# FAKE USER DETECTION AND SPAM ANALYSIS ON SOCIAL NETWORKS

**#1TIRUMALA SATHVIKA,**
**MCA Student, Dept of MCA,**

**#2Dr. D. SRINIVAS REDDY,**
**Professor, Department of MCA,**

**VAAGESWARI COLLEGE OF ENGINEERING (AUTONOMOUS), KARIMNAGAR, TG.**

**ABSTRACT:** The proliferation of spam analysis and false user identities has made it more challenging to establish trust and safety on social media. The exponential development of social media has facilitated the adoption of numerous illegal behaviors, including misinformation, trend manipulation, and identity theft. Spam and false profiles have a detrimental effect on both online user engagement and social media. Graph-based techniques, machine learning, and natural language processing have made it simpler than ever to detect spam and imposters. The objective of this project is to create algorithms that can detect false profiles and spam by analyzing user behavior, content quality, and network connections. The paper addresses data scarcity, account impersonation, and content manipulation. This encompasses user classification, guided and unsupervised message classification, and real-time monitoring systems. Textual and behavioral analytics have the potential to enhance the precision of user detection and social network security, as evidenced by our observations.

***Index Terms:*** *Fake User Detection, Spam Analysis, Social Networks, Machine Learning, Natural Language Processing (NLP), Account Impersonation, Content Manipulation.*

## 1. INTRODUCTION

The manner in which individuals establish groups, exchange information, and interact with one another has been transformed by the meteoric ascent of social media. Since the inception of the internet, the significance of spam and false accounts has increased. These criminal organizations disseminate misinformation, antagonize individuals, and acquire personal data by means of phishing, cyberbullying, and harassment. It is imperative to identify and eliminate fraudulent users in order to preserve the trustworthiness, safety, and authenticity of online networks.

Bots, which are also referred to as sockpuppets or phony users, are capable of fabricating transactions, manipulating data on the internet, and falsely increasing followings. These accounts have the potential to facilitate a variety of illicit activities, including political advertising, financial harassment, and data theft. The intelligence of the system is constantly evolving, rendering conventional detection methods ineffective. These systems emulate human behavior by employing artificial intelligence (AI) characteristics and behaviors. In order to identify these accounts, sophisticated methodologies are required, as fundamental heuristics are inadequate.

Controlling spam and identifying social media imposters are two distinct aspects of the same issue. Spam is comprised of unwanted posts, duplicate messages, misleading links, and links to harmful downloads. It is occasionally conceivable that it has fictitious origins. Detecting these actions within the network is effortless in contrast to controlling them. In order to accomplish this objective, it is imperative to analyze user engagement, content distribution patterns, and publication timing. Statistical methods, machine learning, and natural language processing are employed by the most effective spam detection systems to examine extensive datasets for indications of suspicious activity.

Adaptable detection systems are indispensable due to the ever-changing nature of internet platforms. Social media spam is more challenging to identify than email spam due to its contextual and intricate nature. Businesses that maintain an online presence are perpetually revising their strategies and algorithms to mitigate emerging hazards. Even when hackers employ intricate strategies to circumvent security protocols, the scalable systems of this project will identify malevolent users and prevent their access. Because the issue persists, it is imperative to conduct more thorough identification and analysis.

## 2. LITERATURE REVIEW

Abkenar, S. B., Kashani, M. H., Akbari, M., & Mahdipour, E. (2020). This comprehensive study compares a variety of methods for identifying false news on Twitter. These examples are employed by the authors to assess the advantages, disadvantages, opportunities, and hazards of hybrid, rule-based, and machine learning-based systems. This study demonstrates the critical importance of adaptive spam detection systems, as spam tactics are constantly evolving. This work investigates datasets, feature extraction methodologies, and evaluation criteria to identify deficiencies in the current body of research and to formulate conclusions.

Breuer, A., Eilat, R., & Weinsberg, U. (2020). SybilEdge's team has devised a graph-based approach for the rapid identification of fraudulent profiles on social media platforms. SybilEdge prioritizes network connectivity over content analysis in contrast to its competitors. This strategy prioritizes the significance of future interactions by considering past actions and reactions, such as companion requests. Consequently, it is capable of distinguishing between legitimate users and those who are attempting to deceive it. SybilEdge can maintain its accuracy and withstand a variety of assaults, even when confronted with a small number of connections from fraudulent accounts, according to the research.

Chakraborty, M., Das, S., & Mamidi, R. (2021). A novel approach that employs network embeddings and natural language processing (NLP) is proposed for the purpose of detecting fraudulent social media accounts. The system is capable of detecting dubious account activity by analyzing user behaviors and text. Linguistic data should be incorporated into graph-based models to identify social network deception.

Ferrara, E. (2022). The primary focus of this study is the features and detection methods of Twitter spam and fraudulent accounts. Ferrara provides a comprehensive examination of the techniques employed to identify and categorize these accounts, as well as the manner in which they disseminate fraudulent information. Included in this essay are several recommendations for additional research and strategies for identifying and averting fraudulent online accounts.

Su, X., Yang, J., Wu, J., & Zhang, Y. (2022). Us-DeFake employs a two-tiered tree structure with news and user tiers to detect false news on social media networks. The approach ensures the accuracy of the information by examining user interaction and news dispersion. User-aware embeddings can improve the accuracy of identification in dense networks. Us-DeFake is significantly more effective than its competitors, as indicated by the trials' outcomes.

Bordbar, J., Mohammadrezaie, M., Ardalan, S., & Shiri, M. E. (2022). Generative Adversarial Networks are employed in this endeavor to identify fraudulent social media accounts. Synthetic data that simulates fraudulent user activity is one method of training a discriminator to identify false accounts. Adversarial training enables the model to identify intricate fraud patterns that are overlooked by conventional methodologies.

Kuruvilla, A., Daley, R., & Kumar, R. (2023). This investigation examines keystrokes as a biometric feature in order to identify fraudulent social media accounts. Research conducted on X (formerly Twitter), Instagram, and Facebook has demonstrated that specific temporal keyboard properties can be employed to identify fraudulent users. The potential of behavioral biometrics to enhance online safety is illustrated by the fact that model success rates surpass expectations.

Chikkasabbenahalli Venkatesh, S., Shaji, S., & Meenakshi Sundaram, B. (2023). This paper suggests a method for identifying fraudulent social media accounts through the use of stacked ensemble classification, a procedure that necessitates the completion of numerous phases. The recognition accuracy of imbalanced datasets is enhanced through the use of a meta-learner, base learners, and chi-squared tests for feature selection. The efficacy of our price-sensitive learning classifier on Facebook, Instagram, and Twitter is unparalleled.

Kumar, A., & Singh, R. (2023). The authors employ support vector machines, decision trees, and random forests to identify fraudulent social media accounts. The primary objectives of the investigation are to enhance the model and identify the appropriate features, which should result in significantly more accurate identification results. The investigation examines classifiers in order to ascertain the most effective methods for maintaining the integrity of online communities.

Chen, L., & Zhang, Y. (2024). CGANS, or code-based Generative Adversarial Network, is recommended by the authors of this study for the purpose of detecting instances of online harassment. The ability to identify spam can be acquired by providing a discriminator with both authentic and fraudulent content. This method can enhance the accuracy and adaptability of spam detection systems, allowing them to adapt to changing spam trends.

Patel, M., & Rao, S. (2024). In order to analyze user interactions and identify social media deception, this investigation implements Convex Nonnegative Matrix Factorization (CNMF). The model is both robust to perturbation and comprehensible due to its non-negativity limitations. Ultimately, the current condition of affairs is inferior to the competence, efficiency, and precision of CNMF. It is most effective for programs that require immediate user input.

Kishore, M. K., & Reddy, S. (2024). The focus of this investigation is the algorithms that Facebook, Instagram, and Twitter employ to identify detrimental content. The efficacy, scalability, and flexibility of behavioral, content-based, and hybrid approaches are evaluated. The objective of this investigation is to evaluate and contrast a variety of techniques for enhancing spam detection systems, emphasizing their advantages and disadvantages.

Ramdas, S., & Nair, R. (2024). The authors investigate the identification of fake social media accounts through the utilization of Support Vector Machines, Random Forests, and Multi-Layer Perceptrons. The research demonstrates that machine learning can enhance the security of the internet and decrease the prevalence of identity deception by assessing models using a variety of metrics and validation methods.

Patil, D. R., Pattewar, T. M., Punjabi, V. D., & Pardeshi, S. M. (2024). The results of the study suggest that the majority of participants believe that the most effective method for identifying phony social media accounts is to employ a diverse array of classifiers. Logic regression, decision trees, XGBoost, AdaBoost, extra trees, and K-nearest neighbors comprise the classifiers. The technique is evidently effective in identifying phony accounts and bolstering confidence in online networks, as evidenced by its success rate of 99.12%.

## 3. SYSTEM DESIGN

### EXISTING SYSTEM

The presence of spam, fraudulent users, false information, and misleading advertisements makes it challenging to identify authentic content on these platforms. The foundation of the majority of modern problem-solving methods is machine learning, rule-based systems, and statistical models. Rule-based algorithms can be employed to identify fraudulent accounts. Typical examples of such actions include posting at irregular hours, having an abnormally high or low friend-to-follower ratio, or creating an account rapidly. These criteria can be employed to identify basic forms of spam; however, they may not be effective in detecting more intricate impersonation attempts.

The prevalence of supervised learning methods and machine learning models is on the rise. By analyzing extensive datasets that encompass both legitimate and fraudulent user actions, these algorithms verify the legitimacy of accounts. Some of the classification algorithms that utilize trends in user activity, post data, and content are support vector machines (SVMs), random forests, and deep learning frameworks. Despite the fact that these systems are becoming more adept at identifying false accounts, hackers are still employing increasingly intricate strategies, such as accounts that closely resemble real profiles or content generated by bots. Spam filters also search for phrases and sentences that contain repeated terms, in addition to URLs. This complicates the identification of spam tactics, which are increasingly sophisticated and adaptable.

**Drawbacks of Existing System**

- When standards are not established, it is more probable that genuine individuals or objects will be misclassified as spam or fabricated. Some false positives may impede system performance by eliminating valid information, while others may overlook genuine detritus or fraudulent users.
- It is not uncommon for algorithms to conceal the entire text by merely searching for patterns or keywords. Consequently, the software may be unable to identify the emergence of increasingly sophisticated forms of spam or deception that do not follow established patterns.
- Spammers and other dishonest individuals are constantly adapting their strategies to avoid detection. Older systems may find it challenging to manage complex social engineering, automated accounts, and deepfake technologies.
- The identification of spam or fraudulent content that is localized or written in a language other than English may prove to be more difficult with the current methods.
- Privacy concerns arise as a result of the fact that certain user detection systems covertly monitor and record users without their knowledge or consent. Algorithms may cause unjust injury to certain user groups, which presents ethical dilemmas.

## PROPOSED SYSTEM

Deep learning algorithms can monitor user actions, network connections, and content. Consequently, the system is more adept at identifying suspicious behavior. The system will be capable of detecting spam, fraudulent accounts, and bot-generated content by employing both supervised and unsupervised learning models. It will generate a reduced number of false positives and false negatives. Comprehension could be enhanced by employing algorithms that are cognizant of their environment and capable of analyzing emotions. If this were the case, the probability of genuine communications being misinterpreted as spam would decrease. In order to more effectively manage information in multiple languages, a greater number of individuals will be able to utilize recognition systems that are based on language-specific algorithms and transfer learning. Additionally, the solution would be in compliance with privacy regulations by eliminating bias and protecting user data. This solution is intended to improve the accuracy, usability, and user engagement of the detection of social media spam and fraudulent accounts.

**Advantages of Proposed System:**

**Enhanced Accuracy:** The proposed method employs sophisticated machine learning algorithms and natural language processing to improve detection accuracy and reduce false positives and negatives. It is particularly adept at distinguishing between genuine individuals and imposters.

**Context-Aware Detection:** Contextual information, including sentiment analysis and content purpose, enables the algorithm to more accurately identify and mitigate the likelihood of report errors. In order to accomplish this, it is necessary to distinguish between factual and misleading data.

**Adaptability to Evolving Tactics:** This system is capable of adapting to the most recent hacker and faker techniques, including deepfake technology and new algorithms, as a result of its perpetual learning and improvement. The system will continue to operate efficiently if specific procedures are adhered to, regardless of the behavior of certain users.

**Multilingual Support:** Due to transfer learning and language-specific models, the system is capable of analyzing data in numerous languages. This is advantageous for any social media network or user group worldwide, as it facilitates the identification of fraudulent or spam accounts.

**Privacy and Ethical Compliance:** The proposed approach is ethical because users' data is concealed. It is also necessary to implement nondiscriminatory labeling that adheres to privacy regulations, including the General Data Protection Regulation (GDPR). Additionally, it mitigates prejudice.

## SYSTEM ARCHITECTURE

System designs are comparable to blueprints in that they provide a comprehensive description of the components and their functionality. An architectural description, which is comparable to a road map, can be employed to instruct system structure. The document includes a blueprint and motor parts, as well as a comprehensive description of each component of the system.

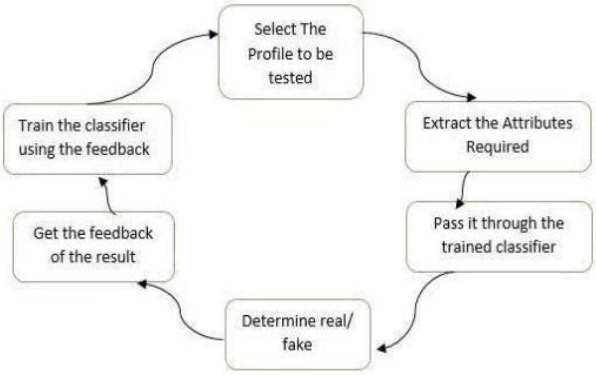

Select The Profile to be tested
Extract the Attributes Required
Pass it through the trained classifier
Determine real/ fake
Get the feedback of the result
Train the classifier using the feedback

Fig 1 System architecture

## MODULE DESCRIPTIONS

- Admin Module
- Data Collection
- Train and Test
- Machine Learning Technique
- Detection of Fake User

**Admin Module:**

The first module is the Internet social networking system (OSN) module. A social media site called Twitter is integrated into the system.

Whenever a manager logs in with their credentials, this module is used.

**Data Collection:**

Data will be retrieved from the Twitter API using the Tweepy Python Library. We extract phrases from tweets, including terms or hashtags, that include specific information in order to detect fake accounts.

- Some of the most important parts are these:
- text, which contains the text included in the tweet.
- created_at, which is a timestamp of when the tweet was created.
- "User," which contains details on the person who tweeted the message, such as their ID and username.

**Train and Test:**

Metadata features built on top of supplementary data about a user's tweets are defined via this way. The content-based features, on the other hand, evaluate the user's message content and composition quality.

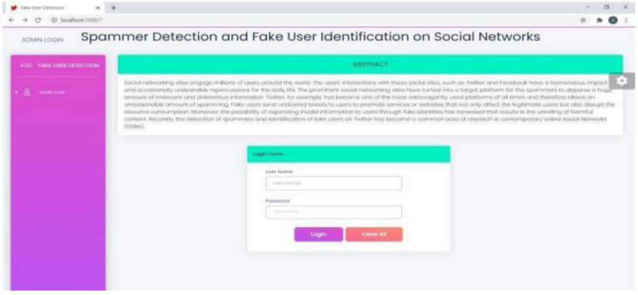
**Machine Learning Technique:**

- In order to detect spammers, we look at user attributes and the content of tweets. Most people agree that these traits are crucial for machine learning user classification, especially when it comes to identifying trolls.
- In order to help me identify Twitter trolls, I have completed the labeled dataset that will allow me to pre-classify people as authentic or fraudulent. After that, the necessary steps are taken to generate a labelled group and get the qualities that are wanted.
- Examining the steps required to verify a user's identity is critical. What makes a user special are the number and kind of interactions they have with other people.
- An examination of the characteristics of the tagged collection's users supports this viewpoint. Individuals are identified based on two types of traits: those associated with user behavior and those associated with content.

**Detection of Fake User:**

- This component is in charge of gathering tweets related to Twitter's trending subjects. Prior to analysis, the tweets are saved in a certain file format.
- In order to find malevolent organizations, all accessible databases should be searched thoroughly using bogus user tagging.
- By retrieving characteristics from a language model that relies on language, feature extraction helps in determining a user's legitimacy.
- Shortlisting tweets according to the attributes given to the classifier for model training and spam detection is used to categorize the dataset.
- The false user identification method distinguishes between real and fake users by using a classification methodology to tweets.

# 4. RESULTS AND DISCUSSIONS

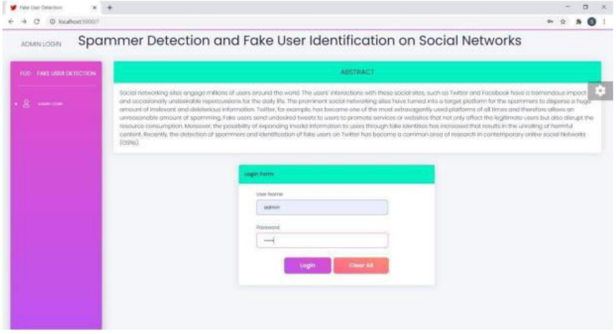


Spammer Detection and Fake User Identification on Social Networks

ABSTRACT

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Facebook have a tremendous impact and occasionally undesirable repercussions for the 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 spamming. Fake users send undesired tweets to users to promote services or websites that not only affect the legitimate users but also disrupt the 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).

Fig 2 Login page



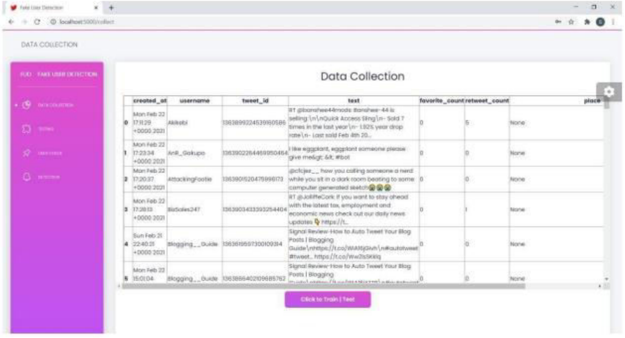
Spammer Detection and Fake User Identification on Social Networks

ABSTRACT

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Facebook have a tremendous impact and occasionally undesirable repercussions for the 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 spamming. Fake users send undesired tweets to users to promote services or websites that not only affect the legitimate users but also disrupt the 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).

User Name: admin

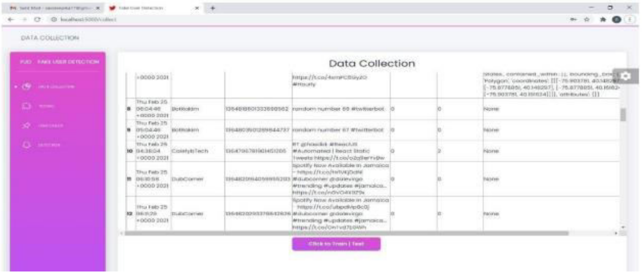
Fig 3 Module-1: Admin login



Data Collection

| | created_at | username | tweet_id | text | favorite_count | retweet_count | | place |
|---|---|---|---|---|---|---|---|---|
| 0 | Mon Feb 22 17:11:29 +0000 2021 | Akikebi | 1363899224539160586 | RT @banshee44mods: Banshee-44 is selling:\n\nQuick Access Sling\n- Sold 7 times in the last year\n- 1.02% year drop rate\n- Last sold Feb 4th 20... | 0 | 5 | None | |
| 1 | Mon Feb 22 17:23:34 +0000 2021 | AnR_Gakupo | 1363902264469950464 | I like eggplant, eggplant someone please give me&gt; &lt; #bot | 0 | 0 | None | |
| 2 | Mon Feb 22 17:20:37 +0000 2021 | AttackingFootie | 1363901520479898173 | @cfcjez__ how you calling someone a nerd while you sit in a dark room beating to some computer generated sketch😭😭😭 | 0 | 0 | None | |
| 3 | Mon Feb 22 17:28:13 +0000 2021 | BizSales247 | 1363903433393254404 | RT @JolliffeCork: If you want to stay ahead with the latest tax, employment and economic news check out our daily news updates 👇 https://t... | 0 | 1 | None | |
| 4 | Sun Feb 21 22:40:21 +0000 2021 | Blogging__Guide | 1363619557300109314 | Signal Review-How to Auto Tweet Your Blog Posts \| Blogging Guide\nhttps://t.co/WIAI6jGivh\n#autotweet #tweet... https://t.co/Ww2lsSKKIq | 0 | 0 | None | |
| 5 | Mon Feb 22 15:01:04 | Blogging__Guide | 1363866402109685762 | Signal Review-How to Auto Tweet Your Blog Posts \| Blogging [illegible] | 0 | 0 | None | |

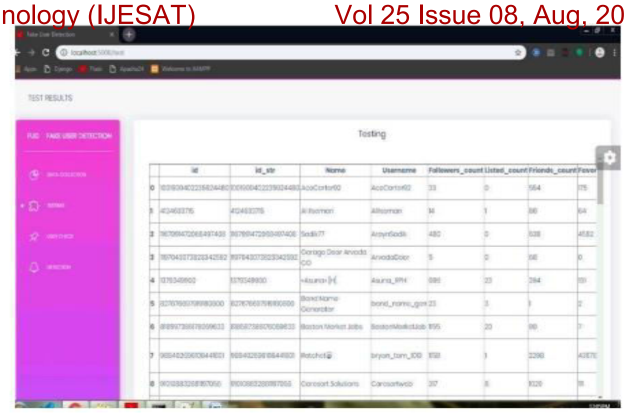
Fig 4 Module-2: Data Collection



Data Collection

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | +0000 2021 | | | https://t.co/4smPCBdyzO #Hourly | | | States', contained_within: [], bounding_box: {'type': 'Polygon', 'coordinates': [[[-75.903781, 40.148297], [-75.877805, 40.148297], [-75.877805, 40.16162], [-75.903781, 40.161624]]]}, 'attributes': {}} |
| 8 | Thu Feb 25 06:04:46 +0000 2021 | BotRakim | 1364818601332686562 | random number 66 #twitterbot | 0 | 0 | None |
| 9 | Thu Feb 25 05:04:46 +0000 2021 | BotRakim | 1364803501289644737 | random number 67 #twitterbot | 0 | 0 | None |
| 10 | Thu Feb 25 04:36:04 +0000 2021 | CodelyticTech | 1364796791901451205 | RT @hasdid: #ReactJS #Automated \| React Static Tweets https://t.co/o2q9erYvBw | 0 | 2 | None |
| 11 | Thu Feb 25 06:10:58 +0000 2021 | DubCorner | 1364820954059955203 | Spotify Now Available in Jamaica - https://t.co/hVVKjDdNl #dubcorner @dalevingo #trending #updates #jamaica... https://t.co/nGVO4X1l29x | 0 | 0 | None |
| 12 | Thu Feb 25 06:11:29 +0000 2021 | DubCorner | 1364820093378842626 | Spotify Now Available in Jamaica - https://t.co/ubpdMpGc0J #dubcorner @dalevingo #trending #updates #jamaica... https://t.co/Dn1Vd7E9Wh | 0 | 0 | None |

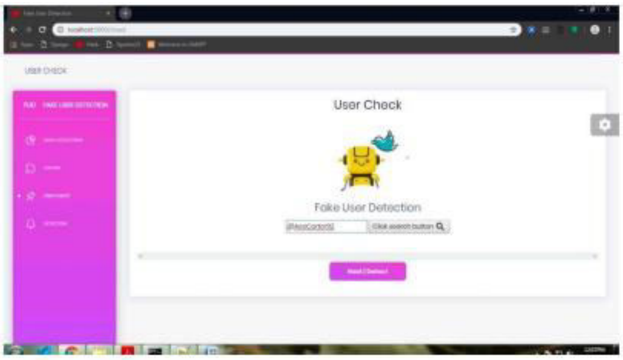
Fig 5 Data Collection



Testing

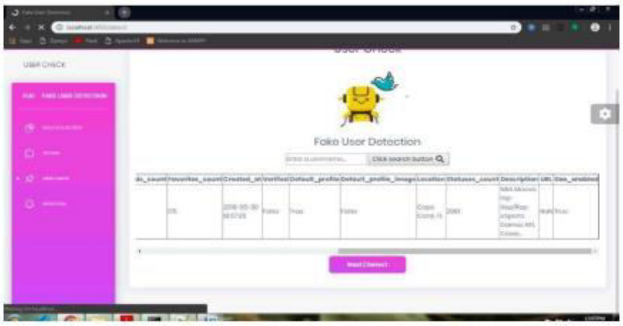
| | id | id_str | Name | Username | Followers_count | Listed_count | Friends_count | Favo |
|---|---|---|---|---|---|---|---|---|
| 0 | 1031809402235824480 | 1031809402235824480 | AceCarter92 | AceCarter92 | 33 | 0 | 564 | 175 |
| 1 | 413463376 | 413463376 | Al Rozman | Allrozman | 14 | 1 | 88 | 64 |
| 2 | 1167099472066497408 | 1167099472066497408 | Sadik77 | ArayinSadik | 480 | 0 | 538 | 4582 |
| 3 | 1197043373823342592 | 1197043373823342592 | Garage Door Arvada CO | ArvadaDoor | 5 | 0 | 66 | 0 |
| 4 | 1375349802 | 1375349800 | ~Asuna~ [H] | Asuna_RPH | 695 | 23 | 294 | 151 |
| 5 | 827676697089183000 | 827676697089183000 | Band Name Generator | band_name_gen | 23 | 3 | 1 | 2 |
| 6 | 889973889760099633 | 889973889760099633 | Boston Market Jobs | BostonMarketJob | 1195 | 20 | 90 | 7 |
| 7 | 965402096108448201 | 965402096108448201 | Ratchet🙃 | bryan_tom_100 | 1158 | 1 | 2298 | 42676 |
| 8 | 910108832268187050 | 910108832268187050 | Carosort Solutions | Carosortweb | 317 | 8 | 1026 | 18 |

Fig 6 Module -3: Testing Data



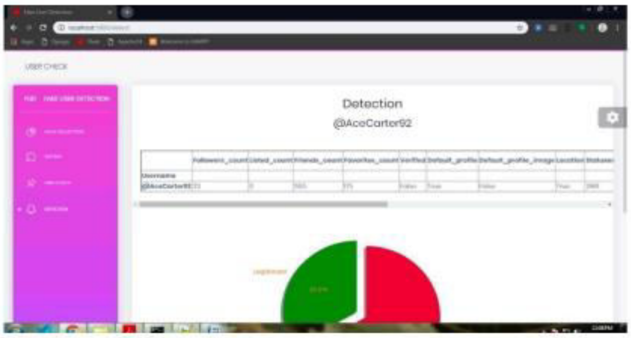
@AceCarter92

Fig 7 User Check



| ds_count | Favorites_count | Created_at | Verified | Default_profile | Default_profile_image | Location | Statuses_count | Description | URL | Geo_enabled |
|---|---|---|---|---|---|---|---|---|---|---|
| | 175 | 2018-05-30 18:57:25 | False | True | False | Cape Coral, FL | 2061 | NBA Mavericks Hip Hop/Rap sports Dallas, NFL Cowb... | [illegible] | True |

Fig 8 Details of the user are entered for verification



Detection

@AceCarter92

| | Followers_count | Listed_count | Friends_count | Favorites_count | Verified | Default_profile | Default_profile_image | Location | Statuses |
|---|---|---|---|---|---|---|---|---|---|
| Username | | | | | | | | | |
| @AceCarter92 | 33 | 0 | 565 | 175 | False | True | False | True | 2061 |

Fig 9 Details of the user are entered for verification

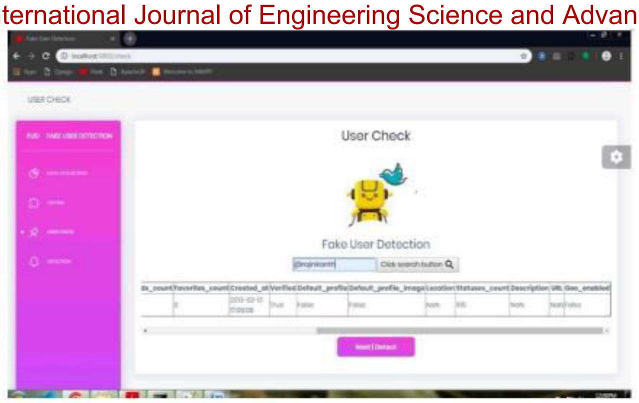


Fig 10 Enter the user details

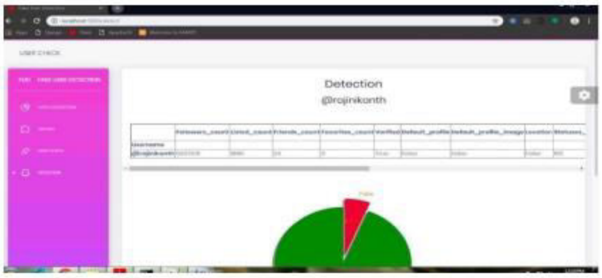


Fig 11 System verification of the user

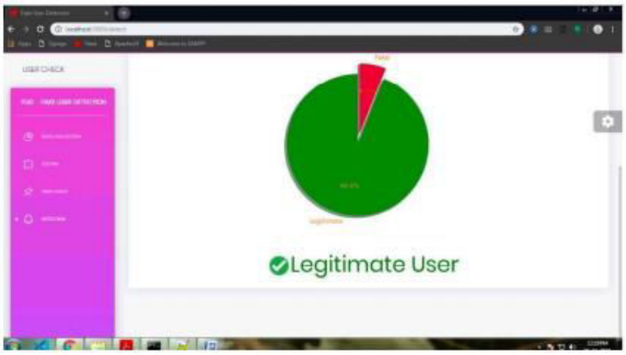


Fig 12 Genuine user

## 5. CONCLUSION

Finally, in order to keep online platforms honest, it is critical to detect fake accounts and sort through social media trash. The expansion of social media has coincided with an increase in the difficulty of detecting and controlling schemes. The spread of false information, the establishment of fake accounts, and the accumulation of an overwhelming amount of spam are among these problems. To make the process of identifying bad behavior easier, data analytics tools, natural language processing (NLP) techniques, and advanced machine learning algorithms are available.

The ability of social media platforms to distinguish between real users and spambots has been improved by the analysis of user activity, content, and network data. Furthermore, spam analysis makes it easier to remove irrelevant content that damages the platform's credibility and user experience.

## REFERENCES

1. Abkenar, S. B., Kashani, M. H., Akbari, M., & Mahdipour, E. (2020). Twitter Spam Detection: A Systematic Review. arXiv preprint arXiv:2011.14754.
2. Breuer, A., Eilat, R., & Weinsberg, U. (2020). Friend or Faux: Graph-Based Early Detection of Fake Accounts on Social Networks. arXiv preprint arXiv:2004.04834.
3. Chakraborty, M., Das, S., & Mamidi, R. (2021). Detection of Fake Users in SMPs Using NLP and Graph Embeddings. arXiv preprint arXiv:2104.13094.
4. Ferrara, E. (2022). Twitter Spam and False Accounts: Prevalence, Detection, and Characterization. arXiv preprint arXiv:2211.05913.
5. Su, X., Yang, J., Wu, J., & Zhang, Y. (2022). Mining User-aware Multi-relations for Fake News Detection in Large Scale Online Social Networks. arXiv preprint arXiv:2212.10778.
6. Bordbar, J., Mohammadrezaie, M., Ardalan, S., & Shiri, M. E. (2022). Detecting Fake Accounts Through Generative Adversarial Network in Online Social Media. arXiv preprint arXiv:2210.15657.
7. Kuruvilla, A., Daley, R., & Kumar, R. (2023). Spotting Fake Profiles in Social Networks via Keystroke Dynamics. arXiv preprint arXiv:2311.06903.
8. Chikkasabbenahalli Venkatesh, S., Shaji, S., & Meenakshi Sundaram, B. (2023). A Fake Profile Detection Model Using Multistage Stacked Ensemble Classification. Proceedings of Engineering and Technology Innovation, 24(1), 118–136.
9. Kumar, A., & Singh, R. (2023). Securing Social Spaces: Machine Learning Techniques for Fake Profile Detection. Social Network Analysis and Mining, 14(1), 99.
10. Chen, L., & Zhang, Y. (2024). CGANS: A Code-Based GAN for Spam Detection in Social Media. Social Network Analysis and Mining, 14(1), 79.

11. Patel, M., & Rao, S. (2024). Dynamic Spam Detection in Social Networks Leveraging Convex Nonnegative Matrix Factorization for Enhanced Accuracy and Scalability. ResearchGate.
12. Kishore, M. K., & Reddy, S. (2024). Comparative Analysis of Spam Detection Techniques Across Social Media Platforms. International Journal of Engineering & Science Research, 14(2), 114–123.
13. Ramdas, S., & Nair, R. (2024). Leveraging Machine Learning for Fraudulent Social Media Profile Detection. Cybernetics and Information Technologies, 24(1), 118–136.
14. Patil, D. R., Pattewar, T. M., Punjabi, V. D., & Pardeshi, S. M. (2024). Detecting Fake Social Media Profiles Using the Majority Voting Approach. EAI Endorsed Transactions on Scalable Information Systems, 11(3), e4264.