10.48047/jocaaa.2024.33.07.55

Social Network Security Framework Employing Textual Patterns and Extreme Classifier for Spam User Detection

Karramareddy Sharmila[1*], Udaykiran Bhargava Gollamandala[2], Usthulamuri Penchalaiah[3]

[1]Department of Computer Science and Engineering, Vaagdevi Engineering College, Bollikunta, Warangal, Telangana 506005

[2]Department of Electronics and Communication Engineering, Mother Teresa Institute of Science and Technology, Sathupally, Telangana 507303

[3]Department of Electronics and Communication Engineering, Geethanjali Institute of Science and Technology, Gangavaram, S.P.S.R, Andhra Pradesh 524137

[*]**Correspondence: Karramareddy Sharmila (sharmilakreddy@gmail.com)**

Abstract— The rapid expansion of Online Social Networking (OSN) platforms such as Twitter has led to a significant rise in spam content and fake user accounts, creating major challenges for user safety, platform integrity, and computational resources. This study presents an effective approach for detecting Twitter spammers and identifying fraudulent users. The process begins with comprehensive data pre-processing to eliminate noise and irrelevant information from the Twitter dataset. Subsequently, informative textual, linguistic, and user-behavioral features are extracted using the Multinomial Naive Bayes (MNB) technique. These extracted features are then utilized to train an Extreme Learning Machine (ELM) classifier, capable of efficiently distinguishing between genuine and spam accounts. Extensive experiments conducted on a real-world Twitter dataset validate the effectiveness of the proposed framework. The findings reveal that integrating MNB-based feature extraction with ELM classification yields high accuracy, precision, recall, and F1-score, demonstrating strong potential for reliable spammer and fake user detection on Twitter.

Keywords— *online social networks, machine learning algorithms, extreme learning machine, Spammers, Twitter spam identification*

I. INTRODUCTION

In recent years, OSNs such as Twitter, Facebook, and Sina Weibo have emerged as significant platforms for information sharing, communication, and social connections. The user base of Twitter, for instance, grew from 200 million monthly active users (MAU) in 2012 to 328 million in 2017, with an astonishing rate of 20 million tweets being posted per hour. While SNs have enriched people's lives, they have also brought about security concerns. Attackers exploit SNs to spread various forms of attacks, including phishing, drive-by downloads, and malicious code injections [1]. Research indicates that up to 15 percent of Twitter accounts are actually bots rather than genuine users, and malicious URLs are commonly employed by attackers to initiate cyberattacks [2]. Attackers deceive users by impersonating well-known accounts, displaying ads for discounted merchandise, or exploiting trust between friends to trick victims into clicking on malicious URLs. These deceptive practices either direct sufferers to websites which can be used for phishing or infect their structures with malware, which ultimately effects in important monetary losses for human beings, corporations, governments, and different corporations. When it involves filtering URLs that users share, the majority of SNs employ blacklisting techniques like Google Safe Browsing, Phishing Tank, and URIBL. However, there is usually a delay in updating the blacklists, and research have shown that 90 percentage of victims click on malicious URLs before those URLs are discovered and brought to the blacklist [3]. Researchers have developed some of specific techniques to defend open source networks (OSNs) from attacks in an effort to offer customers with a

10.48047/jocaaa.2024.33.07.55

secure environment on SNs. The currently available techniques of detection may be broken down into two primary categories. The first category consists of several detection techniques that are based on the relationship graph of the social network. Since OSNs encompass diverse relationships, researchers construct social graphs using these relationships [4]. By analysing user characteristics within the graph, detection algorithms can be developed to identify suspicious communications or users. The second category contains several detection strategies that are derived from various machine learning techniques. Data from social networks are mined by researchers for a variety of characteristics, including information on individual users, social habits, friend ties, and message content [5]. These features are then utilized to train machine learning classifiers that can identify malicious messages or users.

It has been known for quite some time that spam is a big concern; nevertheless, the effect that it has had on the infrastructure of worldwide networks has recently reached pandemic proportions. At first, users could just delete spam messages; but, as spam got more widespread, less reliable client-side spam filtering technologies appeared [6]. Initially, users could simply delete spam messages. The users were required to manually check any communications that may have been considered spam to guarantee that any vital messages were not accidentally removed. This resulted in a loss of time for the users. As a direct result of this, governments began considering the enactment of anti-spam laws, and businesses started marketing spam filtering solutions to operators of mail servers and Internet service providers. At first, it was thought that economics alone could fast remove spam. It was hypothesized that if 95% of spam were filtered out, the costs for spammers to reach the same audience would increase by a factor of 20. It was a logical assumption to think that high-accuracy filters could remove spam since very few spammers had profit margins that were substantial enough to tolerate the extra expenses [7]. But things turned rather differently than expected. Even with client-side and server-side filters working together, there is still a significant percentage of spam that is able to get through to users' inboxes [8], despite the fact that commercial anti-spam filters boast success rates of more than 95%. The insidious character of spam, which makes it difficult to recognize using computer systems, is one factor that leads to the ineffectiveness of current anti-spam measures. While there are some communications that are unequivocally considered spam, such as those that promote illegal substances, pornography, fraud, or viruses, there are also a great number of gray areas in which material that one user thinks to be spam may really be useful information for another user [9]. As a result, it may not be prudent to limit the potential of email as a medium for the dissemination of mass communication owing to the annoyance caused by spam. Recent approaches propose the development of peer-to-peer (P2P) networks [10] for collaborative knowledge sharing about spam among users. While these approaches represent steps towards P2P collaborative spam filtering, they often overlook aspects of message confidentiality and robust.

The rest of the paper is organized as follows: section2 gives the detailed analysis of literature survey with drawbacks. Section3 gives the detailed analysis of proposed method with MNB feature extraction, ELM classifier method. Section 4 gives the detailed simulation results of proposed method. Further, the conclusion of the proposed is presented in section 5.

II. LITERATURE SURVEY

As part of their presentation, Ramesh and colleagues [11] offered an innovative approach to the identification of spam. The approach that is being developed has been given the acronym I2FELM, which stands for Improved Incremental Fuzzykernel-regularized Extreme Learning Machine, which is developed on the basis of a regularized extreme learning machine and given the aforementioned name. Its goal is to accurately detect spam on the social media platform Twitter. Kumar et al. [12] came up with a hybrid architecture as a solution for identifying spam on Twitter. This strategy proved successful. Combining the SMOTE sample method with the Edited Nearest Neighbors (ENN) methodology results

10.48047/jocaaa.2024.33.07.55

in the SMOTE-ENN sampling strategy. Its objective is to supply balanced data, which is subsequently supplied to a range of deep learning classification algorithms so that it may be determined whether or not the tweet in question is spam or ham. The network that was proposed by Abkenar et al. has been referred to by the name Chimp Sailfish Optimization-based Deep Neuro Fuzzy Network with random forest classifier (RFC). This is the word that has been given to the network. [13]. The proposed scheme, which makes use of a deep learning classifier, is able to produce effective performance even when it is applied to high-dimensional data in the context of a real platform situation. Using methods from machine learning and deep learning, Rodrigues et al. [14] suggested a real-time method for analyzing sentiment on Twitter and detecting spam on the platform. The fundamental purpose of the research that is being proposed is to develop a system that is capable of determining if a tweet is "spam" or "ham" and evaluating the sentiment that is communicated by the tweet.

Ahraminezhad et al. [15] proposed an smart ensemble class approach as a method of figuring out the presence of junk mail in OSNs. In order to streamline the modeling manner and reduce down on its stage of complexity, the heterogeneous ensemble learning framework that turned into just brought uses navie bayes classifier (NBC). This framework is primarily based on stack generalization. The proposal become made through Zeng, et al. [16]. This article offers a emblem-new method for detecting bogus accounts on Twitter this is primarily based on resampling and makes use of a semi-supervised shape of self-training. The help vector machine (SVM) was evolved, this offers an evidence of the concept of semi-supervised self-training studying and then applies it to the actual Twitter account facts set that become amassed from Kaggle. This is carried out inside the context of the framework that has been provided. In the area of cybersecurity, Dutta et al. [17] recommended using a singular Chaotic Ant Swarm with Weighted Extreme Learning Machine (CAS-WELM) with the purpose of recognizing and classifying faux news. The CAS-WELM technique changed into evolved with the intention of differentiating among actual and fraudulent news. Khan et al. [18] proposed a brand new activation function that is based totally at the psi characteristic of M and redescend the M-estimation approach paired with the smooth l2-norm weight loss features with a purpose to lessen the bad effects which might be because of outliers. This became executed to be able to make the distribution of the records greater uniform. This became completed so one can minimize the impact that the outliers have. The psi functions that have been cautioned for various M and redescending M-estimation approaches are extra versatile, allowing for the creation of a space with greater distinguishable traits.

A technique for the identity of spam the use of synthetic intelligence turned into counseled by Prabhu Kavin et al. [19] to be used on Twitter. In this method, the authors built a model by means of the usage of a random wooded area technique, an artificial neural community, and a vector support system. The gravitational search algorithm as well as the choice tree are each components of a singular hybrid strategy that changed into currently pronounced with the aid of Vives et al. [20] with the objective of locating Twitter spammers. This method changed into developed with the reason of locating spammers on Twitter. This technique changed into evolved for the aim of monitoring Twitter. They noted their approach as the HGSDT. The person decision tree (DT) approach is incapable of coping with the issues to hand in view that it's miles prone to instability and fails to provide acceptable effects while managing increasing portions of effective facts for a certain characteristic.

III. PROPOSED METHOD

The proliferation of social networking sites has basically converted the manner individuals have interaction and interact with every different on a international scale. Platforms like Twitter and Facebook have gathered hundreds of thousands of active users, shaping daily existence in various approaches. However, these structures have also come to be breeding grounds for spammers who

10.48047/jocaaa.2024.33.07.55

exploit them to disseminate huge volumes of irrelevant and dangerous facts. Among those structures, Twitter sticks out as one of the most notably used systems, making it noticeably liable to an unreasonable amount of unsolicited mail. Spammers on Twitter employ various methods, which include the advent of fake user money owed, to send undesired tweets selling offerings or websites. This not handiest makes it harder for genuine customers to use the network, but it also puts a stress on the assets which can be made to be had with the aid of the platform. The proliferation of faux identities additionally contributes to the spread of wrong data, which in turn contributes to the distribution of fabric this is dangerous. As an instantaneous outcome of this, the identification of spammers and the finding of fake users on Twitter have grow to be key subjects of study inside the area of OSNs.

Figure 1 shows the proposed technique block diagram. This examine goals to discover a technique to the troubles of junk mail and faux person identity on Twitter using a deep gaining knowledge of technique called ELM. To compare how desirable ELM is in recognizing junk mail, its overall performance is in comparison to that of other device getting to know algorithms, consisting of Random Forest, Naive Bayes, and Support Vector Machine. To set up the many approaches for coping with unsolicited mail, a taxonomy is proposed primarily based on their capacity to recognize special types of unsolicited mail. These categories encompass (i) junk mail in trending subjects, (ii) junk mail based on URLs, (iii) junk mail from fake users, and (iv) junk mail in trending content. By identifying the numerous strategies used to fight junk mail on Twitter, researchers benefit from a better expertise of the strategies employed. In addition, the suggested methodologies are assessed in line with a number of unique elements, inclusive of user traits, content characteristics, graph traits, structural characteristics, and temporal traits. The have a look at offers a complete comparison of those strategies, highlighting their strengths and weaknesses in figuring out spam. The major objective is to create a treasured aid for researchers within the discipline of Twitter junk mail detection. This is accomplished by organising a centralized platform that presents current advances in Twitter spam detection, permitting researchers clean access to key highlights and advancements in this region. Moreover, the take a look at emphasizes the significance of utilising advanced device mastering algorithms like ELM and compares their performance in opposition to traditional strategies.

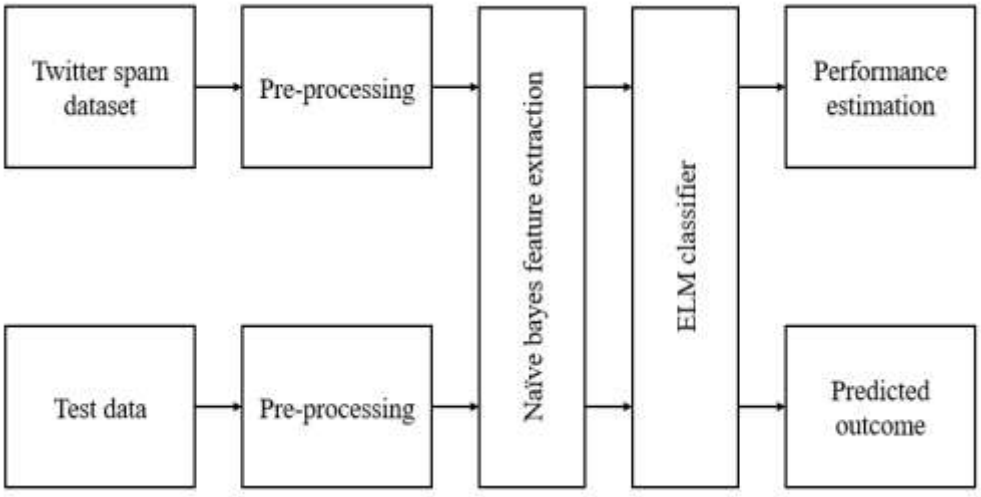


Fig. 1. Block diagram for the suggested system

A. Data Preprocessing

Before the statistics may be fed into any classifier, it ought to first be pre-processed by means of going through some of different processes. This is achieved so that the set of rules could be able to correctly become aware of the data and offer the absolute excellent version feasible. One of the tactics

10.48047/jocaaa.2024.33.07.55

that fall beneath the class of pre-processing is formatting and facts cleaning. The facts have to first be formatted in order for the classifier so that you can interpret them in an appropriate way. Converting the facts type into a textual content file or into a flat layout are simply examples of the many various avenues that may be pursued with the intention to attain this goal. There are a outstanding many greater opportunities available as properly. There are a first rate quantity of other ability guides of motion as nicely. Cleaning is a method for handling the lacking values of a records set, including lacking labels or values of sure statistics, set residences which are manually performed via plurality balloting for the matching values of other times, and even by means of deleting sure instances that negatively impact the classifier mastering technique. Cleaning is likewise a way for maintaining the set residences manually, that's achieved by plurality balloting for the values of different instances that suit. This may be handled through the cleaning system. Utilizing plurality voting for the values of different instances of the set, cleaning is also a way for manually maintaining the set attributes. This is completed via using the set. This is executed a good way to find values which can be like minded with one another. In addition to being a method for managing set houses, cleaning is also a manner for doing it manually thru using plurality vote casting for the values of other times' residences. This form of control may be carried out through cleaning. The purpose of doing this is to locate properties that are a match. In addition, cleaning details involves getting rid of private information that might compromise the privacy of some individuals.

B. *Naive Bayes Feature Extraction*

According to Bayesian theory, any characteristic of a certain class is unrelated to any other characteristics of the class in any way. As a result, the Naive Bayes (NB) algorithm has been suggested for use as a probabilistic classifier. NB requires much less time to train as compared to other classification modes, and it is able to efficiently tackle the issue of learning from small sample sizes. Let's imagine that D is a training sample set with class labels for n-patterns, and that Y is an event vector. The reason for the occurrence of the occurrence Y, which is regulated by the design that has the largest posterior probability, is presented in the following paragraphs.

$$P(C_i|Y) > P\big(C_j|Y\big) \text{ for } 1 \le j \le n, j \ne i \tag{1}$$

Here, $P(C_i)$ is the likelihood that the class will be selected. The prior probability of Y is denoted by the symbol P(Y). The posterior probability is denoted by the symbol $P(C_i|Y)$. $P(Y\ |C_i)$ is the notation used to represent the posterior probability of Y given the value of Ci. It should be brought to everyone's attention that $P(Y)$ remains unchanging regardless of class; hence, the only thing that needs to be done is to maximize the numerator of $P(C_i|Y)$. When it is possible to determine the class prior probabilities, it is optimal to maximize the $P(C_1) = P(C_2) == P(C_n)$ and $P(Y\ |C_i)$ values. In any other case, the class prior probability may be derived by using the formula $P(C_i) = |C_i, D/|D$, where the notation $|C_i, D|$ denotes the total number of instances of class C_i present in dataset D. Within this formula, the total number of observations is denoted by the letter D. In order to cut down on the amount of complex calculation that is necessary in order to estimate $P(Y\ |C_i)$, The design of the classifier makes advantage of the occurrences that are independent of one another in terms of the conditions under which they occur. This is done in order to decrease the amount of time spent on the task. Then,

$$P(Y|C_i) = \prod_{k=1}^{n} P(y_k|C_i) = P(y_1|C_i) \times P(y_2|C_i) \times \dots P(y_n|C_i) \tag{2}$$

The probabilities $P(y1|Ci), P(y2|Ci),, P(yn|Ci)$ are calculated from the training set, and y_k denotes the value of an event for the data set Y. In order to obtain the class label of Y, the probabilities $P(Y\ |C\_i)P(C\_i)$ are estimated for each class C_i.

$$(Y|C_i)P(C_i) > P\big(Y|C_j\big)P(C_j) \text{ for } 1 \le j \le n, j \ne i \tag{3}$$

10.48047/jocaaa.2024.33.07.55

C. *ELM Classifier*

The ELM model has recently been implemented for use with single-layer NN. When using the ELM model, the links between the input and hidden layers are decided upon using a random selection process, but they remain fixed and do not shift in any way. After then, the output weights are modified by trying to reduce the error rate as much as possible over a rectilinear system. When we are training ANN with N hidden neurons and transfer function $f(x)$ to learn M distinct samples(x_i, t_i). In the following order, number the equations. Using a right tab stop, you should arrange the equation numbers inside the parentheses such that they are flush right, as in (1). You may condense the notation of your equations by using the solidus (/) operator, the exp function, or the necessary exponents. When referring to numbers and variables, Roman symbols should be italicized, while Greek symbols should not be. Instead of a hyphen, a negative sign should be written with a long dash. When an equation is a component of a sentence, such as in or, it should be punctuated with commas or periods.

$$H\beta = T \tag{4}$$

Here, H positions for the matrix of the hidden layer, and is shown by:

$$H = \begin{bmatrix} f(w_1.x_1 + b_1) & \cdots & f(w_n.x_1 + b_n) \\ \vdots & \ddots & \vdots \\ f(w_1.x_m + b_1) & \cdots & f(w_n.x_m + b_n) \end{bmatrix} \tag{5}$$

Here, $w_j = [w_{j1}, w_{j2}, \ldots, w_{jk}]^T, (j = 1,2,\ldots,N)$ is the vector of weight linking jth hidden node and input node, and bj the hidden bias of jth node; $w_j.x_i(i = 1,\ldots,M)$ denotes the inner product of w_j and x_i; $\beta = [\beta_1, \beta_2, \ldots, \beta_N]^T$, the weights output matrix $\beta_j = [\beta_{j1}, \beta_{j2}, \ldots, \beta_{jd}]^T * U$.

$$t_i = \sum_{j=1}^{n} b_j f(w_j.x_j + b_j) \tag{6}$$

The W output are computed using the LS method introduced in equation (7) as follows:

$$\hat{\beta} = H^*T \tag{7}$$

Here, H^* is inverse matrix of H. ELM with MP inverse approach leads to obtaining better performance with enhanced training rate.

10.48047/jocaaa.2024.33.07.55

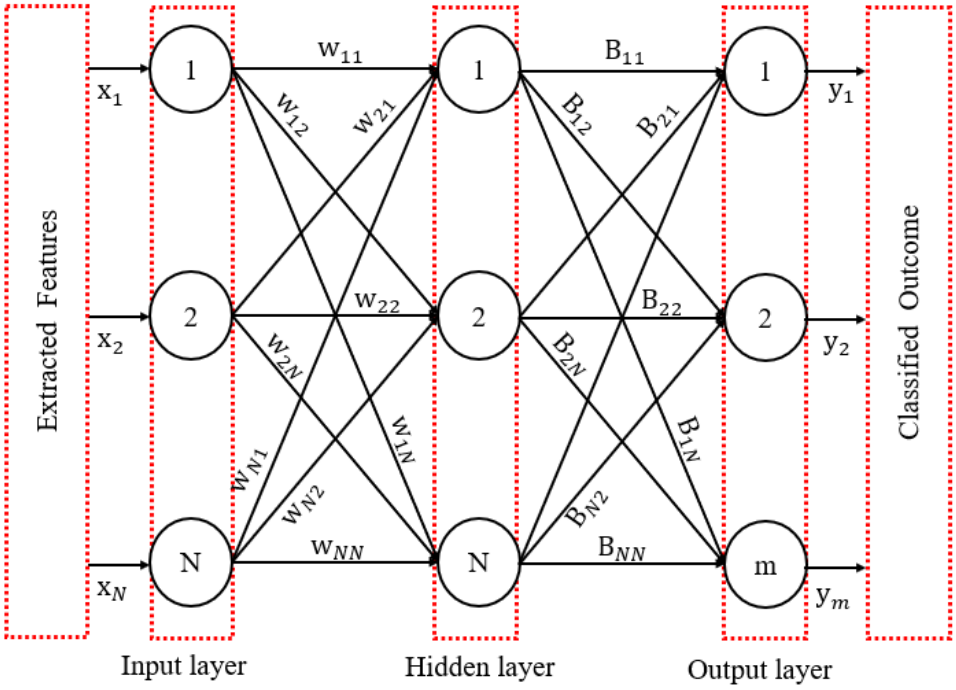


Fig. 2. Hidden neurons in hierarchical ELM

IV. RESULTS AND DISCUSSIONS

This section gives detailed analysis of simulation results and discussions. Further, the performance of proposed method is compared with the other approaches using same dataset.

A. Dataset

In the UtkML's Twitter Spam Detection Competition, the goal is to develop a classifier that can distinguish between "Quality" content and "Spam" tweets. Spam in this context refers to unwanted content posted by known fake Twitter accounts, including politically motivated messages, automatically generated content, meaningless posts, and clickbait. The dataset provided for the competition contains the following columns:

"Tweet": This column contains the text of the tweet itself.

"Following": This indicates the total number of users that the account that published the tweet is now following.

"Followers": It indicates the number of people who are following the account that posted the tweet.

"Actions": This column keeps track of the total number of likes, replies, and retweets that the tweet has gotten since it was posted.

"Is_retweet" is a binary value, and a value of 0 indicates that the tweet in question is not a retweet, while a value of 1 show that the tweet in question is in fact a retweet.

"Location" is the name of the column that stores the user's handwritten location information that is included on their profile. There is a possibility that it is not a conventional place and that it is "Unknown." or represented in various formats such as "NY," "New York," or "Upper East Side."

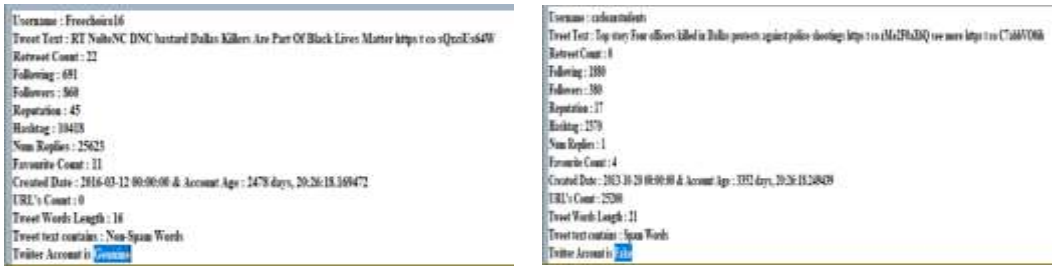
"Type": This column categorizes the tweet as either "Quality" or "Spam."

10.48047/jocaaa.2024.33.07.55

The task is to train a classifier using this dataset to accurately identify and classify tweets as either "Quality" or "Spam" based on the provided features.

B. Results

Figure 3 illustrates the user details in the dataset, distinguishing between a genuine user and a fake user. The image represents a genuine user, indicating that the associated account is authentic and does not engage in deceptive or malicious activities.



(a) (b)

Fig. 3. User details of dataset. (a) Genuine user. (b) Fake user.

Genuine users typically share legitimate content, interact with others in a meaningful manner, and have a genuine presence on the platform. The image represents a fake user, suggesting that the associated account is not genuine and may be involved in deceptive or malicious activities. Fake users often generate false content, promote spam URLs, exploit trending topics for their advantage, or masquerade as legitimate users to deceive others. Figure 4 shows the detected fake accounts, and spam accounts statistics. The detection of user status, including false content, spam URLs, trending topics, and fake accounts, is a crucial step in the evaluation process of each tweet. By identifying and flagging such accounts, it becomes possible to analyse and assess the tweets for false information, spam URLs, trending topics manipulation, and the presence of fake users. This aids in maintaining the integrity and security of the platform and ensuring a trustworthy user experience. Here, every characteristic was extracted from the tweet's dataset, after that, an analysis of those characteristics was done to determine whether or not a tweet is spam. In the text box that is shown above, each record's value is separated by a blank line. Each tweet record displays values such as tweet text, followers, following, etc., along with information on whether the account is false or authentic and if the tweet text includes phrases that are considered spam or words that are not considered spam.

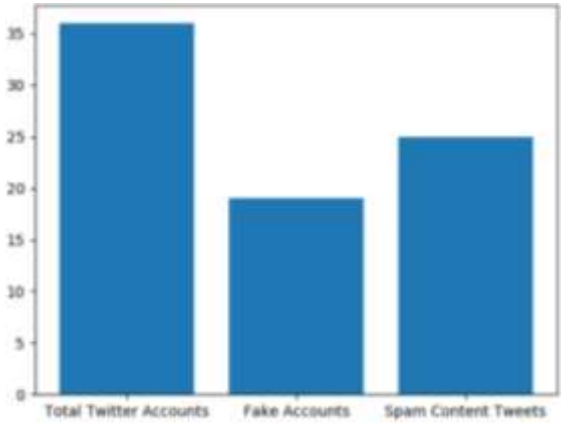


Fig. 4. Detetected Fake Accounts, Spam Content Accounts.

10.48047/jocaaa.2024.33.07.55

Table 1 shows the performance of various methods. Here, the proposed ELM resulted in improved performance as compared to other methods, such as RFC [13], NBC [15] , and SVM [16]. The proposed ELM method achieves a 59.73% improvement in accuracy, a 57.63% improvement in precision, a 72.41% improvement in recall, and an 80.63% improvement in F1-Measure compared to RFC [13]. Compared to NBC [15], the proposed ELM method shows a 59.73% improvement in accuracy, a 57.63% improvement in precision, a 72.41% improvement in recall, and an 80.63% improvement in F1-Measure. The proposed ELM method demonstrates a 59.73% improvement in accuracy, a 57.63% improvement in precision, a 72.41% improvement in recall, and an 80.63% improvement in F1-Measure compared to SVM [16].

Table 1. Performance evaluation

Method	Accuracy	Precision	Recall	F1-Measure
RFC [13]	60.0	52.77	55.76	48.86
NBC [15]	66.66	55.00	59,61	53.41
SVM [16]	86.66	43.33	50.0	46.42
Proposed ELM	95.84	83.3	96.15	88.001

V. CONCLUSION

This research specializes in solving the problems given via junk mail and fraudulent user debts on Twitter by detecting spammers and figuring out fake customers. This changed into done thru the identity of spammers and fake customers. The research efficiently hired a pre-processing approach to dispose of noise and inappropriate information from the Twitter dataset. Furthermore, MNB changed into applied to extract informative functions considering textual, linguistic, and consumer-precise characteristics. These capabilities have been then used to educate the ELM classifier, ensuing in powerful discrimination between spam and valid user accounts. The fulfilment of the method that become advanced changed into shown by the complete checks that were done on a genuine Twitter dataset. The aggregate of MNB function extraction and ELM class achieved excessive accuracy, precision, don't forget, and F1-rating in identifying spammers and fake customers on Twitter. Further research may be conducted to explore the overall performance of different function extraction techniques and gadget gaining knowledge of algorithms for spam detection and fake user identification on Twitter.

REFERENCES

[1] Jimoh, R. G., et al. "Experimental evaluation of ensemble learning-based models for twitter spam classification." 2022 5th Information Technology for Education and Development (ITED). IEEE, 2022.

[2] Ouni, Sarra, Fethi Fkih, and Mohamed Nazih Omri. "BERT-and CNN-based TOBEAT approach for unwelcome tweets detection." Social Network Analysis and Mining 12.1 (2022): 144.

[3] Li, Siyu, et al. "SybilFlyover: Heterogeneous graph-based fake account detection model on social networks." Knowledge-Based Systems 258 (2022): 110038.

[4] Park, Jeongeun, Jinmo Gu, and Ha Young Kim. "“Do not deceive me anymore!” interpretation through model design and visualization for instagram counterfeit seller account detection." Computers in Human Behavior 137 (2022): 107418.

10.48047/jocaaa.2024.33.07.55

[5] Shahzad, Ahmed, et al. "COVID-19 vaccines related user's response categorization using machine learning techniques." Computation 10.8 (2022): 141.

[6] Alothali, Eiman, Kadhim Hayawi, and Hany Alashwal. "SEBD: A Stream Evolving Bot Detection Framework with Application of PAC Learning Approach to Maintain Accuracy and Confidence Levels." Applied Sciences 13.7 (2023): 4443.

[7] Macas, Mayra, Chunming Wu, and Walter Fuertes. "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities." Computer Networks 212 (2022): 109032.

[8] Ahmad, Tahir, et al. "Efficient Fake News Detection Mechanism Using Enhanced Deep Learning Model." Applied Sciences 12.3 (2022): 1743.

[9] Kavin, B. Prabhu, et al. "Research Article Machine Learning-Based Secure Data Acquisition for Fake Accounts Detection in Future Mobile Communication Networks." (2022).

[10] Srinivas, M., et al. "Spammer Detection in Social Networks using ML and NLP." 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). IEEE, 2022.

[11] Ramesh, Mr P., et al. "Spammer Detection and Fake User Identification on Social Networks." Mathematical Statistician and Engineering Applications 71.4 (2022): 5197-5212.

[12] Kumar, Chanchal, Taran Singh Bharti, and Shiv Prakash. "A hybrid Data-Driven framework for Spam detection in Online Social Network." Procedia Computer Science 218 (2023): 124-132.

[13] Abkenar, Sepideh Bazzaz, et al. "Learning textual features for Twitter spam detection: A systematic literature review." Expert Systems with Applications (2023): 120366.

[14] Rodrigues, Anisha P., et al. "Real-time twitter spam detection and sentiment analysis using machine learning and deep learning techniques." Computational Intelligence and Neuroscience 2022 (2022).

[15] Ahraminezhad, Ali, Musa Mojarad, and Hassan Arfaeinia. "An intelligent ensemble classification method for spam diagnosis in social networks." Int J Intell Syst Appl 14.1 (2022): 24-31.

[16] Zeng, Ziming, et al. "A novel semi-supervised self-training method based on resampling for Twitter fake account identification." Data Technologies and Applications 56.3 (2022): 409-428.

[17] Dutta, Ashit Kumar, et al. "Optimal Weighted Extreme Learning Machine for Cybersecurity Fake News Classification." Computer Systems Science & Engineering 44.3 (2023).

[18] Khan, Adnan, et al. "Robust Extreme Learning Machine Using New Activation and Loss Functions Based on M-Estimation for Regression and Classification." Scientific Programming 2022 (2022).

[19] Prabhu Kavin, B., et al. "Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks." Wireless Communications and Mobile Computing 2022 (2022): 1-10.

[20] Vives, Luis, et al. "A novel hybrid approach of gravitational search algorithm and decision tree for twitter spammer detection." International Journal of Modern Physics C 33.05 (2022): 2250060.