Computers, Materials & Continua
DOI:10.32604/cmc.2022.021212
Article

Tech Science Press

Deep Learning Empowered Cybersecurity Spam Bot Detection for Online Social Networks

Mesfer Al Duhayyim[1], Haya Mesfer Alshahrani[2], Fahd N. Al-Wesabi[3], Mohammed Alamgeer[4], Anwer Mustafa Hilal[5,*] and Mohammed Rizwanullah[5]

[1]Department of Natural and Applied Sciences, College of Community-Aflaj, Prince Sattam bin Abdulaziz University, Saudi Arabia
[2]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Saudi Arabia
[3]Department of Computer Science, King Khalid University, Muhayel Aseer, Saudi Arabia & Faculty of Computer and IT, Sana'a University, Sana'a, Yemen
[4]Department of Information Systems, King Khalid University, Muhayel Aseer, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Anwer Mustafa Hilal. Email: a.hilal@psau.edu.sa
Received: 27 June 2021; Accepted: 29 July 2021

Abstract: Cybersecurity encompasses various elements such as strategies, policies, processes, and techniques to accomplish availability, confidentiality, and integrity of resource processing, network, software, and data from attacks. In this scenario, the rising popularity of Online Social Networks (OSN) is under threat from spammers for which effective spam bot detection approaches should be developed. Earlier studies have developed different approaches for the detection of spam bots in OSN. But those techniques primarily concentrated on hand-crafted features to capture the features of malicious users while the application of Deep Learning (DL) models needs to be explored. With this motivation, the current research article proposes a Spam Bot Detection technique using Hybrid DL model abbreviated as SBD-HDL. The proposed SBD-HDL technique focuses on the detection of spam bots that exist in OSNs. The technique has different stages of operations such as pre-processing, classification, and parameter optimization. Besides, SBD-HDL technique hybridizes Graph Convolutional Network (GCN) with Recurrent Neural Network (RNN) model for spam bot classification process. In order to enhance the detection performance of GCN-RNN model, hyperparameters are tuned using Lion Optimization Algorithm (LOA). Both hybridization of GCN-RNN and LOA-based hyperparameter tuning process make the current work, a first-of-its-kind in this domain. The experimental validation of the proposed SBD-HDL technique, conducted upon benchmark dataset, established the supremacy of the technique since it was validated under different measures.

Keywords: Cybersecurity; spam bot; data classification; social networks; twitter; deep learning

1 Introduction

Cybersecurity is a phenomenon comprised of a group of processes, methodologies, policies, and technologies which collaborate together to protect the availability, confidentiality, and integrity of software programs, computing resources, network, and data from different types of attacks [1]. Cyber defense mechanism exists at network, data, application and host level. It has a plethora of tools namely, antivirus software, Intrusion Protection System (IPS), firewalls, and Intrusion Detection System (IDS) that work in silos to prevent the attacks and identify the security breaches [2]. Several attackers are still at the benefits since they have to detect one susceptibility in the system that requires protection. For example, in case of an increase in the amount of internet-linked system, the attack apparently raises resulting in higher threat of attacks. Further, adversaries have become highly complex. Because the emerging malware and zero-day exploits avoid the security actions which allow them to continue for a long period of time without any announcement [3]. Zero-day activities are attacks that have not been faced already, but frequently differ on known attacks. To exacerbate the problems, the attack mechanism is being commoditized, which allows the rapid distribution of challenges without requiring any knowledge about the emerging exploits.

With the development of information patterns, there is a drastic change experienced in service modes and social networks too. Social networks provide a transmission platform in which the users could maintain, establish, and expand several inter-personal relations [4]. Few common social networks Weibo, Twitter, Facebook, and so on. The significant increase in the amount of social network users is helps in the rapid growth of amount of attacks [5]. Such malicious behaviour results in increasing the network loads, destroying the normal network order, privacy disclosures, and threatening of the social network reputation system which altogether results in severe loss for the ordinary users. Presently, spammers in social networks have intelligent, diverse, and complex features. When compared with conventional spam distribution that occurs *via* e-mail, social network spams are highly complex to identify, highly deceptive, and pose a great risk to normal users. Thus, spam detections in social network platforms are valuable and significant in different scenarios of user privacy protection, public opinion analysis, network environment security, and so on.

Social network users are increasing and their open nature makes them perfect targets for automated programs (Bots). Spam messages and malicious interaction behaviors are created using these spam bots and it severely thrashes the security and trust of social platforms [6]. Thus, the efficient detection of these spam bots has significant real-world importance in the growth of OSNs. Prior researches, conducted on anomaly account recognition, have primarily concentrated on the recognition of anomaly messages/accounts using a simple relation structure or single feature set. But, spam bots have advanced in the recent years and are able to avoid the existing complex detection techniques [7]. Hence, spam bots could utilize the advanced intelligence approaches to evade the present anomaly detection scheme.

Relative studies [8] have applied ML applications in overcoming cyber challenges but did not involve DL techniques. Another author described DL method for cyber security though these techniques are narrowed-down group of cyber security applications. The study conducted by Xin et al. [9] emphasized on complete set of cyberattacks interrelated to ID and target limitations in dataset and research fields for upcoming module improvement. In Apruzzese et al. [10], the author summarized the work covering attacks exclusively compared with spam detection ID and malware analyses. However, the study did not cover malicious domain terms that are generally utilized by botnets. In Wickramasinghe et al. [11], the researchers summarized and reviewed the works that concentrated on defending cyber physical schemes. In Al-Garadi et al. [12], a review of DL and ML

techniques was conducted to safeguard the IoT technologies. Being an exclusive study, it covered a broad range of cyberattack kinds, and a spectrum of DL methods including CNN, RNN and GAN for spam detection.

Zhao et al. [13] proposed a novel semi-supervised graph embedding module on the basis of graph attention network to detect the spam bots in social networks. In this method, a detection module is created by aggregating feature and neighbour relations and a difficult technique is learnt to integrate distinct neighbourhood relations among the nodes so as to operate the directed social graph. Le et al. [14] proposed a new IDS architecture to overcome the IDS problem. The projected architecture has three major phases. The creation of a SFSDT module i.e., feature selection method is the initial phase. The purpose of creating SFSDT is to create an optimal feature subset in original feature sets. This method is a hybrid of SFS and DT models. The next phase is to create many IDS modules for training the optimally-selected feature subsets. Several RNNs are available such as conventional RNN, LSTM, and GRU.

Zhao et al. [15] proposed a heterogeneous stacking-based ensemble learning architecture to ameliorate the effect of class imbalance on spam detection in social network. The presented architecture contains combining and base modules. In base component, 6 distinct base classifications are adapted and this classification diversity is used in the construction of a novel ensemble input member. In combination element, the researchers introduced a cost-sensitive learning to DNN training. Gnanasekar et al. [16] presented a 3-layer social bots detection technique based on DL method. Joint substance highlight extraction layer is the initial layer which focuses on the component extraction of tweet contents and its connections. In next layer, tweet metadata fleeting element gets extracted since the tweet metadata is viewed as worldly data and this transient data is utilized as LSTM contribution to extract a user's social action transient component. Then, element intertwining layer integrates the detached joint substance with worldly highlight in order to identify the social bots.

The current research paper develops a spam bot detection technique using hybrid DL model, named SBD-HDL. The proposed SBD-HDL model involves hybridization of Graph Convolutional Network (GCN) with Recurrent Neural Network (RNN) model for spam bot classification process. In order to improve the detection performance of GCN-RNN model, hyperparameter tuning process takes place using Lion Optimization Algorithm (LOA). The hybridization of GCN-RNN and LOA-based hyperparameter tuning process remain the novelty of current work. The proposed SBD-HDL technique was experimentally validated on a benchmark dataset and the outcomes were examined under different measures.

2 The Proposed Model

Fig. 1 demonstrates the working process of the proposed SBD-HDL model. The proposed SBD-HDL technique comprises of different stages of operations such as pre-processing, GCN-RNN-based classification, and LOA-based parameter optimization. The detailed working flow of these processes is discussed in the succeeding sections.

2.1 Problem Formulation

Spam bot detection is basically a binary classifier problem. It aims at creating the classification that can precisely allocate the labels to accounts in test set, according to the feature of set of social networks/trained user. This section defines the process involved. If assuming the social graph $G = (V, E)$, then the objective of spam bot detection problem is to learn a classifier function $f: N \rightarrow Y$. In the event of a provided training set, social network account nodes, present in set N, are categorized

under accurate classes using the reliability label 'Y' with multi element data in account propagation. Each kind of data in account propagation that involve account data and network framework data must be combined efficiently.

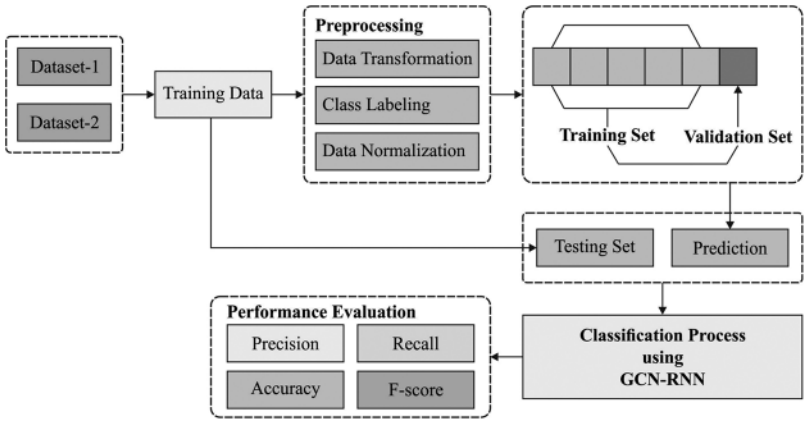

Figure 1: Overall process of the proposed method

2 Phase I: Data Pre-Processing

In data pre-processing, the input customer data is pre-processed through three stages such as data transformation, class labeling, and data normalization. Initially, the input data in .xls format is converted into.csv format. Secondary, class labeling procedure is performed where the samples are assigned for equivalent classes. Thirdly, data normalization model takes place utilizing min-max dataset as determined below.

$$Min - Max.Norm = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{1}$$

2.3 Phase II: Data Classification

When OSN data is pre-processed, GCN-RNN model is used in the classification of users into either legitimate users or bots.

In order to implement natural language processing applications like answer to questions, a knowledge base can store the relationships and entities should be created accordingly. However, the present knowledge base techniques generally lose huge number of data. It only needs the development of codec models in the graph method and softmax can be used on every node. Graph convolutional network [17] tend to recover the missing entities/relationships that could also execute the task of entity classification. The test result on few datasets shows that these network frameworks can improve the problems that arise from lost data in the knowledge base.

Though DL has attained substantial results in few AI techniques, non-Euclidean domain data also exists widely and should be analyzed. It becomes inevitable to define the physical or molecular or biological modules using nodes and its connections with one another. Graphical modeling of this data is an optimum learning technique. Graph NN could create graph modules by disseminating the data among these nodes. However, the graph data has high complexity and robust irregularities. The present DL techniques usually consider that these nodes are interrelated and are inappropriate for this modeling type. Alternatively, convolution, a method frequently utilized in DL, could not be directly

utilized in graph modeling. The objective of network-embedded technique is to maintain the locations and structure of entire nodes.

In real-world applications like traffic flow, knowledge graphs, and social networks, huge number of data exists through a graph structure. Graph semi-supervised learning method is utilized in the management of situations in which all the nodes in data have not been labeled, while few nodes possess certain labels/categories. GCN is determined in this manner: The determination graph is, every node feature is obtained as input, and the adjacency matrix of relationship with node is A. The aim is to provide the output for feature matrix that denotes the labelled/learned data of unlabeled nodes. The equation for two layers of GCN semi-supervised node classifier is displayed in Eq. (2):

$$Z = f(X, A) = softmax\left(\widehat{A}ReLU\left(\widehat{A}XW^{(0)}\right)W^{(1)}\right) \tag{2}$$

where $W^{(0)}$ implies the input of hidden layer whereas the 'H' feature maps to hidden weight matrix. $W^{(1)}$ represents the hidden output weight matrix. Mainly, RNN is utilized in handling the problems related to order input and output. It can be a scalable DNN. LSTM is frequently utilized in RNN due to which this feature gets influenced by long time input. LSTM is extensively utilized in image analysis, speech modeling, text recognition, etc. Generally, regular LSTM has an issue *i.e.*, it could not differentiate the features for significant classification of the portions. One more drawback is the complexity of exploding/vanishing gradients. The technique is to relate attention weight for every input vector, thus the output also transmits this data. As previously stated, GCN/RNN technique still could not resolve the problem of huge network structures and long training time while its efficiency is also not good in case of less data and label. Fig. 2 depicts the structure of RNN model.

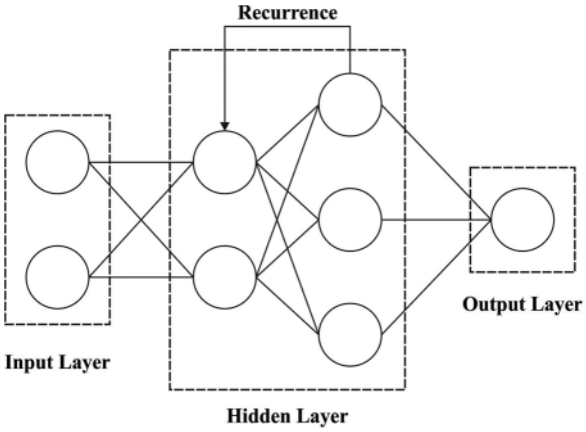

Figure 2: Structure of RNN model

The current study proposed an enhanced 2D graph CNN RNN and GCN hybrid structure for the classification of spam bots. A network module, depending upon GCN and notice LSTM, is created to construct and train the graph structures' representation on the basis of documents, relationships, and words. Thus, long-term relations and framework of whole text graphs could be maintained in an embedded graph for in-depth description of the textual connections and execution of reliable text classification [18]. GCN is the initial layer of hybrid framework which includes input layer, output layer, and multiple hidden layers. Once a sequence instance is processed using an adequate length of time, the attention methods are completely utilized through data aggregation from previous times to abstract further output vectors.

2.4 Phase III: Hyperparameter Tuning

In order to improve the detection performance of GCN-RNN model, hyperparameter tuning process takes place *via* LOA. Lion Optimization Algorithm (LOA) is simulated based on the nature of lions. Lions mostly depict a superior level of collaboration as well as aggression. It is generally structured into two types such as Resident Lions (RL) and Nomad Lions (NL). RL usually lives in groups and are named as pride (P). The second type lives separately or rarely it also lives as pairs. Lions commonly hunt as groups. Several lionesses obligingly effort to surround the prey in different points and attack the prey. Male Lions (ML) and some lionesses go to rest and delay the hunter lioness. Lions endure mating procedure at some time while the lioness mates with several partners also. Obviously, lions mark their territories through urine. In LOA, the performances are mathematically determined to model the optimization technique. A primary population is created as a group of randomly-created solutions, in the name of lions, in LOA. At primary population (%N), certain cases are selected as NL whereas rest of the population (RL) is separated as *P* subset (prides) in an arbitrary manner. S denotes the number of lionesses while the residual lions are male.

LOA primarily creates the population in an arbitrary manner in solution space. It assumes all the solutions as 'lion'. In order to overcome N_v dimension optimization issue, the lion is determined as follows.

$$\text{Lion} = [u_1, u_2, u_3, \ldots, u_{N_v}] \tag{3}$$

Besides, the cost (fitness value of all the lions) is defined as the estimation of cost function as provided herewith.

$$\text{fitness value of lion} = f(\text{Lion}) = f(u_1, u_2, u_3, \ldots, u_{N_v}) \tag{4}$$

In the beginning, N_{pop} solutions are randomly generated in search space. %N of solutions get elected as NL in an arbitrary manner. The residual populations are separated as P pride. All the solutions in LOA correspond to exact gender and continued constant in the optimization procedure.

In each P, a definite amount of females look up to prey in group so as to feed the member in P group. This hunter lion follows specific methods to surround and catch the prey. In general, lions follow nearly similar pattern to hunt the prey. In hunting, if a hunter improves their separate fitness, the prey avoids moving to a novel place as signified in Eq. (5).

$$\text{PRY}' = \text{PRY} + \text{rando}(0, 1) \times \text{PRYI} \times (\text{PRY} - \text{Hter}) \tag{5}$$

where PRY implies the current place of prey, Hter represents the novel place of hunter to attack the prey and PRYI is the % of improvement in hunter fitness. The novel place of hunters that go to left and right wings are as follows.

$$\text{Hter}' = \begin{cases} \text{rando}((2 \times \text{PRY} - \text{Hter}), \text{PRY}), & (2 \times \text{PRY} - \text{Hter}) < \text{PRY} \\ \text{rando}(\text{P}, (2 \times \text{PRY} - \text{Hter})), & (2 \times \text{PRY} - \text{Hter}) > \text{PRY} \end{cases} \tag{6}$$

The novel places of center hunters are formed as determined in Eq. (7):

$$\text{Hter}' = \begin{cases} \text{rando}(\text{Hter}, \text{PRY}), & \text{Hter} < \text{PRY} \\ \text{rando}(\text{PRY}, \text{Hter}), & \text{Hter} > \text{RPY} \end{cases} \tag{7}$$

rando(a, b) gives an arbitrary number between a and b. These hunting performances propose few advantages in attaining the optimum solutions. Thus, the territory of all prides contain individual optimum places, obtained by all the members in pride. It makes use of LOA to store the optimal

solution gained before the time period which is helpful to enhance the solution in LOA. Therefore, the novel place for a Female Lion (FL) is signified as follows

$$FL' = FL + 2D \times \text{rando}\,(0,1)\,\{R1\} + U\,(-1,1) \times \tan\,(\theta) \times D \times \text{rando}(0,1)\{R2\} \tag{8}$$

$$\{R1\}\,.\,\{R2\} = 0, ||R2|| = 1$$

where FL defines the current place and *D* provides the distance between FL's place and the elected points selected by competition choice in pride's territory. {R1} implies the vector and its primary point is the earlier place of FL. It concentrates on the elected place nearby {R2} and is perpendicular to {R1}.

All the MLs in *P* travel everywhere in the territory of pride. To imitate this naturally, the % R of pride territory is randomly elected and the lions travel accordingly. But, while roaming, if a resident male defines the novel place which is superior to the present place, the optimum visited solution gets upgraded. Roaming is powerful local search and makes use of LOA to search the solution so as to enhance it. NL and its adjustable roaming naturally use LOA to search the solution space in arbitrary manner and keep track of the local optimum. In previous methods, the novel places of NL are determined as follows

$$Lion_{ij}^{'} = \begin{cases} Lion_{ij} & if > pr_i \\ RANDO_j & otherwise \end{cases} \tag{9}$$

where $Lion_i$ stands for the current place of i^{th} NL lions, j represents the dimensional, $rando_j$ signifies uniform arbitrary number between 0 and 1, *RANDO* refers to arbitrarily-formed vector in search space, and pr_i indicates the probability calculated by all NLs in an independent manner as expressed below.

$$\text{pr}_\text{i} = 0.1 + \min\left(0.5, \frac{(\text{NL}_\text{i} - \text{Bst}_\text{NL})}{\text{Bst}_\text{NL}}\right) \tag{10}$$

where NL_i and Bst_NL denote the cost of current places of i^{th} lions from NL and the optimum cost of NL correspondingly.

Mating is a vital process that guarantee the lions to be itself and provides an opportunity for lions to connect with other members of the herd. In all Ps, %Ma of FLs mate with at least one resident male which is elected in an arbitrary manner similar to P so as to generate offspring. Mate function is a linear group of parents to produce two novel offspring. LOA connects the data between the mates and the novel cubs get characters from both the genders.

In all the Ps, if an ML obtains maturity, it is powerful and fights with other MLs in the P. The beaten lion leaves P and develops NL. In parallel, if an NL male is actually strong, it fights with RL male in P while NL develops itself to become RL and the action continues conversely. LOA uses the defense function to keep the very powerful MLs as solution since it plays an important role in LOA.

According to switch and migration activities, lions in one P to other gets their way of life modified and the resident female develops NL. Conversely, it enhances the variety of target pride by their place in previous pride. It also paves a way to transmit amongst lions. To all Ps, the maximal amount of females gets calculated as S% of population of P. In case of migration function, few females are randomly elected and NL is developed. If the elected FLs migrate in P and develop a NL, new and old NL females get organized according to their fitness values. The processes involved in LOA are shown in Algorithm 1.

Algorithm 1: Pseudocode of LOA

1. Create arbitrary sample of lions, N_{pop}.
2. Initialization of Nomad Lion and pride.
   i. Arbitrarily elect %N (% of lions that are nomad) of iN_{pop} as nomad lion. Divide rest of the lions into a number of prides P arbitrarily, and create a territory for every pride.
   ii. In every pride %S (Sex rate) of whole population, S are named as females and the remaining ones are called as males.
3. In every individual pride,
   i. Few arbitrarily-chosen female lions goes for hunting
   ii. Every residual female one in the pride reaches the course of optimal location chosen from the territory.
   iii. For every resident male; %R (Roaming percent) of the territory is carefully chosen and verified. %Ma (Mating probability) of females is chosen with pride mate with one or many resident males. → *New cubs become mature*.
   iv. Weak male gets evaded away from the pride and becomes nomad.
4. For Nomad,
   i. Nomad lion moves arbitrarily in the searching area. %Ma (Mating probability) of nomad female mates with an optimal nomad male.
   ii. Nomad males arbitrarily attack the prides.
5. For every pride,
   i. Few females with 1 rate, migrate from the pride and becomes a nomad.
6. Do
   i. Sort the nomad lion with respect to fitness value. Then, optimal female ones are chosen and dispersed to prides thus satisfying the empty locations of the migrated female.
   ii. Based on the highest permitted number of every individual gender, the nomad lion with minimal fitness value gets discarded.

When the stopping criteria is unsatisfied, jump to Step 3

3 Performance Validation

3.1 Dataset Details

This section deals with investigation and performance of spam bot detection by the proposed SBD-HDL technique. The proposed SBD-HDL technique was tested using two datasets. Dataset 1 has 100 samples, 29 attributes, and 2 class labels. Besides, dataset 2, The Twitter 1KS-10KN dataset [19,20] includes samples with two labels namely, spam bots and legitimate users. It includes a total of 11,000 nodes and 2,342,816 edges.

3.2 Performance Measures

In current research work, spam bot detection performance of the proposed SBD-HDL technique was evaluated using four measures such as

- Precision,
- Recall,

- Accuracy, and
- F-measure

Accuracy can be determined as a ratio of properly classified user profiles over total number of available user profiles and can be defined using Eq. (11):

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \tag{11}$$

Next, precision can be computed as a ratio of the properly-anticipated spam profiles over total number of profiles determined as 'spam'. Alternatively, it denotes the percentage of spam user profiles which are actually spam profiles. Precision can be expressed as follows.

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

Then, recall is the percentage of appropriately-predicted spam profiles over a number of total real spam user profiles, as indicated herewith.

$$Recall = \frac{TP}{TP + FN} \tag{13}$$

F-measure is calculated as the weighted average of both precision and recall. It can be defined using the Eq. (14):

$$Fmeasure = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{14}$$

3.3 Results of the Analysis

Tab. 1 shows the results of comparative analysis of SBD-HDL technique against other methods. Figs. 3 and 4 shows the results for classification performance of the proposed SBD-HDL technique and other techniques before feature selection process. From the results, it is apparent that the proposed SBD-HDL approach produced the maximal classification accuracy over other ML models. When assessing the results in terms of accuracy and precision, it is evident that J48 technique accomplished the least outcome with an accuracy of 89.3% and precision of 89.40%. Next, MLP model gained a slightly increased outcome with an accuracy of 89.3% and precision of 89.40%. Then, RF technique obtained a certainly higher performance with an accuracy of 94.10% and precision of 95.60%. Followed by, NB model showcased a moderately closer result with an accuracy of 95.70% and precision of 96.50%. Though K-NN model portrayed competitive performance with an accuracy of 96.30% and precision of 98.40%, the proposed SBD-HDL technique outperformed existing methods and achieved the highest accuracy of 98.85% and precision of 99.30%.

When investigating the outcomes with respect to recall and F-measure, it is clear that J48 manner accomplished the worst outcomes with a recall of 91.4% and an F-measure of 89.60%. In line with this, MLP method obtained somewhat improved outcome with a recall of 92.6% and an F-measure of 93.30%. Afterwards, RF technique reached a certainly higher efficiency with a recall of 93.80% and an F-measure of 94.10%. Likewise, NB technique demonstrated a moderately closer outcome with a recall of 95.70% and an F-measure of 96%. But, the K-NN model exhibited a competitive performance with a recall of 94.80% and an F-measure of 96.20%. However, the proposed SBD-HDL technique outperformed the existing methods with maximum recall of 98.10% and an F-measure of 97.50%.

Table 1: Results of the analysis of various methods against the proposed model under different measures on dataset-1

Before feature selection *vs*. proposed method				
Methods	Accuracy	Precision	Recall	F-measure
Proposed SBD-HDL	98.85	99.30	98.10	97.50
J48	89.30	89.40	91.40	89.60
k-NN	96.30	98.40	94.80	96.20
MLP	93.30	95.20	92.60	93.30
NB	95.70	96.50	96.00	95.90
RF	94.10	95.60	93.80	94.10
After feature selection *vs*. proposed method				
Proposed SBD-HDL	98.85	99.30	98.10	97.50
Information gain	98.70	98.90	98.60	98.00
Relief	98.10	98.60	97.90	97.90
Chi-square	98.50	98.70	99.00	98.30
Correlation	99.40	97.90	99.60	98.40
Significance	98.60	99.20	99.40	98.20

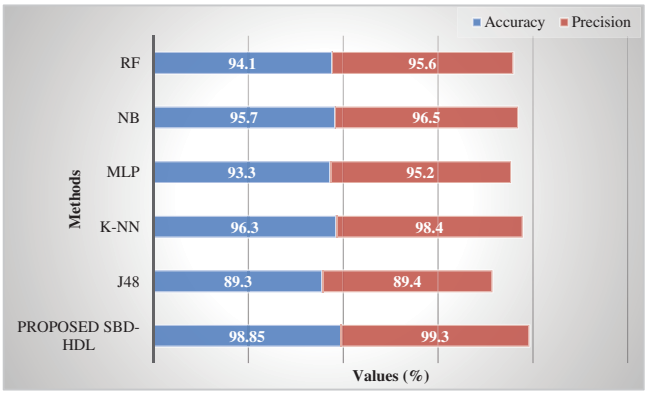

Figure 3: Precision and accuracy analysis: before feature selection *vs*. proposed method

Figs. 5 and 6 show the results of classification performance achieved by SBD-HDL manner and other such algorithms after feature selection process is over. From the outcomes, it is clear that the proposed SBD-HDL method produced maximal classification accuracy over other ML techniques. In analytical results, with respect to accuracy and precision, it is obvious that the relief manner accomplished minimum results with an accuracy of 98.10% and a precision of 98.60%. Chi-square algorithm produced slightly higher results with an accuracy of 98.5% and a precision of 98.70%. In addition, Significance manner reached a certainly higher performance with an accuracy of 98.60%

and a precision of 99.20%. Besides, Information gain method outperformed the previous methods through a moderately closer result *i.e.*, an accuracy of 98.70% and a precision of 98.90%. Eventually, Correlation approach demonstrated a competitive performance with an accuracy of 99.40% and a precision of 97.90%. However, the proposed SBD-HDL methodology outperformed the existing models with high accuracy of 98.85% and a precision of 99.30%.

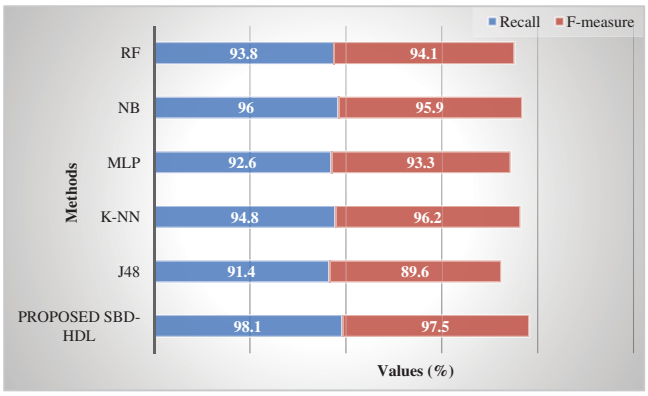

Figure 4: Recall and F-measure analysis: before feature selection *vs*. proposed method

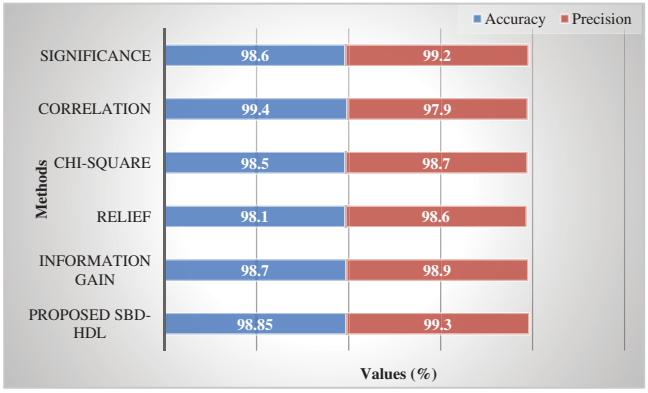

Figure 5: Precision and accuracy analysis: after feature selection *vs*. proposed method

When observing the results in terms of recall and F-measure, it is apparent that the Relief method accomplished the least results with a recall of 97.90% and an F-measure of 97.90%. SBD-HDL model achieved somewhat higher results with a recall of 98.1% and an F-measure of 97.50%. Additionally, information gain manner attained a certainly higher performance with a recall of 98.60% and an F-measure of 98%. At the same time, Chi-square method exhibited a moderately closer outcome with its recall being 99% and F-measure being 98.30%. However, Significance methodology portrayed a competitive performance with a recall of 99.40% and an F-measure of 98.20%. Further, Correlation algorithm accomplished a superior recall of 99.60% and F-measure of 98.40%.

To further confirm the improved performance of SBD-HDL technique, another comparative analysis was conducted and the results are shown in Tab. 2 and Fig. 7. On the applied dataset-2, DT model showcased ineffectual outcomes over other techniques. Followed by, SVM and BP models demonstrated slightly enhanced performance. Concurrently, NN technique showcased somewhat enhanced outcome over SVM and BP models.

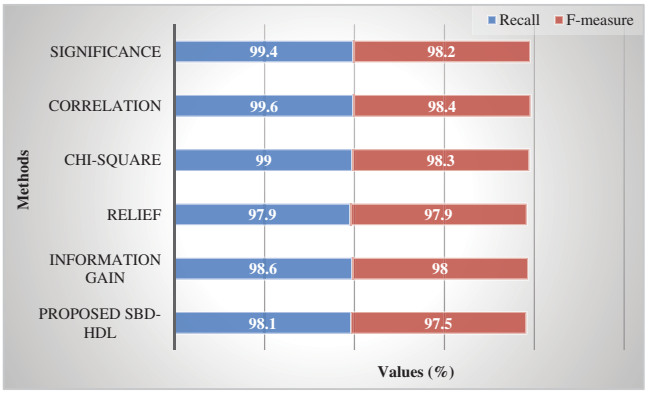

Figure 6: Recall and F-measure analysis: after feature selection *vs*. proposed method

Table 2: Results analysis of the various methods with proposed model in terms of distinct measures on dataset-2

Method	Recall	Precision	F1-score
Proposed SBD-HDL	96.50	97.30	96.90
ABGNN	88.00	93.00	91.00
RF	66.00	88.00	76.00
MLP	73.00	81.00	77.00
BP	54.00	56.00	55.00
Decision tree	66.70	33.30	44.40
Neural networks	63.70	62.70	59.10
Support vector machines	47.10	46.20	44.90
Naive bayesian	91.70	91.70	91.70
GCN	76.00	87.00	81.00
GraphSAGE	80.00	88.00	84.00
GAT	83.00	87.00	85.00

Besides, MLP, GCN, GAT, RF, and GraphSAGE techniques accomplished moderately closer results. Followed by, naïve Bayesian and ABGNN models showcased near optimal results. However, the proposed SBD-HDL technique demonstrated supreme outcomes compared to all other techniques with a maximum precision of 97.3%, recall of 96.5%, and an F1-score of 96.9%. From the aforementioned tables and figures, it is clear that the proposed SBD-HDL approach is an effectual spam bot detection tool for OSN.

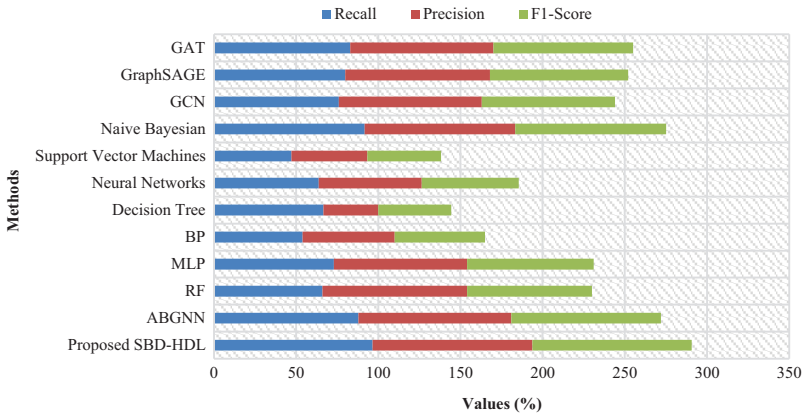

Figure 7: Comparative analysis of SBD-HDL model with existing techniques

4 Conclusion

The current research paper designed a new SBD-HDL technique for spam bot detection in OSN. The proposed SBD-HDL technique focuses on the detection of spam bots present in OSNs. The proposed SBD-HDL technique comprises of different stages such as pre-processing, GCN-RNN-based classification, and LOA-based parameter optimization. The hybridization of GCN-RNN and LOA-based hyperparameter tuning process is the novelty of current research study. In order to improve the detection efficiency of GCN-RNN model, hyperparameter tuning process is performed using LOA. The proposed SBD-HDL technique was experimentally validated on a benchmark dataset and the outcomes were examined under different measures. The results established the supremacy of the proposed approach. In future, the detection performance can be improved by utilizing feature selection and feature reduction approaches.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP 1/53/42). www.kku.edu.sa. This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-Track Path of Research Funding Program.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Gopalakrishnan, D. Ruby, F. Al-Turjman, D. Gupta, I. V. Pustokhina *et al.,* "Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems," *IEEE Access*, vol. 8, pp. 185938–185949, 2020.

[2] D. Berman, A. Buczak, J. Chavis and C. Corbett, "A survey of deep learning methods for cyber security," *Information-an International Interdisciplinary Journal*, vol. 10, no. 4, pp. 122, 2019.

[3] G. N. Nguyen, N. H. L. Viet, M. Elhoseny, K. Shankar, B. B. Gupta *et al.,* "Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing*, vol. 153, no. 2, pp. 150–160, 2021.

[4] I. V. Pustokhina, D. A. Pustokhin, T. Vaiyapuri, D. Gupta, S. Kumar *et al.,* "An automated deep learning based anomaly detection in pedestrian walkways for vulnerable road users safety," *Safety Science*, vol. 142, pp. 105356, 2021.

[5] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan and S. A. Razak, "Malicious accounts: Dark of the social networks," *Journal of Network and Computer Applications*, vol. 79, no. 3, pp. 41–67, 2017.
[6] J. Banumathi, A. Muthumari, S. Dhanasekaran, S. Rajasekaran, I. V. Pustokhina *et al.,* "An intelligent deep learning based xception model for hyperspectral image analysis and classification," *Computers Materials & Continua*, vol. 67, no. 2, pp. 2393–2407, 2021.
[7] V. Porkodi, A. R. Singh, A. R. W. Sait, K. Shankar, E. yang *et al.,* "Resource provisioning for cyber-physical–social system in cloud-fog-edge computing using optimal flower pollination algorithm," *IEEE Access*, vol. 8, pp. 105311–105319, 2020.
[8] J. M. Torres, C. I. Comesaña and P. J. G. Nieto, "Review: Machine learning techniques applied to cybersecurity," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 10, pp. 2823–2836, 2019.
[9] Y. Xin, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.
[10] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in *2018 10th Int. Conf. on Cyber Conflict (CyCon)*, Tallinn, pp. 371–390, 2018.
[11] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe and M. Manic, "Generalization of deep learning for cyber-physical system security: A survey," in *IECON, 2018-44th Annual Conf. of the IEEE Industrial Electronics Society*, Washington, DC, pp. 745–751, 2018.
[12] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali *et al.,* "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.
[13] C. Zhao, Y. Xin, X. Li, H. Zhu, Y. Yang *et al.,* "An attention-based graph neural network for spam bot detection in social networks," *Applied Sciences*, vol. 10, no. 22, pp. 8160, 2020.
[14] T.-T.-H. Le, Y. Kim and H. Kim, "Network intrusion detection based on novel feature selection model and various recurrent neural networks," *Applied Sciences*, vol. 9, no. 7, pp. 1392, 2019.
[15] C. Zhao, Y. Xin, X. Li, Y. Yang and Y. Chen, "A heterogeneous ensemble learning framework for spam detection in social networks with imbalanced data," *Applied Sciences*, vol. 10, no. 3, pp. 936, 2020.
[16] A. Gnanasekar, "Detecting spam bots on social network," *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 2, pp. 850–860, 2021.
[17] L. Gao, J. Wang, Z. Pi, H. Zhang, X. Yang *et al.,* "A hybrid GCN and RNN structure based on attention mechanism for text classification," *Journal of Physics: Conf. Series*, vol. 1575, pp. 012130, 2020.
[18] T.-T.-H. Le, Y. Kim and H. Kim, "Network intrusion detection based on novel feature selection model and various recurrent neural networks," *Applied Sciences*, vol. 9, no. 7, pp. 1392, 2019.
[19] A. Al-Zoubi, J. Alqatawna, H. Faris and M. Hassonah, "Spam profiles detection on social networks using computational intelligence methods: The effect of the lingual context," *Journal of Information Science*, vol. 47, no. 1, pp. 58–81, 2019.
[20] C. Yang, R. Harkreader, J. Zhang, S. Shin and G. Gu, "Analyzing spammers' social networks for fun and profit: A case study of cyber criminal ecosystem on twitter," in *Proc. of the 21st Int. Conf. on World Wide Web - WWW '12*, Lyon, France, pp. 71–80, 2012.