International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 3, May-June 2025

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

SPAMMER DETECTION AND FAKE USER IDENTIFICATION ON SOCIAL

[1]Uppalapati Lalitesh, [2]Mrs.P. Haritha

[1](Student Dept. of Masters of Computer Applications, Amrita Sai Institute of Science and Technology, Andhra Pradesh, India. Email: laliteshchowdhary007@gmail.com)

[2] (Asst.Prof, Dept. of Computer Science & Engineering, Amrita Sai Institute of Science and Technology, Andhra Pradesh, India. Email: inampudiharitha95@gmail.com)

----------**********----------

Abstract:

At present, Vehicular Cloud Computing (VCC) has made it possible for information exchange to take place permanently among vehicles, from any place at any time. VCC delivers two primary services: messages about safety and messages about issues other than safety. As vehicles are limited by their computing and memory, their processing and storage are mainly handled by cloud systems. Even so, because vehicles in networks move and the layouts can change fast, as well as the open communication, this makes the networks open to manipulations and information sharing errors. For these reasons, this paper suggests a framework based on ECC to guarantee secure communication among all devices on the network. The system suggested here is designed to protect confidentiality, integrity and privacy and performs mutual authentication among communicating parties. Moreover, the design includes both a one-way hash function and concatenation to block spoofing, man-in-the-middle and replay attacks. The results of the proposed scheme are checked using main metrics, including packet success ratio, data transfer speed and average delay. The research shows that the scheme is more effective than standard practises when these security steps are not included.

Keywords — *Vehicular Cloud Computing, Elliptic Curve Cryptography, Secure Communication, Authentication, Cybersecurity, Packet Delivery.*

----------**********----------

1. INTRODUCTION

Communication around the world depends on social networking, as millions interact every day on sites like Twitter, Facebook and Instagram. The same technology that helps people stay connected has given way to many unwanted and dangerous posts. The growth of spam and accounts that are not real plays a big role in dispersing unwanted, risky and phoney information.

Although Twitter is popular around the world, it is also a favourite tool for spammers to use. Unwanted tweets shared by fake accounts increase online disruption and result in the use up of valuable services on the platform. Moreover, thanks to fake identities, users might create false statements that can increase harmful acts online.

Today, researchers in online social networks (OSNs) revolve their attention around spotting spammers and fake users. Detecting phoney accounts is a key task for keeping social networks both credible and safe. Because these problems are growing, computerised methods that identify fake accounts are becoming very necessary.

The objective of this work is to build a tool using machine learning that can find spam accounts and fake users on various social platforms. When the system compares user actions, account information and message content, it can correctly sort users into

real or fraudulent accounts. For this purpose, models will learn using signals such as create date, number of followers to following, messages received and similarities in content.

2. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

Plenty of investigations have looked into the problem of detecting spam on Twitter and stopping false user identification and spam actions. Several investigations have examined the methods currently being used by the platform for spam detection, with a view to comparing them and noticing any limitations. Experts have also examined how spammers interact, giving particular importance to false user actions. Yet, there is still a hole in the research about the total spam activities happening on Twitter.

The research aims to close that gap by studying leading methods for spotting spammers and fake users online. A taxonomy is provided in the study to group existing methods for detecting spam on Twitter, covering both their progress and problems.

DISADVANTAGES OF EXISTING SYSTEM:

- **Spread of Harmful Content:** Harmful Information: Spammers put spam, fake news, rumours and malicious content out through Twitter, creating actual harm.
- **User Impersonation:** There aren't good ways to catch users who pretend to be someone else.
- **Obfuscation Techniques:** Links to malware may be hidden from detection by first using a URL shortener.
- **Ineffective Detection Approaches:** Old feature sets mean that current methods only find a limited number of new or unknown forms of spam.
- **Community Disruption:** Spammers hurt everyone on social networks by flooding them with useless content, sometimes making them hard to use.
- **No Unified Method:** Each solution, so far, concentrates on a tiny section such as user behaviour without a strategy for broad detection.

2.2 PROPOSED SYSTEM:

The objective of the proposed framework is to gain better spam detection on Twitter through classifying different types of spam detection approaches. There are four ways the system uses to identify spammers and spot phoney profiles, so it can stop spam activity easily. A few of these are:

1. **False Content Detection:** Businesses should be able to detect false or misleading messages and philtre them out.
2. **URL-Based Spam Detection:** URLs play a big part in today's spam detection because suspicious or shortened web addresses can lead to spam websites.
3. **Spam Detection in Popular Topics:** Many people share spam information. Spotting spam linked to popular topics or hashtags helps to identify it.
4. **Fake User Identification:** Fake User Accounts: You can recognise and remove user accounts only meant to deceive.

The system uses these methods to enhance existing spam-detecting techniques, giving a uniform way to find and recognise spam on Twitter.

ADVANTAGES OF PROPOSED SYSTEM:

- **Comprehensive Spam Detection:** Detects spam by using four different strategies to cover a wide variety of spam behaviours.
- **High Accuracy with Machine Learning:** The system reaches greater than 90% accuracy by using SVM and Random Forest learning techniques on only 22 of the main permissions listed in the manifest.
- **Efficient Analysis:** Using only selected features allows the new method to perform analysis up to 32 times quicker than earlier approaches.
- **Holistic Feature Usage:** With all of these kinds of features, the system is better able to decide and understand users' needs.
- **Educative and Community Support:** Supports both learning and community connexion, helping users deal with spam from schools, businesses and organisations.
- **Ease of Use and Integration:** Offers a simple method of integration and is easily accessible to all users.

3. LITERATURE SURVEY

S.No	Title	Authors	Results/Findings
1	Twitter Fake Account Detection	B. Ercahin, O. Aktas, D. Kilinc, and C. Akyol	Successfully classified fake accounts using a preprocessed dataset and Naïve Bayes.
2	Detecting Spammers On Twitter	F. Benevenuto, G. Magno, T. Rodrigues, V. Almeida	Achieved 70% accuracy for spammers and 96% for non-spammers.
3	Twitter Spam Detection: Survey of New Approaches & Comparative Study	T. Wu, S. Wen, Y. Xiang, W. Zhou	Provided taxonomy and comparative study of methods, discussing open challenges.
4	An Integrated Approach for Malicious Tweets Detection Using NLP	S. Gharge and M. Chavan	Identified malicious tweets from trending topics using content-based features.

4. SYSTEM STUDY FEASIBILITY STUDY

4.1 FEASIBILITY STUDY

The system is assessed for its possibility and value before an organisation implements it. To achieve a successful development and deployment, the study analyses technical, operational, economic and legal dimensions of the system. Three critical feasibility areas are the main focus of the analysis.

- **Economic Feasibility**
- **Technical Feasibility**
- **Schedule Feasibility**

4.2 ECONOMIC FEASIBILITY

With open-source software and libraries, the proposed system is able to save on unnecessary licenced software. In addition, thanks to public data resources like Kaggle, companies can obtain needed data much more affordably. As a consequence, the system becomes both affordable and effective for educational and research environments.

4.3 TECHNICAL FEASIBILITY

From a technical point of view, the system is doable thanks to commonly accepted tools and methods.

- **Programming Language**: The language used in this course is Python which is appreciated in data analysis and machine learning.
- **Libraries**: You have access to a group of libraries like Scikit-learn, NLTK, Matplotlib, Pandas and TensorFlow.
- **Machine Learning Models**: Machine Learning Models use Naïve Bayes and Random Forest since they are efficient and effective when sorting data.
- **Data Format**: The data you'll get from us is Twitter data in JSON format, making it easy to work with and sort.

Lightweight algorithms and models allow the system to run efficiently which requires no advanced hardware.

4.4 OPERATIONAL FEASIBILITY

The system can be used in practise and is designed for simple handling. We build the interface using Python's Tkinter package which helps users quickly handle their data and see the results. With this in place, anyone with basic technical ability can work the system. On top of this, the platform is designed to detect and philtre out spam and fake accounts, saving time and making fewer errors compared to manual review.

5. SYSTEM REQUIREMENTS

5.1 Software Requirements

Category	Requirement
Operating System	Windows 8/9/10/11
Coding Language	Python 3.7
Type of Application	GUI Application
Front-End Technologies	Tkinter API
Backend Technologies	NLTK, Matplotlib, Pandas, Numpy, Scikit-learn
IDE Tool	PyCharm Community Edition 2021
Dataset	36 Twitter Accounts (Kaggle.com)

5.2 Hardware Requirements

Category	Requirement
System Processor	Intel i3 or above
Hard Disk	4 GB minimum or above
Monitor	14/10/12/15-inch Color Monitor
RAM	4 GB minimum or above

6. SYSTEM DESIGN

6.1 SYSTEM ARCHITECTURE

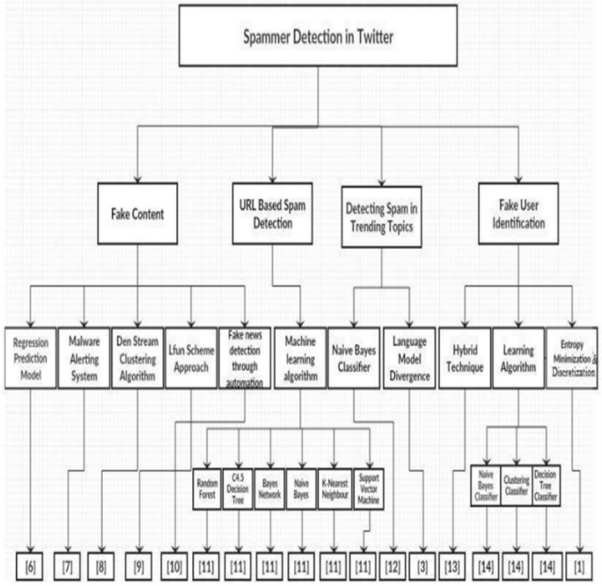
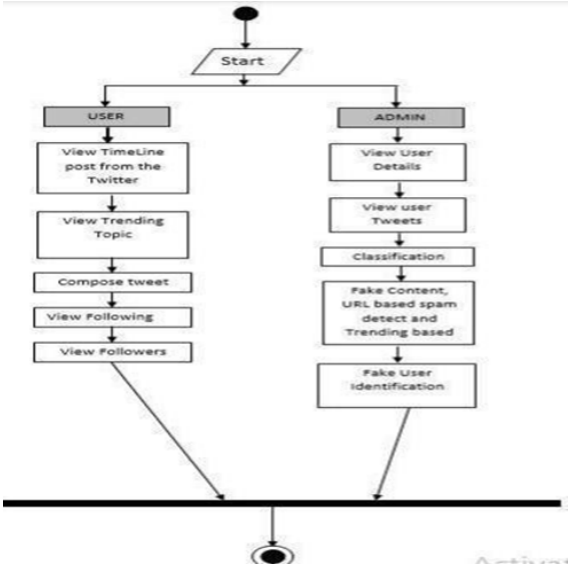
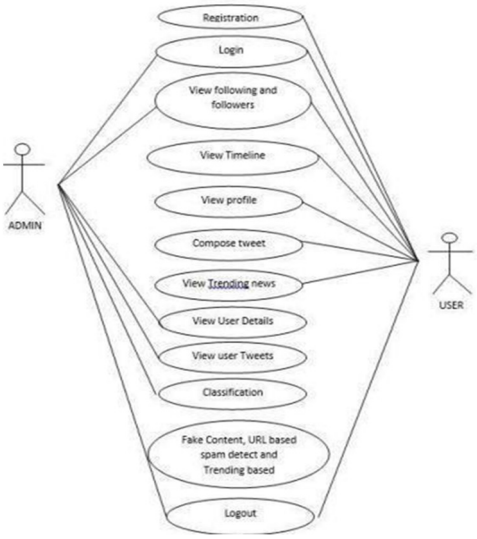


FIGURE 1. Taxonomy of spammer detection/fake user identification on Twitter.

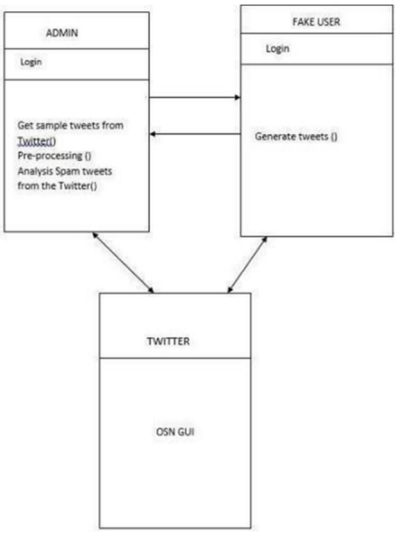
6.2 DATA FLOW DIAGRAM



5.3 USE CASE DIAGRAM



5.4 CLASS DIAGRAM



7. OUTPUT SCREENS

Fig : Use the "Upload" button to bunch the tweets folder into the (Social Media) collection.

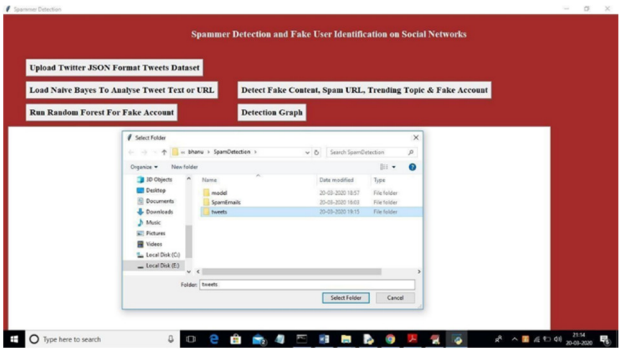


Fig: Make sure to put the 'tweets' folder in JSON format.

Fig: Click here to analyse either my tweets or your own using Naïve Bayes and other techniques.

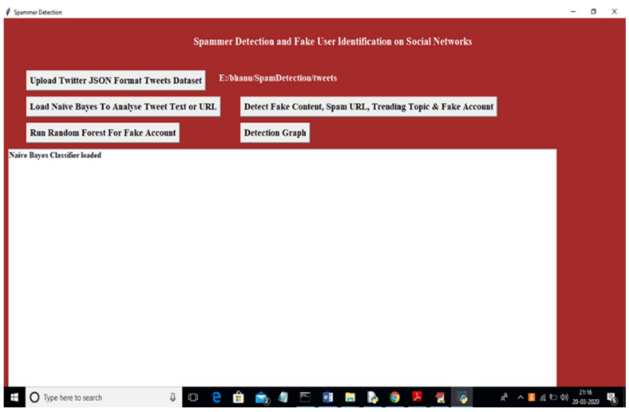


Fig: Click the link to start using Naïve Bayes for analysing tweets.

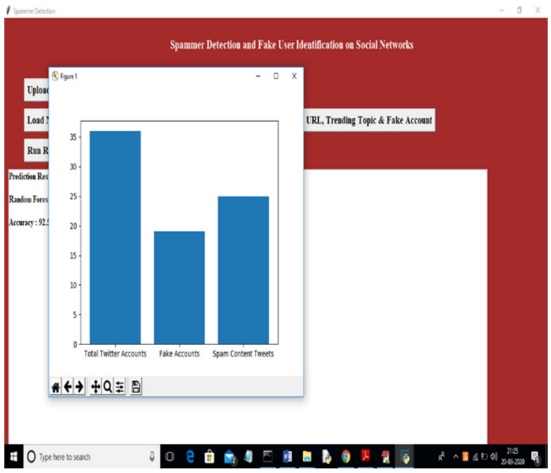


Fig: The x-axis covers results of total tweets

8. CONCLUSION

In this research, we looked at many approaches for finding spammers on Twitter. Each of these approaches was grouped into four main areas: fake content, spam produced from a URL, spam in trending topics and detecting fake users. We looked at how different the methods were in terms of user features, content features, graph features, structural features and time features. I also analysed what the authors hoped to achieve with these methods and what data they used.

This review was written to gather and explain the current best practises for finding spam and fake users on Twitter. Although rapid strides have been made in developing good detection approaches, some important questions have not yet been answered. The problem of misidentifying false news on social media is important since it has strong effects on people's lives and communities. Besides, more research could be done to learn how rumours on social media are distributed. Whilst previous research has investigated statistics for finding rumours, new solutions based on social networks which have shown approachable outcomes, are now needed. Work in these subjects is likely to support more powerful spam catching and help safeguard the Internet.

ACKNOWLEDGEMENT

I am thankful to the Management of Amrita Sai Institute of Science and Technology for giving me an opportunity to work with his project.
I would like to the thank **Dr. M. Sasidhar**, Principal, Amrita Sai institute of science and technology, for his constant encouragement and support during the progress of this work.
I am deeply grateful to **Dr. P. Chiranjeevi**, Professor and Head of the Department, for his valuable guidance and consistent support during the course of the project.
A special note of thanks to my internal guide, **Mrs.P. Haritha**, for her exceptional guidance, constant motivation, and continuous encouragement, which played a crucial role in the successful completion of this project.

UPPALAPATI LALITESH

REFERENCES

[1] C. Chen, S. Wen, J. Zhang, Y. Xiang, J. Oliver, A. Alelaiwi, and M. M. Hassan, "Investigating the deceptive information in Twitter spam," *Future Gener. Comput. Syst.*, vol. 72, pp. 319–326, Jul. 2017.

[2] I. David, O. S. Siordia, and D. Moctezuma, "Features combination for the detection of malicious Twitter accounts," in *Proc. IEEE Int. Autumn Meeting Power, Electron. Comput. (ROPEC)*, Nov. 2016, pp. 1–6.

[3] M. Babcock, R. A. V. Cox, and S. Kumar, "Diffusion of pro- and anti-false information tweets: The black panther movie case," *Comput. Math. Org. Theory*, vol. 25, no. 1, pp. 72–84, Mar. 2019.

[4] S. Keretna, A. Hossny, and D. Creighton, "Recognising user identity in Twitter social networks via text mining," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2013, pp. 3079–3082.

[5] C. Meda, F. Bisio, P. Gastaldo, and R. Zunino, "A machine learning approach for Twitter spammers detection," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2014, pp. 1–6.

[6] W. Chen, C. K. Yeo, C. T. Lau, and B. S. Lee, "Real-time Twitter content polluter detection based on direct features," in *Proc. 2nd Int. Conf. Inf. Sci. Secur. (ICISS)*, Dec. 2015, pp. 1–4.

[7] H. Shen and X. Liu, "Detecting spammers on Twitter based on content and social interaction," in *Proc. Int. Conf. Netw. Inf. Syst. Comput.*, pp. 413–417, Jan. 2015.

[8] G. Jain, M. Sharma, and B. Agarwal, "Spam detection in social media using convolutional and long short term memory neural network," *Ann. Math. Artif. Intell.*, vol. 85, no. 1, pp. 21–44, Jan. 2019.

[9] M. Washha, A. Qaroush, M. Mezghani, and F. Sedes, "A topic-based hidden Markov model for real-time spam tweets filtering," *Procedia Comput. Sci.*, vol. 112, pp. 833–843, Jan. 2017.

[10] F. Pierri and S. Ceri, "False news on social media: A data-driven survey," 2019, arXiv:1902.07539. [Online]. Available: https://arxiv.org/abs/1902.07539.

[11] S. Sadiq, Y. Yan, A. Taylor, M.-L. Shyu, S.-C. Chen, and D. Feaster, "AAFA: Associative affinity factor analysis for bot detection and stance classification in Twitter," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Aug. 2017, pp. 356–365.

[12] M. U. S. Khan, M. Ali, A. Abbas, S. U. Khan, and A. Y. Zomaya, "Segregating spammers and unsolicited bloggers from genuine experts on Twitter," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 551–560, Jul./Aug. 2018.

