JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

DETECTING SPAMERS AND IDENTIFING FAKE TWITTER USERS

Shaik Abdul Hameed1, Javangula Vamsinath2, M.Venkata Krishna Rao3, Shaik Mabasha4 , Stalin David D5

12 3 Assistant Professor, Department of CSE, Vnr Vignana Jyothi Institute of Engineering & Technology, Hyderabad

4 Assistant Professor, Department of IT, Bapatla Engineering College, Bapatla

5Associate Professor, Department of IT, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, 600062, Tamil Nadu

abdulhameed_sk@vnrvjiet.in1, vamsinath_j@vnrvjiet.in2, venkatakrishnarao_cse@vnrvjiet.in3, mabashapec@gmail.com4, sdstalindavid707@gmail.com5

ABSTRACT:

Researchers were drawn to the discovery of spam on social networking sites. Spam detection is a difficult task in keeping social networks secure. To protect users from all types of dangerous assaults and to maintain their security and privacy, it is critical to spot spam on social networking sites. Spammers' risky manoeuvres result in significant community destruction in the true world. On Twitter, spammers have a variety of aims, including distributing false information, fake news, rumours, and spontaneous comments. Spammers achieve their destructive goals using adverts and a variety of other methods, such as supporting several mailing lists and then sending spam messages at random to broadcast their interests. The original users, also referred to as non-spammers, find these behaviours annoying.

I. INTRODUCTION

Users of the internet rely on Online Social Networks (OSN) to carry out daily tasks such as sharing content, reading news, sending messages, reviewing things, and discussing events. Twitter has become the most used programme for disseminating news, and it is used by people of all ages. Twitter is a popular social networking website with approximately 300 million monthly users and 500 million daily tweets. People use Twitter for a variety of purposes, including information, job hunts, education, and the implementation of marketing initiatives. With only one swipe, people can find out what's going on in different countries around the world. There's also a possibility that tweets will propagate false or irrelevant information. Many users are being exploited by the spammers who may entice users with harmful content that claims to deliver free accessories or other evasion strategies that take the user's personal information and use it unfairly[1-12].

To safeguard consumers from all kinds of dangerous assaults and to maintain their security and privacy, it is critical to spot spam on OSN sites. Spammers' risky manoeuvres result in significant community destruction in the real world.

Submitted: 21/10/2022 **Accepted**: 24/11/2022

The purpose of this study is to uncover multiple strategies for detecting spam on Twitter and to provide a taxonomy that puts these approaches into different categories. We discovered four approaches for reporting spammers that can help detect user impersonation for classification. These techniques can be used to find spammers: (i) fake user identification, (ii)urlbased spam detection, (iii) spam detection in popular subjects, & (iv)spam detection in popular subjects.

1.1Spammer in Twitter

Spammers' activities are aided by Twitter's ever increasing popularity and the platform's many useful uses. In order to achieve their own personal aims, like phishing, scamming, virus propagation, spamming, and etc, spammers forward unsolicited tweets with trending hash tags or hazardous URLs are used to deceive users and redirect them to malicious websites.. Therefore, in order to fight spammers, both Twitter and researchers employ a variety of detecting approaches. There are numerous ways for Twitter users to report undesired tweets that they believe to be spam.

This entire spamming must be managed and required measures must be taken to suppress spammers' actions. To classify ham and spam, several businesses utilise spam filters. As a result, Twitter's mobile application includes various spam filters that use machine learning techniques to restrict spam. However, depending on the training and algorithm efficiency, these spam detection filters have varying accuracies and performance scales.

We used the feature-independent algorithm Nave bayes to detect spam trending topics and spam URLs in this paper.

1.2 Fake content and fake user in Twitter

Different sorts of social networking have developed various online activities that have rapidly piqued the interest of many users during the emergence of online social networking. On the other side, they are suffering from an increase in the number of bogus accounts generated. Fake accounts are those that don't actually belong to real persons. False accounts spread false information, deceptive online ratings, and spam. Fake accounts are against Twitter's Terms of Service. They are acting in a prohibited way. Examples of automated account interactions include posting harmful links, engaging in aggressive following behaviours like mass following or unfollowing, creating multiple accounts, updating the same topic more than once, posting links with unrelated tweets, and abusing the reply and mention features. Real accounts are those that adhere to the Twitter Rules[13-25].

The behaviour of consumer accounts from which spam tweets were generated was examined for false tweet consumer accounts. People with sizable followings shared the majority of the phoney tweets. The tweet analysis sources were then evaluated using the medium in which they were sent. Most tweets that include any type of information were written on mobile devices, while non-informative tweets were created using web interfaces.

II. LITERATURE REVIEW

To detect spam on social media, various studies have been conducted. The goal of this paper [1] was to use a deep learning method for identifying spam in social media. It advocated using LSTM and CNN neural structures to create a deep learning-based solution. The model is enhanced by including semantic information in the representation of words using knowledge bases like WordNet and Concept Net. By giving testing words that previously had a random value since they weren't observed in the training a better semantic vector representation, these knowledge bases improve performance.

The detection of bogus accounts using discretization is depicted in the second research article [2]. This research developed a method for detecting bogus accounts on the social networking site Twitter. The proposed approach aims at illuminating the impact of discretization on the Nave-Bayes classification algorithm on social network data. They used Entropy Minimization Discretization (EMD) to analyse the results of the Nave Bayes method on numerical features. In other cases, the accuracy using Nave Bayes was only improved from 85.55 percent to 90.41 percent by pre-processing the dataset using the discretization technique on specific characteristics.

on numerical characteristics The characteristics of Twitter spam detection were given, along with a review of their efficacy, in A Review of Twitter's Spam Detection Techniques [3]. According to the study, Twitter is the most popular microblogging service, drawing spammers who use it to aggressively follow and unfollow legitimate users, spread malicious software, and advertise via URLs shared in tweets, phish legitimate users, and hijack trending topics to catch their attention. Among the suggested methods are (1) account based spam detection methods, (2) tweet-based spam detection methods, (3) graph-based spam detection methods, and (4) hybrid spam detection methods.

Associative Affinity Factor Analysis [4] is also used to propose a solution. This paper provides a new methodology for bot identification stance detection and called Associative Affinity Factor Analysis (AAFA). The recommendable approach uses AAFA to identify original people from bots & to find stance in bipolar affinities. This is the first organisation to utilise machine learning algorithms in election prediction to effectively detect the reality behind the amount of social media popularity and Twitter followers by separating actual followers from sponsored bots. When compared to numerous current approaches, the findings reveal that the proposed AAFA framework achieves good accuracy. `

A study article titled A Survey on Spammer Behaviours in Popular Social Media Networks [5] includes a variety of survey results. The proposed system is divided into the following categories:- 1)Spams based on text

2) Spam based on comments
3) Spam that has been discovered in bookmarking systems

4) Spam in text messages and emails
5) Spam in online video

Text-based spams are the classification of cyborg, human, & bot accounts on Twitter using 500K accounts as a test set. Based on these findings, a categorization system was created, which included (1) an entropy based component, (2) an entropy based component, and (3) an entropy based component (2) (3) a spam-detection component, (4) a component for account attributes, & (5) a decision-maker.

Using NLP, a method for detecting fraudulent tweets has been developed [6]. This study provides a method for detecting spam on Twitter depend on two novel aspects: the spam-tweets detection without knowing the consumers past background, the other based on language analysis for detecting spam in such themes that are popular at the time. Using linguistic tools, this research attempts to detect spam tweets. The main aim of this work was to employ the SVM classifier to analyse tweets on Twitter, which produced standard findings. A disadvantage is that data-driven decisions take more time and money, and they do not always result in better overall outcomes or make a conclusion more or less valid, or "true."

To identify bogus news via social media, a data driven survey was undertaken [7]. This survey aims to provide a thorough look at current developments in the detection, classification, and mitigation of fake news that circulates on social media, as well as the challenges and open questions that remain for further investigation in the field. This study used a data-driven methodology and focused on classifying the traits used to characterise false information in each investigation, as well as the datasets used to train classification systems. Training requires patience; depending on the volume of data, building a model from scratch without using a trained model can take weeks to work well[26-32].

In the paper A Topic-Based Hidden Markov Model for Real-Time Spam Tweets Filtering [8], we looked at how a time-dependent sequential data-based model influenced the capacity to recognise topic-based spam tweets in real-time. The authors formalised a dynamic, time-dependent model known as a first-order Hidden Markov Model (HMM). The HMM is the most effective choice for high-quality topic-based tweets when compared to conventional time independent classification models since it has shown its ability to precisely identify spam tweets. These methods are not suitable for filtering tweets in real-time detection since they rely on data from Twitter's servers.

To identify spammers, the paper [9] suggests employing SVM. Supervised information is an essential part of a detection system's success since identifying social spammers is a classification challenge. The Collective Matrix Factorization serves as our inspiration as we proceed to include supervised data into the aforementioned matrix factorization utilising social information. Support Vector Machine's (SVM) well-known hinge loss is used as the classification model. The gradient computation is carried out using the smoothed hinge loss.

Since each training sample is processed using all available resources, frequent updates, which employ stochastic gradient descent to improve the loss function, are computationally costly. The detection of spam tweets may be accomplished with the help of a data clustering algorithm [10]. By establishing multiple criteria for spam identification and then using a clustering algorithm based on the data stream, this study detects spam tweets. The tweets may be clustered by the DataStream Algorithm, which views outliers as spam. When this algorithm is correctly calibrated, the ability to identify spam tweets is improved, and when compared to earlier experiments, the false positive rate falls to its lowest level. 89 percent of all spam tweets may be found using the suggested strategy. Even though this system misses 11% of spam tweets, every valid message is mistakenly labelled as spam.

The report [11] outlines in full and clearly the differences between fake and real account users on Twitter. To begin, it is necessary to understand the learning algorithms for identifying fraudulent Twitter users. Content-based identification, url based identification, fake hot topic identification, and false user identification are four forms of twitter account identification. The support vector machine was utilised to identify the bogus account, which improved the accuracy of the results (Tsou, Zhang, & Jung. (2017)). The detection of bogus accounts begins with the extraction of feature data and the identification of missing data for specific attributes. The friends of both the fake and real accounts were evaluated using the feature extracted, and the followers of both the real and phoney accounts were analysed in the next phase. On social networks, bogus user identification and content are common [12]. Presented taxonomy of Twitter spam identification techniques, including false contented recognition, URL-based spam identification, spam location in inclining points, and phoney client recognition strategies[33-40]. It also provided an analysis of the introduced techniques based on some features, including content features, client features, structure features, time features, and chart features. The approaches' predetermined goals and employed datasets were also assessed. Scientists might anticipate help from the planned audit in discovering information on standardised, best-in-class Twitter spam identification techniques. There are still certain open areas that analysts should closely monitor despite the emergence of successful and practical methods for spam detection and phoney client identification on Twitter.

Multi objective hybrid feature selection was used to find false accounts on the Twitter social network[13].Because the classifier system must be applied on a large volume of data and in real time to find bogus accounts in online social networks, the feature selection process in classification-based techniques is critical. Furthermore, researchers frequently study and investigate detected features in order to better understand the behaviour of bogus accounts. It suggests that the feature selection process's stability is an important factor to consider. Furthermore, stability by itself is not considered an adequate measure for evaluating the selected features, and it is frequently paired with classification performance. This study uses a multiobjective hybrid technique to find the best effective feature set for finding false accounts on the Twitter social networks. Experiments on two Twitter datasets demonstrated that the

proposed strategy may yield more optimal and balanced results than other methods currently in use. With a modest tweak in the feature set, the proposed approach can be used to detect phoney accounts on a variety of social networks, which could be a future study's goal.

In this paper[14], they created a revolutionary deep learning-based Twitter spam detection strategy that corrects the flaws in current deep learning and machine learning-based spam detection techniques. In addition to a mixed classifier that considers both users' twitter text and meta-data, they developed a text-based classifier that just analyses users' tweet text. The experiment's findings show that this method works better than competing DL- and ML-based methods. This technique achieves the highest accuracy for datasets I and II, with 99.68 percent and 93.12 percent, respectively[41].

The proposed spam detection method [15] made optimal use of a selection of readily accessible attributes. Since they don't rely on prior tweets, which are usually not available on Twitter, they are excellent for identifying spam in real time. Testing a variety of machine learning models with a dataset orthogonally obtained from the research data demonstrates the value and resilience of the recommended feature set. The performance of the different models is consistent and much better than the baseline. Additionally, it was found that automated spam accounts have a recognisable pattern, with cyclical spikes in activity. Any real-time filtering programme can employ the suggested spam tweet detection method[42-44].

In this paper[16], they propose a neural network based ensemble strategy for finding spam at the tweet level that blends classical feature-based methods and deep learning. They used CNN to explore with numerous word embeddings. They used the HSpam and 1KS10KN data sets. While the 1KS10KN data set is uneven, the HSpam data set is balance. The bulk of the cases in the 1KS10KN data set are nonspam. Algorithms for machine learning are frequently biassed in favour of the majority class. This is why, for CNNs with non static channels the recall of the HSpam data set is strong compared to the low recall of the 1KS10KN data set. For both the 1KS10KN and HSpam data sets, the suggested technique outperforms all existing methods. Even the model trained with a modest number of examples functioned wonderfully when applied to a large number of unseen tweets. In every experiment, it was discovered that the proposed technique performed better than the standard procedures. For the HSpam14 data set, feature based algorithms perform poorly when compared to deep learning techniques.

In this paper[17], they looked at how to detect spammers on Twitter. They scavenged Twitter for almost 54 million user profiles, all of their tweets, and follower and follower connection information. Based on this dataset and manual investigation, they created a tagged collection with users classified as spammers or non-spammers. As a result, the users of this tagged collection may be classified, revealing a number of features that could be used to separate spammers from non-spammers. Our characterization work will be used to develop a spammer detection system. Using a classification technique, they were able to correctly identify a large

percentage of spammers while only misclassifying a small percentage of legal users. It also entails examining various tradeoffs for our categorization strategy, as well as the influence of various attribute sets.

[18] In this paper, Over the course of seven days, they gathered more than 9 million tweets on hourly popular topics using Twitter's streaming API. We collected tweet properties from the raw data provided by the API that had previously been found as being helpful in the detection of spam. And then trained a naïve Bayes classifier for tweet categorization using a hand-labeled random sample of about 1500 tweets, which they then put to the test using 10-fold cross validation. We were able to get data on the prevalence of spam generally, among subjects, and the impact of spam on topic rankings by using this classifier to filter the trending topic data. Overall, the frequency of spam in trending topics appears to be consistent with earlier research, which pointed to a 3% spam rate in Twitter messages. The amount of spam included by each subject varied significantly, as we found when comparing the observed spam frequencies across themes using a chi squared goodness of fit test. The re-ranking of subjects after our spam filter was applied had very little effect on the current rankings. The Longevity of Topics finding seemed to go against what they had previously learned, and it was a Spam Incidence. The mystery was resolved by examining the power law distribution of topic popularity. Conclusion: Spammers do not directly influence Twitter's trending topics; rather, they opportunistically pick topics with appealing qualities.

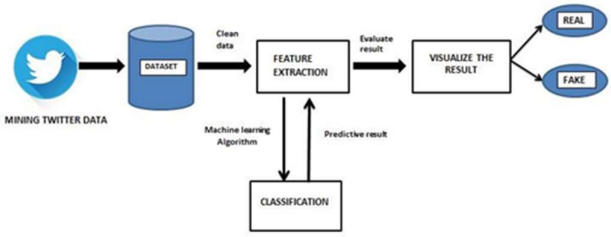
This research proposes an innovative and robust approach dubbed SpamCom[19] for detecting spammer communities in the online social network Twitter based on overlapping community structure, topological, behavioural, and content properties. The culprits are identified based on content similarities and connectivity with spammer accounts after detecting common community structures in Twitter. Finally, the spammers are selected from the suspects based on the content, account age, location, and behavioural characteristics of each user. This method overcomes spammers' dual conduct of posing as legitimate users while performing nefarious operations. The discovered spammers are grouped together to form a core spammer network that has spread throughout social media. Despite the fact that the proposed approach requires considerably more testing, preliminary results show that it is capable of detecting spammers. Furthermore, this is the first examination of the spammer community structure that exists in social media.

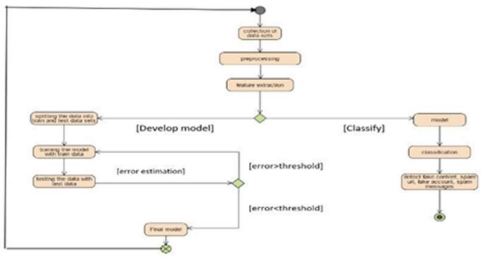
Out of 356 publications published between 2010 and 2020, this paper [20] did a thorough SLR, covering 55 of the most pertinent studies. The research methodology, tools, evaluation parameters, and evaluation methodologies for each item were described, statistically analysed, and examined. Recall (23 percent), F-measure (18 percent), precision (17 percent), and accuracy (14 percent) were found to be the most generally considered evaluation metrics for RQ3, while FPR, ROC, FNR, and specificity were largely neglected. According to RQ4, Weka had the highest proportion of usage of all assessment tools in the papers reviewed. A taxonomy

was also offered to provide a clear image of Twitter spam detection methods. The five classifications used to classify Twitter spam detection systems based on feature analysis were content analysis techniques (15%), user analysis approaches (9%), tweet analysis approaches (9%), network analysis approaches (11%), and hybrid analysis approaches (11%). (56 percent).Finally, they emphasised unresolved concerns, obstacles, and potential future directions.

III. PROPOSED SYSTEM

- The aim of the project is to effectively detect the fake accounts, fake content, spam trending topic, spam URLs on Twitter social network.
- • Detection of spammers on social media sites in order to distinguish between genuine human tweets and spam tweets.
- Using techniques like Random forest, Naive Bayes classification we can detect whether tweets contains normal message or spam message.
- Social networks may improve their market reputation by spotting and eliminating such spam content. Social networks would lose appeal if they did not get rid of spam communications.

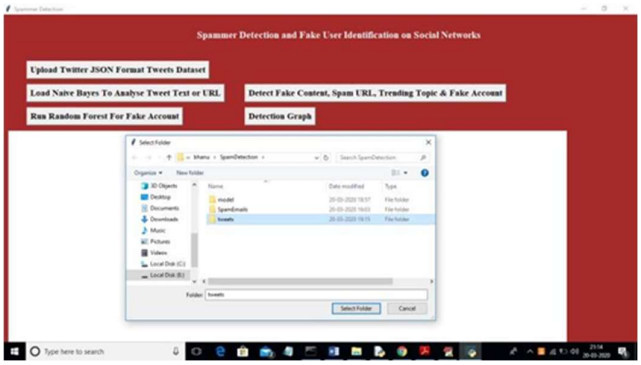




- To perform detection we are using twitter dataset and 4 different techniques called Fake Content, Spam URL Detection, Spam Trending Topic & Fake consumer Identification.
- Using above 4 techniques we can identify whether tweet is normal or spam and then using Random Forest data Mining algorithm we will train above dataset to classify number of spam and non-spam tweets or fake or non-fake accounts.

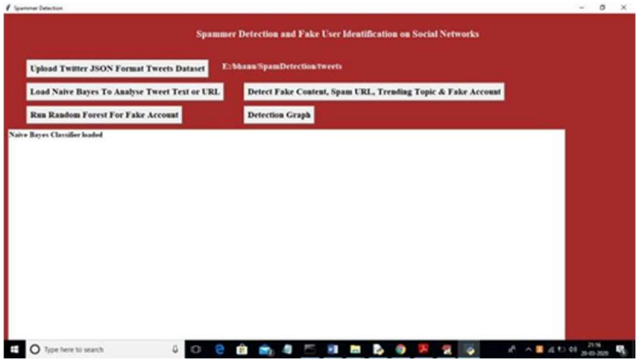
IV. IMPLEMENTATION

Click the "Upload Twitter JSON Format Tweets Dataset" button in the aforementioned window, then upload the tweets folder.

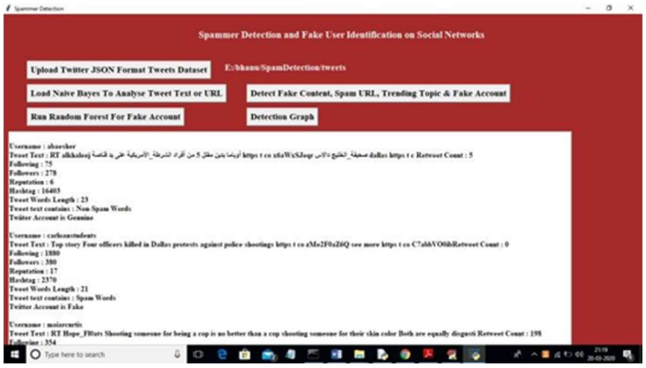


The "tweets" folder, which contains tweets in JSON format from multiple people, is what I uploaded to the screen you see above. To read tweets, click the "open" button now.

All tweets from all users are loaded on the screen above. The Naive Bayes classifier will now be loaded when you click the "Load Naive Bayes To Analyze Tweet Text or URL" button.

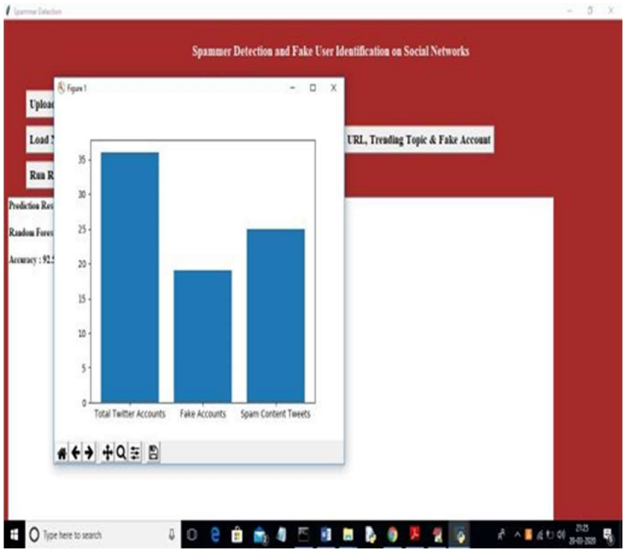


Click on "Detect Fraudulent Content, Spam URL, Trending Topic & Fake Account" on the screen above to analyse each tweet for fake content, spam URLs, and fake accounts using the Naive Bayes classifier and other above-mentioned techniques.



All characteristics from the tweet collection are extracted and analysed in the screen above to determine if a tweet is spam or not. Each tweet record displays data such as TWEET TEXT, FOLLOWERS, FOLLOWING, etc. with account is false or real and tweet text includes spam or non-spam phrases. In the text field above, each record value is separated by an empty line. To train a random forest classifier using the characteristics of the retrieved tweets, click the "Run Random Forest Prediction" button. This model will be used to forecast or identify false or spam accounts for incoming tweets. For more information on each tweet, scroll down above the text box.

Click the "Detection Graph" button to view a graph of the total number of tweets, spam, and bogus accounts. In the screen above, we calculated the random forest prediction accuracy to be 92%.



The total number of tweets, false accounts, and tweets with spammed language are shown on the x-axis in the graph above, while their count is shown on the y-axis.

V. CONCLUSION

The development of an analytical technique for locating spammers on Twitter is presented in the study. We also displayed taxonomy of Twitter spam detection techniques, which mentioned the identification of false information, spam detection based on URLs, the positioning of spam at inclining spots, and the identification of phoney clients. We also examined the newly offered strategies in light of a few criteria, including those of the consumer, the content, the chart, the structure, and the time. The approaches' predetermined goals and employed datasets were also looked at. Scientists might anticipate help from the planned audit in finding information on standardised, best-in-class Twitter spam identification techniques. Despite the improvement of effective and practical methods for spam detection & client impersonation detection.

VI.REFERENCES

1. David, D. S., Arun, S., Sivaprakash, S., Raja, P. V., Sharma, D. K. et al. (2022). Enhanced Detection of Glaucoma on Ensemble Convolutional Neural Network for Clinical Informatics. CMC-Computers, Materials & Continua, 70(2), 2563–2579.
2. David, D. S., Anam, M., Kaliappan, C., Arun, S., Sharma, D. K. et al. (2022). Cloud Security Service for Identifying Unauthorized User Behaviour. CMC-Computers, Materials & Continua, 70(2), 2581–2600.
3. Jayachandran, A., and D. Stalin David. "Textures and Intensity Histogram Based Retinal Image Classification System Using Hybrid Colour Structure Descriptor." Biomedical and Pharmacology Journal, vol. 11, no. 1, 2018, p. 577+. Accessed 12 Feb. 2021.
4. D. Stalin David, 2019, “Parasagittal Meningiomia Brain Tumor Classification System based on MRI Images and Multi Phase level set Formulation”, Biomedical and Pharmacology Journal, Vol.12, issue 2, pp.939-946.

5. Thendral R., David D.S. (2022) An Enhanced Computer Vision Algorithm for Apple Fruit Yield Estimation in an Orchard. In: Raje R.R., Hussain F., Kannan R.J. (eds) Artificial Intelligence and Technologies. Lecture Notes in Electrical Engineering, vol 806. Springer, Singapore. https://doi.org/10.1007/978-981-16-6448-9_27
6. D. S. David and A. Jeyachandran, "A comprehensive survey of security mechanisms in healthcare applications," 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-6, doi: 10.1109/CESYS.2016.7889823.
7. Stalin David, D., Jayachandran, A. A new expert system based on hybrid colour and structure descriptor and machine learning algorithms for early glaucoma diagnosis. Multimed Tools Appl 79, 5213–5224 (2020). https://doi.org/10.1007/s11042-018-6265-1.
8. D Stalin David, A Jayachandran, 2018,Robust Classification of Brain Tumor in MRI Images using Salient Structure Descriptor and RBF Kernel-SVM, TAGA Journal of Graphic Technology, Volume 14, Issue 64, pp.718-737.
9. D Stalin David, 2016, Robust Middleware based Framework for the Classification of Cardiac Arrhythmia Diseases by Analyzing Big Data, International Journal on Recent Researches In Science, Engineering & Technology, 2018, Volume 4, Issue 9, pp.118-127.
10. M. Rajdhev, D. Stalin David, "Internet of Things for Health Care", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 800-805, March-April 2017.
11. P. Prasanth, D. Stalin David, "Defensing Online Key detection using Tick Points", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 758-765, March-April 2017.
12. Sudalaimani, D. Stalin David, "Efficient Multicast Delivery for Data Redundancy Minimization over Wireless Data Centres", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 751-757, March-April 2017.
13. R. Abish, D. Stalin David, "Detecting Packet Drop Attacks in Wireless Sensor Networks using Bloom Filter", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 730-735, March-April 2017.
14. Vignesh, D. Stalin David, "Novel based Intelligent Parking System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 724-729, March-April 2017.
15. D Stalin David, 2020, ‘Diagnosis of Alzheimer's Disease Using Principal Component Analysis and Support Vector Machine, International Journal of Pharmaceutical Research, Volume 12, Issue 2, PP.713-724.
16. Jaswanth K S, Dr. D. Stalin David, "A Novel Based 3d Facial Expression Detection Using Recurrent Neural Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 48-53, March-April 2020.

17. D Stalin David, 2020, 'An Intellectual Individual Performance Abnormality Discovery System in Civic Surroundings' International Journal of Innovative Technology and Exploring Engineering, Volume 9, Issue 5, PP.2196-2206.
18. D Stalin David, 2020, 'Machine learning for the prelude diagnosis of dementia', International Journal of Pharmaceutical Research, Volume 13, Issue 3, PP.2329-2335.
19. David, D.S. and Y. Justin, 2020.A Comprehensive Review on Partition of the Blood Vessel and Optic Disc in RetinalImages.Artech J. Eff. Res. Eng. Technol., 1: 110-117.
20. D. Stalin David and A.A. Jose, 2020. Retinal image classification system for diagnosis of diabetic retinopathy using SDCMethods.Artech J. Eff. Res. Eng. Technol., 1: 87-93.
21. D. Stalin David and T. Joseph George, 2020. Identity-based Sybil attack detection and localization.ArtechJ. Eff. Res. Eng. Technol., 1: 94-98.
22. David, D.S. and L. Arun, 2020.Classification of brain tumor type and grade using MRI texture and shape in a machine learning scheme.Artech J. Eff. Res. Eng. Technol., 1: 57-63.
23. David, D.S., 2020. Retinal image classification system for diagnosis of diabetic retinopathy using morphological edgedetection and feature extraction techniques.Artech J. Eff. Res.Eng. Technol., 1: 28-33.
24. David, D.S., 2020. A novel specialist system based on hybrid colour and structure descriptor and machine learningalgorithms for early diabetic retinopathy diagnosis.Artech J. Eff. Res. Eng. Technol., 1: 50-56.
25. David, D.S. and M. Samraj, 2020.A comprehensive survey of emotion recognition system in facial expression.Artech J. Eff. Res. Eng. Technol., 1: 76-81.
26. David, D.S. and L. Arun, 2020. Multi-view 3D face renovation with deep recurrent neural networks. ArtechJ. Eff. Res. Eng. Technol., 1: 64-68.
27. David, D.S. and S. Namboodiri, 2020.Improvement of framework for the grouping of CA diseases by investigating bigdata.Artech J. Eng. Appl. Technol., 1: 7-14.
28. Stalin David D , Saravanan M, 2020, 'Multi-perspective DOS Attack Detection Framework for Reliable Data Transmission in Wireless Sensor Networks based on Trust', International Journal of Future Generation Communication and Networking , Volume 13, Issue 4, PP.1522–1539.
29. J. K. S and D. S. David, "A Novel Based 3D Facial Expression Detection Using Recurrent Neural Network," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp. 1-6, doi: 10.1109/ICSCAN49426.2020.9262287.
30. Stalin David D, Saravanan M, "Enhanced Glaucoma Detection Using Ensemble based CNN and Spatially Based Ellipse Fitting Curve Model", Solid State Technology, Volume 63, Issue 6, PP.3581-3598.
31. Stalin David D, Saravanan M, Jayachandran A, "Deep Convolutional Neural Network based Early Diagnosis of multi class brain tumour classification", Solid State Technology, Volume 63, Issue 6, PP.3599-3623.
32. D. Jayakumar; Dr.U. Palani; D. Raghuraman; Dr.D. StalinDavid; D. Saravanan; R. Parthiban; S. Usharani. "CERTAIN INVESTIGATION ON MONITORING THE LOAD OF

SHORT DISTANCE ORIENTEERING SPORTS ON CAMPUS BASED ON EMBEDDED SYSTEM ACCELERATION SENSOR". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2477-2494.
33. R. Parthiban; S. Usharani; D. Saravanan; D. Jayakumar; Dr.U. Palani; Dr.D. StalinDavid; D. Raghuraman. "PROGNOSIS OF CHRONIC KIDNEY DISEASE (CKD) USING HYBRID FILTER WRAPPER EMBEDDED FEATURE SELECTION METHOD". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2511-2530.
34. Dr.U. Palani; D. Raghuraman; Dr.D. StalinDavid; R. Parthiban; S. Usharani; D. Jayakumar; D. Saravanan. "AN ENERGY-EFFICIENT TRUST BASED SECURE DATA SCHEME IN WIRELESS SENSOR NETWORKS". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2495-2510.
35. Dr. D. Stalin David; R. Parthiban; D. Jayakumar; S. Usharani; D. RaghuRaman; D. Saravanan; Dr.U. Palani."MEDICAL WIRELESS SENSOR NETWORK COVERAGE AND CLINICAL APPLICATION OF MRI LIVER DISEASE DIAGNOSIS". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2559-2571.
36. D.Raghu Raman; D. Saravanan; R. Parthiban; Dr.U.Palani; Dr.D.Stalin David; S. Usharani; D. Jayakumar."A STUDY ON APPLICATION OF VARIOUS ARTIFICIAL INTELLIGENCE TECHNIQUES ON INTERNET OF THINGS". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2531-2557.
37. D.Saravanan; Dr.D.Stalin David; S.Usharani;D.Raghuraman; D.Jayakumar; Dr.U.Palani; R.Parthiban. “AN ENERGYEFFICIENT TRAFFIC-LESS CHANNEL SCHEDULING BASED DATA TRANSMISSION INWIRELESS NETWORKS”. European Journal of Molecular & Clinical Medicine, 2020, Volume 7, Issue 11, Pages 5704-5722.
38. S. Usharani; D.Jayakumar; Dr.U.Palani; D.Raghuraman; R.Parthiban; D.Saravanan; Dr.D.Stalin David. “INDUSTRIALIZED SERVICE INNOVATIONPLATFORM BASED ON 5G NETWORK AND MACHINELEARNING”.European Journal of Molecular & Clinical Medicine, 2020, Volume 7, Issue 11, Pages 5684-5703.
39. P Gopala Krishna, D StalinDavid, “AN EFFECTIVE PARKINSON'S DISEASE PREDICTION USING LOGISTIC DECISION REGRESSION AND MACHINE LEARNING WITH BIG DATA”, Turkish Journal of Physiotherapy and Rehabilitation; 32(3), Pages 778-786.
40. Jaswanth K S, Dr. D. Stalin David, "A Novel Based 3d Facial Expression Detection Using Recurrent Neural Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 48-53, March-April 2020.
41. T. Babu, H. Roopa, Arvind Kumar Shukla, D. Stalin David, S. Jayadatta, A.S. Rajesh, Internet of things-based automation design and organizational innovation of manufacturing enterprises,MaterialsToday:Proceedings,2021,ISSN:2214-7853, https://doi.org/10.1016/j.matpr.2021.10.459.
42. M. Chandragowda, C. Gnanavel, D. Saravanan, D. Stalin David, R. Parthiban, A.S. Rajesh,Consequence of silanee combination representative on the mechanical possessions of

sugarcane bagasse and polypropylene amalgams,Materials Today: Proceedings,2021, ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.10.455.
43. T.V.V. Pavan Kumar, Shafqat Nabi Mughal, Radhika Gautamkumar Deshmukh, S. Gopa Kumar, Yogendra Kumar, D. Stalin David,A highly consistent and proficient class of multiport dc-dc converter based sustainable energy sources,Materials Today: Proceedings, 2021,ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.10.458.
44. David, D.S. Enhanced glaucoma detection using ensemble based CNN and spatially based ellipse fitting curve model. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-021-03467-4.