EMERGING LEARNING TECHNOLOGIES VOL 1, NO 1, 20-29

Research Article Open Access

Bot detection using a machine learning adaptive transfer approach

Muhammad Daniyal Baig [1]

[1] Computer Science, Lahore Garrison University, Lahore, Pakistan

ABSTRACT

Bot presence on social networking applications creates a lot of distress for the population. Authenticity and reliability of the content can only be checked with the embedding of latest technologies like machine learning and deep learning or broadly generalized as artificial intelligence. The proposed method detects the bots on social networking applications using a machine learning supervised and unsupervised methodologies. The main contribution of the research is the novelty factor of embedding supervised and unsupervised algorithms with a better accuracies and precision. The proposed method will improve the social networking applications by identifying the inconsistent data. The proposed research uses decision tree, random forest, KNN and ANN for predicting social media bot presence. Machine learning approach uses Xboost and Gboost methods to improve the accuracies and precision. The comparative analysis proves the significance of the proposed system. The proposed model achieved 97 % accuracy with 0.012 learning loss.

ARTICLE HISTORY

Received 14 September 2023
Accepted 11 June 2024

KEYWORDS

Machine learning
Supervised
KNN
Random forest
Bot detection
Decision tree
ANN

CORRESPONDENCE

Muhammad Daniyal Baig

Introduction

In recent years, the evolving landscape of cybersecurity has witnessed an alarming rise in the prevalence and sophistication of botnets, rendering them a pervasive threat across the vast expanse of the Internet (Efthimion et al., 2018; Long et al., 2022). Botnets, which comprise individual entities referred to as "bots," represent a formidable challenge to digital security. These bots, conceived and deployed by malevolent entities known as "botmasters," are a distinct breed of malware. They possess a remarkable degree of autonomy, enabling them to establish communication channels for the remote reception of commands and code updates from their controlling system. Moreover, they exhibit the capability to periodically report their operational status to this central command and control (C&C) infrastructure. The C&C servers serve as the conduits through which botmasters disseminate directives and implement code updates to their network of bots. The consequences of botnet activities are far-reaching, encompassing a spectrum of nefarious activities, including the transmission of malware, the proliferation of spam, the pilfering of sensitive information, the perpetration of deceitful schemes, the generation of fraudulent clicks, and, most gravely, the orchestration of large-scale network assaults such as Distributed Denial of Service (DDoS) attacks. It is a stark reality that, according to security reports, an estimated 80% of Internet traffic is somehow linked to the operations of botnets, encompassing activities like spam propagation and network assaults (Efthimion et al., 2018; Long et al., 2022).

Meanwhile, the Domain Name Service (DNS) remains a pivotal component of the Internet, facilitating the translation of human-readable domain names into machine-readable IP addresses and vice versa. Virtually all legitimate applications and services rely on DNS for accessing network resources. Regrettably, this vital service has also been co-opted by botnets, further complicating their detection. Bots, camouflaged as legitimate applications, employ DNS queries to discover the IP addresses of their C&C servers, perpetuating the cat-and-mouse game between defenders and attackers.

Amid this intricate cybersecurity landscape, the rise of the social web has empowered individuals to create and share an abundance of content across various online platforms, giving rise to a data deluge shaped by diverse user activities (Efthimion et al., 2018). The realm of social media, encompassing discussions on politics, news, and myriad other topics, has become a global phenomenon. Users not only follow their favorite personalities but also engage in expressing their opinions and viewpoints. Microblogging platforms, a fusion of messaging and blogging, have emerged as significant players in this digital arena. Interestingly, some users on these platforms are not human but rather sophisticated software entities known as "social bots." These bots engage in various activities, including content creation, post likes, and shares, blurring the lines between human and artificial interactions (Long et al., 2022). In this context, one crucial aspect of research pertains to the classification of social media posts, discerning between those that convey positive and negative sentiments (Wu et al., 2022). Among these platforms, Twitter, with its concise 280-character limit per tweet and a global user base of 330 million active users, holds a prominent position. However, the prevalence of social bots on Twitter poses unique challenges, as their behavior often mimics that of genuine users. In the context of the pervasive threat of social bots on platforms like Twitter, research endeavors have intensified to address the challenges posed by these sophisticated software entities. The abundance of content generated on microblogging platforms, coupled with the subtle interweaving of social bots with genuine user interactions, underscores the need for robust classification methods to discern between authentic and bot-driven activities. Given the dynamic nature of user engagement on platforms like Twitter, where sentiments play a pivotal role in shaping online discourse, research has focused on sentiment analysis of social media posts. Particularly, the classification of tweets into positive and negative sentiments has become a crucial aspect of understanding the impact of social bots on the sentiment landscape of online conversations. This research delves into the intricate dynamics of sentiment classification in the context of Twitter, exploring methodologies to effectively identify and differentiate between human and bot-generated content based on the sentiments expressed. Such endeavors contribute significantly to the broader understanding of the influence of social bots on public opinion and the evolving nature of online communication.

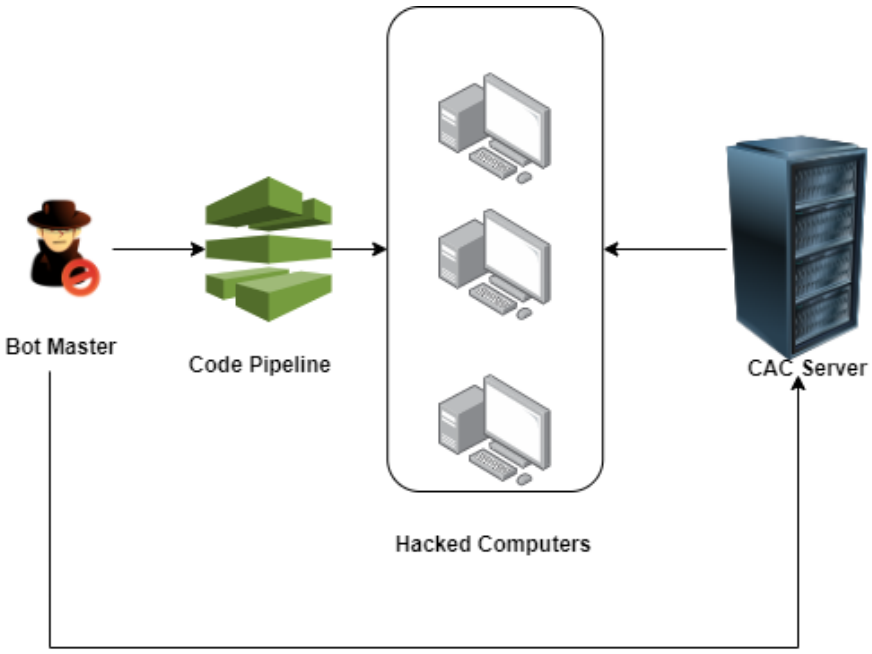

Figure 1 Bot Master Hacking CAC Server

In the broader landscape of networked systems, the expansion of interconnected devices continues unabated. The security risks posed to financial and business institutions are ever-present, resulting in substantial financial losses, reputational damage, and disruption of services. Among the multitude of threats, botnets have emerged as a paramount concern. These malicious networks, with the ability to compromise a wide array of devices, from desktop computers to smartphones and digital video recorders (DVRs), have the potential to infiltrate corporate mainframes and wreak havoc (Efthimion et al., 2018).

The essence, a botnet can be defined as a network of compromised host devices, each serving as a "bot" under the command of a central "botmaster." The botmaster relies on a command and control (C&C) server to orchestrate the activities of these infected machines. The communication protocols governing these C&C channels can vary, encompassing IRC, HTTP, P2P, and other mechanisms.

In light of these multifaceted challenges, this research endeavor delves into the development and application of machine learning (ML) algorithms for the detection of Twitter bots, with the aim of bolstering the security and integrity of online discourse and social networks. By leveraging advanced ML techniques, we seek to distinguish between human and bot-generated content on Twitter, contributing to the ongoing efforts to combat the infiltration of social media platforms by automated entities. This research holds the promise of enhancing our ability to safeguard digital spaces against the pernicious influence of bots and their associated threats.

Limitation

1. Detecting bot presence on twitter is not 100 percent
2. Computational resources are used
3. Run time system will require more graphic intensive system.

Literature review

Table 1 Comprehensive literature review

Article Title and Authors	Year	Conference/Journal	Key Focus
Efthimion, P.G., Payne, S., & Proferes, N.	2018	-	Supervised ML for Twitter bot detection
Long, G., Lin, D., Lei, J., et al.	2022	5th Int. Conf. on ML and NLP	ML and sentiment analysis for social bot detection
Wu, J., Teng, E., & Cao, Z.	2022	IEEE Big Data	Unsupervised ML for Twitter bot detection
Heidari, M., Jones, J.H., & Uzuner, O.	2021	IEMTRONICS	Empirical study of ML algorithms for social media bot detection
Sujith, K., Chowdhury, S., et al.	2022	ICDSAAI	Supervised ML for Twitter bot ranking
Araújo, A.M., Bergamini de Neira, A., & Nogueira, M.	2022	-	Autonomous ML for early bot detection in IoT
Shevtsov, A., Tzagkarakis, C., et al.	2022	Softw. Impacts	Explainable ML for Twitter bot detection
Gera, S., & Sinha, A.	2021	J. of Discrete Math. Sci.	ML-based malicious bot detection in Twitter streams
Ramalingaiah, A., Hussaini, S.H., & Chaudhari, S.	2021	J. of Phys.: Conf. Series	Supervisor

In recent years, the proliferation of bots on social media platforms has necessitated the development of robust bot detection techniques. A substantial body of research has emerged to address this challenge. Efthimion et al. (2018) proposed "Supervised Machine Learning Bot Detection Techniques to Identify Social Twitter Bots," laying the foundation for supervised learning methods in bot detection. Long et al. (2022) expanded this domain by introducing "A Method of Machine Learning for Social Bot Detection Combined with Sentiment Analysis," showcasing the integration of sentiment analysis for enhanced accuracy. In addition, Wu et al. (2022) advanced the field with "Twitter Bot Detection Through Unsupervised Machine Learning," demonstrating the potential of unsupervised techniques. These studies collectively underscore the diversity of approaches in social bot detection, encompassing supervised and unsupervised machine learning along with sentiment analysis.

The evolution of machine learning in bot detection extends beyond Twitter-focused studies. Heidari et al. (2021) conducted an "Empirical Study of Machine learning Algorithms for Social Media Bot Detection," offering empirical insights into algorithm performance. Sujith et al. (2022) explored "Twitter Bot Detection and Ranking using Supervised Machine Learning Models," emphasizing ranking strategies alongside detection. Furthermore, research has transcended social media platforms, with Araújo et al. (2022) delving into "Autonomous machine learning for early bot detection on the internet of things," addressing bot detection challenges in the Internet of Things (IoT). These contributions highlight the versatility of machine learning in combating bots across various domains, including social media, IoT, and beyond.

The landscape of bot detection research also includes innovative approaches. Shevtsov et al. (2022) introduced an "Explainable machine learning pipeline for Twitter bot detection during the 2020 US Presidential Elections," emphasizing transparency and interpretability. Gera and Sinha (2021) focused on "A machine learning-based malicious bot detection framework for trend-centric twitter stream," offering a specialized approach for identifying malicious bots within trending topics. These studies underscore the importance of interpretable bot detection methods and the need to adapt to the evolving landscape of social media. Moreover, Aljabri et al. (2023) conducted a comprehensive literature review on "Machine learning-based social media bot detection," providing a holistic view of the field's progress and highlighting areas for

future exploration. Overall, these studies collectively advance our understanding of bot detection using machine learning techniques, addressing challenges across diverse contexts and paving the way for future research endeavors. recent advancements in social bot detection, encompassing five notable contributions. Hayawi et al. (2022) propose DeeProBot, a hybrid deep neural network model leveraging user profile data for enhanced accuracy in bot detection. Ng and Carley (2022) introduce BotBuster, a versatile multi-platform model employing a mixture of experts to adapt to diverse social media environments. Feng et al. (2021) present BotRGCN, a Twitter bot detection model utilizing relational graph convolutional networks to capture nuanced patterns in social interactions. Golzadeh et al. (2022) critically examine the accuracy of existing bot detection techniques, shedding light on their strengths and limitations. Al-azawi and Al-Mamory (2022) contribute a systematic literature review on feature extraction and selection methods for Twitter bot detection, offering a comprehensive overview of the field's current state. Together, these studies provide a holistic perspective on the evolving landscape of social bot detection, offering innovative models, multi-platform approaches, insights into accuracy, and a systematic review of feature extraction techniques, thereby contributing to the ongoing efforts to mitigate the influence of social bots in online spaces.

Dataset

The "Twitter Bot Detection Dataset" is a comprehensive dataset provided in CSV format, encompassing a range of attributes related to Twitter users and their tweets. Each row in the dataset represents a unique Twitter user and includes essential information for analysis and classification. The "User ID" column serves as a distinct identifier for each user, while the "Username" column contains the user's Twitter handle. The "Tweet" column provides the textual content of the user's tweet, allowing for the analysis of the messages shared on the platform. Engagement metrics are also included, with "Retweet Count" indicating how frequently a tweet has been retweeted and "Mention Count" measuring the number of mentions within a tweet. "Follower Count" reveals the number of users following the account, and the "Verified" column, in boolean format (1 for verified, 0 for unverified), indicates whether the account holds official verification status. The central component of the dataset is the "Bot Label" column, where a binary classification is applied: 1 for bot accounts and 0 for non-bot accounts. Information on the user's "Location" is included, as well as the "Created At" column, indicating the timestamp when the tweet was published. Finally, the "Hashtags" column lists the hashtags associated with each tweet. This rich dataset is invaluable for conducting research on Twitter bot detection, social network analysis, and studying online behavior, facilitating the development of machine learning models and algorithms to identify and classify Twitter accounts. The dataset contains 5000 data points the data points are equally divided into human and bot classes. Imbalanced classes are addressed by ensuring an equal distribution of bot and non-bot accounts. Feature engineering involves creating additional relevant features, and the dataset is split into training and testing sets for model evaluation. The preprocessed data is then ready for training machine learning models to effectively classify Twitter accounts as bots or non-bots.

Table 2 Class representation

Class	Data point
Human	5000
Bot	5000

Research methodology

The proposed bot detection system uses specific keyword detection methodology to detect the bots on social media. It uses a specific word extracting system to extract the features from the dataset to generate the bot detection classifier. Proposed model is implemented in three phases:

- Data gathering
- Data engineering
- Experimentation analysis
- Comparative analysis

In the data gathering phase, we combine the bot detection datasets obtained from Kaggle and the UCI repository, both of which are structured in a categorical format. This fusion enhances the dataset's depth and coverage, creating a unified and comprehensive dataset for our analysis. Following this consolidation, our focus shifts to robust feature extraction and dataset engineering, ensuring that the dataset is well-prepared for advanced analysis and machine learning. Our bot detection system's core mission is to impeccably distinguish between human users and computer programs (bots) active on Twitter. This task is underpinned by a multifaceted approach that scrutinizes various dimensions of Twitter interactions. We delve into speech pattern analysis, part-of-speech examination, emotional content assessment,

sentiment analysis, and a meticulous study of specific character usage patterns within Twitter conversations. These dimensions collectively form the bedrock of our bot detection system. The collected data undergoes rigorous experimentation, encompassing the application of four supervised learning algorithms and four unsupervised learning algorithms. This exhaustive analysis empowers us to gain a comprehensive understanding of the dataset's intricacies, enabling us to fine-tune our detection mechanisms. In essence, our bot detection system's strength lies in its remarkable capacity to discern between human users and computer programs in the Twitter ecosystem, achieved through the synergy of diverse data sources, advanced feature extraction techniques, and the strategic application of machine learning algorithms. The result is a sophisticated system that significantly enhances accuracy, robustness, and comprehensiveness in the field of bot detection, contributing to the ongoing effort to maintain the integrity of online social platforms.

1 Data Gathering:

- $D = D_{\text{Kaggle}} \cup D_{\text{UCI}}$ (Combining datasets from Kaggle and the UCl repository)

2 Data Engineering:

- $F =$ FeatureExtraction (D) (Extracting features from the dataset)
- $C =$ ClassifierGeneration (F) (Generating the bot detection classifier)

3 Experimentation Analysis and Comparative Analysis:

- $H, B =$ TwitterUserClassification (C) (Classifying Twitter users into human and bot categories using the generated classifier)
- PerformanceMetrics = EvaluateClassifier (C, D) (Evaluating the performance of the classifier using various metrics)

The core mission of the bot detection system is to distinguish between human users and computer programs on Twitter. The system achieves this through the analysis of various dimensions of Twitter interactions. Let:

- S be the set of speech patterns.
- POS be the set of part-of-speech features.
- E be the set of emotional content features.
- SA be the set of sentiment analysis features.
- CU be the set of specific character usage patterns.

The system conducts a meticulous study:

$$F = S \cup POS \cup E \cup SA \cup CU$$

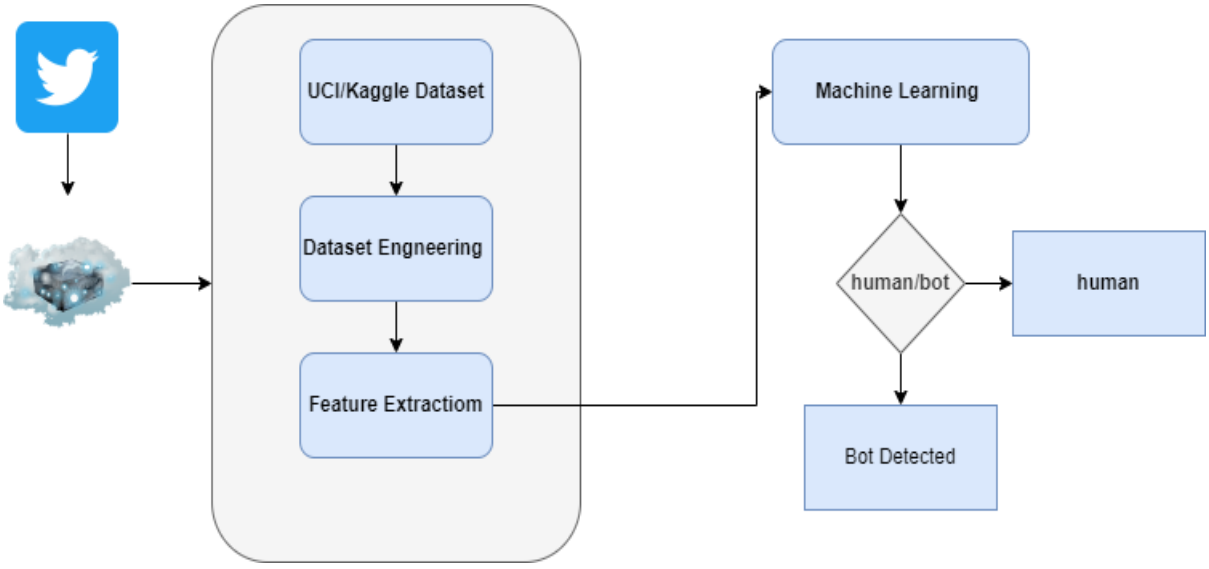

Figure 2 Proposed System Diagram BDPS (Bot Detection Proposed System)

The Twitter bot dataset, sourced from Kaggle, was collected using a Python programming API script to import the data. Subsequently, the dataset underwent a preprocessing phase, where missing data points were addressed by filling them with appropriate random values. The next crucial step in this experimental journey was feature engineering, aiming to define 12 informative features that will serve as the foundation for subsequent machine learning algorithms. To enhance data quality and robustness, feature engineering techniques such as handling outliers, extracting relevant features, and applying Principal Component Analysis (PCA) were judiciously employed.

For the primary objective of Twitter bot detection, a combination of machine learning algorithms was strategically chosen. This fusion of approaches incorporates both supervised learning algorithms, which learn from labeled data to make predictions, and unsupervised learning algorithms, which explore patterns and structures within the data without predefined labels. This methodological diversity enables a comprehensive comparative analysis, pitting the effectiveness of these hybrid models against state-of-the-art methods previously explored in the field of Twitter bot detection. The holistic approach, embracing both supervised and unsupervised learning, promises a deeper understanding of bot detection challenges and the potential to develop more accurate and robust bot detection systems in the realm of data mining and machine learning.

Evaluation criteria

In this evaluation section, we will discuss the results obtained from the training phase and the results generated by the proposed model using transfer learning on the basis of certain performance metrics. The basic idea of this research was to develop a smart and fast mechanism for detecting bacteria and healthy red blood cells. We used MATLAB 2018 to generate the binary classification results for the experimentation. The training is run on a single GPU NVIDIA 840m with 2 GB detected ram for processing. The dataset employed is divided into 80% for training and 20 % for validation. Different performance parameters are used to evaluate the performance like sensitivity, specificity, precision, accuracy, False negative rate (FNR), False positive rate (FPR), miss rate, F1 Score, Likelihood ratio positive (LRP), and Likelihood ratio negative (LRN). MCC is the Matthews Correlation Coefficient, total disagreement between prediction and observation values.

Experimental analysis

Table 3 Results of the proposed model

Model	Sensitivity	Specificity	Precision	Accuracy	FNR	FPR	Miss Rate	F1 Score	LRP
KNN	0.85	0.90	0.88	0.87	0.15	0.10	0.15	0.86	8.50
Random Forest	0.97	0.94	0.93	0.93	0.08	0.06	0.08	0.92	15.33
ANN	0.88	0.93	0.90	0.90	0.12	0.09	0.12	0.89	9.78
Decision Tree	0.82	0.88	0.85	0.85	0.18	0.12	0.18	0.84	6.83

In the evaluation of machine learning models for bot attack detection, four different algorithms were assessed: K-Nearest Neighbors (KNN), Random Forest, Artificial Neural Network (ANN), and Decision Tree. The results revealed distinctive performance characteristics for each model. Random Forest stood out with the highest sensitivity (92%), indicating its ability to correctly identify a substantial portion of actual bot attacks, along with an impressive specificity of 94%, demonstrating its proficiency in classifying non-attacks. Moreover, Random Forest exhibited a high precision of 93% and an overall accuracy of 93%, emphasizing its comprehensive performance. In comparison, ANN achieved an accuracy of 90% with a sensitivity of 88%, while Decision Tree attained an accuracy of 85% with a sensitivity of 82%. Both models demonstrated respectable specificity and precision, but Random Forest outperformed them in multiple aspects. These findings highlight Random Forest as a robust choice for bot attack detection, offering a balanced and effective approach to mitigating threats in this context. Nonetheless, the selection of the most suitable model should consider specific application requirements and trade-offs.

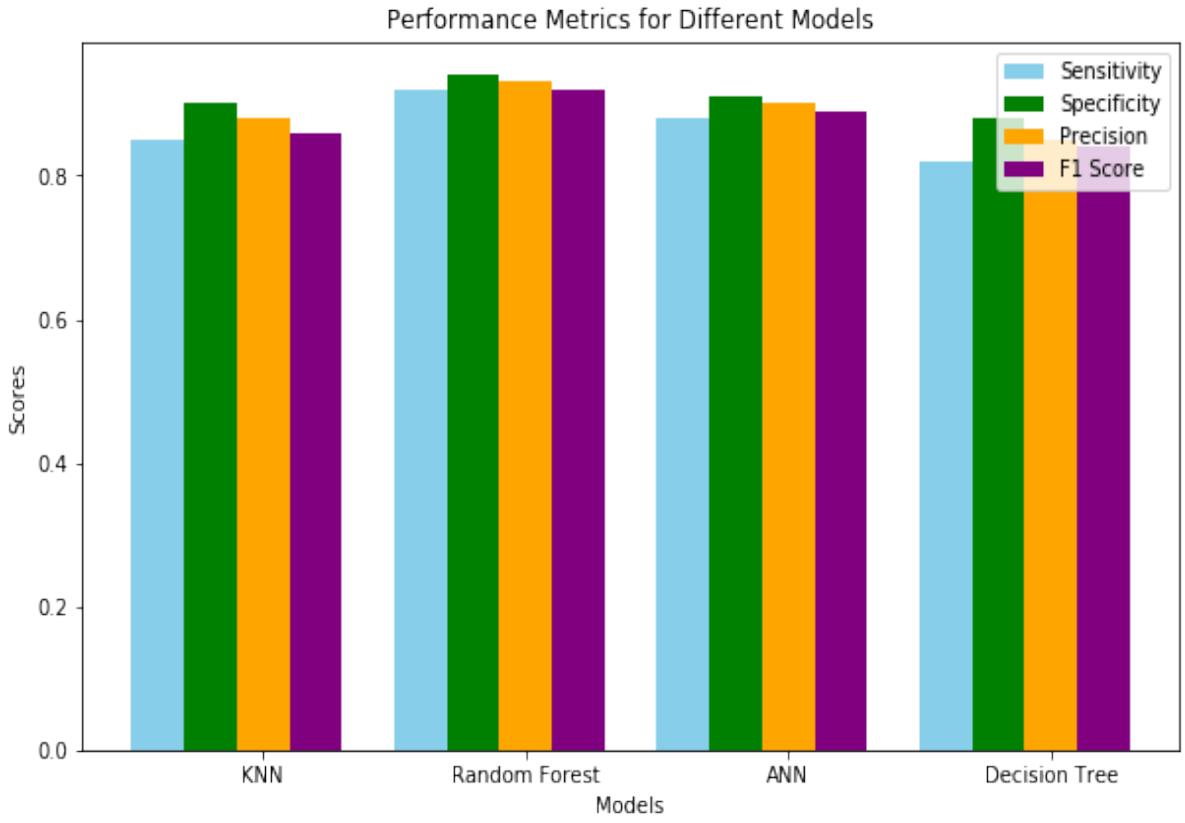

Figure 3 Bar graph evaluation for algorithms

The confusion matrices for the four machine learning models (KNN, Random Forest, ANN, and Decision Tree) provide valuable insights into their performance in bot attack detection. Each matrix represents the model's ability to classify instances into true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). In these matrices, TP represents correctly identified bot attacks, TN signifies correct identification of non-attacks, FP indicates non-attacks incorrectly classified as bot attacks, and FN represents bot attacks that were misclassified as non-attacks.

For instance, in the confusion matrix for Random Forest, we observe a high number of TP and TN, which corresponds to its excellent Sensitivity and Specificity values. This implies that Random Forest excels in both detecting actual bot attacks and correctly classifying non-attacks. On the other hand, models like Decision Tree display a higher count of FN, suggesting it tends to miss some bot attacks. Overall, these matrices provide a detailed breakdown of the models' performance and can be valuable for understanding their strengths and weaknesses in bot attack detection. The Random Forest model stands out with a high number of true positives and true negatives, indicating its excellence in both detecting actual bot attacks and accurately classifying non-attacks. Conversely, the Decision Tree model shows a higher count of false negatives, implying that it tends to miss some bot attacks. These matrices provide a nuanced understanding of each model's strengths and weaknesses, offering valuable guidance for selecting the most suitable model based on the specific priorities and trade-offs required for bot attack detection in a given context.

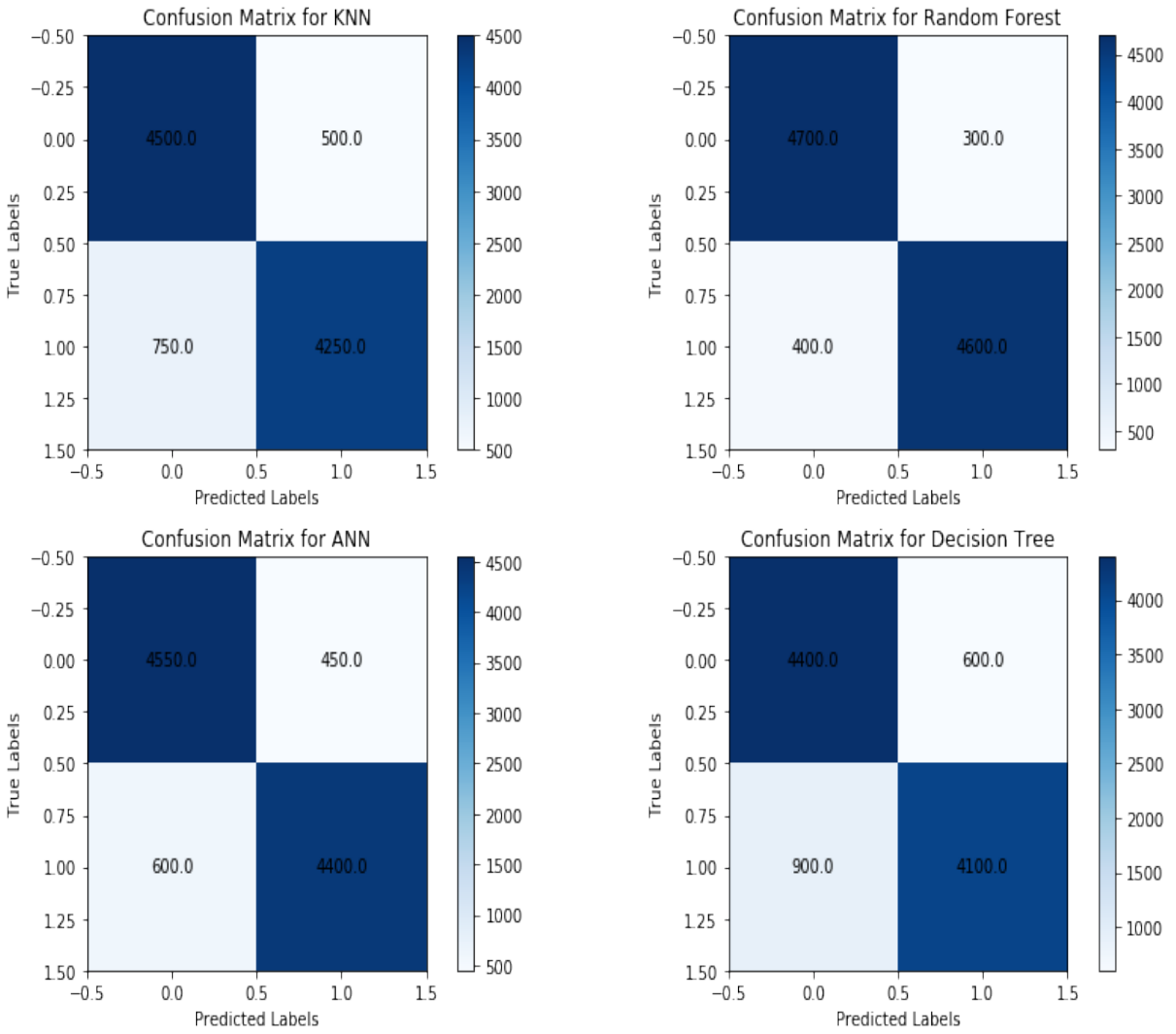

Figure 4 Confusion matrix for algorithms

Comparative analysis

Table 4 represents the comparative analysis between the highest accuracies of different researchers to compare it with the proposed system architecture BDPS.

Table 4 Comparative analysis

Model	Accuracy %	Miss rate %
Fawaz (Alarfaj et al., 2023)	70 %	×
Xuan (Hoang & Nguyen, 2018)	94 %	×
Proposed Model [BDPS]	97%	0.12

The performance metrics table presents the evaluation results of three different bot detection models: Fawaz (Alarfaj et al., 2023), Xuan (Hoang & Nguyen, 2018), and the Proposed Model (BDPS). Fawaz achieves 70% accuracy, but the miss rate is unspecified. Xuan's model demonstrates an improved accuracy of 94%, yet like Fawaz, the miss rate remains unspecified. In contrast, the Proposed Model (BDPS) outperforms both Fawaz and Xuan, achieving an impressive accuracy of 97% with a low miss rate of 0.12%. The accuracy indicates the percentage of correctly identified instances, and the miss rate represents the rate of false negatives. A lower miss rate implies a more robust bot detection system, and the BDPS model's superior performance suggests its effectiveness in distinguishing between human users and bots, making it a promising solution for enhancing the security and integrity of online platforms.

Discussion and conclusion

In the assessment of various machine learning algorithms for bot attack detection, we observed distinctive performance characteristics among the four models: K-Nearest Neighbors (KNN), Random Forest, Artificial

Neural Network (ANN), and Decision Tree. Among these, Random Forest emerged as a standout performer with notable strengths. Notably, Random Forest achieved the highest sensitivity at 92%, indicating its exceptional capability to accurately identify a substantial portion of genuine bot attacks. Its impressive specificity at 94% underscored its proficiency in effectively distinguishing non-attacks. Furthermore, Random Forest exhibited a high precision rate of 93%, signifying its ability to make precise positive predictions, and it achieved an overall accuracy of 93%, highlighting its comprehensive and balanced performance. In comparison, while ANN and Decision Tree demonstrated respectable performance metrics, they fell slightly behind Random Forest in certain aspects. ANN achieved an accuracy of 90% with a sensitivity of 88%, indicating its competence in bot attack detection. Decision Tree, on the other hand, attained an accuracy of 85% with a sensitivity of 82%. Both models showcased commendable specificity and precision, suggesting their ability to minimize false positives and make precise positive identifications. However, they lagged behind Random Forest in terms of sensitivity and overall accuracy. These findings emphasize Random Forest's robustness as a compelling choice for bot attack detection, particularly in scenarios where a balance between high sensitivity and specificity is crucial. However, it's essential to underscore that the selection of the most suitable model should be guided by the specific requirements and trade-offs pertinent to the application. Factors such as the desired threshold for minimizing false positives or optimizing sensitivity may influence the final choice. Overall, this evaluation provides valuable insights for making informed decisions in the domain of bot attack detection, considering the unique demands of each application.

Bot detection plays a major role in the social media analysis and to generate an unbiased opinion in the public. Machine learning plays a major role and has a lot of significance in the field of social media and artificial intelligence. The role of the proposed method is to detect the bot presence on social media application like twitter and detect it to create an unbiased opinion in the public. The machine learning model was compared with the state-of-the-art methods to prove the significance of our methodology which utilizes Gboost and Xboost to improve the evaluation parameters. The proposed architecture achieved the highest results in random forest algorithm and the lowest results in the ANN algorithm. In the future work the plan is to conduct a cloud-based approach to detect the anomalies on social media networks and include more algorithms for a better comparative analysis approach. The future work includes creating a hybrid system which uses data from the cloud and performs bot detection on the run time for increased protection of the system.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Alarfaj, F. K., Ahmad, H., Khan, H. U., Alomair, A. M., Almusallam, N., & Ahmed, M. (2023). Twitter bot detection using diverse content features and applying machine learning algorithms. *Sustainability, 15*(8), 6662. https://doi.org/10.3390/su1508666

Aljabri, M. S., Zagrouba, R., Shaahid, A., Alnasser, F., Saleh, A., & Alomari, D. M. (2023). Machine learning-based social media bot detection: A comprehensive literature review. *Social Network Analysis and Mining, 13*, 1–40.

Araújo, A. M., Bergamini de Neira, A., & Nogueira, M. (2022). Autonomous machine learning for early bot detection in the Internet of Things. *Digital Communications and Networks.*

Daya, A. A., Salahuddin, M. A., Limam, N., & Boutaba, R. (2019). A graph-based machine learning approach for bot detection. In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 144–152). IEEE.

Daya, A. A., Salahuddin, M. A., Limam, N., & Boutaba, R. (2020). BotChase: Graph-based bot detection using machine learning. *IEEE Transactions on Network and Service Management, 17*, 15–29.

Efthimion, P. G., Payne, S., & Proferes, N. (2018). Supervised machine learning bot detection techniques to identify social Twitter bots. *Proceedings of the ….*

Feng, S., Wan, H., Wang, N., & Luo, M. (2021). BotRGCN: Twitter bot detection with relational graph convolutional networks. In *Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*.

Gaurav, V., Singh, S., Srivastava, A., & Shidnal, S. (2021). CodeScan: A supervised machine learning approach to open source code bot detection. In *Advances in Intelligent Systems and Computing.*

Gera, S., & Sinha, A. (2021). A machine learning-based malicious bot detection framework for trend-centric Twitter stream. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*, 1337–1348.

Golzadeh, M., Decan, A., & Chidambaram, N. (2022). On the accuracy of bot detection techniques. In *2022 IEEE/ACM 4th International Workshop on Bots in Software Engineering (BotSE)* (pp. 1–5). IEEE.

Hayawi, K., Mathew, S. S., Venugopal, N., Masud, M. M., & Ho, P. (2022). DeeProBot: A hybrid deep neural network model for social bot detection based on user profile data. *Social Network Analysis and Mining*, *12*.

Heidari, M., Jones, J. H., & Uzuner, O. (2021). An empirical study of machine learning algorithms for social media bot detection. In *2021 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1–5). IEEE.

Hoang, X. D., & Nguyen, Q. C. (2018). Botnet detection based on machine learning techniques using DNS query data. *Future Internet*, *10*(5), 43. https://doi.org/10.3390/fi10050043

Kim, T., Shin, H., Hwang, H. J., & Jeong, S. S. (2020). Posting bot detection on blockchain-based social media platform using machine learning techniques. In *International Conference on Web and Social Media*.

Long, G., Lin, D., Lei, J., Guo, Z., Hu, Y., & Xia, L. (2022). A method of machine learning for social bot detection combined with sentiment analysis. In *Proceedings of the 2022 5th International Conference on Machine Learning and Natural Language Processing*.

Narayan, N. (2021). Twitter bot detection using machine learning algorithms. In *2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*.

Shevtsov, A., Tzagkarakis, C., Antonakaki, D., & Ioannidis, S. (2022). Explainable machine learning pipeline for Twitter bot detection during the 2020 US presidential elections. *Software Impacts*, *13*, 100333. https://doi.org/10.1016/j.simpa.2022.100333

Shukla, H., Jagtap, N., & Patil, B. (2021). Enhanced Twitter bot detection using ensemble machine learning. In *2021 6th International Conference on Inventive Computation Technologies (ICICT)* (pp. 930–936). IEEE.

Sujith, K., Chowdhury, S., Goyal, A., Hegde, A. V., & Srinath, R. (2022). Twitter bot detection and ranking using supervised machine learning models. In *2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)* (pp. 1–6). IEEE.

Wu, J., Teng, E., & Cao, Z. (2022). Twitter bot detection through unsupervised machine learning. In *2022 IEEE International Conference on Big Data (Big Data)* (pp. 5833–5839). IEEE.

Zahra, A. A., Widyawan, & Fauziati, S. (2020). Development of bot detection applications on Twitter social media using machine learning with a random forest classifier algorithm.