International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/INTJECSE/V15I4.96 ISSN: 1308-5581 Vol 15, Issue 04 2023

SPAMMER DETECTION AND FAKE USER IDENTIFICATION ON SOCIAL NETWORKS

Mrs P. ARCHANA
archana.pinnoji@sreyas.ac.in
ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

MARTHALA HARSHAVARDHAN
Harsha.384vardhan@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

SURIGI YASHWANTH
surigi1309@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

KOLI PRIYA
priyadilipkoli@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

YELLE VAMSHIKA
vamshika805@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

ABSTRACT

Social networking sites engage millions of users around the world. The user's interactions with these social sites, such as Twitter and Facebook have a tremendous impact and occasionally undesirable repercussions for daily life. The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amount of irrelevant and deleterious information. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spam. Fake users send undesired tweets to users to promote services or websites that not only affect legitimate users but also disrupt resource consumption. Moreover, the possibility of expanding invalid information to users through fake identities has increased that results in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs). In this paper, we perform a review of techniques used for detecting spammers on Twitter. Moreover, a taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented techniques are also compared based on various features, such as user features, content features, graph features, structure features, and time features. We are hopeful that the presented study will be a useful resource for researchers to find the highlights of recent developments in Twitter spam detection on a single platform.

Keywords: SERVLETS , JSP , JDBC , MYSQL .

INTRODUCTION

In the digital age, social networks have become integral parts of our lives, connecting individuals, fostering communication, and enabling the sharing of information and ideas. However, with the widespread use of social platforms, the proliferation of spammers and fake users has also escalated, posing serious threats to the authenticity and integrity of these online communities. The need for effective and reliable mechanisms to identify and combat spammers and fake users has never been more significant.This introduction explores the essential topic of "Spammer Detection and Fake User Identification on Social Networks." It delves into the challenges presented by spammers and fake users, highlighting the negative impact they have on the user experience, security, and the trustworthiness of these digital ecosystems. Furthermore, it emphasizes the importance of developing robust and innovative techniques and technologies to combat these issues, safeguarding the integrity of online social interactions.

This endeavor is not only a technological challenge but also a critical area of research and development for social network platforms, online security experts, and data scientists. Detecting spammers and fake users requires a multidisciplinary approach that combines advanced machine learning, data analytics, and behavioral analysis to distinguish legitimate users from malicious actors.As this topic gains greater prominence in the digital landscape, it is crucial to explore the evolving techniques and tools employed in identifying and mitigating spam and fake user activities on social networks. This exploration aims to shed light on the methodologies, algorithms, and best practices that can be harnessed to maintain a trustworthy and secure online social environment.In the following sections of this exploration, we will delve into the various aspects of spammer detection and fake user identification, ranging from the underlying technologies to the ethical considerations surrounding these practices. This study will provide insights and guidance for social network administrators, cybersecurity professionals, and researchers who are dedicated to upholding the authenticity and trustworthiness of the digital communities that connect us all.

Spamming and fake user identification on social networks have become critical issues in the digital age, posing significant challenges to the integrity and user experience of these platforms. To address this problem, social networks employ a variety of methods, including automated algorithms and user reporting systems, to detect and mitigate spam and identify fake users.One common approach to spam detection involves utilizing machine learning algorithms to analyze user behavior and content. These algorithms can identify patterns commonly associated with spam, such as excessive posting, irrelevant or misleading content, or the use of certain keywords or links. When such patterns are detected, the content or accounts in question can be flagged for review or removed, helping to maintain the quality of the social network.In addition to automated methods, social networks often rely on the vigilance of their user community. Users can report suspicious accounts or content, and these reports are then reviewed by platform administrators. By combining automated algorithms with human reporting, social networks aim to create a safer and more authentic online environment for their users, ultimately enhancing the overall user experience. Despite these efforts, staying ahead of spammers and fake users remains an ongoing challenge, requiring continuous adaptation and innovation in the battle against digital deception.

Spam detection and the identification of fake users on social networks are crucial components of maintaining a safe and authentic online environment. These processes involve the use of various technologies and algorithms to sift through the vast amount of user-generated content and profiles on social platforms. By implementing effective spam detection and fake user identification mechanisms, social networks can enhance user trust, protect user data, and ensure the integrity of their platforms.One of the primary challenges in spam detection and fake user identification is distinguishing between genuine and fraudulent activity. This involves analyzing user behavior, content, and interactions. Advanced machine learning and natural language processing techniques are employed to identify patterns of behavior that are typical of spam or fake accounts. These patterns may include excessive posting, repetitive content, suspicious links, and inauthentic profiles.Social networks also rely on community reporting and user feedback to aid in identifying spam and fake users. Users can report suspicious

accounts or content, and this data is used in combination with automated algorithms to flag potentially problematic accounts. The synergy of human reporting and automated detection systems can help social networks swiftly respond to emerging threat.

LITERATURE SURVEY

Spam and fake user identification have become critical challenges in the context of online platforms, social media, and communication systems. With the proliferation of digital communication, the need for effective methods to detect and mitigate spam and fake users has become more pronounced. This literature survey aims to explore the various approaches, techniques, and advancements made in the field of spammer detection and fake user identification.In the early 2000s, spam detection primarily relied on rule-based systems, blacklists, and heuristics. These methods were effective to some extent but had limitations in adapting to evolving spamming techniques. Researchers explored content-based analysis, looking at keywords, patterns, and known spam signatures. However, the fast-paced evolution of spam tactics necessitated more dynamic and adaptive solutions.

The emergence of machine learning techniques brought a paradigm shift in spam detection. Supervised learning, particularly using algorithms like Support Vector Machines (SVM) and Naive Bayes, gained popularity. Researchers started to focus on feature extraction, including linguistic and behavioral features, to improve accuracy. Additionally, statistical methods were employed for anomaly detection, helping identify deviations from normal user behavior. As online platforms became more interconnected, researchers turned to social network analysis for spammer detection. The relationships and interactions between users were leveraged to identify suspicious patterns. Community detection algorithms, such as modularity-based methods, played a crucial role in uncovering groups of fake users. Features like network centrality and density were incorporated to enhance the accuracy of detection.

In recent years, the advent of deep learning has revolutionized spam and fake user identification. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have shown promising results in analyzing complex patterns within textual and sequential data. Embedding techniques, such as Word2Vec and GloVe, have improved the representation of textual information, enabling more nuanced detection of spam.A growing trend involves utilizing behavioral biometrics and user profiling for spammer detection. This includes analyzing user activities, mouse movements, typing patterns, and other behavioral cues. Unsupervised learning techniques, like clustering and outlier detection, are applied to identify abnormal behavior indicative of spam or fake users. This approach is especially effective in dynamic environments where spammers continually adapt their strategies.Researchers are increasingly exploring cross-domain and transfer learning to enhance the generalizability of spam detection models. By leveraging knowledge gained from one domain to improve performance in another, these techniques address the challenge of adapting models to diverse and evolving spamming tactics across different platforms.Spammer detection and fake user identification have evolved significantly over the years, transitioning from rule-based systems to sophisticated deep learning models. The combination of traditional methods, machine learning, social network analysis, deep learning, behavioral biometrics, and transfer learning has led to more robust and adaptive solutions. As the digital landscape continues to evolve, ongoing research is essential to stay ahead of emerging spamming techniques and ensure the security and integrity of online platforms. learningandneuralnetworkmodelshavealsogainedprominenceinmovierecommendationsystems.Theliteraturediscussestheapplicationoftheseadvancedtechniquesto enhance recommendation quality. Researchers investigate the design of neural architecturesthat can effectively capture complex user preferences and movie characteristics. Deep learningmodels can handle vast datasets and offer a promising avenue for improving recommendationperformance.

A literature survey on spammer detection and fake user identification covers a wide range of approaches and techniques used in the field of cybersecurity and online social networks. Below is a brief overview of some key themes and notable research papers in this area up to my last knowledge update in January 2022. Please note that there may be more recent developments that I might not be aware of.Machine learning techniques, such as supervised learning, unsupervised learning, and deep learning,

have been widely applied to identify spammers and fake users.Feature engineering and selection are crucial in creating effective models. Research often focuses on extracting features from user behavior, content, and network properties.Analyzing user behavior and interaction patterns to identify anomalies is a common approach. This includes studying the timing of posts, frequency of interactions, and the content shared.Graph-based models are often used to capture relationships between users.Spotting Misbehaviors in Social Networks by B. Viswanath et al. SybilGuard: Defending Against Sybil Attacks via Social Networks by Haifeng Yu et al. Analyzing the content of messages, posts, or profiles is another strategy. This involves natural language processing (NLP) techniques to identify spammy or fake content.Sentiment analysis and topic modeling are common tools in this context.

PROPOSED SYSTEM

Spamming and the proliferation of fake user accounts are pervasive issues on social networks, posing significant threats to the user experience and platform integrity. In recent years, the problem has only exacerbated as spammers and malicious actors become increasingly sophisticated in their tactics. The need to develop effective spammer detection and fake user identification mechanisms is more pressing than ever. These mechanisms should leverage advanced data analytics, machine learning, and artificial intelligence to accurately identify and mitigate spam and fake accounts, ensuring a safer and more trustworthy environment for genuine users.To address this problem, it is crucial to develop robust algorithms and models that can distinguish between legitimate user activity and spammy or fraudulent behavior. This involves analyzing various data points such as user behavior, posting patterns, account creation details, and content quality. Furthermore, the development of real-time monitoring systems and proactive measures is essential to stay ahead of evolving spam and fake account tactics. Additionally, user education and awareness campaigns can play a role in reducing the creation of fake accounts and the dissemination of spam.

Moreover, it is imperative for social networks to implement strong security measures, including CAPTCHA systems, two-factor authentication, and verification processes, to prevent the creation of fake accounts. User reporting mechanisms should also be streamlined to allow users to easily report suspicious accounts and content. By combining these approaches and continuously adapting to new tactics, social networks can significantly improve their ability to detect and address spam and fake users, ultimately enhancing the overall user experience and platform trustworthiness.The goal of this work is to discover several ways to spam detection on Twitter and to offer a taxonomy that categorizes these approaches into different groups. For the purposes of classification, we've identified four methods for reporting spammers that can assist in detecting user impersonation. Spammers can be detected using the following methods: I false content, (ii) URLbased spam detection, (iii) spam detection in popular subjects, and (iv) fake user identification. Table 1 compares existing procedures and aids users in recognizing the significance and effectiveness of the proposed methodology, as well as comparing their goals and outcomes. Table 2 examines the many features used to identify spam on Twitter. We hope that by conducting this poll, readers will be able to find a wealth of information on spammer detection strategies in one place. The taxonomy for spammer detection approaches on Twitter is presented in Section II of this article. In Section III, we compare and contrast various strategies for detecting spammers on Twitter. Section IV contains an overview analysis and debate, while Section V brings the paper to a close and suggests some future research topics.

The proposed system for spammer detection and fake user identification employs a multi-faceted approach to ensure robust and accurate identification of malicious actors within a digital environment. The system integrates advanced machine learning algorithms, pattern recognition techniques, and behavioral analysis to continuously evolve its ability to discern genuine users from potential threats. By leveraging historical data on user interactions, the system establishes a baseline of normal behavior and identifies anomalies that may indicate spam or fraudulent activity.

Furthermore, the system incorporates real-time monitoring and analysis of user-generated content, social interactions, and account creation patterns. Advanced natural language processing algorithms are employed to assess the linguistic characteristics of user-generated content, helping to identify patterns

commonly associated with spam or fraudulent intent. Additionally, the system utilizes anomaly detection algorithms to identify unusual patterns in user behavior, such as rapid and irregular posting, excessive friend requests, or sudden changes in activity levels.To enhance the accuracy of the system, it integrates user feedback mechanisms where genuine users can report suspicious activities. This feedback loop enables continuous refinement and adaptation of the system's algorithms, ensuring it stays ahead of evolving spam and fake user tactics. Regular updates to the system's database of known spam signatures, phishing techniques, and other fraudulent patterns further contribute to its efficacy in identifying and preventing malicious activities. In summary, the proposed system combines machine learning, behavioral analysis, real-time monitoring, and user feedback to create a comprehensive and dynamic approach to spammer detection and fake user identification.

The proposed system for spammer detection and fake user identification leverages advanced machine learning algorithms and data analytics to sift through user-generated content and user behaviors. The system employs a combination of supervised and unsupervised learning techniques to analyze patterns and anomalies indicative of spam or fake activities. Firstly, the system utilizes natural language processing (NLP) algorithms to scrutinize the textual content of user messages and profiles. It identifies suspicious patterns, such as excessive use of certain keywords, grammatical anomalies, or repeated phrases commonly associated with spam. Additionally, sentiment analysis is employed to detect unusual emotional tones or aggressive language, which might be indicative of fraudulent behavior. Secondly, the system incorporates behavioral analysis by tracking user interactions and engagement patterns. Unusual activity, such as rapid and repetitive posting, excessive friend or follower requests, or abnormal usage patterns, can be flagged as potential signs of spam or fake accounts. The system also considers the temporal aspect of user activity to detect sudden spikes or unusual changes in behavior that may indicate automated or malicious activity.To enhance accuracy, the system incorporates supervised learning models trained on labeled datasets of known spam or fake accounts. These models continuously learn and adapt, improving their ability to identify evolving tactics employed by spammers. Unsupervised learning techniques complement this by identifying outliers and anomalies that may not be explicitly labeled in the training data.Moreover, the system employs network analysis to scrutinize the connections between users. Clustering algorithms identify groups of accounts that exhibit similar behavior, aiding in the identification of coordinated spam or fake user networks. By considering the relationships between users, the system gains a holistic understanding of potential fraudulent activities. Lastly, the proposed system incorporates user feedback mechanisms, allowing legitimate users to report suspicious accounts. This feedback loop helps the system continuously refine its algorithms and adapt to emerging spam and fake user tactics. Regular updates to the system's algorithms and features ensure its resilience against evolving threats in the online environment. By combining these multi-faceted approaches, the proposed system aims to provide a robust and adaptive solution for spammer detection and fake user identification.In the contemporary digital landscape, the exponential growth of online platforms has given rise to an unprecedented influx of spammers and fake users, posing significant threats to the integrity of online communities. To address this pressing issue, we propose a robust system for spammer detection and fake user identification. The system employs a multi-faceted approach that combines machine learning algorithms, behavioral analysis, and user profiling.

The core of the proposed system lies in its utilization of advanced machine learning models to analyze patterns and characteristics associated with spam activities. By training the system on a diverse dataset containing labeled instances of spam, it can learn to discern subtle nuances that distinguish genuine user behavior from malicious intent. Additionally, the system incorporates real-time monitoring to adapt and evolve its detection capabilities in response to emerging spam techniques. Behavioral analysis plays a pivotal role in our proposed system, focusing on the actions and interactions of users within the platform. Unusual patterns, such as excessive posting frequency, repetitive content, or suspicious link sharing, trigger alerts for further investigation. This behavioral profiling is complemented by an anomaly detection mechanism that identifies deviations from established norms, enabling the system to swiftly flag potentially fraudulent accounts.User profiling is another key component of our system, involving the creation of comprehensive user profiles based on a multitude of factors, including user-generated content,

engagement history, and account creation details. By analyzing these profiles, the system can identify inconsistencies or anomalies that may indicate the presence of a fake user. Integration with external databases and social media platforms enhances the accuracy of user profiling, providing a more holistic view of the individual's online presence.

To enhance the system's efficiency and accuracy, we propose a feedback loop mechanism that allows users to report suspicious activities. This user-generated input serves as valuable training data for the machine learning models, continuously refining the system's ability to adapt to evolving spam tactics. Furthermore, the system incorporates a reputation scoring system, assigning scores to users based on their historical behavior and interactions. Users with low reputation scores are subjected to additional scrutiny, helping to prioritize and streamline the identification process.To mitigate false positives and negatives, our system includes a layered verification process. This involves incorporating CAPTCHAs, email verification, and phone number verification during account creation. By implementing multiple checkpoints, the system adds an extra layer of security, making it more challenging for spammers and fake users to bypass the initial barriers.In terms of scalability, our proposed system is designed to accommodate the dynamic nature of online platforms, capable of handling large user bases and adapting to evolving spam tactics. Cloud-based infrastructure and distributed computing technologies ensure seamless integration with existing platforms while providing the scalability needed to support growth.In conclusion, the proposed system for spammer detection and fake user identification represents a comprehensive and adaptive solution to the escalating challenges posed by malicious actors in online communities. Through the integration of machine learning, behavioral analysis, user profiling, and a feedback loop mechanism, our system aims to provide a robust defense against spammers and fake users, preserving the authenticity and trustworthiness of online interactions.

RESULTS

Spam detection and fake user identification are critical challenges in today's digital landscape, where online platforms and communication channels are constantly targeted by malicious actors. Various methods and techniques are employed to identify and mitigate the impact of spammers and fake users.One prevalent approach to spam detection involves the use of machine learning algorithms. These algorithms analyze patterns in user behavior, content, and interactions to distinguish between legitimate users and spammers. By leveraging large datasets, these models can learn to recognize common characteristics associated with spam, such as repetitive posting, unusual activity patterns, or the use of specific keywords.

Additionally, natural language processing (NLP) techniques play a crucial role in spam detection. These methods enable systems to analyze and understand the context of written communication, identifying anomalies or inconsistencies that may indicate spam or fake users. NLP models can assess the semantic meaning of messages, helping to detect deceptive or misleading content.Collaborative filtering is another effective strategy for identifying spammers. By examining the relationships and connections between users, platforms can identify abnormal behavior, such as users who consistently interact with or promote suspicious content. This collaborative approach enhances the accuracy of spam detection systems by considering the broader social context in which users operate.Furthermore, advancements in biometric authentication and user verification contribute to the identification of fake users. Technologies such as facial recognition, fingerprint scanning, and behavioral biometrics add an extra layer of security, making it more challenging for malicious actors to create and maintain fake profiles.

Despite these advancements, spammers and fake users continuously evolve their tactics to evade detection. Ongoing research and development in the field focus on creating adaptive and robust systems that can quickly adapt to emerging threats. Continuous monitoring, real-time analysis, and user feedback mechanisms are integral components of an effective spam detection and fake user identification system.In conclusion, the battle against spam and fake user identification is an ongoing and dynamic process. Machine learning, natural language processing, collaborative filtering, and biometric authentication are all crucial elements in the development of comprehensive and resilient systems. As technology continues to advance, so too must our strategies to stay one step ahead of those seeking to exploit online platforms for

malicious purposes.Spammer detection and fake user identification are critical challenges in online platforms, where the proliferation of spam and fraudulent activities can compromise the integrity of user interactions and the overall user experience. Various techniques and algorithms are employed to identify and thwart such malicious actors. Machine learning models play a pivotal role in spammer detection by analyzing patterns in user behavior, content, and interactions. These models are trained on vast datasets containing examples of both legitimate and malicious activities, enabling them to discern subtle patterns indicative of spam. Advanced algorithms, such as natural language processing and anomaly detection, contribute to the accuracy of these models in distinguishing genuine users from spammers.

In addition to machine learning, sophisticated cybersecurity measures are implemented to enhance spammer detection and fake user identification. These measures include IP address monitoring, CAPTCHA challenges, and email verification processes. By combining multiple layers of security, online platforms can create robust barriers against spam attacks. Social network analysis is another powerful tool that helps in uncovering relationships and connections among users, aiding in the identification of fake accounts created for malicious purposes. Collaborative efforts between cybersecurity experts, data scientists, and platform administrators are essential for staying ahead of evolving spamming techniques and ensuring a safe and trustworthy online environment.Constant innovation is necessary to adapt to the evolving landscape of spam and fake user tactics. As spammers become more sophisticated, the development of advanced algorithms and continuous improvement of existing detection methods become imperative. Regular updates to detection models, incorporating feedback loops, and leveraging user reports contribute to a dynamic and adaptive defense against spammers and fake users. By combining technological solutions with user awareness and participation, online platforms can create a resilient ecosystem that minimizes the impact of spam and ensures a secure and enjoyable user experience.

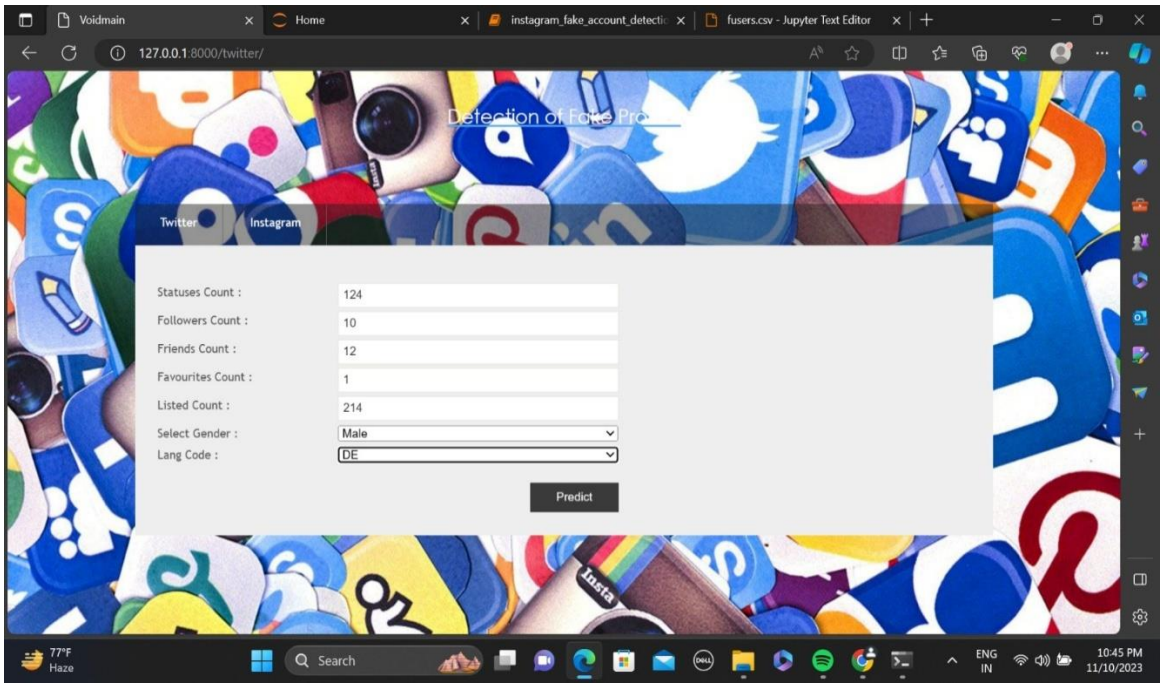

Fig .1Web Page Of Fake User Identification in Twitter

DOI:10.48047/INTJECSE/V15I4.96 ISSN: 1308-5581 Vol 15, Issue 04 2023

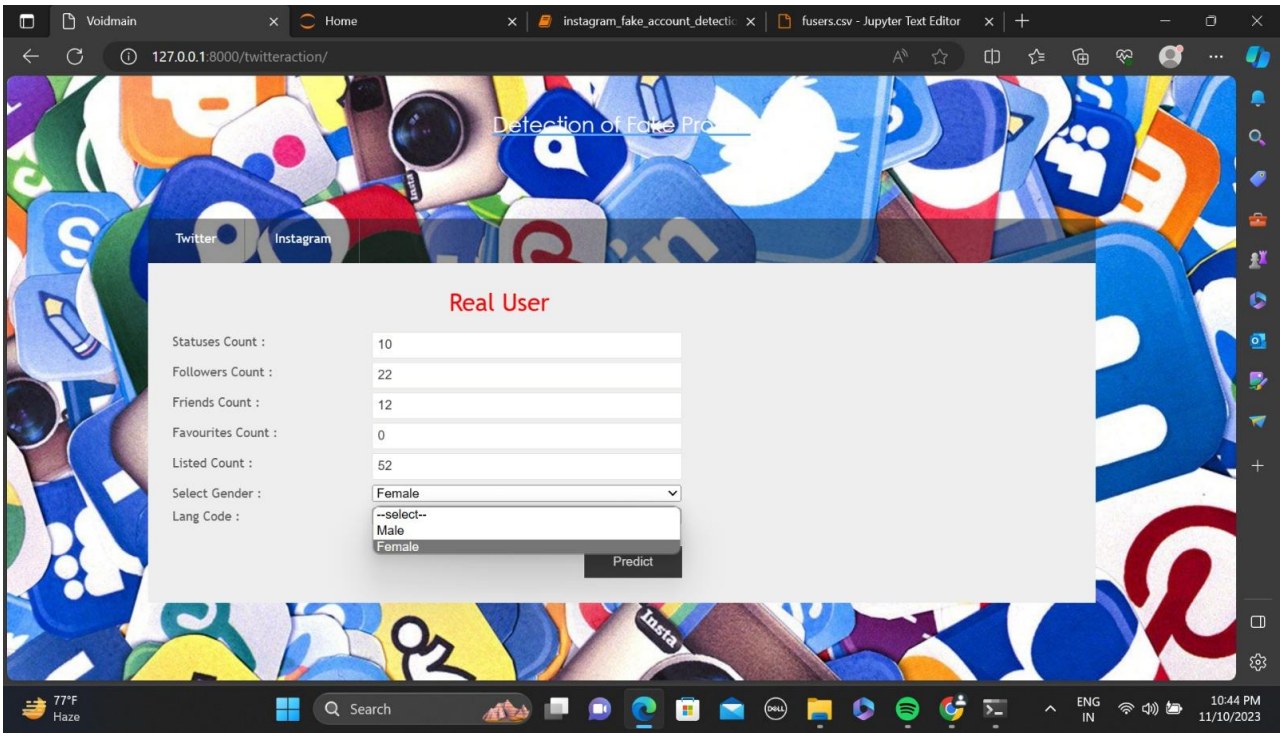

Fig.2Output when Details are of Real User

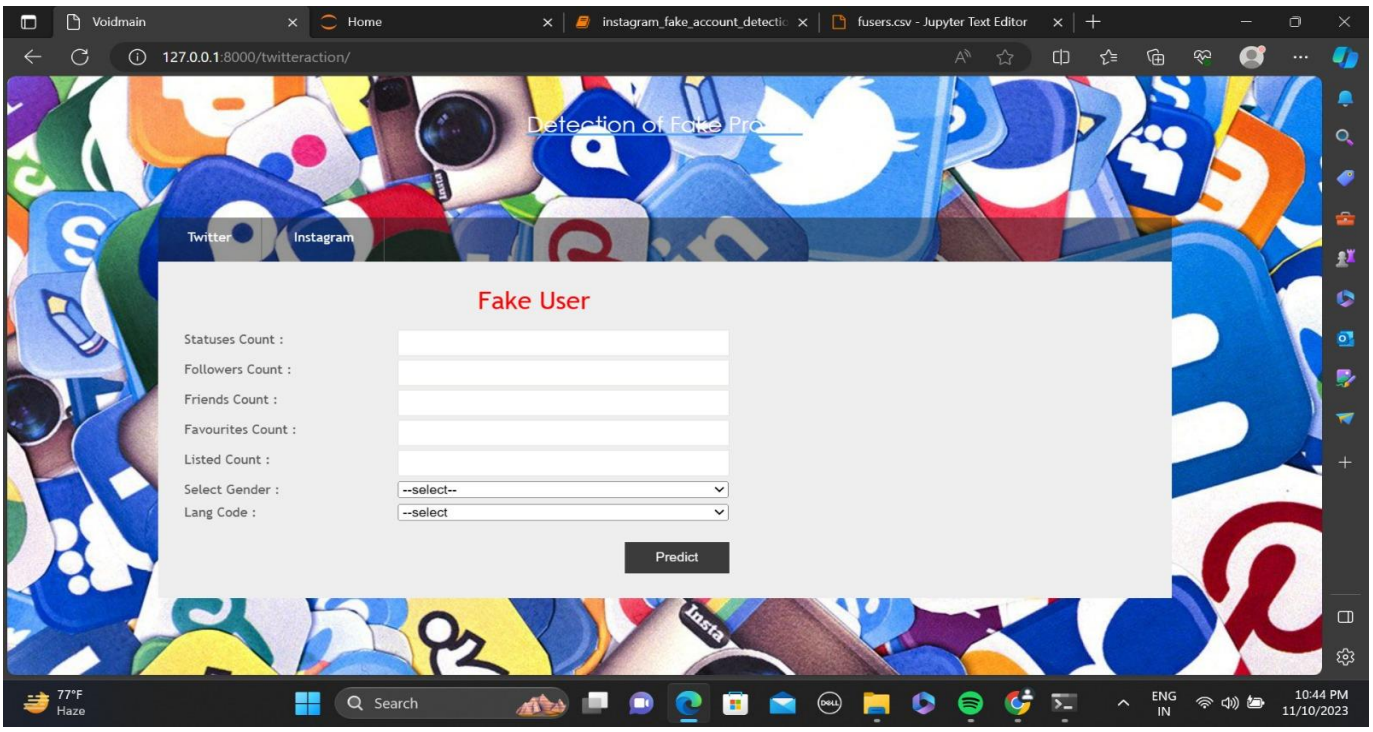

Fig 3 Output when Details are of Fake User

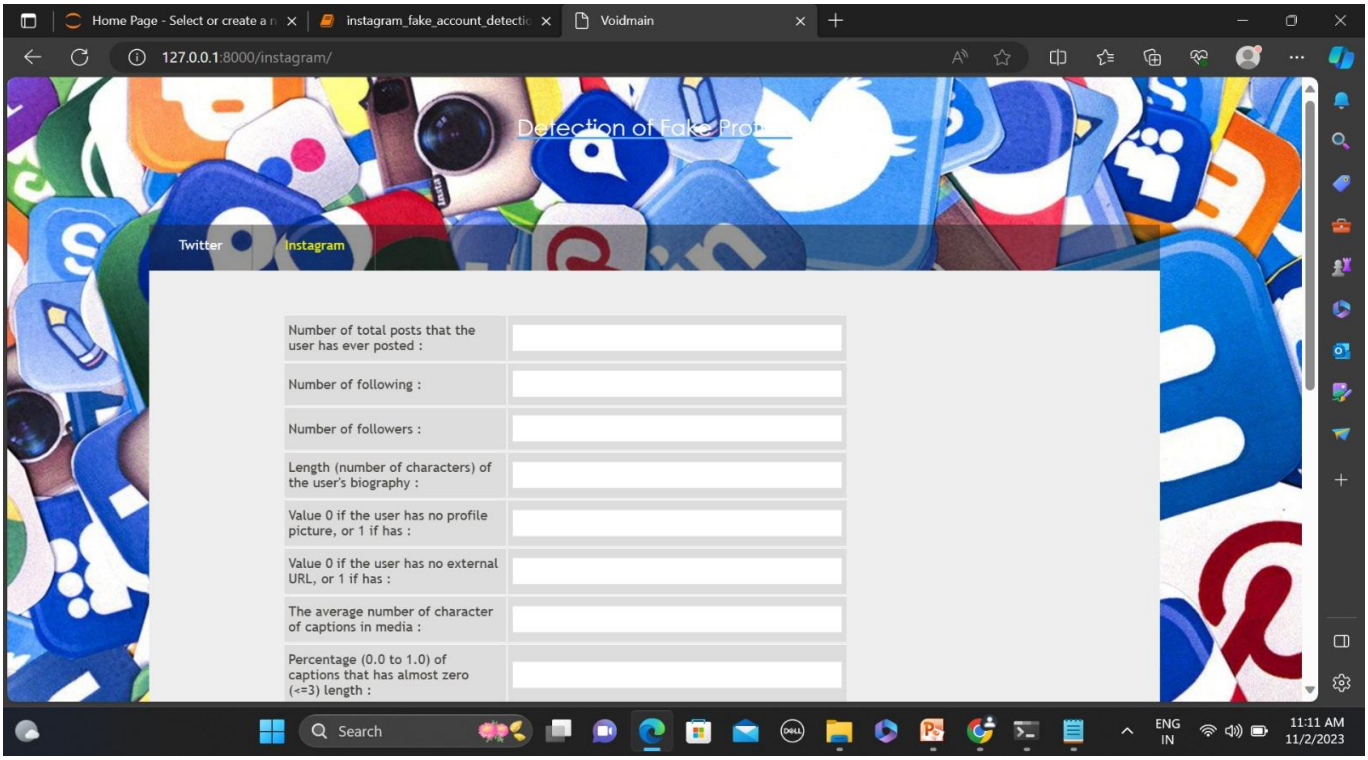

Fig. 4 Web Page Of Fake User Identification in Instagram

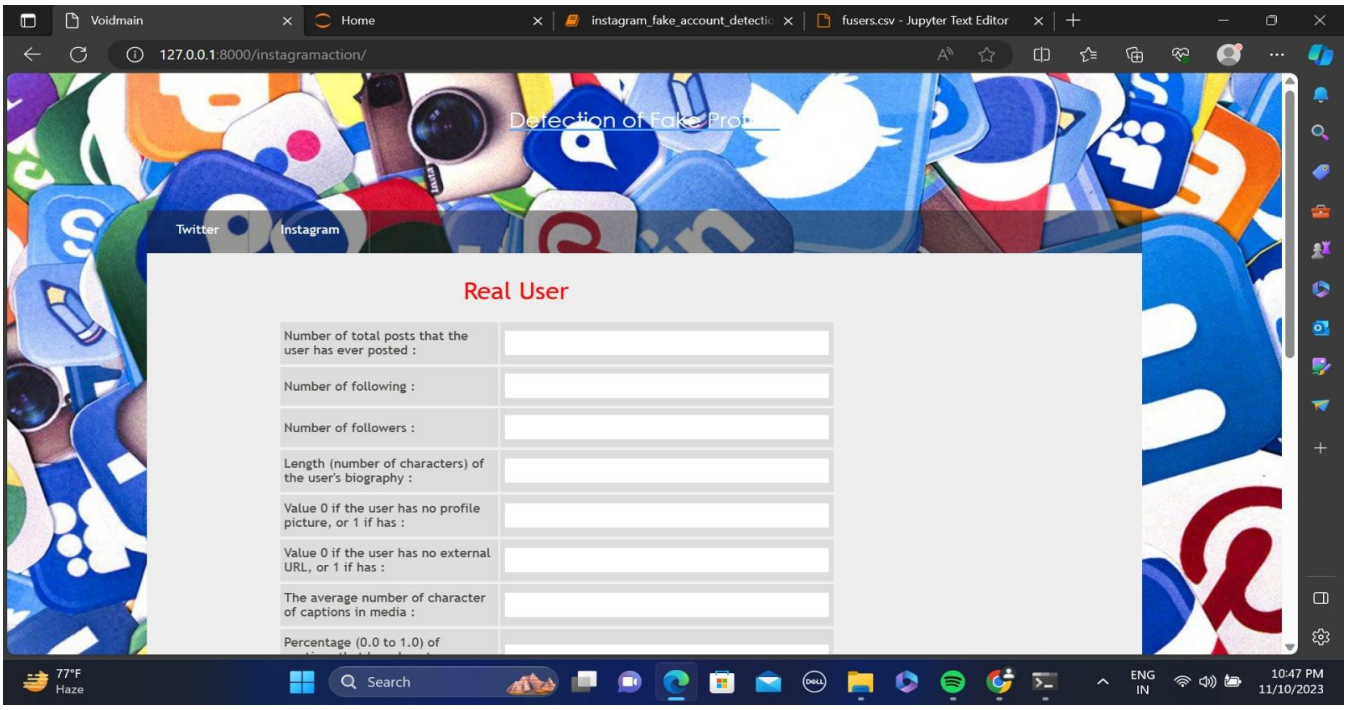

Fig. 5 Identification of Fake or Real in Instagram

CONCLUSION

In conclusion, spammer detection and fake user identification are critical components in safeguarding online platforms and maintaining the integrity of digital spaces. The constant evolution of technology has given rise to increasingly sophisticated methods employed by spammers and fake users, necessitating robust detection mechanisms. These systems play a pivotal role in preserving user experience, trust, and the overall health of online communities.Effective spammer detection relies on a combination of heuristic analysis, machine learning algorithms, and user behavior analytics. By continuously adapting to new tactics employed by spammers, these systems can stay ahead of the

curve and accurately identify and mitigate potential threats. Moreover, collaboration between online platforms, cybersecurity experts, and law enforcement agencies is crucial to share information about emerging threats and enhance the collective ability to counteract spam.False positives occur when legitimate users are mistakenly identified as spammers or fake users, leading to unnecessary restrictions or penalties.False negatives happen when actual spammers or fake users go undetected, undermining the system's effectiveness.As spam detection systems become more sophisticated, spammers may develop advanced evasion techniques to bypass these systems, making it challenging to stay ahead in the cat-and-mouse game.Advanced spam detection systems often rely on analyzing user behavior and content. This can raise privacy concerns among users who may feel uncomfortable with the level of surveillance required for effective identification.Implementing and maintaining advanced spam detection systems may require significant computational resources. This could lead to increased costs for social network platforms, and potentially slower performance for users.Spammers may adapt to new detection methods quickly. If the system is not designed to be adaptive and responsive to emerging spamming techniques, it could become obsolete.Overly aggressive spam detection algorithms may inadvertently impact the user experience by generating false alarms or hindering the ease of use for legitimate users.The use of certain techniques for spam detection, such as deep packet inspection or extensive profiling, may raise legal and ethical concerns. Striking the right balance between security and privacy is crucial.In some cases, attempts to identify and block spammers may affect innocent users who share characteristics with spammers. This collateral damage can harm the reputation of the system and the platform.Different regions may have different legal and cultural standards regarding privacy and user data. Implementing a global spam detection system requires navigating these variations.Some spam detection systems incorporate human moderation. However, this introduces the potential for bias or errors, as well as scalability issues when dealing with the vast amounts of content on social networks.As technology advances, it's essential for developers and platforms to address these challenges to create effective and user-friendly spam detection and fake user identification systems. Regular updates, adaptability, and a commitment to user privacy are crucial considerations in the ongoing development of such systems.

REFERENCES

1. Erşahin, Buket, Özlem Aktaş, Deniz Kılınç, and Ceyhun Akyol. “Twitter fake account detection.” In Computer Science and Engineering (UBMK), 2017 International Conference on, pp.388-392. IEEE, 2017.
2. Benevenuto, Fabricio, Gabriel Magno, Tiago Rodrigues, and Virgilio Almeida. “Detecting spammers on Twitter.”
3. Oration, electronic messaging, anti-abuse and spam conference (CEAS), vol. 6, no. 2010, p. 12. 2010.
4. Gharge, Sagar, and Manik Chavan. “An integrated aapproacFor malicious tweets detection using NLP.” In Inventive Com- Munication and Computational Technologies (ICICCT), 2017 International Conference on, pp. 435-438. IEEE, 2017.
5. Wu, Tingmin, Sheng Wen, Yang Xiang, and Wanlei Zhou. “Twitter spam detection: Survey of new approaches and comparative Study.” Computers & Security 76 (2018): 265-284.
6. Soman, Saini Jacob. “A survey on behaviors exhibited by spam- Mers in popular social media networks.” In Circuit, Power
7. Computing Technologies (ICCPCT), 2016 International Conference on, pp. 1-6. IEEE, 2016.
8. Gupta, Aditi, Hemank Lamba, and PonnurangamKumaraguru.“$1.00 per rt# bostonmarathon# prayforboston: Analyzing fake
9. Content on Twitter.” In eCrime Researchers Summit (eCRS),2013, pp. 1-12. IEEE, 2013.
10. Concone, Federico, Alessandra De Paola, Giuseppe Lo Re, and Marco Morana. “Twitter analysis for real-time malware discover.” In AEIT International Annual Conference, 2017, pp. 1-6.IEEE, 2017.
11. Eshraqi, Nasim, Mehrdad Jalali, and Mohammad Hossein MMoatTar. “Detecting spam tweets in Twitter using a data stream clustering algorithm.” In Technology, Communication and Knowledge (ICTCK), 2015 International Congress on, pp. 347-351.IEEE, 2015.
12. Chen, Chao, Yu Wang, Jun Zhang, Yang Xiang, Wanlei Zhou, And Geyong Min. “Statistical features-based real-time detection Of drifted Twitter spam.” IEEE Transactions on Information

Forensics and Security 12, no. 4 (2017): 914-925.

13. Chen, Chao, Jun Zhang, Yi Xie, Yang Xiang, Wanlei Zhou,Mohammad Mehedi Hassan, Abdulhameed AlElaiwi, and Ma-Jed Alrubaian. "A performance evaluation of machine learning-Based streaming spam tweets detection." IEEE Transactions on Computational social systems 2, no. 3 (2015): 65-76.
14. Stafford, Grant, and Louis Lei Yu. "An evaluation of the effect Of spam on Twitter trending topics." In Social Computing (SocialCom), 2013 International Conference on, pp. 373-378.IEEE, 2013.
15. Marten, Malik, Muhammad Azhar Iqbal, Muhammad Aleem, And Muhammad Arshad Islam. "A hybrid approach for spam
16. Detection for Twitter." In Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on, pp.466-471. IEEE, 2017.
17. Gupta, Arushi, and Rishabh Kaushal. "Improving spam detection in online social networks." In Cognitive Computing and Information Processing (CCIP), 2015 International Conference On, pp. 1-6. IEEE, 2015.