**Frontiers in Computer Science and Artificial Intelligence**
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

**| RESEARCH ARTICLE**

# Parallel Deep Learning for Cybersecurity-Oriented Multi-Platform Social Media Bot Detection

**Md Shakhawat Hossen[1]✉, Md Reduanur Rahman[2], Md Abdul Alim[3], Nasrin Akter Tohfa[4], Mamunur Rahman[5], Iftekhar Rasul[6]**

[1] *Master's in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA*
[2] *Master's in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA*
[3] *Master's in Information Technology Management, St. Francis College, Brooklyn, New York, USA*
[4] *Master's in Information Systems Security, University of the Cumberlands, Williamsburg, Kentucky, USA*
[5] *Master of Science in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA*
[6] *Master's in Information Technology Management, St. Francis College, Brooklyn, New York, USA*

**Corresponding Author**: Md Shakhawat Hossen, **E-mail**: mhossen.student@wust.ed

**| ABSTRACT**

Social media is a key unit of today's cyber communication society; however, being widely available, social media networks also contribute to the diffusion of social bots, which are then abused for forging global digital weapons, such as spreading fake news, organized manipulation and infiltration, or malicious propaganda actions. However, identifying these bots in a multi-platform setting is difficult due to the heterogeneity of data structures and behaviours, as well as platform-specific issues.

In this paper, we have presented a parallel DNN-based social media bot detection model for various platforms. The proposed architecture has a multi-head parallel structure sharing the latent representations and simultaneously learning the shared latent features and platform-specific independent detections. What it allows, however, is for the framework to handle both generic bot prototype behaviours and platform-specific functionalities in a single solution that scales well.

The proposed approach is evaluated on two real-world datasets taken from Twitter and TikTok, including behavioural, engagement, and account-level features. Experiments show strong and consistent detection performance across the tested platforms. The detection heads on Twitter reach 94.47% accuracy, 94.42% F1-score, and a ROC-AUC of 94.77%, while those on TikTok obtain an accuracy of 91.29%, an F1-score of 92.92% and a ROC-AUC score of 96.30%. High precision–recall performance also confirms the effectiveness of the proposed system in detecting automated harmful accounts with low false positive rates.

**| KEYWORDS**

Cyber Security, Bot Detection, Artificial Intelligence, Social Media.

**| ARTICLE INFORMATION**

**ACCEPTED:** 01 January 2026 **PUBLISHED:** 05 January 2026 **DOI:** 10.32996/jcsts.2026.5.2.3

## 1. Introduction

The emergence of social networks has ushered in the new era of information production, dissemination and consumption globally. Article content It is no secret that Twitter and TikTok have taken become powerhouses when it comes to public communication, advertising in the push to build virtual communities. But this propagation of bots has also facilitated the rise of social bots who are now used for malicious activities such as: (a) blizzard spamming that floods a system with thousands or millions of posts in order to overwhelm service providers, (b) peddling porn materials and adult dating services, (c) spreading rumors to influence stock market effectively, and even backupugador monopoly (d) trying to rally political supporters. Therefore, social bots have become a major and growing concern in cyber security [1], [2].

Social media bots can help adversaries determine how to manipulate online conversation and maintain maximum influence without being detected. These traditional bot detection systems, either based on rule-based criteria or hand-crafted features along with classic machine learning methods, are likely to fail when faced with platforms discrepancies and dynamic behaviors that bots deploy [3]. In addition, service-specific detection models usually fail to analyze the common behaviors of bots that use more than one online social network (OSN) as their platforms due to bot diversity, and are thus not suitable to real cyber security applications [4].

Recent developments in deep learning have been shown to significantly improve automated threat detection by allowing models to learn intricate non-linear representations of vast data [5]. In social media studies, deep learning has demonstrated effective detection of bots based on content-based bots, behavioral bots and network-based bots using low-level features [6], [7]. However, the majority of current deep learning models are proposed for single-platform scenario that severely limits their application in multiplatform cyber security environment where coordinated malicious behaviors across multiple social networks start at the same time.

To alleviate these shortcomings, parallel and multi-task learning frameworks can be potential solutions. Through simultaneously learning several related tasks with shared internal representations, the parallel deep learning model can enhance generalization ability and avert overfitting by making effective use of crossdomain knowledge [8]. In cyber-security scenarios, such architectures allow for the joint detection of threats in different data sources, while retaining platform-specific deselection capabilities [9].

Inspired by these issues, this paper introduces a parallel deep learning cyber security framework for bot detections in social media across different platforms. The proposed model is designed using a multi-head neural network structure that simultaneously learns common latent representations and separate output heads for the platform-specific classification. Such an architecture enables the framework to model not just general bot tendencies as well as diagram-specific idiosyncrasies in an integrated and scalable fashion.

Our proposed approach is assessed on datasets from Twitter and TikTok, where Twitter is chosen as complete social network since interaction dynamics can be observed during recent events there, while presence of ground truth of positive engagements at TikTok runs contrary. Extensive experiments show that the proposed model achieves high accuracy, F1-score and AUC on two different platforms, demonstrating the capability and stability of our model for multi-platform bot detection. The findings indicate that parallel deep learning is a cyber security-oriented and commercially viable solution to automatically neutralize social media threats in today's world.

## 2. Literature Review

Detecting social media bots has garnered much attention in the academia as it helps to keep online platforms secure, intact and trustworthy. Beginning with the first studies, work concentrated on rule-based and heuristically-derived machine learning methods that used user metadata, posting rate and network properties in order to classify automated postings across users. Chu et al. [10] presented one of the earliest technical architectures for bot detection based on themes, proving early detection system infeasibility while pointing out that the proposed solutions were not scalable and adaptive.

Then, they also proposed more sophisticated behavioral and graph-based methods when bot behavior became more human-like. Varol et al. [11] collected multiple human–bot interaction datasets and found that for there to be a robust detection, simple heuristics do not work. Cresci et al. [12] elaborated on this matter by presenting the notion of “social spambots” that can evade conventional social spam detection mechanisms by imitating natural social behavior. This discovery highlighted the necessity of adopting more flexible and intelligent detection schemes.

This emphasis on deep learning has drastically changed bot detection research. Deep learning algorithms have allowed for automated feature extraction from high-dimensional data and have greatly increased the accuracy of detection. [13] showed that deep neural nets outperform traditional classifiers by learning complex behavioral representations in raw features. Similarly, Yang et al. [14] considered neural models in the arms race against evolving spammers, specifically demonstrating benefit of deep architectures in adversary settings that evolve dynamically.

In spite of these progress, mot deep learning-based bot detection systems suffer from single-platform and do not work well in practice due to the fact that malicious bots across multiple platforms would be adopted at the same time. Ferrara et al. [15] observed that cross-platform coordination is a characteristic of contemporary bot campaigns, but has received comparably little attention in detection research. This gap has spurred the research towards cross-domain and transfer learning.

Cross-platform challenges have also been successfully addressed by multi-task and parallel learning frameworks. Ruder [16] gave an extensive survey of multi-task learning in deep neural networks and showed the advantage shared representation can bring for generalization on related tasks. In the area of cyber security, Buczak and Guven [17] have emphasized how machine learning systems that blend heterogeneous datasets are effective for threat detection, strengthening the applicability of parallel learning.

More recent research has started to focus on platform-aware deep learning models. Alhosseini et al. [18] leveraged a mouthful of mouth-based behavioral information in a deep learning design for bot detection, and showed promising results but targeted

at speci c platform. Similarly, Hayawi et al. [19] used deep learning methods for social bot detection and did not particularly focus on multi-platform scalability or parallel model construction.

In conclusion, current work shows the power of deep learning in these problems but also states inherent restrictions when it comes to covering multi-platform scenarios. Parallel Cyber Security–Diven Model To the best of our knowledge, only a small fraction of works so far take a parallel approach to model shared and platform-specific representations at the same time. This paper bridges this gap by applying a parallel deep learning architecture for multi-platform social media bot detection, providing a scalable and effective solution in line with the modern cyber security needs.

## 3. Methodology

In this section, we discuss the proposed parallel deep learning-based cybersecurity approach to multi-platform social media bot detection. Figure 1 The workflow of the system in the whole system, the data collection, pre-processing, parallel model training, and model evaluation. We went through it all and did the work.

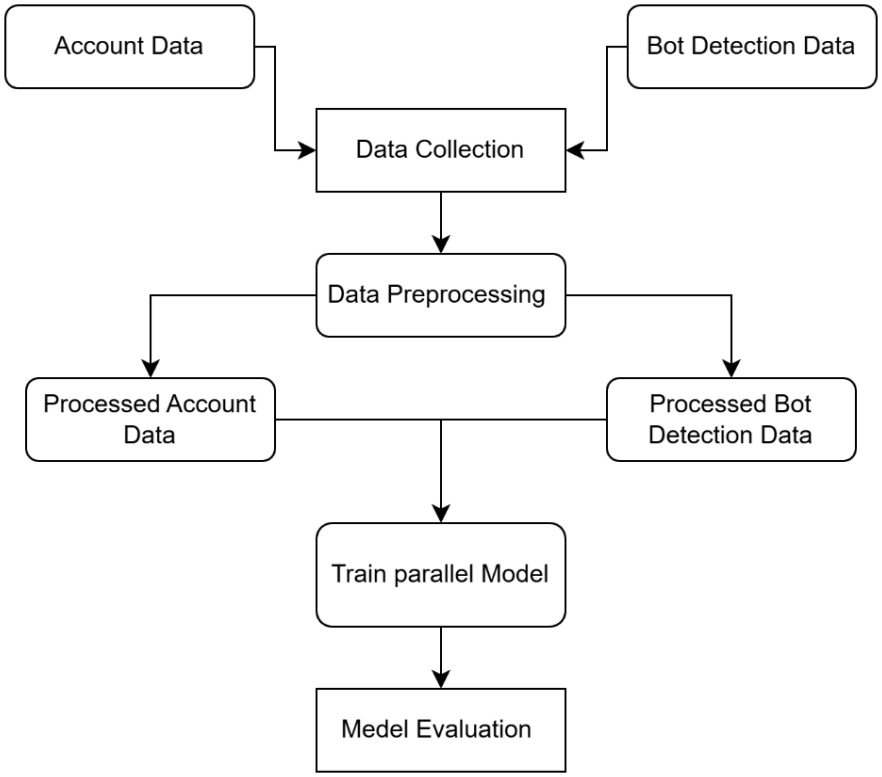


Figure 1 : Methodology Diagram

### *3.1 Data Collection*

The proposed approach considers two heterogeneous datasets which model various aspects of activity on social media. The profile-level dataset includes various attributes about followers and followed, such as their links in the network, activities on it and metadata. The bot detection dataset contains engagement and behavioural features engineered from user actions: like posting activity, reaction stats, and bot label.

They are generated independently separately and integrated as one in the framework for multi-platform learning. This factorization allows the system to model platform unique properties, while remaining general for cross platform deployment - a necessity in cyber security settings where threat actors are active across social media platforms.[20]

### *3.2 Data Preprocessing*

Data preprocessing is an important step for the quality of data and robustness of models. First, the missing values are managed by employing relevant strategies such as complete-case approach and statistical imputation. Unused objects or repeated ones are filtered to reduce complexity and learn efficiently.

For encoding of the categorical attributes, and for scaling of numerical features to have similar ranges we employ one hot encoding and StandardScaler respectively. And for imbalanced datasets, a careful sampling strategy is used to avoid biased learning.[21] A pre-processing step results in two cleaner datasets, evolved account data and bot detection data, which are used as inputs for the parallel learning model.

### *3.3 Parallel Deep Learning Model Architecture*

At the heart of our framework is parallel multi-head deep learning architecture figure 2, developed for simultaneous multi-platform bot detection. The model is composed of shared hidden layers that learn general representations bot behavior and independent output heads for the various social networks.

Each output head receives training signal for binary classification of a user being human-operated and operated by an automatic bot. This design enables the model to learn common behavioral patterns on different social platforms as well as the unique playground properties, which benefits generalization and detection performance. The parallel architecture also facilitates scalability, and therefore the developed framework is applicable to real-world cyber security tasks with multiple data sources.

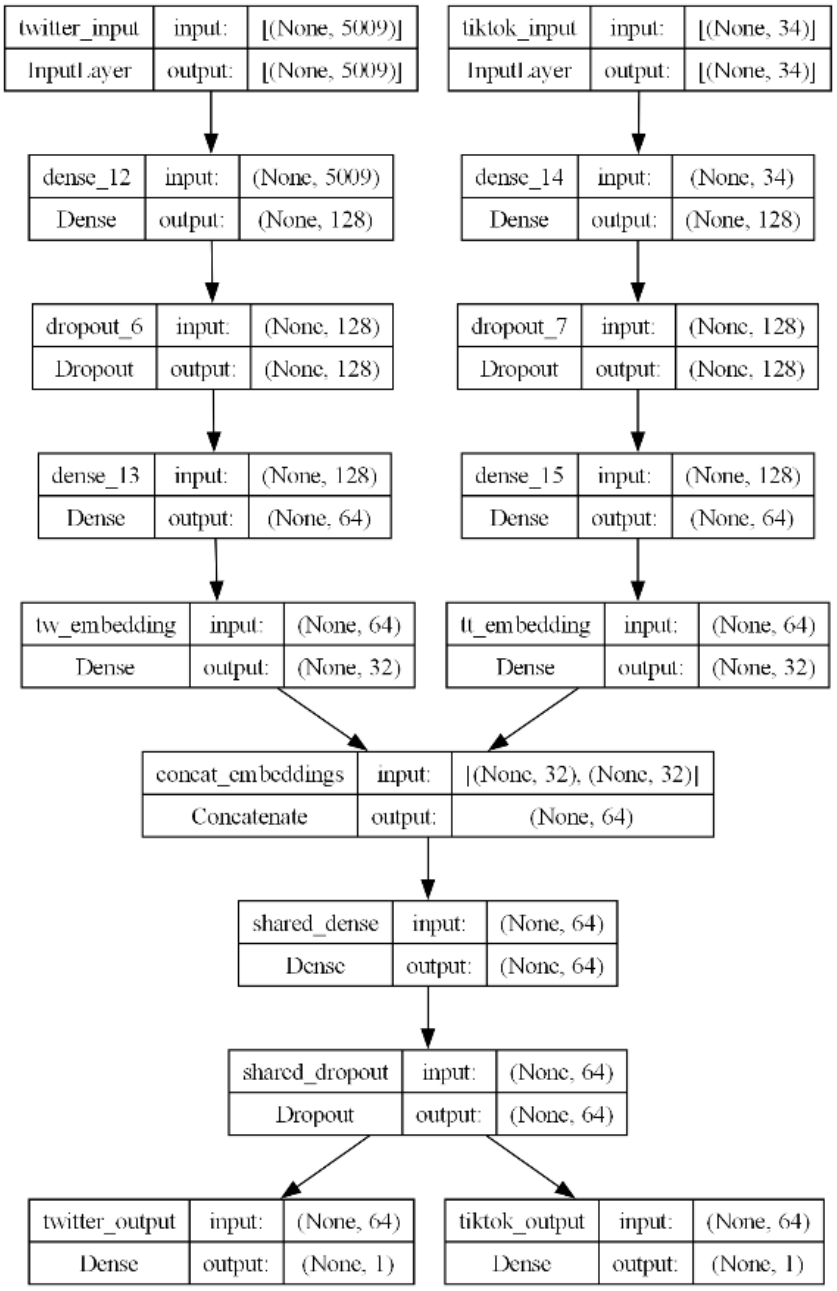


Figure 2 : Parallel Model Architecture

### *3.4 Model Training*

The processed user information and processed bot detection data are input to the parallel model for training. The layers are shared and become optimized together and each output head computes its own loss function. The total training objective is a weighted summation of platform-specific losses, which ensures a balanced learning over the platforms.[22]

An adaptive optimisation algorithm with learning rate scheduling was utilised to train the model to ensure stable convergence. Early stopping and saving the best of performing model's checkpoints are adapted to avoid overfitting. Such training manner ensures effective learning as while high detection performance can be maintained on different platforms.

### *3.5 Model Evaluation*

We also evaluate the trained model with the traditional classification metrics typically utilized in cyber security research, i.e., accuracy, precision, recall (i.e., TPR), F1-score, ROC-AUC and PR-AUC. Error estimates in terms of false positive rates and false negative rates are produced considering confussion matrix as well as classification report for each platform.

Evaluation is done separately on each output head, to allow a detailed comparison of model with platform-specific performance. This in-depth assessment methodology guarantees not only the accuracy but also the reliability and deployability of our framework to real industrial multi-platform cyber security systems.[23]

## 4. Experimental Result

In this section, we present the experimental evaluation of our parallel deep-learning framework on the detection of social-media bots driven by cybersecurity. We study behaviour of training, validation progress and final classification result for each platform-specific weighted output head. The analyses, taken together, demonstrate effectiveness and generalization behavior as well as strengths and limitations across platforms that are used and the datasets used and deployment considerations in real-world monitoring.

### *4.1 Training and Validation Performance*

Training was performed up to 30 epochs but early stopping based on the loss from the Twitter output head was employed in order to avoid overfitting. As shown in Fig. X, the training and validation losses both decrease rapidly at the initial epochs meaning highly effective learning and a steady convergence.

The training loss decreases dramatically on the first five epochs, while it gradually decreases and converges eventually. Likewise, the validation loss monotonically decreases until convergence. The best validation performance was obtained at Epoch 10, the validation Twitter loss of which was 0.1975. Thereafter, no useful betterment was glimpsed and early stopping occurred at Epoch 18. This action is an indication that the model generalizes properly and has not overfitted displayed in figure 3.

The fact that the training and validation curves are so close, shows that our suggested parallel architecture is robust and also learning rate scheduling and regularization techniques have really worked out with such an excellent result.

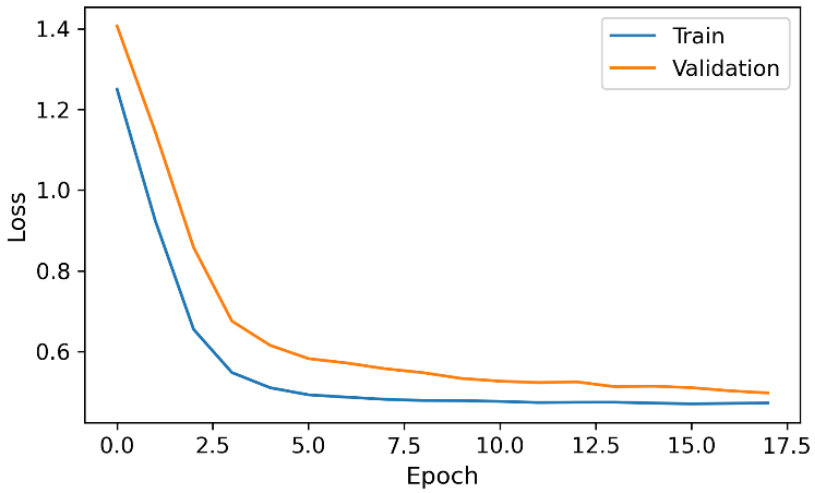


Figure 3: Train vs validation performance

### *4.2 Twitter Bot Detection Results*

The detection performance of the Twitter output head is good and stable. Table 1 represents The performance of the model is 94% for accuracy, 94% for precision, 94% for recall and F1-score is 94%. These findings suggest the model can reliably detect bots, with a low false positive rate.

The ROC-AUC and PR-AUC scores of 94.77% and 93.32%, respectively, also verify that the model can differentiate bot from human accounts at different decision thresholds. From the confusion matrix, we have 1908 True negatives and 1871 true positives with a small number of misclassifications which shows the accuracy of the detection method.

In general, the Twitter head has a good tradeoff between precision and recall so that it can be applied to real world cyber security applications where the false positives and false negatives need to be minimized.

Table 1 : Classification report of Bot Detection

| Class | Precision | Recall | F1-Score | Support |
|---|---|---|---|---|
| Human (0) | 0.94 | 0.95 | 0.95 | 2004 |
| Bot (1) | 0.95 | 0.94 | 0.94 | 1996 |
| Accuracy | - | - | 0.94 | 4000 |
| Macro Avg | 0.94 | 0.94 | 0.94 | 4000 |
| Weighted Avg | 0.94 | 0.94 | 0.94 | 4000 |

### *4.3 TikTok Bot Detection Results*

Results of the TikTok output head are also strong despite variations in dataset scale and platform behaviour. It has an accuracy of 91%, precision 91%, recall 90% and F1-score 91% shown in table 2.

Particularly, the TikTok head achieve better result, which shows great class separability and ranking power. High recall value also indicates the good performance of the model in detecting bot accounts, it is critical in cybersecurity domain as missing to detect malicious actors can lead to devastating results.

The confusion matrix reveals even only 17 of the false negatives and that model is very sensitive for bot activity. Although the false positive rate has increased slightly relative to that of Twitter head, this amount of "misclassification" is a result of a conscious bias for bot detection and threshold adjustment can be used in deployment settings.

Table 2 : Classification report of TickTok Bot Detection

| Class | Precision | Recall | F1-Score | Support |
|---|---|---|---|---|
| Human (0) | 0.92 | 0.85 | 0.89 | 239 |
| Bot (1) | 0.91 | 0.95 | 0.93 | 358 |
| Accuracy | - | - | 0.91 | 597 |
| Macro Avg | 0.91 | 0.90 | 0.91 | 597 |
| Weighted Avg | 0.91 | 0.91 | 0.91 | 597 |

### *4.3 Cross-Platform Performance Analysis*

The experimental results demonstrate the superiority of the proposed parallel multi-head architecture to deal with heterogeneous social media platforms. The twitter head has a better tradeoff between precision and recall, whereas the TikTok head aims for maximal recallings being excellent at capturing malicious automation.

The consistently high AUC and PR-AUC values (table 3) on both platforms indicates that the approach of shared representation learning can effectively model general bot behavior, yet is adaptive for specialized platform patterns. The results demonstrate that parallel deep learning is viable and effective in the multi-platform bot detection problem for cyber security applications.

Table 3 : Auc analysis

| Platform | ROC-AUC | PR-AUC |
|---|---|---|
| Twitter | 0.9477 | 0.9332 |
| TikTok | 0.9630 | 0.9749 |

## 5 Evaluation

Confusion matrices on both Twitter and platforms reveal that the proposed parallel deep learning can achieve great performance in the detection of social media bots. Figure 4 represents For the Twitter data, a total of 1908 human accounts and 1871 improper bot accounts are correctly identified by this model with only few mistakes on other types (a rather balanced and reliable detection ability). This further illustrates the strength of the model and its adequacy in cyber security applications, where precision and trust are important.

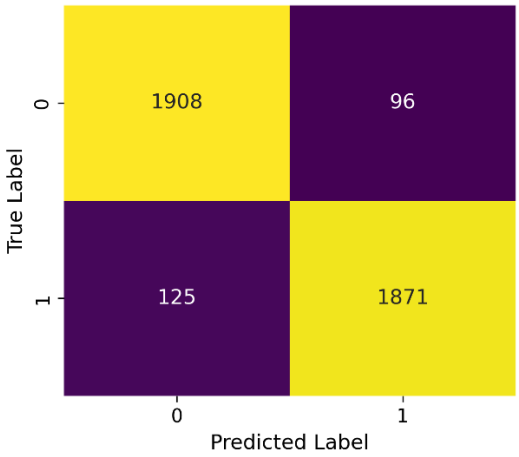


Figure 4: Twitter classification report

Figure 5 represents for the TikTok dataset, 341 bot accounts are correctly pinpointed from the model with only 17 false negatives which shows a strong bias towards identification of malicious automative behavior. The number of false positives (35) is a bit high compared to the data size, but it's better not to miss any threat, thus this trade-off leads to a higher recall, vital in cyber security settings for finding undetected threats. Overall, the results indicate that the proposed parallel architecture well manages platform-dependent detection specifications while sustaining good cross-platform performanc.

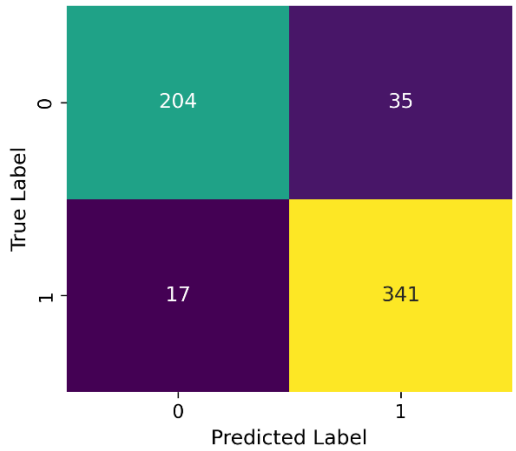


Figure 5: TikTok classification report

**6 Conclusion**

In this paper, we proposed a parallel deep learning-based cyber security framework for identifying social media bots on various platforms. By using a multi-head architecture with shared representations and platform-specific output layers, the proposed method well captures not only common but also platform-specialized bot behaviors. This architecture leads to scalable and robust detection in diverse social media contexts.

Empirical studies on Twitter and TikTok datasets show that our method yields strong and stable performance with high accuracy, F1-score and AUC for both platforms. An examination of the confusion matrices also supports the model's robustness, with low levels of misclassifications and good trade-off between precision and recall. Specifically, the approach has been found to attain an elevated output recall when testing on TikTok platform that detects severe malicious automation which is more beneficial in cybersecurity use-cases.

The findings collectively substantiate the superiority of parallel learning in multi-platform bot identification and it's potential to offer a practical defense measure against automated cyber threats. In the future we will add support for other social networks to have an even more coherent framework, real time detection as well and ethical evaluation of explainable AI in order to provide trust on the decision made by the model.

**Funding**: This research received no external funding
**Conflicts of Interest**: Declare conflicts of interest or state "The authors declare no conflict of interest."
**ORCID iD (if any)**
**Publisher's Note**: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers.

**References**

[1]. Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96–104. https://doi.org/10.1145/2818717
[2]. Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017). Online human-bot interactions: Detection, estimation, and characterization. In Proceedings of the 11th International AAAI Conference on Web and Social Media (ICWSM) (pp. 280–289).
[3]. Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2012). Detecting automation of Twitter accounts: Are you a human, bot, or cyborg? IEEE Transactions on Dependable and Secure Computing, 9(6), 811–824. https://doi.org/10.1109/TDSC.2012.75
[4]. Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race. In Proceedings of the 26th International World Wide Web Conference (WWW) (pp. 963–972). https://doi.org/10.1145/3038912.3052550
[5]. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539
[6]. Kudugunta, S., & Ferrara, E. (2018). Deep neural networks for bot detection. Information Sciences, 467, 312–322. https://doi.org/10.1016/j.ins.2018.08.019
[7]. Yang, C., Harkreader, R. C., & Gu, G. (2013). Empirical evaluation and new design for fighting evolving Twitter spammers. IEEE Transactions on Information Forensics and Security, 8(8), 1280–1293. https://doi.org/10.1109/TIFS.2013.2267732
[8]. Ruder, S. (2017). An overview of multi-task learning in deep neural networks. arXiv. https://arxiv.org/abs/1706.05098
[9]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
[10]. Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2012). Detecting automation of Twitter accounts: Are you a human, bot, or cyborg? IEEE Transactions on Dependable and Secure Computing, 9(6), 811–824.
[11]. Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017). Online human-bot interactions: Detection, estimation, and characterization. In Proceedings of the International AAAI Conference on Web and Social Media (ICWSM) (pp. 280–289).
[12]. Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). The paradigm-shift of social spambots. In Proceedings of the 26th International World Wide Web Conference (WWW) (pp. 963–972).
[13]. Kudugunta, S., & Ferrara, E. (2018). Deep neural networks for bot detection. Information Sciences, 467, 312–322.
[14]. Yang, C., Harkreader, R. C., & Gu, G. (2013). Empirical evaluation and new design for fighting evolving Twitter spammers. IEEE Transactions on Information Forensics and Security, 8(8), 1280–1293.
[15]. Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. First Monday, 22(8).
[16]. Ruder, S. (2017). An overview of multi-task learning in deep neural networks. arXiv. https://arxiv.org/abs/1706.05098
[17]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[18]. Alhosseini, S., Bin Tareaf, M., & Miranskyy, A. (2019). Detecting Twitter bots using deep neural networks. In Proceedings of the IEEE International Conference on Big Data (pp. 2218–2226).
[19]. Hayawi, K., Mathew, S., Venkatraman, S., & Sattar, P. (2020). Towards fake news classification using deep learning. Computers, 9(4).
[20]. Zareen, S., Al Bagiro, S. R. I. K., Abdullah, K. B., Alam, M. Z., & Altemimi, M. A. H. (2025). Leveraging artificial intelligence for advanced threat detection and response in modern cybersecurity frameworks.
[21]. Melon, M. M. H., Arafat, Y., Zareen, S., Alsharfa, R. M., & Abdullah, M. (n.d.). Phishing detection in the age of NLP: Leveraging deep and machine learning for enhanced accuracy.
[22]. Zareen, S., Suha, S. H., Hossain, K., & Bhuiyan, T. (2025). AI-powered road damage detection for enhanced safety and life protection.
[23]. Hossain, K., Zareen, S., & Khandakar, S. (2021). Cyber threat detection using voice and speech analysis.