, and P. Yong, “Quit Playing Games with My Heart: Understanding Online Dating Scams,” in *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 9148, M. Almgren, V. Gulisano, and F. Maggi, Eds., in Lecture Notes in Computer Science, vol. 9148. , Cham: Springer International Publishing, 2015, pp. 216–236. doi: 10.1007/978-3-319-20550-2_12.

[19] X. He, Q. Gong, Y. Chen, Y. Zhang, X. Wang, and X. Fu, “DatingSec: Detecting Malicious Accounts in Dating Apps Using a Content-Based Attention Network,” *IEEE Trans. Dependable Secure Comput.*, pp. 1–1, 2021, doi: 10.1109/TDSC.2021.3068307.

[20] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty, “Automatically Dismantling Online Dating Fraud,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1128–1137, Jul. 2019, doi: 10.1109/TIFS.2019.2930479.

[21] M. La Morgia, A. Mei, F. Sassi, and J. Stefa, “The Doge of Wall Street: Analysis and Detection of Pump and Dump Cryptocurrency Manipulations,” *ACM Trans. Internet Technol.*, vol. 23, no. 1, pp. 1–28, Feb. 2023, doi: 10.1145/3561300.

[22] A. S. Bello, J. Schneider, and R. Di Pietro, “LLD: A Low Latency Detection Solution to Thwart Cryptocurrency Pump & Dumps,” in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dubai, United Arab Emirates: IEEE, May 2023, pp. 1–9. doi: 10.1109/ICBC56567.2023.10174922.

[23] M. La Morgia, A. Mei, F. Sassi, and J. Stefa, “Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations,” in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, Honolulu, HI, USA: IEEE, Aug. 2020, pp. 1–9. doi: 10.1109/ICCCN49398.2020.9209660.

[24] S. Hu, Z. Zhang, S. Lu, B. He, and Z. Li, “Sequence-Based Target Coin Prediction for Cryptocurrency Pump-and-Dump,” 2022, doi: 10.48550/ARXIV.2204.12929.

[25] N. N. Ho-Dac, S. J. Carson, and W. L. Moore, “The Effects of Positive and Negative Online Customer Reviews: Do Brand Strength and Category Maturity Matter?,” *J. Mark.*, vol. 77, no. 6, pp. 37–53, Nov. 2013, doi: 10.1509/jm.11.0011.

[26] G. Pasi, M. Viviani, and A. Carton, “A Multi-Criteria Decision Making approach based on the Choquet integral for assessing the credibility of User-Generated Content,” *Inf. Sci.*, vol. 503, pp. 574–588, Nov. 2019, doi: 10.1016/j.ins.2019.07.037.

[27] E. F. Cardoso, R. M. Silva, and T. A. Almeida, “Towards automatic filtering of fake reviews,” *Neurocomputing*, vol. 309, pp. 106–116, Oct. 2018, doi: 10.1016/j.neucom.2018.04.074.

[28] N. C. S. Ram, G. Vakati, J. V. Nadimpall, Y. Sah, and S. K. Datla, “Fake Reviews Detection Using Supervised Machine Learning,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 5, pp. 3718–3727, May 2022, doi: 10.22214/ijraset.2022.43202.

[29] R. Mohawesh, S. Xu, M. Springer, Y. Jararweh, M. Al-Hawawreh, and S. Maqsood, “An explainable ensemble of multi-view deep learning model for fake review detection,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 8, p. 101644, Sep. 2023, doi: 10.1016/j.jksuci.2023.101644.

[30] S. Rayana and L. Akoglu, “Collective Opinion Spam Detection: Bridging Review Networks and Metadata,” in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Sydney NSW Australia: ACM, Aug. 2015, pp. 985–994. doi: 10.1145/2783258.2783370.

[31] J. Banks, “Online gambling and crime: a sure bet?,” *ETHICOMP J.*, 2012, Accessed: Jan. 12, 2024. [Online]. Available: https://shura.shu.ac.uk/6903/

[32] J. G. Cloward and B. L. Abarbanel, “In-Game Currencies, Skin Gambling, and the Persistent Threat of Money Laundering in Video Games,” *UNLV Gaming Law J.*, vol. 10, no. 1, Mar. 2020, [Online]. Available: https://scholars.law.unlv.edu/glj/vol10/iss1/6

[33] K. Bergman and S. Rajput, “Revealing and Concealing Bitcoin Identities: A Survey of Techniques,” in *Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Virtual Event Hong Kong: ACM, May 2021, pp. 13–24. doi: 10.1145/3457337.3457838.

[34] J. Crawford and Y. Guan, “Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy,” in *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, New York, NY, USA: IEEE, May 2020, pp. 38–45. doi: 10.1109/SADFE51007.2020.00013.

[35] A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, “Improving Cryptocurrency Crime Detection: CoinJoin Community Detection Approach,” *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 4946–4956, Nov. 2023, doi: 10.1109/TDSC.2023.3238412.

[36] B. Haslhofer, R. Stütz, M. Romiti, and R. King, “GraphSense: A General-Purpose Cryptoasset Analytics Platform,” 2021, doi: 10.48550/ARXIV.2102.13613.

[37] Y. Zhou *et al.*, “Analyzing and Detecting Money-Laundering Accounts in Online Social Networks,” *IEEE Netw.*, vol. 32, no. 3, pp. 115–121, May 2018, doi: 10.1109/MNET.2017.1700213.