



Twitter Malicious Account and Content Detection using Machine Learning

JMSV Ravi Kumar¹, M. Babu Reddy², Siva Chintaiyah Narni³, Jala Prasad Rao⁴, M.Srikanth⁵

Associate Professor¹, Assistant Professor^{2,3,4,5}

Department of IT^{1,5}, Department of Computer Science², Department of CSE^{3,4}

SRKR Engineering College^{1,5}, Krishna University, Machilipatnam², Seshadri Rao Gudlavalleru Engineering College³,

Aditya Engineering College (A)⁴

(Received: 07 January 2024

Revised: 12 February 2024

Accepted: 06 March 2024)

KEYWORDS

Online social network, fake content detection, fake user's detection, tweets.

ABSTRACT:

The capacity to link individuals all over the globe to share media and ideas has contributed to the meteoric rise in popularity of social networks. Making false accounts is a big problem on these networks, and one that consumers are really worried about. As an example, Twitter permits an excessive quantity of spam because it has grown into one of the most widely utilized platforms ever. False accounts promote unwanted services or websites through tweets, which impacts legitimate users and disrupts resource utilization. A popular field of research in current online social networks is the detection of spammers and the identification of fraudulent users on Twitter. Recent polls conducted by research delegates included a taxonomy that classifies Twitter spammers into two broad categories. The first group deals with the topic of detecting fake content, which is often accomplished through the use of a regression prediction model, or lfun scheme. Fake User Identification is another subcategory that focuses on identifying fraudulent Twitter users using a combination of user- and content-based criteria.

I. INTRODUCTION

Moods, opinions, and news are just some of the things that users of the microblogging service Twitter can exchange with one another. Instantaneous transmission to followers allows users to disseminate received information to a far larger audience when they tweet. Con artists can readily take advantage of those who are naive about online social networks. Protecting social media platforms from spam is no easy feat. In order to protect users from many types of harmful attacks and to maintain their security and privacy, it is crucial to identify spam on social networking sites. Twitter spammers transmit false information, fake news, and other forms of misinformation for a variety of reasons. tales, and unscheduled communications. The initial users, who are referred to as original users, are disrupted by these activities. Also, the online social media sites' reputation takes a hit.

Publish the same update many times. The goal of spammers is to trick Twitter users into thinking they are receiving unwanted messages. We can learn about the necessary security measures to take on a daily basis and in our social media interactions through text detection. Here, we need to identify malicious and undesired social media profiles so we can free up storage space. Protecting social media platforms from spam is no easy

feat. Recognizing fraudulent users on social media platforms is critical for protecting users from various forms of cybercrime and ensuring their privacy and security. When spammers use these dangerous tactics, it wreaks havoc on the community offline. This occurs because, in order to evade detection by security organizations, spammers alter the text of tweets while maintaining the semantics. Therefore, we suggest the lfun method as a solution to the imposter user problem. One of the primary goals is to identify fraudulent users and content.

II. LITERATURE SURVEY

In order to identify spam on Twitter, a number of studies have been conducted. The topic of Twitter impersonation has also been the subject of several surveys. Here at Tegmental, we've compiled a list of all the latest strategies for Twitter spam detection. The survey provides an analysis of these methods in comparison. However, the authors surveyed spammers on Twitter and found that they displayed very different habits. A literature evaluation is also included in the report, which confirms that spammers indeed exist on the social network Twitter. There is a void in the current literature, even though there has been numerous research studies on the subject. Hence, to fill the void, we typically examine developments in Twitter's spammer detection and false user identification



systems.

This paper's objective is to catalog several methods for Twitter spam detection and to group them into various groups. In terms of categorization, we have found two ways to report spammers that can aid in detecting user impersonation. False information about the sender and recipient can help identify spammers. It not only compares the aims and outcomes of different methodologies, but it also compares current procedures, which helps consumers understand the relevance and efficacy of the suggested methodology. This compares various methodologies.

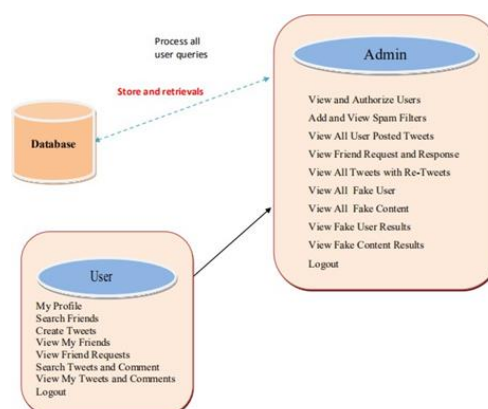
characteristics utilized for the purpose of detecting Twitter bots. Methods for Detecting False Content: After reviewing a comparative survey that compares many methods for detecting bogus content, we settled on the Lfun Scheme Approach method because of its superior performance and accuracy. In addition, the likelihood of users being exposed to hazardous content due to the expansion of inaccurate information through false identities has increased. Identifying spammers and fraudulent Twitter users has recently been a standard subject of study for contemporary online social networks. The purpose of this paper is to provide a comprehensive overview of the methods now in use to identify Twitter spammers. We chose the Fun Scheme Approach, one of several recommended methods, for detecting bogus content because of its superior performance.

Faiza Masoodi and Ghana Ammadi conducted research on methods for identifying fake users. Conducted by Faiza Masoodi and Ghana Ammadi: This study discusses several methods and ultimately selects a hybrid approach. Hybrid Technique combines user- and content-based approaches and incorporates Bow Technique as one method. Using the aforementioned method, the authors of this study were able to spot the spam that fraudulent individuals were constantly posting on popular social media platforms like Twitter. By detecting and identifying bogus users, this strategy helps to protect legitimate users from spammers' destructive content and boosts the social networking site's reputation.

III. PROPOSED SYSTEM

An elaborate categorization of spammer detection approaches is provided by the suggested system. The proposed taxonomy for spammer identification is displayed by the system. Recent polls have classified these spammers into two groups: those who spread false information and those who utilize false identities. Models, techniques, and detection procedures are the foundation of each class of identification methods. To begin with, there is a particular group. The

first group deals with methods for identifying false material, such as the Lfun scheme approach and regression models, while the second group identifies false users by using hybrid strategies, such as the bow technique. These methods detect the spam and label the sender as an imposter. Measurements for social reputation, (ii) metrics for global engagement, (iii) metrics for subject engagement, (iv) metrics for likability, and (v) metrics for credibility were used to detect the spread of fraudulent content.



Potential Benefits of the Suggested Approach: The typical quantity of verified accounts classified as spam or not spam and (ii) the quantity of accounts that users have followers. It also makes it easier to detect the constant stream of false content that Twitter spammers create. To forecast the future expansion of bogus content and guarantee the overall influence of those who disseminate it, the authors used the Lfun scheme model. This enhances the credibility of the social media platform.

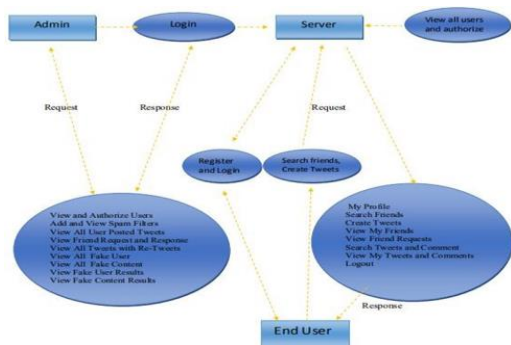
IV. IMPLEMENTATION METHODOLOGY:

There are a lot of techniques used for fake content detection and fake user identification from many surveys done. Out of which we chose bow technique for fake content detection in which classifying the words that are generally used by the fake users like bad words into different categories of spam filter names and if those spam words are found in the tweets they put then the content will be a given a spam filter name accordingly and considered it as a fake content.

The same goes for identifying the imposters. The Lfun



technique is selected from various alternatives because it can detect continuous spam produced by Twitter and flag users as fake if they repeatedly tweet about the same topic in an effort to create rumors, spread fake news, or attract unwanted attention. The admin module and the user module are both part of this. Using a valid username and password, the admin can access the admin module. Once logged in, he will be able to do things like see all user-posted tweets, all friend requests and responses, all tweets with retweets, all fake users, all fake content, all fake user results, and all fake content results. He can also add and view spam filters. Numerous users (n). Before performing certain tasks, users are required to register. Once the registration is successful, he will need to wait for the administrator to authorize his account. After that, he can enter the permitted login credentials and access the system. The user can access their profile, search for friends, create tweets, view their friends, view friend requests, search for tweets and comments, view their own tweets and comments, and finally, log out of their account.



RESULTS AND DISCUSSION

Fake Users and Content Detection on Twitter

Authorize Users and Detect Account Status

ID	User Image	User Name	Email	Mobile	Address	Status	Account Status
11		Ch.Neeraja	neerujaneeraj@gmail.com	9949558676	Isichal varapeta,rjplmndry	Authorized	Normal
12		h.rohith	rohith@gmail.com	9967654	Jaybhawanadrfgh	Authorized	Normal

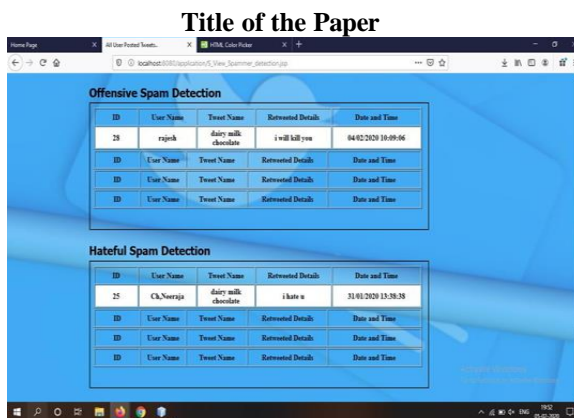
fig(1):Initial status of the user after login

Before any operations are made in each user's account, the status of each user who has registered, been authorized by the admin, and successfully logged in is shown in figure 1.



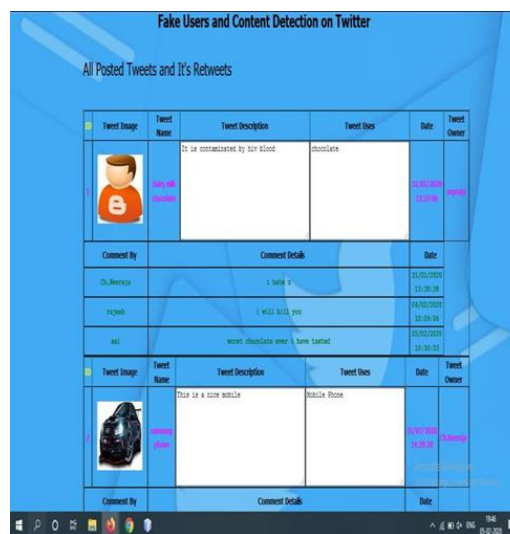
fig(2):Spam categories based on the spam words used by the fake users

The admin can add and inspect many more terms in his module, and the various categories illustrated in fig. (2) demonstrate the filtering of spam words using a spam filter name.



fig(3): User tweet and it's re-tweets

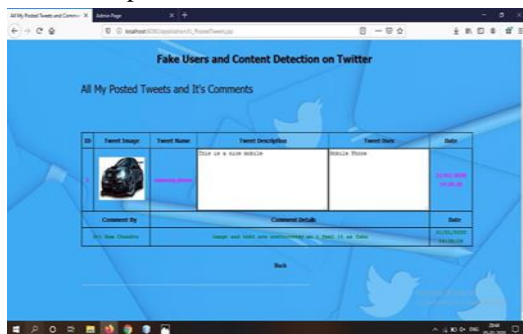
Figure 3 shows the user module view, where he can see his own tweets as well as those of his friends. The view also shows the time and name of the retweeted user.



fig(4): All users posted tweets and their re-tweets



Figure 4 shows the admin module. Here, the admin may see every single tweet that a user has sent, as well as any retweets. Each tweet includes the user's name, the name of the tweet, a description, and the time the user posted it.



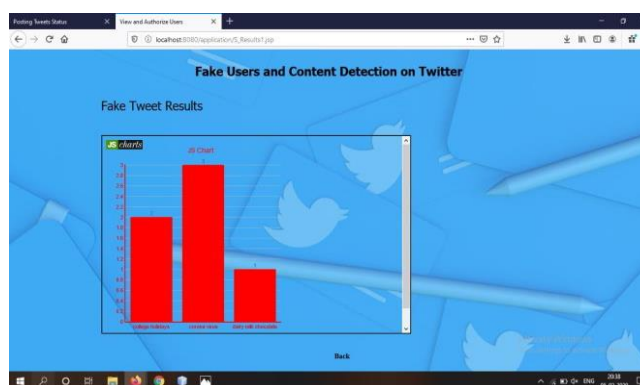
fig(5): Fake Content detection

Figure 5 displays tabular data from each spam category, including user names, tweet names, content, posting date and time, and any false content the admin has identified based on user-used spam words.

	b.rohith	rohith@gmail.com	9987654	jaytrestedrfgh	Authorised	Normal
	supraja	twinklomehta1610@gmail.com	9023478972	okytresdfcvbnjklqerty	Authorised	Fake User
	Sri Ram Chandra	sriram@gmail.com	9023478972	rajahmundry	Authorised	Normal

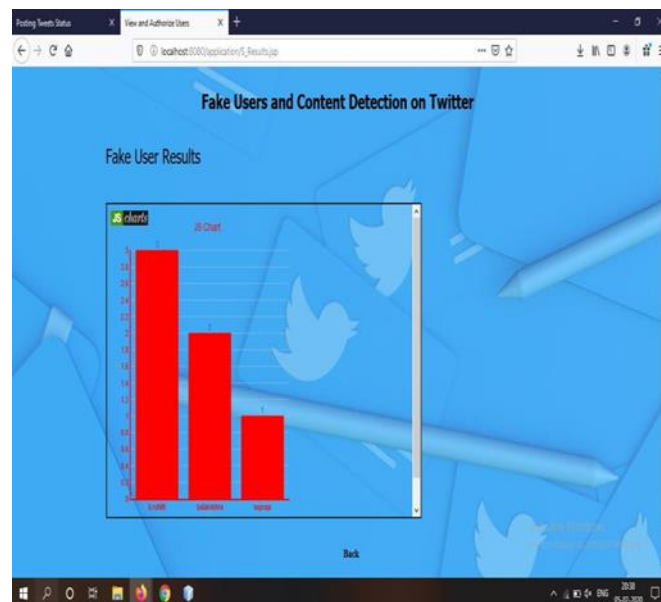
fig(6):Final status of the user

Based on their account activity, such as the material they post and the frequency with which they tweet about a particular subject, we can tell whether a user is legitimate or not (see fig. 6).



fig(7):Results of fake tweets posted

A visual depiction of the totality of the false tweet content, including the name of the tweet and the frequency with which it was sent on the specific subject, is shown in figure 7.



fig(8): Results of fake users detected

The fig(8) shows the graphical representation of the overall fake users detected through their action they performed like continuous spam produced by the users by showing the user name and the number of times they tried to produce the spam content.

CONCLUSIONS AND FUTURE SCOPE

We reviewed methods for identifying Twitter spammers. Furthermore, we also provided a taxonomy of methods for detecting spam on Twitter, classifying them as either fake content detection or fake user detection. Researchers are hoping that this evaluation will provide a centralized source of knowledge on advanced Twitter spam detection systems. There are still several unanswered questions that need a lot of study, even though researchers have developed excellent methods for Twitter spam detection and fake user identification. The most significant problem with social media is the proliferation of phony accounts and the subsequent flood of unwelcome tweets that invade the privacy of real users. We detect spammers by looking for false content and by looking for fake users. We have used the most effective methods for dealing with these two types of spam, such as the lfun scheme approach and the bow technique, which are based on features like emotion analysis. We need to identify



spam by determining the frequency of harmful word usage, the types of harmful word combinations, and the frequency of each word. Additionally, we will flag a user as fraudulent if they frequently tweet about the same issue. Last but not least, the administrator will showcase all the false user-generated information and results.

REFERENCES

1. B.Venkateswarlu, Bhargavi Pandreka: "Spammer Detection and Fake user Identification", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 8 Issue 11, November-2019.
2. Faiza Masood, Ghana Ammad, Ahmad Almogren: "Spammer Detection and Fake User Identification on Social Networks", Special Section On Roadmap To 5g: Rising To The Challenge.
3. Varad Vishwarupe, Mangesh Bedekar, Milind Pande, Anil Hiwale1, "Intelligent Twitter Spam Detection: A Hybrid Approach", Springer WS4 International Conference on Smart Trends in Systems, Security and Sustainability, At London.
4. B. Erçahin, Ö. Akta³, D. Kiliç, and C. Akyol, "Twitter fake account detection," in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388392. F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting spammers on Twitter," in Proc. Collaboration, Electron. Messaging, Anti- Abuse Spam Conf. (CEAS), vol. 6, Jul. 2010, p. 12.
5. S. Gharge, and M. Chavan, "An integrated approach for malicious tweets detection using NLP," in Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT), Mar. 017, pp. 435438.
6. T. Wu, S. Wen, Y. Xiang, and W. Zhou, "Twitter spam detection: Survey of new approaches and comparative study," Comput. Secur., vol. 76, pp. 265284, Jul. 2018.
7. S. J. Soman, "A survey on behaviors exhibited by spammers in popular social media networks," in Proc. Int. Conf. Circuit, Power Comput. Tech- nol. (ICCPCT), Mar. 2016, pp. 16.
8. A. Gupta, H. Lamba, and P. Kumaraguru, "1.00 per RT #BostonMarathon # prayforboston: Analyzing fake content on Twitter," in Proc. eCrime Researchers Summit (eCRS), 2013, pp. 112.
9. F. Concone, A. De Paola, G. Lo Re, and M. Morana, "Twitter analysis for real-time malware discovery," in Proc. AEIT Int. Annu. Conf., Sep. 2017, pp. 16.
10. N. Eshraqi, M. Jalali, and M. H. Moattar, "Detecting spam tweets in Twitter using a data stream clustering algorithm," in Proc. Int. Congr. Technol., Commun. Knowl. (ICTCK), Nov. 2015, pp. 347351.
11. C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, "Statistical features-based real-time detection of drifted Twitter spam," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 914925, Apr. 2017.
12. C. Buntain and J. Golbeck, "Automatically identifying fake news in popular Twitter threads," in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Nov. 2017, pp. 208215.
13. C. Chen, J. Zhang, Y. Xie, Y. Xiang, W. Zhou, M. M. Hassan, A. AlElaiwi, and M. Alrubaian, "A performance evaluation of machine learning-based streaming spam tweets detection," IEEE Trans. Comput. Social Syst., vol. 2, no. 3, pp. 6576, Sep. 2015.
15. "Automatic vehicle number plate recognition system using machine learning." IOP Conference Series: Materials Science and Engineering. Vol. 1074. No. 1. IOP Publishing, 2021.
16. Parvathi, D. S. L., et al. "Emotion Analysis Using Deep Learning." 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2020.
17. Dara, Suresh, et al. "Artificial bee Colony algorithm: a survey and recent applications." International Journal of Pure and Applied Mathematics 120.6 (2018): 313-321.
18. Kumar, Dr Jmsv Ravi, and M. CHANDINI. "SECRBAC: Secure Data In The Clouds." International Journal of Research 5.15 (2018): 95-106.
19. Estharakula, Suresh, and Kumar JMSV Ravi. "EBPH-MAC: Emergency Based Priority Hybrid Medium Access Control for Mobility Aware Cooperative WSN's In Indoor Industrial Monitoring." International Journal of Research 5 (2018): 1456-1465.
20. Kumar, J. M. S. V., et al. "System Testability Assessment and testing with Micro architectures." International Journal of Advanced Research in Computer Science 2.6 (2011).
21. Kumar, J. M. S. V., et al. "Reverse Engineering A Generic Software Exploration Environment Is Made Of Object Oriented Frame Work And Set Of Customizable Tools." International Journal of Advanced Research in Computer Science 2.5 (2011).
22. Kumar, J. M. S. V., et al. "Analyzing the Modern Tool-Supported UML-Based Static Reverse Engineering." International Journal of Advanced Research in Computer Science 3.4 (2012).



23. Kumar, J. M. S. V., et al. "Active Scrutiny Techniques for the Reconstruction of Architectural Views." *International Journal of Advanced Research in Computer Science* 3.1 (2012).
24. N Santha Raju, JMSV Kumar, B Sujatha, "Time series analysis of stock price movements: Insights from data mining using machine learning", *Journal AIP Conference Proceedings*, Volume 2492, Issue 1, Publisher AIP Publishing, 2023.
25. Prayaga Atchyut Pavan, Sattibabu Sattibabu, JMSV Kumar "A deep learning approach to detect malaria" *Journal AIP Conference Proceedings*, Volume 2492, Issue 1, Publisher AIP Publishing, 2023.
26. Ch Bhanu Revathi, JMSV Kumar, B Sujatha "Intracranial hemorrhage detection in human brain using deep learning" *Journal AIP Conference Proceedings*, Volume 2492, Issue 1, Publisher AIP Publishing, 2023.
27. JMSV RAVI KUMAR " Human Activity Recognition using Machine Learning " *Journal AIP Conference Proceedings*, Volume 2492, Issue 1, Publisher AIP Publishing, 2023.
28. J Kumar, A Shahi, R Aytha, G Varri, D Brundavanam " Vehicle theft prevention system using IoT " *Journal AIP Conference Proceedings*, Volume 2492, Issue 1, Publisher AIP Publishing, 2023.
29. J Kumar, TD Nagendra, M Harshitha, AB Prakash " Fake image detection using CNN " *Journal AIP Conference Proceedings*, Volume 2492, Issue 1, Publisher AIP Publishing, 2023.
30. J Kumar, MN Kumar, NV Narendra, P Pradeep " driver drowsiness monitoring system using machine learning svm algorithm " *Journal AIP Conference Proceedings*, Volume 2492, Issue 1, Publisher AIP Publishing, 2023.
31. JMSV RAVI KUMAR " A Symmetric Searchable Encryption Identification of Data on Probabilistic Trapdoors " *International Journal of Engineering and Advanced Technology (IJEAT)*, ISSN: 2249 – 8958, Volume 9, Issue 3, Publisher Blue Eyes Intelligence Engineering & Sciences Publication, 2020.
32. JMSV RAVI KUMAR "Artificial Bee Colony Algorithm: A Survey and Recent Applications" published in *International Journal of Pure and Applied Mathematics*, ISSN 1314-3395, VOLUME 118, ISSUE 24 , Jul-18.
33. JMSV RAVI KUMAR " Authentication for Cloud Services using Steganography" published in *International Journal of Engineering and Technology(UAE)-IJET*, ISSN 2227-524X, VOLUME 7, ISSUE 3.49 , Jul-18.
34. JMSV RAVI KUMAR "A review on task scheduling algorithms in cloud computing and their approaches" published in *International Journal of Pure and Applied Mathematics*, ISSN 1314-3395, VOLUME 118, ISSUE 24, Jul-18.
35. JMSV RAVI KUMAR "Review of Data mining Technique using SaaS on the Cloud" published in *International Journal of Pure and Applied Mathematics*, ISSN 1314-3395, VOLUME 118, ISSUE 24 , Jul-18.
36. JMSV RAVI KUMAR "Smart Controlling, Monitoring and Automation of Street Light System using Raspberry PI " published in *International Journal of Pure and Applied Mathematics*, ISSN 1314-3395, VOLUME 118, ISSUE 24 , Jul-18.
37. JMSV RAVI KUMAR " A Survey on Internet of Things for Healthcare and Medication Management" was authored by JMSV Ravi Kumar published in *International Journal of Pure and Applied Mathematics*, ISSN 1314-3395, VOLUME 118, ISSUE 24 , Jul-18.
38. JMSV RAVI KUMAR " SEC RBAC: Secure Data in the Clouds" was authored by JMSV Ravi Kumar published in *International Journal of Research*, ISSN 2348-6848, VOL 5, ISSUE 15 , Jul-18.
39. JMSV RAVI KUMAR " EBPH MAC: Emergency Based Priority Hybrid Medium Access Control for Mobility Aware Cooperative WSN's In Indoor Industrial Monitoring" published in *International Journal of Research*, ISSN 2348-6848, VOLUME 5, ISSUE 12 , Jul-18.
40. JMSV RAVI KUMAR " Prioritizing software components for realistic reuse" published in *International Journal of Sciences & Applied Research*, ISSN 2394-2401, VOL 4, ISSUE 24, Jul-17.
41. JMSV RAVI KUMAR " Cloud Storage Services and Privacy Protection" published in *International Conference on Research Advancements in Computer Science and Communication*, ISSN 978-93-85100-64-2, VOL 5, ISSUE 3.49, December-16.
42. JMSV RAVI KUMAR "Analyzing the Modern Tool-Supported UML-Based Static Reverse Engineering" published in *International Journal of Advanced Scientific Research and Technology*, ISSN 0976-5697, VOL 3, ISSUE 4, Jul-12.
43. JMSV RAVI KUMAR "Active Scrutiny Techniques for the Reconstruction of Architectural Views" published in *International Journal of Advanced Scientific Research and Technology*, ISSN 0976-5697, VOL 3, ISSUE 1, January-12.
44. JMSV RAVI KUMAR "System Testability Assessment and testing with Micro architectures" published in *International Journal of Advanced Scientific Research and Technology*, ISSN 0976-5697, VOL 2, ISSUE 6, December-11.
45. JMSV RAVI KUMAR "Reverse Engineering A Generic Software Exploration Environment is made of Object-Oriented Frame Work and Set of Customizable Tools" published in *International Journal of Advanced Scientific Research and Technology*, ISSN 0976-5697, VOL 2, ISSUE 5, September-2011.



46. M. Srikanth, "Integrated Technologies for Proactive Bridge-Related Suicide Prevention", *Journal of Namibian Studies*, Volume 1, Issue 33, Pages 2117-2136, ISSN: 1863-5954, Sep 2023.
47. M. Srikanth, "Deep Learning Approaches for Predictive Modeling and Optimization of Metabolic Fluxes in Engineered Microorganism" *International Journal of Research in Science & Engineering (IJRISE)* ISSN: 2394-8299, 3(05), 1-11. <https://doi.org/10.55529/ijrise.35.1.11>, July 2023.
48. M. Srikanth, "Tackling Outliers for Predictive Smallholder Farming Analysis," in *Proceedings of the 2023 3rd International Conference on Smart Data Intelligence (ICSMDI)*, pp. 93-98, IEEE Xplore, March 26, 2023.
49. M. Srikanth, "Blockchain-Based Consensus For A Secure Smart Agriculture Supply Chain," *European Chemical Bulletin*, vol. 12, special issue 4, pp. 8669-8678, 2023. [Online]. Available: [doi: 10.48047/ecb/2023.12.si4.776](https://doi.org/10.48047/ecb/2023.12.si4.776). ISSN: 2063-5346, 2023.
50. M. Srikanth, "Predict Early Pneumonitis in Health Care Using Hybrid Model Algorithms," *Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN)*, vol. 3, issue 03, pp. 14-26, ISSN: 2799-1172, Apr. 2023.
51. M. Srikanth, R. N. V. Jagan Mohan, M. Chandra Naik. (2023). A New Way to Improve Crop Quality and Protect the Supply Chain is to use a Trajectory Network and Game Theory. *Mathematical Statistician and Engineering Applications*, 71(4), 10600-10610. <https://doi.org/10.17762/msea.v71i4.1952>, ISSN: 2094-0343, 2023
52. M. Srikanth, "Auction Algorithm: Peer-To-Peer System Based on Hybrid Technologies for Smallholder Farmers to Control Demand and Supply," *International Journal of Research In Science & Engineering (IJRISE)*, vol. 3, issue 1, pp. 9-23, 2023.
53. M. Srikanth, "Smallholder Farmers Crop Registering Privacy-Preserving Query Processing over Ethereum Blockchain," *Journal of Pharmaceutical Negative Results*, vol. 13, issue 7, pp. 5609-5617, Dec. 2022.
54. M. Srikanth, "The Early Detection of Alzheimer's Illness Using Machine Learning and Deep Learning Algorithms," *Journal of Pharmaceutical Negative Results*, vol. 13, issue 9, pp. 4852-4859, Nov. 2022.
55. M. Srikanth, "Small Holders Farming Predictive Analysis Using Peer-To-Peer Approach," *International Journal of Agriculture and Animal Production*, vol. 2, issue 05, pp. 26-37, Sep. 2022.
56. M. Srikanth, "Using Machine Learning and Neural Networks Technologies, a Bottom-Up Water Process Is Being Used To Reduce All Water Pollution Diseases," *Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN)*, vol. 2, Oct. 2022.
57. M. Srikanth, "Blockchain Enable for Smallholder's Farmers Crop Transaction Using Peer-to-Peer," *Indo-American Journal of Agricultural and Veterinary Sciences*, vol. 10, issue 3, pp. 33-43, Sep. 2022.
58. M. Srikanth, "Protecting Tribal Peoples Nearby Patient Care Centres Use a Hybrid Technique Based on a Distribution Network," *International Journal of Health Sciences*, Jun. 2022.
59. M. Srikanth, "Blockchain-Based Crop Farming Application Using Peer-to-Peer," *Journal of Xidian University*, Apr. 2022.
60. M. Srikanth, "Stop Spread Corona Based on Voice, Face and Emotional Recognition Using Machine Learning, Query Optimization and Blockchain Technology," *Solid State Technology*, Vol. 63 No. 6 (2020)
61. M. Srikanth, "Machine Learning for Query Processing System and Query Response Time Using Hadoop," *IJMTST*, Aug. 2020.
62. M. Srikanth, "Block-level Based Query Data Access Service Availability for Query Process System," *IEEE*, Page 1-9, Jul. 2020.
63. M. Srikanth, "Query Response Time in Blockchain Using Big Query Optimization," *The Role of IoT and Blockchain Techniques and Applications from Computer Science and Information Management*, Apple Academic Press, Exclusive Worldwide distribution by CRC Press Taylor & Francis Group, Jan. 2022.
64. M. Srikanth, "A New Approach for Authorship Verification Using Information Retrieval Features," *Springer-ICSE*, vol. 74, pp. 23-29.
65. M. Srikanth, "An Enhanced and Naive Clustering Algorithm for Text Classification Based on Weight," *International Journal & Magazine of Engineering, Technology, Management and Research*, Dec.012.