**Open Access**
Full Length Article

ORIGINAL ARTICLE

# Detecting Social Bots Activity in Twitter Using Deep Learning Approach

**Hafiza Sana Shamim[1], Asghar Ali Shah[2]**

[1, 2] Department of Computer Science, Bahria University Lahore Pakistan

## ABSTRACT

One of the most popular microblogging social networking sites with millions of users is Twitter. Social bots (also known as spambots) are content-generating robots that exist on social media networks. This study provides an overview of new strategies for distinguishing between social bot accounts and human accounts that have recently appeared. Users have benefited from the deployment of social bots to automate analytical services and improve service quality. On the other hand, social bots have been employed to distribute false information, which can have real-world consequences. The description describes a method for determining if that user is a Bot or a human. The proposal proposes recognizing such accounts by evaluating message predictability because communications published from the same bot account usually follow basic, repeating patterns. The shallow and deep learning algorithms for tweet-based bot detection, as well as their performance outcomes, are also described. To determine if tweets were made by actual people or bots, a machine learning architecture is proposed. Customers' actual voices can be greatly distorted by malicious bots. We categorized millions of open-source functions in the Cresco 2017 datasets. The goal of this study is to look at social bots in the context of user-generated content deep learning.

**Keywords:** Deep Learning, Machine Learning Bot, Human, Detection, Social Media

Author`s Contribution

*[1,2] Data analysis, interpretation and manuscript writing, Active participation in data collection, Conception, synthesis, planning of research, Interpretation, and discussion*

*Address of Correspondence*

*Hafiza Sana Shamim*

*Email: sanashamim785@gmail.com*

Article info.

*Received: Feb 21, 2021*

*Accepted: June 14, 2021*

*Published: June 30, 2021*

***Cite this article:*** *Shamim HS, Shah AI. Detecting social bots activity in Twitter using deep learning approach J. inf. commun. technol. robot. appl.2021; 12(1):36-46*

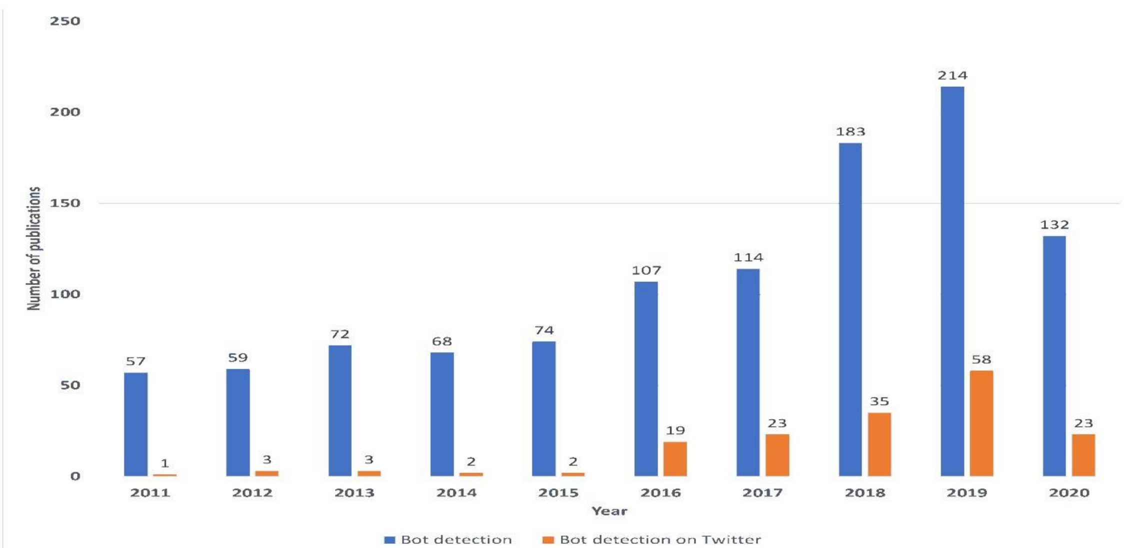
***Funding Source:*** *Nil*

***Conflict of Interest:*** *Nil*

## INTRODUCTION

The use of social media is a computer-based technology that allows the interchange of ideas, opinions, and information through the construction of virtual networks and communities [1]. It is also widely used by businesses to communicate with their customers. According to the world's dynamic web-based media clients, there are 3.5 billion of them. Online media sites such as Facebook, Twitter, LinkedIn, and others are used by businesses to increase brand awareness and revenue. Twitter is one of the most famous interpersonal interaction stages. Mechanized records, then again, utilize these administrations [2]. Bots are mechanized Twitter accounts that convey tweets containing destructive or inaccurate data in an endeavor to influence popular assessment; impact political questions; advance explicit thoughts, items, or administrations, or spread ramous. They can also be used to create fake followers to increase a user's reputation and status [2]. In this study, the proposed change likelihood highlights between client clickstreams dependent on friendly circumstance investigation, just as planning a calculation for distinguishing malevolent social bots dependent on spatiotemporal elements, fully intent on recognizing pernicious social bots on informal community stages in genuine time [3]. Bots are self-programmable autonomous agents that can be used to distribute fake news, and political ideas, and cause conflict to sway people's attitudes. Even though they solely operate on social media, the way they affect people has a real-world impact. Spreading fake news on social media has the potential to sway election results [3]. Partitioned into two classifications: great bots and bad bots. Great bots incorporate web crawlers and visit bots, while bad bots incorporate malicious bots, which represent 20% of all traffic. The explanation they are bad is that they can emulate human conduct, imitate lawful traffic, assault IoT gadgets, and take advantage of their presentation [4]. Among all of these concerns, social media users are the most exposed to data breaches and changes in opinion based on data because they constitute a huge population of active internet users. It is critical to detect such bots to avoid similar accidents [5].

It has been accounted for that there are 3.5 billion dynamic web-based entertainment clients all around the world. Facebook, Twitter, LinkedIn, and other virtual entertainment networks are utilized by associations to further develop brand perceivability and lift their deals [34]. Koggalahewa et al. [35] developed an unsupervised strategy to identify spammers in light of clients' companion acknowledgment produced from clients' post content. In the main quarter of 2010, Twitter had 30 million month-to-month dynamic clients [36].




## BACKGROUND

There were 8.4 million tweets from 3500 human accounts and 3.4 million tweets from 5000 bots in the manually confirmed data set. Human clients reacted to different tweets four to multiple times more oftentimes than bots, as per analysts. Throughout an hour of Twitter use, genuine clients become more involved, with the level of answers increasing [6]. The scope of our investigation is limited to detecting social bots on the Twitter social media platform. We investigate common aspects such as the classifier, datasets, and selected features used in the various detection systems now in use. We also compare how the classifiers are validated using different assessment methodologies. Finally, we discuss the obstacles that remain in the realm of social bot identification, as well as future research possibilities for efforts to address this issue [4]. At the moment, the most widely used method for detecting social bots is based on dynamic content delivered by social bots and the social relationship diagram that surrounds them. To get better classification results, this technology necessitates the analysis of previously acquired data sets and the selection of representative and discrimination features [5]. As the sessions progressed, the length of human users' tweets reduced as well. "The amount of information communicated decreases," Ferrara explains. He contends that the shift is because of intellectual fatigue, in which individuals are less inclined to invest mental energy in making new substances over the long run. According to Aite Group's Fraud & AML practice, before Covid-19, financial institutions observed a 10:1 ratio of bot-based harmful to valid login attempts. Every month, malicious login attempts establish new records [9]. The number of breached data reports increased by 84 percent between 2018 and 2019, hitting 15.1 billion accounts last year. Organized crime-funded fraud operations operate in much the same way as legal firms, with continual recruiting campaigns for AI, bot, and machine learning expertise and offices dedicated to developing breach methods. According to another Help Net Security investigation, login passwords for online banking averaged around $35 on the dark web in June 2020, while payment card details averaged between $12 and $20 each [12]. Many applied research and commercial services connected to AI approaches, such as Deep Learning (DL) and Machine Learning (ML), have recently gained prominence and attention. Sent Sentimentlysis and text analysis are used in social media analysis. These investigations have focused on classification, particularly for search engines and recommender systems [3]. Moreover, it lies among the tentative arrangements of the creators to utilize Sentence-State LSTMs [43], since it has been demonstrated that they yield profoundly aggressive outcomes contrasted with stacked Bidirectional LSTMs [37]. Andriotis and Takasu [38] utilized a few AI calculations to evaluate various arrangements of highlights, including metadata (number of situations with/companions/top picks), content (retweet/hashtag/notice/URL proportion), feeling highlights, and LDA subjects. The writing on bot location has become extremely expensive [39].

For instance, ongoing examinations show that discretionary obstruction, the spread of hostile to immunization paranoid fears, and securities exchange controls are completed utilizing bots [40]. In this paper [41], we concentrated on how bots submit to Benford's regulation Furthermore, we observed that genuine clients comply with it more frequently than bots. Our removal concentrate on shows that a wide range of our elements emphatically adds to improving the model execution [42]. Social networks have been growing in huge amounts at a time in the last ten years [43]. Their span and impact on present-day culture and its working have set out open doors for customary and somewhat new callings, as well as difficulties to forestall the abuse or altering of such amazing assets of social communication [44].

One of these new difficulties has emerged as a product application known as a bot. Bots can be constrained by one or numerous bot masters running robotized undertakings routinely over any PC, gathering of servers, or the web cloud [45,46].

## RESEARCH METHODLOGY

The stream diagram depicts how data flows through the various stages of a Systematic Review. It displays the number of records found, the number of records that were incorporated, and the number of records that were barred, as well as the reasons for avoidances. After that, each article's book indexes should be thoroughly searched for additional relevant articles. This technique, like the critical task, necessitates a first-pass survey (title rejection), a second-pass audit (dynamic prohibition), and a third-pass audit (avoidance by full-text)[10].

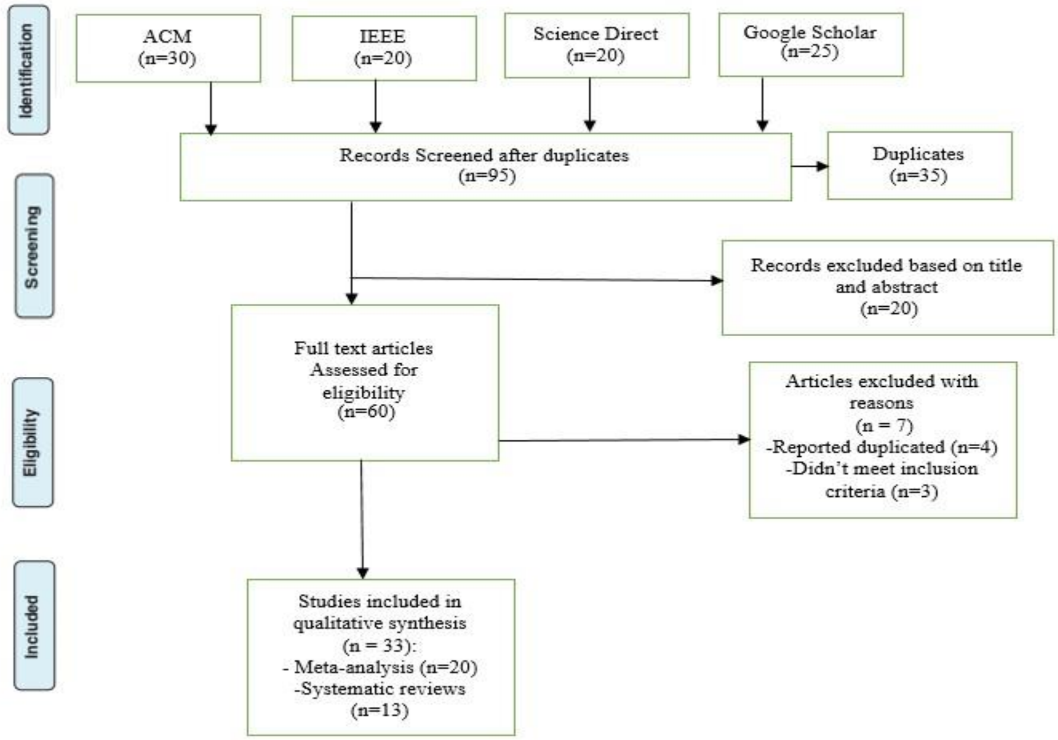



**Figure4. PRISMA**

Today's digital collections are the best places to look for books, magazines, and papers. Due to limited resources and a large number of papers on this subject, we choose three digital libraries for this literature review. We will see, though, that these libraries cover a significant portion of the applicable literature sources for our research. Three different digital libraries were used in this project to carry out a study:

1. IEEE Xplore is a directory of IEEE publications.
2. ACM
3. Google Scholar
4. Science Direct

Many studies have been conducted in the field of image captioning sow narrowed down. Only papers published in the last four years—from 2014 to 2021—were included in the literature review. We filtered out papers that were posted under the computer science subject during our study in the digital library. The literature review covered only articles written in the last four years, from 2005 to 2021. During our research in the digital library, we filtered out papers that were posted under the computer science subject.

**Inclusion and exclusion criteria**

The detection and elimination of dangerous social bots in social media have piqued commercial and academic interest. The commonly used machine learning-based bot detection method results in an imbalance in the number of samples in different categories. Minority samples are detected at a low rate due to classifier bias. To increase the detection accuracy of social bots, we propose an improved conditional generative adversarial network (improved CGAN) to extend imbalanced data sets before applying training classifiers [14]. This paper's key contribution is to demonstrate that the manufactured features that were previously utilized to detect phone accounts generated by bots are not as effective in detecting false accounts generated by people. The challenge of bot detection in social networks is examined in this research. The study focuses on the situation where the account is closed due to privacy settings, and the bot must be recognized through the friend list. With millions of users, Twitter is one of the most popular microblogging social networking platforms. We provide a taxonomy that categorizes the state-of-the-art tweet-based bot detection [15][6]. Users have benefited from the deployment of social bots to automate analytical services and improve service quality. On the other hand, malicious social bots have been employed to distribute false information, which can have real-world consequences. We describe a method for identifying whether or not a user is a bot. Because messages produced from the same bot account frequently follow simple, repetitive patterns, we propose identifying such accounts by measuring message

# RESULTS AND ANALYSIS

## A. Quality Assessment Criteria

**Table2. Categories and grading to access the quality of the selected study**

| Items | Description | Grads |
|---|---|---|
| A | Title | 0=inaccurate<br>1=possibly accurate<br>2=clearly accurate |
| B | Abstract | 0=inaccurate<br>1=possibly accurate<br>2=clearly accurate |
| C | Introduction<br>Background-objective, experimental approach | 0=inaccurate<br>1=possibly accurate<br>2=clearly accurate |
| D | Introduction<br>Objective-primary and secondary | 0=inaccurate<br>1=possibly accurate<br>2=clearly accurate |
| E | Methods<br>Nature of the review permission | 0=inaccurate<br>1=possibly accurate<br>2=clearly accurate |
| F | Method<br>Study Design number of the experimental and control group | 0=inaccurate<br>1=possibly accurate<br>2=clearly accurate |
| G | Method<br>Experimental procedure-precise detail | 0=inaccurate<br>1=possibly accurate<br>2=clearly accurate |

## B. Quality Assessment Table

**Table3. Quality Assessment Results**

| References | A | B | C | D | E | F | G | Total |
|---|---|---|---|---|---|---|---|---|
| A. Derhab, R. Alawwad, K. Dehwah, N. Tariq, F. A. Khan, and J. Al-Muhtadi, “Tweet-Based Bot Detection Using Big Data Analytics,” IEEE Access, vol. 9, pp. 65988–66005, 2021. | 2 | 1 | 2 | 1 | 0 | 2 | 2 | 10 |
| L. Ilias and I. Roussaki, “Detecting malicious activity in Twitter using deep learning techniques,” Applied Soft Computing, vol. 107, p. 107360, 2021. | 2 | 1 | 2 | 0 | 2 | 1 | 0 | 8 |
| M. Nauta, M. Habib, and M. V. Keulen, “Detecting Hacked Twitter Accounts based on Behavioural Change,” Proceedings of the 13th International Conference on Web Information Systems and Technologies, 2017. | 0 | 1 | 0 | 2 | 1 | 0 | 0 | 4 |
| P. Shi, Z. Zhang, and K.-K. R. Choo, “Detecting Malicious Social Bots Based on Clickstream Sequences,” IEEE Access, vol. 7, pp. 28855–28862, 2019. | 1 | 1 | 1 | 2 | 0 | 1 | 0 | 6 |
| X. Liu, “A big data approach to examining social bots on Twitter,” Journal of Services Marketing, vol. 33, no. 4, pp. 369–379, 2019. | 2 | 2 | 1 | 0 | 2 | 1 | 2 | 10 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| I. Pozzana and E. Ferrara, "Measuring Bot and Human Behavioral Dynamics," Frontiers in Physics, vol. 8, 2020. | 2 | 1 | 1 | 0 | 1 | 1 | 2 | 8 |
| D. S. G, "Twitter Bots Detection Using Machine Learning Techniques," International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. VII, pp. 1536–1541, 2021. | 2 | 2 | 1 | 1 | 0 | 1 | 2 | 9 |
| M. Kantepe and M. C. Ganiz, "Preprocessing framework for Twitter bot detection," 2017 International Conference on Computer Science and Engineering (UBMK), 2017. | 0 | 1 | 0 | 2 | 2 | 0 | 2 | 7 |
| –H. Ping and S. Qin, "A Social Bots Detection Model Based on Deep Learning Algorithm," 2018 IEEE 18th International Conference on Communication Technology (ICCT), 2018. | 1 | 1 | 2 | 2 | 1 | 0 | 1 | 8 |
| F. Wei and U. T. Nguyen, "Twitter Bot Detection Using Bidirectional Long Short-Term Memory Neural Networks and Word Embeddings," 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2019. | 1 | 0 | 2 | 0 | 2 | 1 | 0 | 6 |
| V. R, S. S, S. Kp, and M. Alazab, "Malicious URL Detection using Deep Learning," 2020. | 1 | 0 | 2 | 0 | 1 | 1 | 0 | 5 |
| H.-Y. Lam, "A learning approach to spam detection based on social networks." | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 3 |
| M. S. Wessel, "Perception of software bots on pull requests on social coding environments." | 1 | 1 | 1 | 1 | 2 | 1 | 0 | 7 |
| G. Mou and K. Lee, "Malicious Bot Detection in Online Social Networks: Arming Handcrafted Features with Deep Learning," Lecture Notes in C. Cai, L. Li, and D. Zengi, "Behavior enhanced deep bot detection in social media," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017. | 1 | 1 | 0 | 0 | 1 | 0 | 2 | 5 |

### C. Heat Map

**Table4. Quality Assessment Heat Map**

| **References** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **Total** |
|---|---|---|---|---|---|---|---|---|
| A. Derhab, R. Alawwad, K. Dehwah, N. Tariq, F. A. Khan, and J. Al-Muhtadi, "Tweet-Based Bot Detection Using Big Data Analytics," IEEE Access, vol. 9, pp. 65988–66005, 2021. | 2 | 1 | 2 | 1 | 0 | 2 | 2 | 10 |
| L. Ilias and I. Roussaki, "Detecting malicious activity in Twitter using deep learning techniques," Applied Soft Computing, vol. 107, p. 107360, 2021. | 2 | 1 | 2 | 0 | 2 | 1 | 0 | 8 |
| M. Nauta, M. Habib, and M. V. Keulen, "Detecting Hacked Twitter Accounts based on Behavioural Change," *Proceedings of the 13th Internatior Conference on Web Information Systems a Technologies*, 2017. | 0 | 1 | 0 | 2 | 1 | 0 | 0 | 4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| P. Shi, Z. Zhang, and K.-K. R. Choo, “Detecting Malicious Social Bots Based on Clickstream Sequences,” IEEE Access, vol. 7, pp. 28855–28862, 2019. | 1 | 1 | 1 | 2 | 0 | 1 | 0 | 6 |
| X. Liu, “A big data approach to examining social bots on Twitter,” Journal of Services Marketing, vol. 33, no. 4, pp. 369–379, 2019. | 2 | 2 | 1 | 0 | 2 | 1 | 2 | 10 |
| I. Pozzana and E. Ferrara, “Measuring Bot and Human Behavioral Dynamics,” Frontiers in Physics, vol. 8, 2020. | 2 | 1 | 1 | 0 | 1 | 1 | 2 | 8 |
| D. S. G, “Twitter Bots Detection Using Machine Learning Techniques,” International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. VII, pp. 1536–1541, 2021. | 2 | 2 | 1 | 1 | 0 | 1 | 2 | 9 |
| M. Kantepe and M. C. Ganiz, “Preprocessing framework for Twitter bot detection,” 2017 International Conference on Computer Science and Engineering (UBMK), 2017. | 0 | 1 | 0 | 2 | 2 | 0 | 2 | 7 |
| –H. Ping and S. Qin, “A Social Bots Detection Model Based on Deep Learning Algorithm,” 2018 IEEE 18th International Conference on Communication Technology (ICCT), 2018. | 1 | 1 | 2 | 2 | 1 | 0 | 1 | 8 |
| F. Wei and U. T. Nguyen, “Twitter Bot Detection Using Bidirectional Long Short-Term Memory Neural Networks and Word Embeddings,” 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2019, | 1 | 0 | 2 | 0 | 2 | 1 | 0 | 6 |
| V. R, S. S, S. Kp, and M. Alazab, “Malicious URL Detection using Deep Learning,” 2020. | 1 | 0 | 2 | 0 | 1 | 1 | 0 | 5 |
| H.-Y. Lam, “A learning approach to spam detection based on social networks.” | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 3 |
| M. S. Wessel, “Perception of software bots on pull requests on social coding environments.” | 1 | 1 | 1 | 1 | 2 | 1 | 0 | 7 |
| G. Mou and K. Lee, “Malicious Bot Detection in Online Social Networks: Arming Handcrafted Features with Deep Learning,” Lecture Notes in C. Cai, L. Li, and D. Zengi, “Behavior enhanced deep bot detection in social media,” 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017. | 1 | 1 | 0 | 0 | 1 | 0 | 2 | 5 |

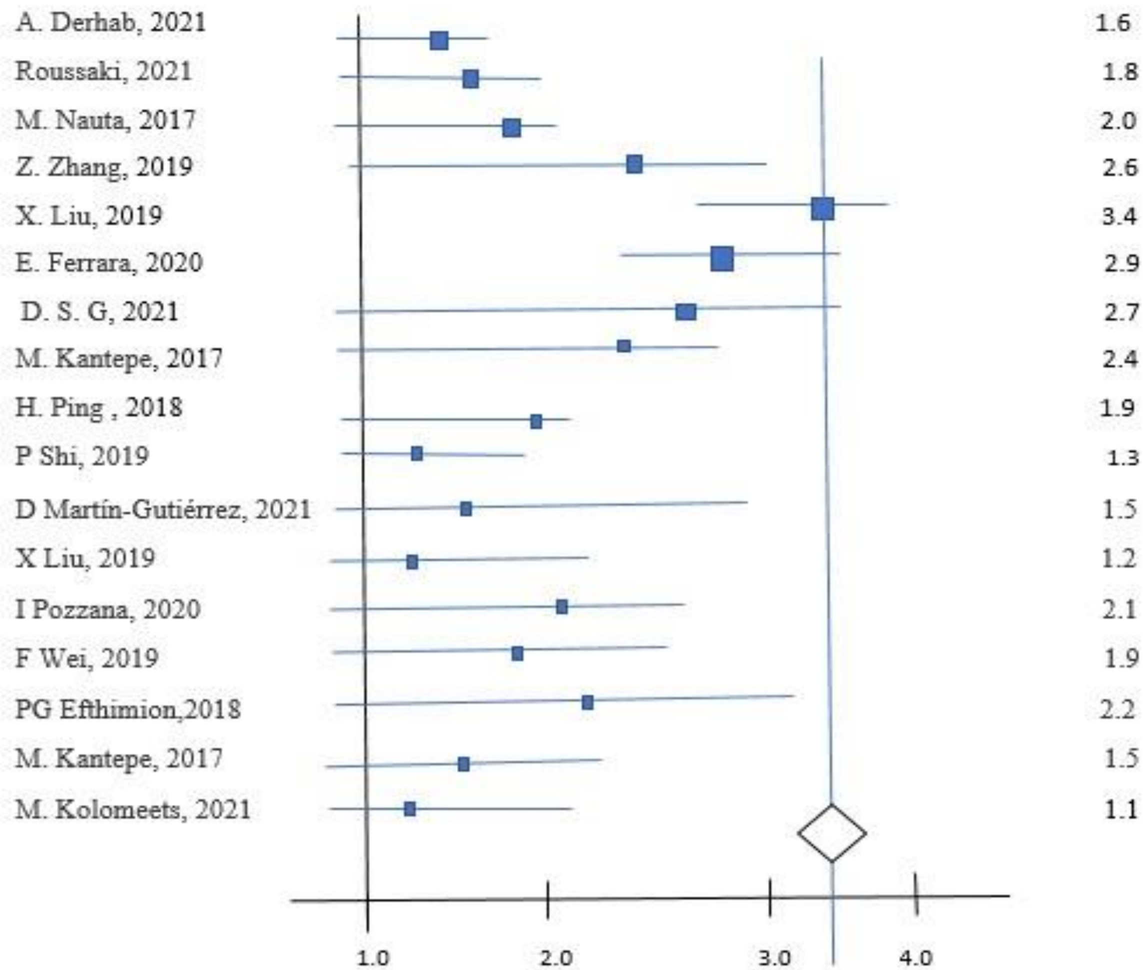



**Figure3. Forest Plot**

## DISCUSSION

In this section, we describe the methods we utilized and the results we acquired from our study of various labeled databases from the bot detection literature. Each of the four databases contains separate datasets containing public information retrieved from Twitter (users and their tweets), as well as relationship information in one (the followers and followings of the users). The used dataset from CRESCI-2017 [25] in this study, two classes in this dataset (Genuine for humans and spambot#1 for bots). Four features in this dataset (listed_count, statuses_count, retweet_count, num_mention). Percentage frequency distribution (PFD). Which contains a mix of user accounts and spambots such as social and traditional. A user and a tweet file are associated with each group name. Users' information is stored in the user file. The twitter file is a collection of tweets that have been made by individuals. The latter method also takes advantage of user attributes, and it has been demonstrated that the performance gap between two baselines on Cresci-17 is significantly larger than on Cresci-15. This demonstrates that, aside from being a toy, Cresci-17 is a more complex example that necessitates bot detectors using more user input to perform properly [28]. A dataset is a logically organized collection of data associated with a specific body of work. There are 2,764 human users and 7,049 bots in the Cresci-17 dataset [28]. Multiple deep learning techniques feature extraction such as word2vec and BERT.

The transformer is an attention mechanism that learns contextual relationships between words (or sub-words) in a text, and BERT takes use of it. The Transformer encoder reads the complete sequence of words at once, unlike directional models that read the text input sequentially (left-to-right or right-to-left) [26]. The word2vec program learns word connections from a huge corpus of text using a neural network model. Once trained, a model like this can detect synonyms and recommend new words for a sentence [27].

## CONCLUSION

RNN is a type of ANN that is specialized for processing sequential data. RNN may be used to develop a deep learning model that can automatically translate a text from one language to another without the need for human interaction. Recurrent neural networks can be used to handle challenges such as text data, speech data, video data, and audio data [28]. The output of the previous time step is fed into the next time step in a fully-connected RNN called a simple RNN [29]. In sequence prediction challenges, LSTM networks are a type of recurrent neural network that can learn order dependence. This is a necessity in a variety of difficult problem domains, such as machine translation and speech recognition, among others. The LSTMs of deep learning is a difficult issue [30]. Bidirectional recurrent neural networks (BRNN) are neural networks with two hidden layers connected to the same output in opposite directions. This sort of generative deep learning's output layer can simultaneously collect knowledge from previous (backward) and future (forward) states [31]. Kyunghyun Cho et al. established gated recurrent units (GRUs) as a gating technique in recurrent neural networks. The GRU is comparable to an LSTM with a forget gate, but it does not have an output gate, therefore it has fewer parameters [32].

## REFERENCES


1. H. Ping and S. Qin, "A Social Bots Detection Model Based on Deep Learning Algorithm," 2018 IEEE 18th International Conference on Communication Technology (ICCT), 2018.
2. Derhab, R. Alawwad, K. Dehwah, N. Tariq, F. A. Khan, and J. Al-Muhtadi, "Tweet Based Bot Detection Using Big Data Analytics," IEEE Access, vol. 9, pp. 65988–66005, 2021.
3. D. Dukic, D. Keca, and D. Stipic, "Are You Human? Detecting Bots on Twitter Using BERT," 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA), 2020.
4. E. Alothali, N. Zaki, E. A. Mohamed, and H. Alashwal, "Detecting Social Bots on Twitter: A Literature Review," 2018 International Conference on Innovations in Information Technology (IIT), 2018.
5. B. Wu, L. Liu, Y. Yang, and X. Wang, "Using Improved Conditional Generative Adversarial Networks to Detect Social Bots on Twitter," IEEE Access, vol. 8, pp. 36664– 36680, 2020.
6. L. Ilias and I. Roussaki, "Detecting malicious activity in Twitter using deep learning techniques," Applied Soft Computing, vol. 107, p. 107360, 2021.
7. E. V. D. Walt and J. Eloff, "Using Machine Learning to Detect Fake Identities: Bots vs Humans," IEEE Access, vol. 6, pp. 6540–6549, 2018.
8. M. Nauta, M. Habib, and M. V. Keulen, "Detecting Hacked Twitter Accounts based on Behavioural Change," Proceedings of the 13th International Conference on Web Information Systems and Technologies, 2017.
9. O. Loyola-Gonzalez, R. Monroy, J. Rodriguez, A. Lopez-Cuevas, and J. I. Mata-Sanchez,
10. "Contrast Pattern-Based Classification for Bot Detection on Twitter," IEEE Access, vol. 7, pp. 45800–45817, 2019.
11. P. Shi, Z. Zhang, and K.-K. R. Choo, "Detecting Malicious Social Bots Based on Clickstream Sequences," IEEE Access, vol. 7, pp. 28855–28862, 2019.
12. D. Martin-Gutierrez, G. Hernandez-Penaloza, A. B. Hernandez, A. Lozano-Diez, and F.
13. Alvarez, "A Deep Learning Approach for Robust Detection of Bots in Twitter Using Transformers," IEEE Access, vol. 9, pp. 54591–54601, 2021.
14. X. Liu, "A big data approach to examining social bots on Twitter," Journal of Services Marketing, vol. 33, no. 4, pp. 369–379, 2019.
15. Pozzana and E. Ferrara, "Measuring Bot and Human Behavioral Dynamics," Frontiers in Physics, vol. 8, 2020.
16. F. Wei and U. T. Nguyen, "Twitter Bot Detection Using Bidirectional Long Short-Term
17. Memory Neural Networks and Word Embeddings," 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPSISA), 2019.
18. D. S. G, "Twitter Bots Detection Using Machine Learning Techniques," International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. VII, pp. 1536–1541, 2021.
19. M. Kantepe and M. C. Ganiz, "Preprocessing framework for Twitter bot detection," 2017 International Conference on Computer Science and Engineering (UBMK), 2017.
20. M. Kolomeets, O. Tushkanova, D. Levshun, and A. Chechulin, "Camouflaged bot detection using the friend list," 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2021.
21. T. Mikolov, M. Karafiát, L. Burget, J.Cernock`y, and S. Khudanpur, "Recurrent neural network-based language model," in Eleventh Annual Conference of the International Speech Communication Association, p. 1045.
22. H. Ping and S. Qin, "A Social Bots Detection Model Based on Deep Learning Algorithm," 2018 IEEE 18th International Conference on Communication Technology (ICCT), 2018.
23. F. Wei and U. T. Nguyen, "Twitter Bot Detection Using Bidirectional Long Short-Term
24. Memory Neural Networks and Word Embeddings," 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPSISA), 2019.

25. V. R, S. S, S. Kp, and M. Alazab, "Malicious URL Detection using Deep Learning," 2020.
26. H.-Y. Lam, "A learning approach to spam detection based on social networks."
27. M. S. Wessel, "Perception of software bots on pull requests on social coding environments."
28. G. Mou and K. Lee, "Malicious Bot Detection in Online Social Networks: Arming Handcrafted Features with Deep Learning," Lecture Notes in Computer Science Social Informatics, pp. 220–236, 2020.
29. Cai, L. Li, and D. Zengi, "Behavior enhanced deep bot detection in social media," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017.
30. L. D. Samper-Escalante, O. Loyola-González, R. Monroy, and M. A. Medina-Pérez, "Bot Datasets on Twitter: Analysis and Challenges," Applied Sciences, vol. 11, no. 9 p. 4105, 2021.
31. (RNN2020)," Recurrent Neural Network" [Online]. Available:
32. https://www.analyticsvidhya.com/blog/2020/02/cnn-vs-rnn-vs-mlp-analyzing-3-types-ofneural-networks-in-deep-learning/
33. L. D. Samper-Escalante, O. Loyola-González, R. Monroy, and M. A. Medina-Pérez, "Bot Datasets on Twitter: Analysis and Challenges," Applied Sciences, vol. 11, no. 9 p. 4105, 2021.
34. (RNN2020)," Recurrent Neural Network" [Online]. Available:
35. https://www.analyticsvidhya.com/blog/2020/02/cnn-vs-rnn-vs-mlp-analyzing-3-typesof-neural-networks-in-deep-learning/
36. "Simple recurrent neural networks" Wikipedia, 08-July-2019. [Online]. Available: https://keras.io/guides/working_with_rnns/
37. "Long Short-Term Memory" Wikipedia, 07-July-2021 [Online].
38. Available: https://machinelearningmastery.com/gentle-introduction-long-short-termmemory-networks-experts/
39. "Bidirectional recurrent neural networks" Wikipedia, 01-Dec-2021 [Online].
40. Available: https://en.wikipedia.org/wiki/Bidirectional_recurrent_neural_networks
41. "Gated recurrent unit" Wikipedia, 24-Nov-2021 [Online]. Available: https://en.wikipedia.org/wiki/Gated_recurrent_unit
42. M. Mohsin, 10 Social Media Statistics You Need to Know in 2021, 2020, [online] Available: https://www.oberlo.com/blog/social-media-marketing-
43. D. Niranjan Koggalahewa, Y. Xu, E. Foo, Spam detection in social networks based on peer acceptance, in Proceedings of the Australasian Computer Science Week Multiconference, 2020, pp. 1–7.
44. J. Clement. (Aug. 2019). Twitter: Number of Monthly Active Users 2010–2019. [Online]. Available: https://www.statista.com/statistics/ 282087/number-of-monthly-active-twitter-users/
45. Y. Zhang, Q. Liu, L. Song, Sentence-state lstm for text representation, 2020, arXiv preprint arXiv: 1805.02474.
46. P. Andriotis, A. Takasu, Emotional bots: Content-based spammer detection on social media, in 2018 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2018, pp. 1–8.
47. Ferrara E. Bots, elections, and social media: a brief overview. In: Disinformation, Misinformation, and Fake News in Social Media. (2020).
48. F. Pierri, A. Artoni, and S. Ceri, "Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections," PLoS One, vol. 15, no. 1, 2020, doi: 10.1371/journal.pone.0227821.
49. M. Kolomeets, D. Levshun, S. Soloviev, A. Chechulin, and I. Kotenko, "Social networks bot detection using Benford's law," in Proc. 13th International Conference on Security of Information and Networks SIN 2020, November 4-7, 2020, Merkez, Turkey
50. Albadi, N., Kurdi, M., Mishra, S.: Hateful people or hateful bots? detection and characterization of bots spreading religious hatred in Arabic social media. CSCW (2019)
51. Ortiz-Ospina, E. The Rise of Social Media. Our World in Data, 18 September 2019. Available online: https://ourworldindata.org/ rise-of-social-media (accessed on 6 October 2020).
52. Orabi, M.; Mouheb, D.; Al Aghbari, Z.; Kamel, I. Detection of Bots in Social Media: A Systematic Review. Inf. Process. Manag. 2020, 57, 102250.
53. Rovetta, S.; Suchacka, G.; Masulli, F. Bot recognition in a Web store: An approach based on unsupervised learning. J. Netw. Comput. Appl. 2020, 157, 102577.
54. Asadi, M.; Jabraeil Jamali, M.A.; Parsa, S.; Majidnezhad, V. Detecting botnet by using particle swarm optimization algorithm based on a voting system. Future Gener. Comput. Syst. 2020, 107, 95–111.
55. H. Ping and S. Qin, "A Social Bots Detection Model Based on Deep Learning Algorithm," 2018 IEEE 18th International Conference on Communication Technology (ICCT), 2018.
56. Derhab, R. Alawwad, K. Dehwah, N. Tariq, F. A. Khan, and J. Al-Muhtadi, "Tweet Based Bot Detection Using Big Data Analytics," IEEE Access, vol. 9, pp. 65988–66005, 2021.
57. D. Dukic, D. Keca, and D. Stipic, "Are You Human? Detecting Bots on Twitter Using BERT," 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA), 2020.
58. E. Alothali, N. Zaki, E. A. Mohamed, and H. Alashwal, "Detecting Social Bots on Twitter: A Literature Review," 2018 International Conference on Innovations in Information Technology (IIT), 2018.
59. B. Wu, L. Liu, Y. Yang, and X. Wang, "Using Improved Conditional Generative Adversarial Networks to Detect Social Bots on Twitter," IEEE Access, vol. 8, pp. 36664– 36680, 2020.
60. L. Ilias and I. Roussaki, "Detecting malicious activity in Twitter using deep learning techniques," Applied Soft Computing, vol. 107, p. 107360, 2021.
61. E. V. D. Walt and J. Eloff, "Using Machine Learning to Detect Fake Identities: Bots vs Humans," IEEE Access, vol. 6, pp. 6540–6549, 2018.
62. M. Nauta, M. Habib, and M. V. Keulen, "Detecting Hacked Twitter Accounts based on Behavioural Change," Proceedings of the 13th International Conference on Web Information Systems and Technologies, 2017.
63. O. Loyola-Gonzalez, R. Monroy, J. Rodriguez, A. Lopez-Cuevas, and J. I. Mata-Sanchez,
64. "Contrast Pattern-Based Classification for Bot Detection on Twitter," IEEE Access, vol. 7, pp. 45800–45817, 2019.
65. P. Shi, Z. Zhang, and K.-K. R. Choo, "Detecting Malicious Social Bots Based on Clickstream Sequences," IEEE Access, vol. 7, pp. 28855–28862, 2019.
66. D. Martin-Gutierrez, G. Hernandez-Penaloza, A. B. Hernandez, A. Lozano-Diez, and F.
67. Alvarez, "A Deep Learning Approach for Robust Detection of Bots in Twitter Using Transformers," IEEE Access, vol. 9, pp. 54591–54601, 2021.
68. X. Liu, "A big data approach to examining social bots on Twitter," Journal of Services Marketing, vol. 33, no. 4, pp. 369–379, 2019.
69. Pozzana and E. Ferrara, "Measuring Bot and Human Behavioral Dynamics," Frontiers in Physics, vol. 8, 2020.

70. F. Wei and U. T. Nguyen, "Twitter Bot Detection Using Bidirectional Long Short-Term
71. Memory Neural Networks and Word Embeddings," 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPSISA), 2019.
72. D. S. G, "Twitter Bots Detection Using Machine Learning Techniques," International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. VII, pp. 1536–1541, 2021.
73. M. Kantepe and M. C. Ganiz, "Preprocessing framework for Twitter bot detection," 2017 International Conference on Computer Science and Engineering (UBMK), 2017.
74. M. Kolomeets, O. Tushkanova, D. Levshun, and A. Chechulin, "Camouflaged bot detection using the friend list," 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2021.
75. T. Mikolov, M. Karafiát, L. Burget, J.Cernock`y, and S. Khudanpur, "Recurrent neural network-based language model," in Eleventh Annual Conference of the International Speech Communication Association, p. 1045.
76. H. Ping and S. Qin, "A Social Bots Detection Model Based on Deep Learning Algorithm," 2018 IEEE 18th International Conference on Communication Technology (ICCT), 2018.
77. F. Wei and U. T. Nguyen, "Twitter Bot Detection Using Bidirectional Long Short-Term
78. Memory Neural Networks and Word Embeddings," 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPSISA), 2019.
79. V. R, S. S, S. Kp, and M. Alazab, "Malicious URL Detection using Deep Learning," 2020.
80. H.-Y. Lam, "A learning approach to spam detection based on social networks."
81. M. S. Wessel, "Perception of software bots on pull requests on social coding environments."
82. G. Mou and K. Lee, "Malicious Bot Detection in Online Social Networks: Arming Handcrafted Features with Deep Learning," Lecture Notes in Computer Science Social Informatics, pp. 220–236, 2020.
83. Cai, L. Li, and D. Zengi, "Behavior enhanced deep bot detection in social media," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017.
84. L. D. Samper-Escalante, O. Loyola-González, R. Monroy, and M. A. Medina-Pérez, "Bot Datasets on Twitter: Analysis and Challenges," Applied Sciences, vol. 11, no. 9 p. 4105, 2021.
85. (RNN2020)," Recurrent Neural Network" [Online]. Available:
86. https://www.analyticsvidhya.com/blog/2020/02/cnn-vs-rnn-vs-mlp-analyzing-3-types-ofneural-networks-in-deep-learning/
87. L. D. Samper-Escalante, O. Loyola-González, R. Monroy, and M. A. Medina-Pérez, "Bot Datasets on Twitter: Analysis and Challenges," Applied Sciences, vol. 11, no. 9 p. 4105, 2021.
88. (RNN2020)," Recurrent Neural Network" [Online]. Available:
89. https://www.analyticsvidhya.com/blog/2020/02/cnn-vs-rnn-vs-mlp-analyzing-3-typesof-neural-networks-in-deep-learning/
90. "Simple recurrent neural networks" Wikipedia, 08-July-2019. [Online]. Available: https://keras.io/guides/working_with_rnns/
91. "Long Short-Term Memory" Wikipedia, 07-July-2021 [Online].
92. Available: https://machinelearningmastery.com/gentle-introduction-long-short-termmemory-networks-experts/
93. "Bidirectional recurrent neural networks" Wikipedia, 01-Dec-2021 [Online].
94. Available: https://en.wikipedia.org/wiki/Bidirectional_recurrent_neural_networks
95. "Gated recurrent unit" Wikipedia, 24-Nov-2021 [Online]. Available: https://en.wikipedia.org/wiki/Gated_recurrent_unit
96. M. Mohsin, 10 Social Media Statistics You Need to Know in 2021, 2020, [online] Available: https://www.oberlo.com/blog/social-media-marketing-
97. D. Niranjan Koggalahewa, Y. Xu, E. Foo, Spam detection in social networks based on peer acceptance, in Proceedings of the Australasian Computer Science Week Multiconference, 2020, pp. 1–7.
98. J. Clement. (Aug. 2019). Twitter: Number of Monthly Active Users 2010–2019. [Online]. Available: https://www.statista.com/statistics/ 282087/number-of-monthly-active-twitter-users/
99. Y. Zhang, Q. Liu, L. Song, Sentence-state lstm for text representation, 2020, arXiv preprint arXiv: 1805.02474.
100. P. Andriotis, A. Takasu, Emotional bots: Content-based spammer detection on social media, in 2018 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2018, pp. 1–8.
101. Ferrara E. Bots, elections, and social media: a brief overview. In: Disinformation, Misinformation, and Fake News in Social Media. (2020).
102. F. Pierri, A. Artoni, and S. Ceri, "Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections," PLoS One, vol. 15, no. 1, 2020, doi: 10.1371/journal.pone.0227821.
103. M. Kolomeets, D. Levshun, S. Soloviev, A. Chechulin, and I. Kotenko, "Social networks bot detection using Benford's law," in Proc. 13th International Conference on Security of Information and Networks SIN 2020, November 4-7, 2020, Merkez, Turkey
104. Albadi, N., Kurdi, M., Mishra, S.: Hateful people or hateful bots? detection and characterization of bots spreading religious hatred in Arabic social media. CSCW (2019)
105. Ortiz-Ospina, E. The Rise of Social Media. Our World in Data, 18 September 2019. Available online: https://ourworldindata.org/ rise-of-social-media (accessed on 6 October 2020).
106. Orabi, M.; Mouheb, D.; Al Aghbari, Z.; Kamel, I. Detection of Bots in Social Media: A Systematic Review. Inf. Process. Manag. 2020, 57, 102250.
107. Rovetta, S.; Suchacka, G.; Masulli, F. Bot recognition in a Web store: An approach based on unsupervised learning. J. Netw. Comput. Appl. 2020, 157, 102577.
108. Asadi, M.; Jabraeil Jamali, M.A.; Parsa, S.; Majidnezhad, V. Detecting botnet by using particle swarm optimization algorithm based on a voting system. Future Gener. Comput. Syst. 2020, 107, 95–111.