International Journal of Advances in
Soft Computing and Intelligent Systems (IJASCIS)
2022, Vol 02, No 01, 01-06

Science Transactions © 2022

Original Paper

A SURVEY ON FAKE PROFILE DECEPTION DETECTION ON SOCIAL MEDIA

Maulik Shah[1] and Hiren Joshi[2]
1 Department of computer science, Gujarat university,
Ahmedabad, India
2 Department of computer science, Gujarat university,
Ahmedabad, India

Abstract

Social media were growing unexpectedly and turn out to be essential factors of many humans' lives. Meanwhile, social media have become a main source for identity deception. From last decades cybercrime on fake profiles has been raised enormously. Current studies had been performed to save you and locate identity deception. This survey provides different deception techniques opted by the authors, categorized from fake profile, profile cloning, fake news, fake identity and so on. This survey provides an in depth evaluate of social media identity deception detection strategies. It also identifies the main research area for the future safety of people on social network. This newsletter is expected to benefit each researcher and social media providers.7y bb'

Keywords

Cyber Security, social media, Identity deception, Fake profile, social Bot.

1. INTRODUCTION

Social networking is the website where every person can have profile and can meet virtually with other person on the website. Each user has unique identity profile on Online Social Network (OSN), which provide communication platform among the users. The user used the social media called as an active user and can communicate with other person by medium of chats, review, comments and likes. Social networking websites are growing rapidly and converting the manner people maintain in contact with each other. This leads to fake profile generation to communicate with people and make fraud over the internet. Social media only require a verified e-mail address to sign up a new account and create a personalized profile [1]. The principal issue is that the facts given in the registration method does now not challenge to any verification method. Therefore, a user can pretend to be a person else with the purpose of deceiving different user. Social media identification deception can possible without any problem. The aim of this research paper is to focus on literature review of papers having worked on detection of fake profiles on social media. We have studied more than 20 papers for the same and try to find out the research gap and resolve it by the more suitable and efficient methodologies as of the future research work to be carried out. Authors have analysed research articles on fake profile detection on social media between the time periods of 2014 to 2022 and represent the interpretation of 21 research papers on the topic. The main sources of articles are the Google scholar and Scopus journals. Social networks are the friendly communication build over the web using computer network among people as political whole carrying comparable interests or have universal cultures etc. User produce content and it is spread over the network in form of text, image, video, audio etc. Some of the social media platforms of current time are Interest, Twitter, Facebook, Snapchat, Google+, Instagram and LinkedIn. Survey [2] represents the reports that there are around 2.93 billion monthly active users in first quarter of the year 2022 at Facebook site. Facebook became the most used online social network

over the world, which exceeded two billion active consumers in the 2nd area of 2017(80% of them 35 years or older), taking simply over 13 years to attain this milestone. In contradict. Metaowned Instagram took 11.2 years and YouTube of Google took just over 14 years to reap this benchmark. The female user is 12.8%. Instagram, Snapchat, LinkedIn has 250+ million monthly active users [3].

Social profiles are an outline of people's social characteristics that uniquely identify them on social media websites including Facebook, LinkedIn etc. Profiles describe any range of characteristics approximately about the individuals, including his or her hobbies, knowledge; expertise affiliations, fame, current interest and its geographic place. Whereas, a fake profile is the illustration of someone, organization or enterprise that does not exist in real world, but make fake existence on social media platforms. These accounts owed often use names and identities that aren't only actual but also supposed to gain extra access to particular people and audiences. These accounts are used to hide the identity of the individual even as sending abusive or threatening messages, impersonating him or her in an try and damage his or her reputation or to purpose misery or to mislead his or her friends and family by means of contacting the victim profile to trick them into conducting malicious content material.

2. Literature Survey

Adikari & Dutta et al. [4] present the work on identifications of fake LinkedIn profiles by data mining approach. They used methods like Neural Network (NN), Support Vector Machine and weighted average (WA) are applied on the limited profiles only. The author got 84% accuracy in fake profile detection and 94% negative rate. Whereas, NN method found to be more suitable and efficient on large number of profiles data set, also the WA method can jointly use with another data mining analysis method for better result.

Fire et al. [5] introduced software named Social Privacy Protector (SPP) to increase the Facebook user's security. SPP is the three-layer architecture; with distinguish working of each layer for the privacy of the user's profile. The working of software is to alarm the user about which friend request to be accepted or rejected. The work can more enhanced with the supervised and unsupervised learning approach for the better reliability of the software quality.

Gurajala et al. [6] make use of crawler for fake profiles detections of Twitter account, and analyze more than 62 million user's account and their characteristics for fake account creation. The ground truth images have higher diversity than the URLs of fake profile set. The work is only identifying the small percentage of fake profile accounts.

The work can be enhanced with large number of profiles data sets as of future enhancement.

Minimum attributes have been introduced by Elazab and Mahmoud et al [7] for detection of fake account on Online Social Network. The five classification algorithms have been applied and the outcome of them is tested, and also tests the accuracy of the work with other researcher's approach.

Tiwari et al [8] depict the working of Bot detection and impact of machine learning in fake profile detection. But the content-based technique can be making more efficient effects on working on identification of fake profiles in online social network.

Singh et al [9] likewise purpose a machine learning approach which helps in finding the fake bot account created by human being on social media platform. It was possible by identifying the frinds list and from the followers list.

Ramalingam et al. [10] has introduced many historical approaches for fake profile detection methodlogies. But furtherfore it seems that some fast-growing techniques like Hadoop or spark need to be used as a part of the solution for large amount of unstructured data of the online social network for the security of the user profiles.

Mohammadrezaei et al [11] depict the Synthetic Minority Oversampling Technique (SMOTE) algorithm and they applied it on sample training data sets. The data sets were trained and validated using cross-validation technique. The technique has limitations on categorization of profile as legitimate or fake account.

Shama Sk et al [12] go for neural network and random forest for predictions of fake profiles on social networks, the algorithm gives 93% accurate results. The author suggests the work can be undertaken by natural language processing techniques for more accuracy and efficiency.

Kotawadekar, R.V. et al. [13] depict the classification steps for fake profile identifications, also the author suggested to work with natural language processing system. It shows the Natural language processing can make significant participation in fake profile detection.

Dey et al. [14] proposed used of two methods Logistic Regression and Random Forest algorithms to detect the fake user profiles in Instagram network. They acquire around 92% accuracy in the algorithm work, which seems highest accuracy than the previous works. The data was preprocessed before algorithm implantation.

Safieddine et al. [15] reviews that Facebook has rolled out a coverage that calls for businesses and individuals actively promoting political activities and commercials to go through identity verification. The article suggests the id check in Facebook to reduce Russian's interference in European elections and education to manage the 2020 US election. For the policy to paintings, the social media platform is the usage of algorithms and AI to become aware of capacity false profiles.

Some wonderful work has been carried out by Pulido et al [16], which depict how fake profiles used to spread the fake news regarding health issued in the world and transformation dimensions of those fake news based on social effects. That creates the hypo between the users of social network sites. They also analyzed the impact of this news on people, categorized as positive or negative. The social impact in social media (SISM) methodology was introduced and used to differentiate the original and fake health news on social media platform.

Pourghomi et al [17] undertook the task of measurement of working of Facebook algorithm of fake profile identifications. The accuracy has been achieved from 3 weeks to 3 days decreasingly in timings. But the other hand this algorithm has question regarding the sharing of confidential id on social media platform. The paper recognizes that the test is the most effective consultant of 1 test with many variables. The capability to manipulate a number of these variables proved to be much less effective in figuring out what triggers an algorithm to identify false profiles. In our opinion, the mixture of faux profile photo, not being selective in building friendships, lack of friendship behaviors which includes likes and feedback from pals and therefore now not having displayed characteristics of human networking are maximum possibly the control variables of the AI algorithm that could be examined in destiny research. A lot of these variables are tough to faux as a character but may be feasible to fake as cyber Bot institution. Facebook and other systems are not probably to provide personal facts approximately the manner their algorithms perform in identifying fake users.

The research project of Mazhar Javed Awan et al. [18] consists of Spark Machine learning libraries together with Random Forest Classifier and other plotting tools. The proposed model was described and results were represented in graphical representation in form of confusion matrix, curve knowledge and ROC plots. The author got 93% accuracy in proposed model and 7% failures in finding the false fake profiles.

Kaur et al [19] consider the machine learning algorithms for fake profile detection. The user taken algorithms are support vector machine (SVM), Neural Network and Random Forest, author found neural network most accurate and suitable for undertaken work among all of them. Vivek solvande et al [20] introduced the framework for fake profile detection.

In Tejaswini S Patil et al [21], the author presents a comprehensive study on distribution of fake and real profiles in online social network. The decision tree techniques made actual

use for the proposed work. Study depicts that whenever the binary separation is required the decision tree technique become more helpful.

3. Conclusion

The trend of usage of social media is a never-ending process and in fact, it is increasing day by day in areas of business, markets, and social people communication. As people find it common medium of communication, the security issues related to it is also increasing in term of fake profile creation and fake news deception. More and more personal details are now available and included on websites, which causing numerous content to be available for the manipulation. In this paper, we reviewed various methods available for fake profile identifications and its causes. The survey provided a comprehensive evolution of critical strategies for fake profile detection in OSNs. We conclude that, regardless of severe present schemes, there is nonetheless no systematic answer for fake profile detection in OSNs which could offer efficient, fast and reliable popularity of user information.

4. Future work

The fake identification is rapidly increased on the Online Social Network (OSN). The false profiles publish fake comments, fake news and fake reviews. The researchers are constantly working on reducing these issues if no longer getting rid of this large trouble on social networks and non-stop enhancement in artificial intelligence and capabilities used to limit this issue and enhance more security in the social networks.

5. References

1. Bahri, L., Carminati, B., & Ferrari, E. (2018). Knowledge-based approaches for identity management in online social networks. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8(5), e1260.
2. Reports on Monthly Active users on Facebook worldwide at https://www.statista.com/statistics/
3. Social Media comparison Info graphic at https://www.leveragestl.com/social-media-infographic/
4. Adikari, S., & Dutta, K. (2014). Identifying fake profiles in linkedin. Proceedings - Pacific Asia Conference on Information Systems, PACIS 2014, 1–30.
5. Fire, M., Kagan, D., Elyashar, A., & Elovici, Y. (2014). Friend or foe? Fake profile identification in online social networks. Social Network Analysis and Mining, 4(1), 1–23. https://doi.org/10.1007/s13278-014-0194-4.
6. Gurajala, Supraja, Joshua S. White, Brian Hudson, and Jeanna N. Matthews. 2015. “Fake Twitter Accounts: Profile Characteristics Obtained Using an Activity-Based Pattern Detection Approach.” ACM International Conference Proceeding Series 2015-July: 1–7.
7. Elazab, Ahmed, and Mahmoud A Mahmoud. 2016. “Fake accounts detection in twitter based on minimum weighted feature”, World.
8. Tiwari, Vijay. 2017. “Analysis and Detection of Fake Profile over Social Network.” Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017 2017-Janua: 175–79.
9. Singh, Naman, Tushar Sharma, Abha Thakral, and Tanupriya Choudhury. 2018. “Detection of Fake Profile in Online Social Networks Using Machine Learning.” Proceedings on 2018 International Conference on Advances in Computing and Communication Engineering, ICACCE 2018: 231–34.

10. Ramalingam, Devakunchari, and Valliyammai Chinnaiah. 2018. “Fake Profile Detection Techniques in Large-Scale Online Social Networks: A Comprehensive Review.” Computers and Electrical Engineering 65: 165–77.
11. Mohammadrezaei, Mohammadreza, Mohammad Ebrahim Shiri, and Amir Masoud Rahmani. 2018. “Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms.” Security and Communication Networks 2018. [12]
12. Shama, Sk, K Siva Nandini, P Bhavya Anjali, and K Devi Manaswi. 2019. “Fake Profile Identification in Online Social Networks.” International Journal of Recent Technology and Engineering 8(4): 11190–94.
13. Kotawadekar, R.V., A.S. Kamble, and S.A. Surve. 2019. “Automatic Detection of Fake Profiles in Online Social Networks.” International Journal of Computer Sciences and Engineering 7(7): 40–45. [14]
14. Dey, Ananya, Hamsashree Reddy, Manjistha Dey, and Niharika Sinha. 2019. “Detection of Fake Accounts in Instagram Using Machine Learning.” International Journal of Computer Science and Information Technology 11(5): 83–90.
15. Pourghomi, P., Dordevic, M., & Safieddine, F. (2020). Facebook fake profile identification: technical and ethical considerations. International Journal of Pervasive Computing and Communications. The Conversation, available at: https://theconversation.com/facebookwants-to-combat-fake-news-with-id checks-with-grave-implications-for-our-privacy116569 (accessed 26 May 2019).
16. Pulido, Cristina M., Laura Ruiz-Eugenio, Gisela Redondo-Sama, and Beatriz Villarejo-Carballido. 2020. “A New Application of Social Impact in Social Media for Overcoming Fake
17. News in Health.” International Journal of Environmental Research and Public Health 17(7).
18. Pourghomi, Pardis, Milan Dordevic, and Fadi Safieddine. 2020. “Facebook Fake Profile Identification: Technical and Ethical Considerations.” International Journal of Pervasive Computing and Communications 16(1): 101–12.
19. Mazhar Javed Awan, Muhammad Asad Khan Zain Khalid Ansari Awais Yasin Hafiz Muhammad Faisal Shehzad. 2021. “Fake Profile Recognition Using Big Data Analytics in Social Media Platforms” International Journal Computer Applications in Technology
20. Kaur, Er. Ashpreet, and Dr. Abhinav Bhandari. 2021. “FAKE SOCIAL PROFILE
21. DETECTION Volume X Issue VI JUNE 2021 Volume X Issue VI JUNE 2021.” X(Vi): 246–52.
22. Vivek Solvande, Vaishnavi Ambolkar, Siddhesh Birmole, Divya Gawas, Dnyanada Juvale. 2021. “IRJET- Fake Profile Identification Using Machine Learning Algorithm.” Irjet 8(4): 60–65.
23. Tejaswini S. Patil, Siddhali A More, Trupti V Todkar, Divya Chirayil 2021. “IRJET – Social Media Fake Profile Detection” Irje, 8(5): 670-73.

Authors

Mr. Maulik Shah

Mr. Maulik Shah is an Ahmedabad-based research scholar at Gujarat University (India). From Veer Narmad South Gujarat University, he earned his M.C.A. He has more than 8 years of experience in the field. Throughout his M.C.A., he worked on several research projects. His areas of interest in research include IoT, blockchain, and cyber security.

Prof. Dr. Hiren Joshi

Prof. Dr. Hiren Joshi is working as a professor of computer science at Dept. of Computer Science, Gujarat University. He has more than 2 decade (20 + years) experience in academic. He has published and presented 30+ research papers in reputed national and international journals. He has written 3 books. He has written 3 chapters in editorial book of national and international publishers. He has served as Ph.D. research supervisor in many universities. He has provided his services as resource person in HRDC in various Universities. He is serving as member of Board of Studies in various universities in Gujarat and other states of India. He has served as NAAC peer team co-ordinator and NAAC peer team member. He has worked as resource person for various programs recorded and broadcasted on DD Girnar and SANDHAN (Live Television Lecture Series from BISAG – Gandhinagar) and in C2C (College to Career program organized by Govt. of Gujarat and Microsoft, telecast by BISAG). He has developed an e-Content on Web Application Development paper for e-PG Pathshala which is an Ministry of Education (MoE) project under NME-ICT initiative. He is a professional member ACM Gandhinagar chapter, CSI Life member and other professional bodies.