International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-2 (April 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.2.33

A Literature Review on Automatic Detection of Fake Profile

Faisal Farooqui[1] and Muhammed Usman Khan[2]
[1]PG Student, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA
[2]Assistant Professor, Department of Computer Science and Engineering, Integral University, Lucknow, INDIA

[1]Corresponding Author: faisalfarooqui007@gmail.com

Received: 27-03-2023 **Revised:** 10-04-2023 **Accepted:** 30-04-2023

ABSTRACT

In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake profiles, online impersonation have also grown. There is no feasible solution exist to control these problems. In this project, we came up with a framework with which automatic detection of fake profiles is possible and is efficient. This framework uses classification techniques like Support Vector Machine, Nave Bayes and Decision trees to classify the profiles into fake or genuine classes. As, this is an automatic detection method, it can be applied easily by online social networks which has millions of profile whose profiles cannot be examined manually.

***Keywords*--** Social Networking, Social Engineering, Social Bots

I. INTRODUCTION

Automatic detection of fake profiles can be challenging as fraudsters often use sophisticated techniques to create fake profiles that are difficult to distinguish from real ones. However, here are some common methods that can be used to detect fake profiles automatically[1].

Profile Completeness: One of the simplest methods to detect a fake profile is to check if the profile is complete or not. A complete profile with a profile picture, contact information, and a detailed bio is more likely to be genuine than an incomplete one[2].

Activity Level: Another factor to consider is the activity level of the profile. If the profile has been inactive for a long time or has no recent activity, it could be a fake one.

Profile Picture: Another common technique used by fraudsters is to use stolen images as their profile picture. Tools like reverse image search can help identify whether the profile picture is original or stolen.

Network Analysis: Another effective way to detect fake profiles is to analyze the network of connections. If a profile has a large number of connections, but all of them have incomplete or fake profiles, it is more likely to be fake[3].

Natural Language Processing: Advanced techniques like natural language processing can also be used to analyze the language used in the profile description and messages. Fake profiles often use generic or repetitive language that can be identified using machine learning algorithms.

IP Address Analysis: Another method is to analyze the IP address of the device used to create the profile. If the IP address is located in a different country or region than the one claimed in the profile, it could be a red flag.

These methods can be combined to create a more effective fraud detection system that can automatically identify and flag fake profiles. However, it is important to note that no method is foolproof, and manual verification may be required in some cases [4].

II. SOCIAL ENGINEERING USED FOR FAKE PROFILE DETECTION

Social engineering techniques can be used to detect fake profiles on social media platforms. Social engineering is the art of manipulating people to gain access to information or resources that are normally protected. Here are some ways social engineering can be used for fake profile detection[5].

Phishing: Phishing is a technique where fraudsters send an email or message that appears to be from a legitimate source but is actually a fake one. By sending a phishing message to the suspected fake profile, one can identify if the account is genuine or not. If the message bounces back or there is no response, it could be an indication of a fake profile.

Social Engineering Interviews: Social engineering interviews involve contacting the suspected fake profile and asking them questions about their personal and professional background. This can help identify if the

profile is genuine or not. If the person is unable to provide satisfactory answers or the information provided does not match with the details in the profile, it could be a fake one.

Fake Profile Creation: In some cases, social engineering can be used to create a fake profile and add the suspected fake profile as a connection. This can help gather more information about the person and identify if the profile is genuine or not[6]

Reverse Social Engineering: Reverse social engineering involves creating a fake persona and attempting to engage with the suspected fake profile. This can help identify if the profile is genuine or not based on the responses received[7].

It is important to note that social engineering techniques should only be used for legitimate and ethical purposes, and it should not be used to gain unauthorized access to personal or sensitive information. Additionally, it is recommended to seek legal advice before using social engineering techniques for fake profile detection

III. ONLINE IMPERSONATION TO DEFAME A PERSON

Online impersonation can be a serious offense, particularly if it is done to defame or harass an individual. Online impersonation refers to the act of creating a fake profile or account on social media or other online platforms using someone else's identity or personal information, with the intent to deceive others[8].

Report the Impersonation: The first step is to report the impersonation to the relevant social media platform or website. Most social media platforms have a reporting mechanism that allows users to report impersonation or fake profiles. The platform will then investigate the report and take appropriate action.

Document Evidence: It is important to document all evidence of the impersonation, including screenshots of the fake profile, any messages or posts made by the impersonator, and any other relevant information that could be used as evidence.

Contact the Authorities: If the impersonation is serious or involves threats or harassment, it is recommended to contact the authorities. Depending on the jurisdiction, online impersonation can be considered a criminal offense, and the impersonator could face legal action.

Contact the Affected Individual's Friends and Family: It is recommended to inform the affected individual's friends and family about the impersonation, so that they are aware of the situation and can support the affected individual.

Seek Legal Advice: If the impersonation has caused significant harm or damage, it may be necessary to seek legal advice from a lawyer who specializes in online defamation and harassment.

It is important to take swift action if someone is impersonating another person online to defame them. Delaying action could result in further harm to the affected individual's reputation and well-being [9]

IV. ON LINE ARTIFICIAL TECHNIQUE USED TO DETECT THE FAKE PROFILE

There are various artificial intelligence (AI) techniques that can be used to detect fake profiles online. Some common techniques are:

Machine Learning: Machine learning algorithms can be used to analyze patterns in user behavior and identify fake profiles based on deviations from normal behavior. For example, machine learning models can be trained to detect abnormal posting frequency, atypical login times, or unusual network connections[9].

Natural Language Processing (NLP): NLP techniques can be used to analyze the language used in the profile description, posts, and messages. By comparing the language used in the suspected fake profile with that of a large database of genuine profiles, NLP models can identify anomalies and flag them as fake profiles.

Image Recognition: Image recognition algorithms can be used to identify fake profile pictures. By comparing the profile picture to a large database of images, image recognition models can detect if the picture is a stock image or has been stolen from another website[10].

Network Analysis: Network analysis techniques can be used to detect patterns in user connections and identify fake profiles based on their connections. For example, network analysis models can be used to detect suspiciously high levels of connections to fake profiles, or to identify clusters of fake profiles that are all connected to each other.

Social Engineering Simulations: AI-powered social engineering simulations can be used to test the effectiveness of anti-fraud measures and detect fake profiles. By creating a simulated environment and introducing fake profiles into the network, organizations can evaluate their detection systems and improve them over time.

These AI techniques can be combined with human oversight and intervention to create more effective fraud detection systems. However, it is important to note that these techniques are not foolproof and should be used in conjunction with other fraud prevention measures, such as two-factor authentication and strong password policies[11].

V. SYSTEM LOAD BALANCING WHILE FAKE PROFILE DETECTION

System load balancing is an important consideration when implementing fake profile detection techniques, especially for large social media platforms that may have millions or even billions of users. The detection process can be computationally intensive, and as a result, it can put a strain on the system's resources[12].

Load balancing techniques can be used to distribute the detection workload across multiple servers, improving system performance and reducing the risk of overload. Here are some load balancing techniques that can be used for fake profile detection:

Round-robin Load Balancing: In round-robin load balancing, incoming requests are evenly distributed across a pool of servers in a cyclic manner. This method ensures that each server receives an equal number of requests over time, reducing the risk of overload.

Weighted Load Balancing: In weighted load balancing, each server is assigned a weight that reflects its processing power. Incoming requests are then distributed to the servers based on their weight. This method ensures that more powerful servers receive a larger share of the workload, improving overall system performance[13].

Least-Connection Load Balancing: In least-connection load balancing, incoming requests are directed to the server with the fewest active connections at the time. This method ensures that the workload is evenly distributed across the servers, reducing the risk of overload.

Dynamic Load Balancing: In dynamic load balancing, the system continuously monitors server performance and adjusts the workload distribution based on current conditions. This method ensures that the workload is always distributed optimally; improving system performance and reducing the risk of overload [14].

Implementing load balancing techniques can help ensure that the system can handle the computational demands of fake profile detection while maintaining optimal performance. It is important to choose the load balancing technique that best fits the specific needs of the system and to monitor the system's performance regularly to ensure that it is operating effectively.

VI. BLOCK CHAIN TECHNOLOGY IN ARTIFICIAL INTELLIGENCE FOR FAKE PROFILE DETECTION

Blockchain technology and artificial intelligence (AI) can be used together for various applications, including fake profile detection. Blockchain is a distributed ledger technology that allows for secure and transparent storage and sharing of data. By combining blockchain with AI, it is possible to create a decentralized, secure, and reliable system for detecting fake profiles[11].

Secure Data Sharing: Blockchain provides a secure and transparent platform for sharing data between different stakeholders, including social media platforms, law enforcement agencies, and users. By using a blockchain-based platform, it is possible to securely share data on fake profiles while protecting users' privacy and preventing data breaches.

Decentralized Identity Verification: Blockchain-based identity verification systems can be used to ensure that users are who they claim to be. By creating a decentralized system that verifies user identities using blockchain, it is possible to reduce the risk of fake profiles[12].

Smart Contracts: Smart contracts can be used to automate the process of fake profile detection. By using AI algorithms to analyze user behavior and detect fake profiles, smart contracts can automatically trigger actions such as suspending the account or notifying law enforcement agencies.

Immutable Records: Blockchain provides an immutable record of all transactions, making it possible to track the creation and activity of fake profiles over time. By analyzing the data stored in the blockchain, AI algorithms can identify patterns of behavior that are indicative of fake profiles.

Incentivization: Blockchain- based incentivization systems can be used to encourage users to report fake profiles. By rewarding users who report fake profiles with tokens or other incentives, it is possible to create a self-regulating system that encourages users to participate in fake profile detection.

VII. SECURITY CONCERN IN FAKE PROFILE DETECTIONS

Fake profile detection raises several security concerns, especially in the context of social media platforms where personal information is shared and stored. Here are some of the key security concerns that need to be addressed when implementing fake profile detection techniques:

Privacy Violations: Fake profile detection techniques may involve collecting and analyzing personal information, such as user behavior and location data. It is essential to ensure that user privacy is protected and that personal information is not misused or shared with third parties without user consent

Data Breaches: The collection and storage of user data for fake profile detection purposes can create a potential target for hackers and cybercriminals. To mitigate this risk, it is crucial to implement robust security

measures, such as encryption and access controls, to protect user data.

System Vulnerabilities: The detection algorithms themselves may be subject to manipulation or attack, either by malicious actors or by unintentional errors in the system. It is crucial to implement regular security audits and testing to ensure that the system is robust and secure against potential threats[15].

Implementing fake profile detection techniques requires careful consideration of security and privacy concerns to ensure that user data is protected, and the system is secure and transparent. By addressing these concerns, social media platforms can improve their ability to detect and prevent the creation of fake profiles, which is critical to maintaining a safe and trustworthy online environment.

VIII. CONCLUSION

Fake profile detection is an essential process to maintain the safety and integrity of online platforms, especially social media. The rise of fake profiles has become a serious concern as they can be used for malicious activities, such as spreading false information, cyberbullying, and online fraud. Artificial intelligence and machine learning algorithms have proven to be effective in detecting fake profiles, as they can analyze large amounts of data and identify patterns of behavior that indicate a profile may be fake. Additionally, social engineering techniques, such as social graph analysis and linguistic analysis, can also help detect fake profiles. However, the detection of fake profiles requires a careful balance between accuracy, privacy, and security. False positives can harm legitimate users, and user privacy must be protected. Therefore, a combination of techniques, such as machine learning, social engineering, and user reports, can provide a more accurate and robust approach to fake profile detection. Furthermore, the use of blockchain technology can enhance the security and transparency of the fake profile detection system. Blockchain can provide a decentralized, secure, and transparent platform for data sharing, identity verification, and smart contracts, which can automate the fake profile detection process

REFERENCES

[1] Khan, W. & Haroon, M. (2022). An efficient framework for anomaly detection in attributed social networks. *International Journal of Information Technology*, *14*(6), 3069-3076.

[2] Khan, W. & Haroon, M. (2022). An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks. *International Journal of Cognitive Computing in Engineering*, *3*, 153-160.

[3] Khan, N. & Haroon, M. (2022). Comparative study of various crowd detection and classification methods for safety control system. *Available at: SSRN 4146666*.

[4] Khan, W. (2021). An exhaustive review on state-of-the-art techniques for anomaly detection on attributed networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 6707-6722.

[5] S. Srivastava, M. Haroon & A. Bajaj. (2013). Web document information extraction using class attribute approach. *4th International Conference on Computer and Communication Technology (ICCCT), Allahabad, India*, pp. 17-22, DOI: 10.1109/ICCCT.2013.6749596.

[6] Husain, Mohammad Salman. (2020). A review of information security from consumer's perspective especially in online transactions. *International Journal of Engineering and Management Research*, *10*(4). Available at SSRN: https://ssrn.com/abstract=3669577.

[7] Haroon, M., Husain, M., Tripathi, M. M., Ahmad, T. & Kumari, V. (2010). Server controlled mobile agent. *International Journal of Computer Applications*, *975*, 8887.

[8] Husain, M. S. & Haroon, D. (2020). An enriched information security framework from various attacks in the IoT. *International Journal of Innovative Research in Computer Science & Technology*.

[9] Siddiqui, Z. A. & Haroon, M. (2022). Application of artificial intelligence and machine learning in blockchain technology. In: *Artificial Intelligence and Machine Learning for EDGE Computing*, pp. 169-185.

[10] Tripathi, M. M., Haroon, M., Jafar, M. & Jain, M. (2010). Maxillofacial surgery using x-ray based face recognition by elastic bunch graph matching. In: *Contemporary Computing: Third International Conference, IC3 2010*, pp. 183-193. Springer.

[11] Siddiqui, Z. A. & Haroon, M. (2023). Research on significant factors affecting adoption of blockchain technology for enterprise distributed applications based on integrated MCDM FCEM-MULTIMOORA-FG method. *Engineering Applications of Artificial Intelligence*, *118*, 105699.

[12] Haroon, M. & Husain, M. (2013). Different types of systems model for dynamic load balancing. *IJERT*, *2*(3).

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-2 (April 2023)
https://doi.org/10.31033/ijemr.13.2.33

[13] Azeem, N. (2020). *Designing a model for speech synthesis using HMM*.

[14] Haroon, M. & Husain, M. (2015, Mar.). Interest attentive dynamic load balancing in distributed systems. In: *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1116-1120. IEEE.

[15] A. M. Khan, S. Ahmad & M. Haroon. (2015). A comparative study of trends in security in cloud computing. *Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India*, pp. 586-590. DOI: 10.1109/CSNT.2015.31.