e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204136 |

Fake Account Detection using Machine Learning Techniques

Prof.V.G.Bharane' Momin Aayman Rafik, Pathan Nafisa Sharif, Suryavanshi Priyanka Dattatray

Department of Computer Engineering, S.B.Patil College of Engineering, Indapur, India

ABSTRACT—The online social networks are a very large growth in the world today, but the attacks are more common, including one of the attacks is the attack of Twitter in this spammer spreading several malicious tweets that can take the form of links or hash tags in the website and online services, which are too harmful for real users. To prevent these attacks, training tweets are added and, moreover, these problems are solved by extracting 12 lightweight functions, like the age of the account, no. of followers, no. to follow, no. of tweets, no. of re-tweets, etc. For the transmission of spam detection from tweets, the discretization of a function is important for the performance of spam detection. There is a great truth in the system that includes a total of 600 public tweets based on the URL-based security tool. Spam detection primarily creates the classification model that includes binary classification and can also be solved using the automatic learning algorithm. Machine learning algorithms such as the Naïve Bayesian classifier or the vector support machine classifier have informed the behavior of the models. The system reported the impact of data-related factors, such as the relationship between spam and non-spam, the size of training data and data sampling, and detection performance. The implemented system function is the detection of simple and variable tweets of spam over time. The system shows how spam detection is a major challenge and bridges the gap between performance appraisals and focuses primarily on data, features and patterns to identify the real user and inform the user of spam when providing the valuable response binary. The contribution work is to detect the tweets of spam in real time, because the new tweets come in the form of sequences and use the updated training data set.

KEYWORDS-Machine Learning, Parallel Computing, Spam Detection, Scalability, Twitter

I. INTRODUCTION

Online social networking sites like Twitter, Facebook, Instagram and some online social networking companies have become extremely popular in recent years. People spend a lot of time in OSN making friends with people they are familiar with or interested in. Twitter, founded in 2006, has become one of the most popular microblogging service sites. Around 200 million users create around 400 million new tweets a day for spam growth. Twitter spam, known as unsolicited tweets containing malicious links that the non-stop victims to external sites containing the spread of malware, spreading malicious links, etc., hit not only more legitimate users, but also the whole platform Consider the example because during the election of the Australian Prime Minister in 2013, a notice confirming that his Twitter account had been hacked. Many of his followers have received direct spam messages containing malicious links. The ability to order useful information is essential for the academic and industrial world to discover hidden ideas and predict trends on Twitter. However, spam generates a lot of noise on Twitter. To detect spam automatically, researchers applied machine learning algorithms to make spam detection a classification problem. Ordering a tweet broadcast instead of a Twitter user as spam or non-spam is more realistic in the real world.

II. PROPOSED SYSTEM

- The collection of tweets with respect to trending topics on Twitter. After storing the tweets in a particular file format, the tweets are subsequently analyzed.

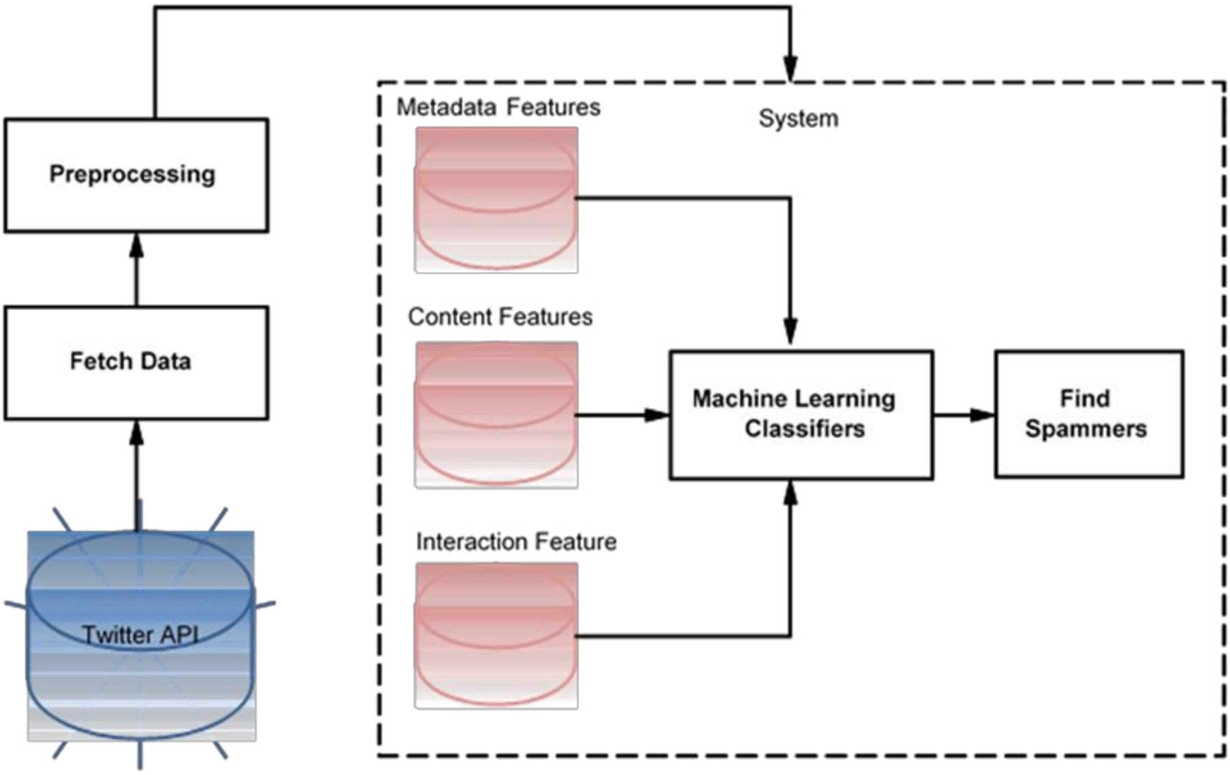
- Labelling of spam is performed to check through all datasets that are available to detect the malignant URL.

- Feature extraction separates the characteristics construct based on the language model that uses language as a tool and helps in determining whether the tweets are fake or not.

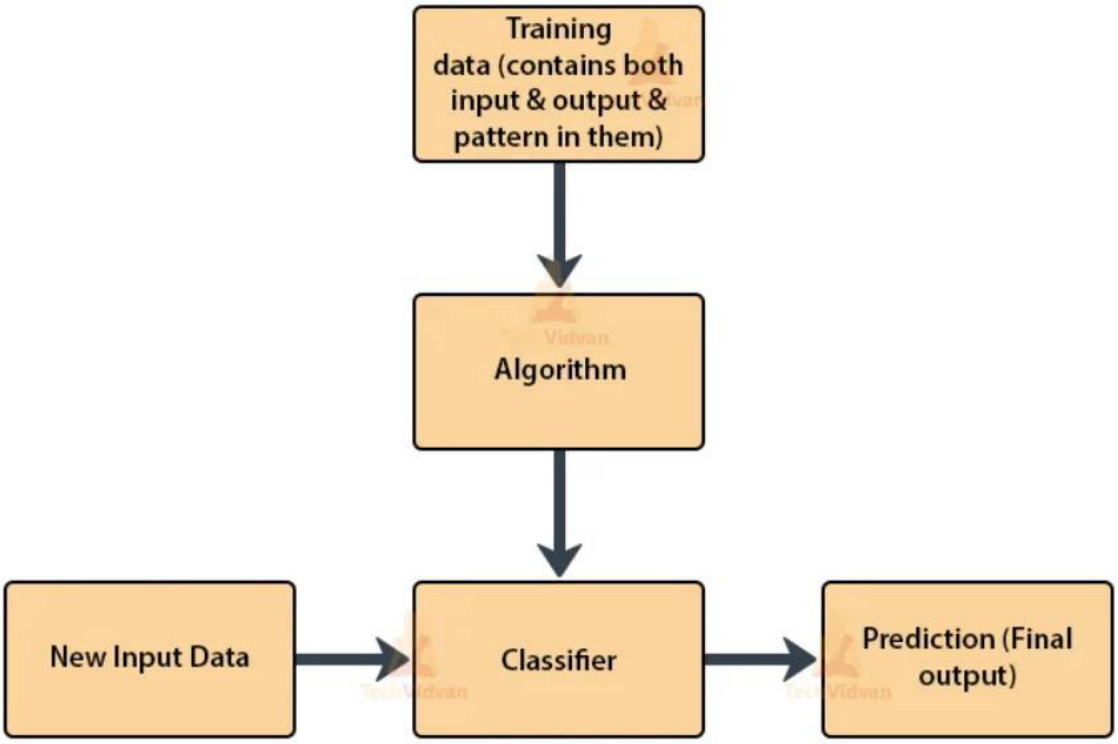
- The classification of data set is performed by shortlisting the set of tweets that is described by the set of features provided to the classifier to instruct the model and to acquire the knowledge for spam detection.

- The spam detection uses the classification technique to accept tweets as the input and classify the spam and non-spammer.

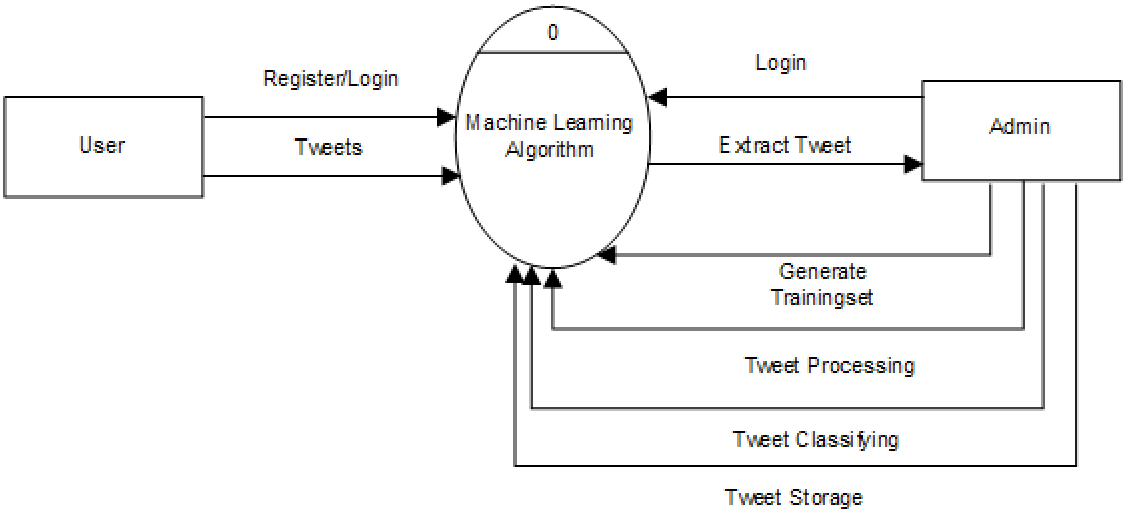
Architecture



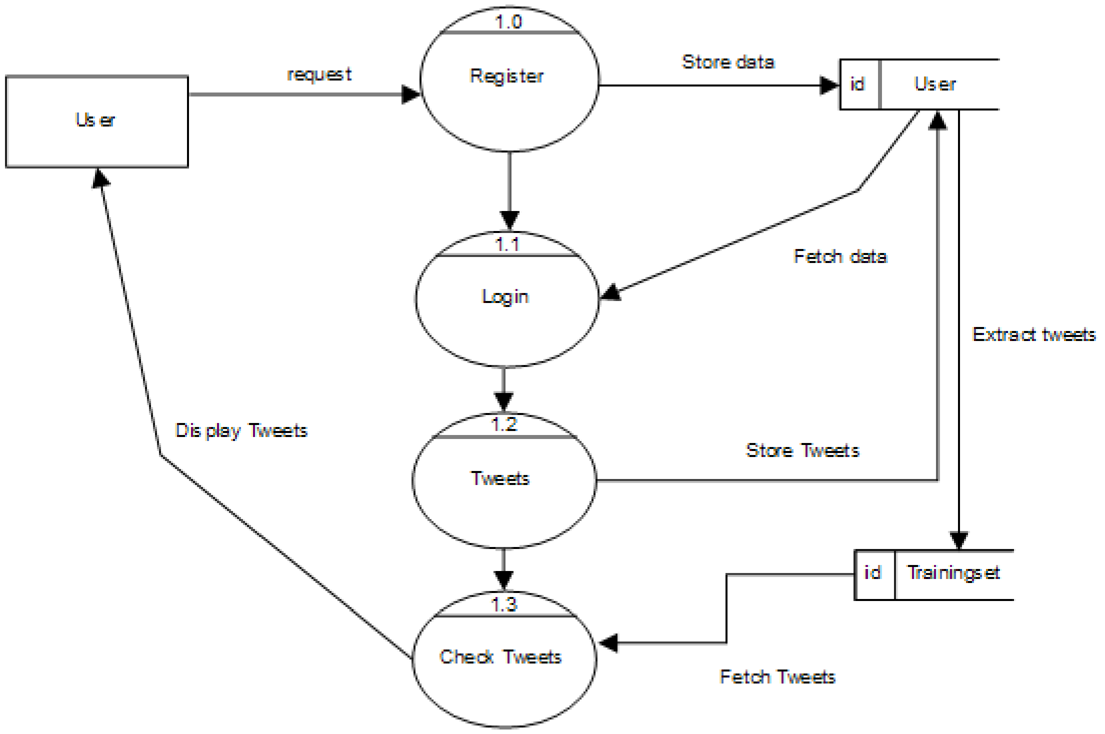
Algorithm flowchart


Training data (contains both input & output & pattern in them)
Algorithm
New Input Data
Classifier
Prediction (Final output)

DFD Diagram
Level 0



Level 1



III. ADVANTAGES

- To categories the Spammers and Non-spammers.
- To work on a performance evaluation such as Precision, Recall, F-measure.
- To categorize the tag based tweets and link based tweets.
- To try to improve detection accuracy using deep learning algorithms.

IV. APPLICATION

- Social Media Application
- Spam Detection Applications

V. CONCLUSION

In this Project, System found that classifiers ability to detect Twitter spam reduced when in a near real-world scenario since the imbalanced data brings bias. System also identified that Feature discretization was an important preprocess to ML-based spam detection. Second, increasing training data only cannot bring more benefits to detect Twitter spam after a certain number of training samples. System should try to bring more discriminative features or better model to further improve spam detection rate.

REFERENCES

[1] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, “Aiding the detection of fake accounts in large scale social online services,” in Proc. Symp. Netw. Syst. Des. Implement. (NSDI), 2012, pp. 197–210.

[2] G. Stringhini, C. Kruegel, and G. Vigna, “Detecting spammers on social networks,” in Proc. 26th Annu. Comput. Sec. Appl. Conf., 2010, pp. 1–9.

[3] J. Song, S. Lee, and J. Kim, “Spam filtering in Twitter using sender receiver relationship,” in Proc. 14th Int. Conf. Recent Adv. Intrusion Detection, 2011, pp. 301–317.

[4] K. Lee, J. Caverlee, and S. Webb, “Uncovering social spammers: social honeypots + machine learning,” in Proc. 33rd Int. ACM SIGIR Conf. Res.Develop. Inf. Retrieval, 2010, pp. 435–442.

[5] Nathan Aston, Jacob Liddle and Wei Hu*, “Twitter Sentiment in Data Streams with Perceptron,” in Journal of Computer and Communications, 2014, Vol-2 No-11.

[6] K. Thomas, C. Grier, D. Song, and V. Paxson, “Suspended accounts in retrospect: An analysis of Twitter spam,” in Proc. ACM SIGCOMM Conf. Internet Meas., 2011, pp. 243–258.

[7] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, “Design and evaluation of a real-time URL spam filtering service,” in Proc. IEEE Symp. Sec. Privacy, 2011, pp. 447–462.

[8] X. Jin, C. X. Lin, J. Luo, and J. Han, “Socialspamguard: A data mining based spam detection system for social media networks,” PVLDB, vol. 4, no. 12, pp. 1458–1461, 2011.

[9] S. Ghosh et al., “Understanding and combating link farming in the Twitter social network,” in Proc. 21st Int. Conf. World Wide Web, 2012, pp. 61–70.

[10] H. Costa, F. Benevenuto, and L. H. C. Merschmann, “Detecting tip spam in location-based social networks,” in Proc. 28th Annu. ACM Symp. Appl. Comput., 2013, pp. 724–729.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details

www.ijirset.com