Financial Fraud Detection on Social Networks Based on a Data Mining Approach

http://doi.org/10.21272/fmir.6(4).119-124.2022

Victoria Bozhenko, https://orcid.org/0000-0002-9435-0065

Ph.D., Postdoctoral Researcher, Tubingen University, Germany; Associate Professor of the Economic Cybernetics Department, Sumy State University, Ukraine

Serhii Mynenko, https://orcid.org/0000-0003-3998-9031

Assistant of the Economic Cybernetics Department, Sumy State University, Ukraine

Artem Shtefan, https://orcid.org/0000-0003-4277-3709

Student, Sumy State University, Ukraine

Corresponding author: s.minenko@uabs.sumdu.edu.ua

Abstract. *The article summarizes the arguments and counter-arguments within the scientific debate on the issue of researching financial frauds in the Internet. The main goal of the research is to develop methodological principles for identifying financial cyber fraud in social networks based on the analysis of comments to identify relevant text patterns that may indicate manipulation attempts and further fraud. The urgency of solving this scientific problem is due to the fact that the mass involvement of Internet users in social interactions in the virtual environment has contributed to the development of various criminal schemes, as well as personal data that is initially entered during registration and information that is published in social networks can be used by a fraudster to carry out illegal financial transactions. The study of the issue of identifying financial fraud in social networks in the article is carried out in the following logical sequence: collecting comments with a corresponding request under publications in the social network using the Instaloader tool; combining comments into groups based on content similarity; conducting preliminary processing of text data (decomposing the text into simpler components (tokens) and reducing similar word forms to their main dictionary form); determination of the level of similarity of text data using the cosine of similarity; building clusters of text data that can indicate the presence of signs of financial fraud under relevant comments in social networks. Instagram was chosen to identify fraudulent operations in social networks. The analysis of comments on the social network Instagram to identify text patterns showed that offers and appeals from specific groups of people and promoted in comments with the help of spam are dangerous. Based on the results of the study, it was concluded that national regulators need to strengthen public control of the Internet, as well as improve the security system at the technical level by using the latest machine learning methods to identify attempts to commit illegal actions with the subsequent imposition of sanctions on such users in social networks.*

Keywords: fraud, detection system, social media, social engineering, data mining.

JEL Classification: G4, C55.

Type of manuscript: research paper.

Received: 6.10.2022 **Accepted:** 15.11.2022 **Published:** 30.12.2022

Funding: There is no funding for this research

Publisher: Sumy State University

Cite as: Bozhenko, V., Mynenko, S. & Shtefan, A. (2022). Financial Fraud Detection on Social Networks Based on a Data Mining Approach. *Financial Markets, Institutions and Risks*, 6(4), 119-124. http://doi.org/10.21272/fmir.6(4).119-124.2022

Introduction

The popularity of social media is growing at a very high pace, and more than half of the world's population are active users of social media. Thus, according to the data of Datareportal, as of October 2022, the number of their active users is 4.74 billion, which is 59,3% relative to the population of the Earth. It is worth noting that the rate of growth is determined at +4,2% annually (*Data Reportal*, 2022).

Such widespread involvement of Internet users in social interactions in the virtual environment has contributed to the development of various criminal schemes, which are widely used by fraudsters today. Personal information that is initially entered into the registration process and information that is published on social networks can be used by a fraudster to make illegal financial transactions. In this article, the fraud is considered in the context of social engineering, which is monitored in the Ukrainian- and Russian-speaking segment of social networks, since citizens of Ukraine who become victims of fraud lose their purchasing power, which, in turn, gains mass character, negatively affects the development of the national economy and the trust in the financial sphere. According to the Eurobarometer survey, 11% of Europeans were hacked by the fraud of their social networks accounts and email accounts (in France this indicator is 20% of respondents, Austria – 16%, Luxembourg – 17%) 1.

Social engineering is a scientific study of how groups or individuals are affected by their activities, investigating the causes of different behaviors, and the environment and circumstances to which they are exposed (1, 6, 13). Our concentration on this science is dictated by the frequent use of its techniques by attackers, who seek to gain one or another benefit from their victims in social media.

In the United States, about 25% of all reported fraud losses in 2021 were caused by irrational behavior in social networks 2. Over 2017-2021 years, cyber fraud increased more than 80 times in social networks. As for the age group, in 2021, people aged 18 to 39 were twice as often reported about the loss of money due to this fraud as older people.

The spread of social media for illegal activity is explained by the relative ease of training the techniques of fraud because working with them mostly does not require powerful computer equipment or special knowledge. There are forums dedicated to this topic, where social engineers anonymously discuss the situations in which they had to act, etc., so basic skills of manipulation can be studied by any potential offender, though many contents on such websites are limited to access (*Zelenka guru*, 2022).

All of the above confirms the relevance of a deep analysis of social networks to counteract cyber fraud and money laundering in the conditions of digitization of the economy of Ukraine and social life in all its aspects.

Thus, the research aims to analyze social network comments to identify certain text templates used by community members, which may indicate attempts of manipulation by readers and further fraud. If there is a large amount of data, achieving this goal requires the use of a parser of generally available content, as well as data-mining software, to perform the task of clustering the aggregate of received records and to distinguish the most interesting, from the point of view of finding potentially fraudulent intentions.

Literature review

The modern integration of social networks in social life encourages the members of the world scientific community to do research in many aspects to study in detail the impact they have on different aspects of human activity.

Since their inception, social networks are constantly supported and updated by developers, and their capabilities become wider, including for entrepreneurs of different sizes, so Gil Appel, Lauren Grewal, Rhonda Hadi, and Andrew T. Stephen tried to forecast the future of social media in marketing research (Appel, et al., 2019); in general, having analyzed the scientific base of Scopus, we found that the role of social networks in marketing is devoted to a large number of scientific works. Matteo Cinelli, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi, and Michele Starnini studied the effect of the echo chambers in the virtual social relations environment because the urgency of the problem cannot be overestimated: Having formed a circle of like-minded people, which, under the influence of certain factors, was isolated from the external information environment, a person specifically taken may not be aware of the misperception because of the absence of views different from the consideration (Cinelli, et al., 2021). The social network as a phenomenon is, without exaggeration, one of the centers of activity of the global society; the digital hub, in which the history of the information age is generated, therefore the attention paid by scientists from the sphere of social sciences is justified.

Another component of our research is social engineering. Fatima Salahdine and Naima Kaabouch studied methods of manual or computer attacks of fraudsters with the ability to use the human propensity to trust the Internet (Salahdine & Kaabouch, 2019). It should be noted that judging by the quantitative results of the search for the bibliographic database of Scopus, this topic is paid much less attention compared to social networks (as of November 7, 2022 – 403806 references of the key "social media" against 23365 references of the key "social engineering").

Representatives of the national scientific community also consider the issue of social networks, though not so deeply, as compared to foreign colleagues. Having carried out search work according to the relevant keywords, we have found the research, which covered aspects, and corresponding problems of the present on the considered social networks. For example, Shtonda R. M., Palamarchuk N. A. And Ostrovsky S. M. social media were considered in terms of threats to Ukraine's national cyber security system: the topic is especially relevant in the current war in Ukraine, when the opponent tries to undermine the security situation inside the country, including information and digital (Shtonda, et al., 2018). Vasilyk A. V. and Ischenko O. V. studied the use of social networks by commercial organizations to attract staff, from the position of the design of company profiles in the sense of esthetics, filling content, the desire to be involved in building a particular brand, etc. (Vasilyk & Ischenko, 2018).

At this stage, in the area of Ukrainian science, social engineering is mainly considered on a basis identical to foreign research.

The phenomenon of the level of social networks that they have acquired for society, as well as their accompanying cybersecurity, needs more thorough study today, the importance of which will never be exaggerated in the future and now.

Methodology and research methods. Instagram has been chosen to identify fraudulent activities in social networks. This is due to the fact that according to the results of the research of IT company GlobalLogic, as of July 2022 this resource of social media in Ukraine has counted more than 16,1 million registered users, whereas Facebook had 15,45 million Ukrainian users in the same period (*GlobalLogic Ukraine*, 2022).

Instagram, a network of bright photo and video content, is often generated by influencers who show their bright and successful lives. Therefore, the target audience of this social network is an ambitious group of population - young people (according to the Law of Ukraine "On promoting social status and development of youth in Ukraine", young people from 14 to 35 years (*Law of Ukraine*, 2021)), on the needs of which can speculate criminals who possess skills of social engineering. With the knowledge about the social network described, the process of research was started to achieve the set goal.

Comments under posts by popular bloggers on Instagram were chosen for analysis, because, from the attacker's point of view, a well-written manipulation comment can be a starting point for a successful crime: an interested reader can write to a person who is a social engineer.

For the mass collection of comments, was used the Instaloader tool which is assigned to download publications from Instagram in full or in part (*GitHub*). It works in Python programming language; with all the features required for parsing the above-mentioned content, the work was done through the editor console of Visual Studio Code. Set of parameters, which was set for parsing: Instaloader --user-agent Mediapartners-Google --login communte88 --comments --no-pictures --no-videos --no-captures --no-metadata-json --no-profile-pic profile *profile name*.

JSON files this is a result of the collection of comments from the publications, which had the following pairs of names\values, which were interesting to us:

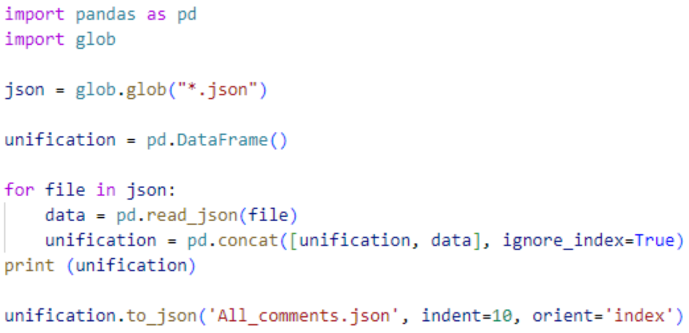
– "text" : "",

– "owner-id" : "",

– "username" : ""

The above information is sufficient to identify the particular user who has posted a comment, if necessary. It is worth noting that during the operation described, we were guided by the concept of intelligence based on open sources (OSINT). In this case, this means that the data was collected only from publications that were in public profiles, that is, the author did not need to be a subscriber to access the contents of the page.

It is best to use databases with many observations to identify similar features in the texts for clustering, so after receiving many data (762 JSON files with comments), it was decided to merge them into collections that were based on the content criterion that was published by one or another blogger. For this purpose, the software solution in Python language has been developed using the module glob to get access to the directory with all necessary files, as well as the library pandas for carrying out the consolidation of all uploaded records (Figure 1).



```
import pandas as pd
import glob

json = glob.glob("*.json")

unification = pd.DataFrame()

for file in json:
    data = pd.read_json(file)
    unification = pd.concat([unification, data], ignore_index=True)
print (unification)

unification.to_json('All_comments.json', indent=10, orient='index')
```

Figure 1. Program code for merging files

Source: Compiled by authors.

To solve the problem of clustering, "Orange Data Mining" software was chosen, which provides a wide range of tools for visualization of data analysis and machine learning (*Orange Data Mining*). By default, the given software solution does not have the tools for text mining, but developers have provided the possibility to install the necessary add-on.

Analysis of this kind requires input in the form of collections of text documents (Corpus). The Excel spreadsheet format is quite acceptable for download, so the content of the .json files that contain the collected comments was imported into the .xlsx file that was created using Excel Power Querry.

For the research needs, a model has been built, the visualization of which is shown in the figure below (Figure 2).

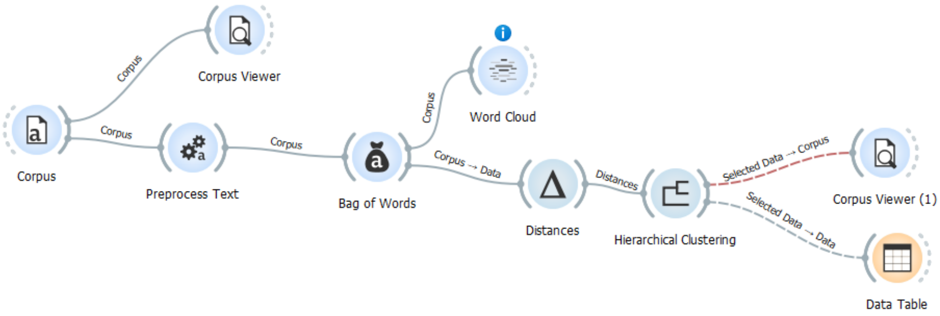


Figure 2. Model visualization for text clustering

Source: Compiled by authors.

We consider it necessary to detail the structure of this model, so we will consider each of the nodes that together form an integral system for distribution table observations on separate clusters:

- The Corpus module loads a text file containing the data for analysis.
- The Corpus Viewer allows you to view the contents of a document either immediately after it has been loaded or at any stage of the modeling process.
- The task of the Preprocess Text node is to lay out the text on the simplest components (tokens), to reduce words to the base, without subfixes or endings (stemming), as well as to bring similar word forms to their basic verbal form (lemmatization). This tool allows you to translate all text into lowercase letters, remove punctuation marks and graphic elements in the form of emojis, set stop words, etc. Thus, artificial intelligence will be able to work with the investigated data mass.
- Bag of words allows you to draw words contained in the observation in the form of numbers. Thus, you can determine the similarity of expressions, using the next step of the Distances node.
- The work of the Distances tool is to calculating the distance between rows or columns in the data set. The distance between the records prepared for this process was calculated using a cosine of similarity (a

cosine of the angle between the two vectors of the space of the loaded document), which gives an estimate: how two observations are similar among themselves (where -1 - records have different topics; 1 - records are identical).

➢ Word Cloud is a tool that allows you to view the cloud of the most used words in the aggregate of text, which helps to define the subject of the texts from the file. Placing it after Preprocess Text says that the cloud is cleared of all non-informative elements.

The Hierarchical Clustering widget performs hierarchical clustering of data based on distance matrices and creates a corresponding dendrogram with which to interact. Connected to the reviewed Corpus Viewer node allows for investigation of a specific cluster selected. The tools and methods used in the research process have allowed us to obtain the results described below.

Results

Within the framework of our research, we were interested in blogs related to the following segments of activity: bookmakers' companies, entertainment or life blogs, as well as content about investments and finance.

Sports betting acts on the emotional state of some people, causing nervous anxiety from the prediction of winning a team. After conducting search work in this direction it is found that registered and accordingly executed accounts in Instagram have only the function of arbitration traffic in Telegram channels: there are no attempts of interaction with the audience; all the posts of channels have tags with pseudonyms of the mentioned messenger; the profile header contains keywords for better ranking in the search engine of the social network and a link that focuses attention on.

In such profiles, there is almost no sign of users activity (no data for further analysis), because a large share of subscribers is growing artificially - with the help of bots. The result of the research of this category of blogs: possible fraudulent manipulations, connected with the excitement of citizens about sports events, not spread in the considered social network; resources used for criminal purposes, mostly, are in the Telegram messenger, which is not in the area of interests of this research.

Bloggers who tell about their bright life often form an audience who wants to start earning too much money by example a content creator, while not making much effort to achieve this goal. Among the comments gathered under the posts of such bloggers, we managed to separate a cluster that contains a very concentrated number of spam, compared to other groups. Of course, there are many identical or similar comments under posts, but often they have a goal to simply draw the attention of their idol.

In the course of a study of the category of financial bloggers, it was revealed that their target audience is often mothers on maternity leave, who are looking for methods of passive source of income. Users from this cohort are already more conscious; it is noticeable that their thoughts are given by one finished comment. We note that the number of comments under the posts of popular authors in this direction, mostly, is not so large, compared to the previously considered category, spam is almost absent. We assume that such bloggers have moderators who are engaged in clearing spam and, in general, suspicious texts.

The result of the analysis can be formalized as follows: caring, including its reputation, financial bloggers are engaged in moderation of comments, preventing fraudulent manipulation, spam, etc. At this stage, having achieved the objective of the study, it is necessary to draw conclusions and propose recommendations to interested parties.

Conclusions

The analysis of comments on the Instagram social network to identify text templates used by community members that may indicate attempts by readers to manipulate and further fraud showed:

➢ not in all the niches the social engineer can be carried out crimes within the social network, because in some information directions in Instagram simply no interaction with the potential target audience.

➢ those suggestions and appeals that are very interesting for both specific groups of people and the public, and are promoted in comments by spam, are dangerous.

➢ some blogger groups that teach their audience complex things and have a high level of responsibility are involved in checking, including comments on suspicious texts published by other users, spam, etc.

Accordingly, readers of Instagram and other social networks are worth trying to critically assess the appeals and proposals that can easily solve their actual problems, as fraudsters exploit very desirable things by a person to obtain benefits at the expense of others. Bloggers need to take care of the trust in their publications and their reputation, in general, therefore it is necessary to ensure the maximum security of their subscribers. To do this, first of all, it is necessary to control the discussion inside the community. The State Service for Special Communication and Information Protection of Ukraine should further improve public control over the Internet, in particular, in social networks, to prevent individual incidents of cyber fraud from spreading, becoming a mass phenomenon, which may negatively affect the social situation within the country. Meta company needs to improve its security system at the technical level by developing and improving neural networks that can detect attempts to commit illegal actions and further impose sanctions on these Instagram users.

Funding: This research was funded by a grant from the Ministry of Education and Science of Ukraine (No. s/r 0121U100467, 0122U000783).

References

1. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt. DUT. [Information and cyber security: socio-technical aspect. DUT] (in Ukrainian) [Link]

2. Vasylyk, A. V., & Ishchenko, O. V. (2018). Vykorystannia sotsialnykh merezh u suchasnomu rekrutynhu Ukrainy. [Vasylyk, A. V., & Ishchenko, O. V. (2018). Use of social networks in modern recruiting of Ukraine] Ekonomichnyi prostir, 131, 53–63. (in Ukrainian) [Link]

3. Vtracheni mozhlyvosti: ukraintsi nadaiut bilshu perevahu rozvazhalnym sotsmerezham, nizh profesiinomu LinkedIn. [Missed opportunities: Ukrainians give more preference to entertainment social networks than to professional LinkedIn] GlobalLogic Ukraine. (in Ukrainian) [Link]

4. Pro spryiannia sotsialnomu stanovlenniu ta rozvytku molodi v Ukraini, Zakon Ukrainy No. 2998-XII (2021) (Ukraina). [On promoting the social formation and development of youth in Ukraine, Law of Ukraine No. 2998-XII (2021) (Ukraine)] (in Ukrainian) [Link]

5. Sposoby manipulyatsii fpazami. [Phrase manipulation methods] (n.d.). Zelenka.guru. (in Russian) [Link]

6. Tykhomyrova, Ye. (2021). Sotsialna inzheneriia. [Tikhomirova, E. (2021). Social engineering]. In *Advances in Technology and Science*, 225–228. Library of Congress Cataloging-in-Publication Data. (in Ukrainian) [Link]

7. Shtonda, R. M., Palamarchuk, N. A., & Ostrovskyi, S. M. (2018). Sotsialni merezhi v interneti yak instrument zahrozy natsionalnii systemi kiberbezpeky Ukrainy. Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy, 190–192. Natsionalna akademiia Sluzhby bezpeky Ukrainy. [Social networks on the Internet as a tool of threat to the national cyber security system of Ukraine. Actual problems of state information security management, 190–192. National Academy of the Security Service of Ukraine] (in Ukrainian) [Link]

8. Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2019). The future of social media in marketing. *Journal of the Academy of Marketing Science*, *48*(1), 79–95. [Link]

9. Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, *118*(9), Article e2023301118. [Link]

10. *Data Mining*. (n.d.). Orange Data Mining - Data Mining. [Link]

11. *The Global State of Digital in October 2022 – DataReportal – Global Digital Insights*. (n.d.). DataReportal – Global Digital Insights. [Link]

12. *Instaloader – Download Instagram Photos and Metadata*. (n.d.). Instaloader — Download Instagram Photos and Metadata. [Link]

13. Jakobsson, M. (2016). *Understanding Social Engineering Based Scams*. Springer New York, NY. [Link]

14. Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. [Link]