Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.031181
Article

Tech Science Press

Spotted Hyena Optimizer with Deep Learning Driven Cybersecurity for Social Networks

Anwer Mustafa Hilal[1,2,*], Aisha Hassan Abdalla Hashim[1], Heba G. Mohamed[3], Lubna A. Alharbi[4], Mohamed K. Nour[5], Abdullah Mohamed[6], Ahmed S. Almasoud[7] and Abdelwahed Motwakel[2]

[1]Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, 53100, Malaysia
[2]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj, 16278, Saudi Arabia
[3]Department of Electrical Engineering, College of Engineering, Princess Nourah bint Abdulrahman University, P. O. Box 84428, Riyadh, 11671, Saudi Arabia
[4]Department of Computer Science, College of Computers and Information Technology, Tabuk University, Tabuk, 47512, Saudi Arabia
[5]Department of Computer Sciences, College of Computing and Information System, Umm Al-Qura University, Mecca, 24382, Saudi Arabia
[6]Research Centre, Future University in Egypt, New Cairo, 11845, Egypt
[7]Department of Information Systems, College of Computer and Information Sciences, Prince Sultan University, Riyadh, 12435, Saudi Arabia
*Corresponding Author: Anwer Mustafa Hilal. Email: a.hilal@psau.edu.sa

Received: 12 April 2022; Accepted: 22 June 2022

Abstract: Recent developments on Internet and social networking have led to the growth of aggressive language and hate speech. Online provocation, abuses, and attacks are widely termed cyberbullying (CB). The massive quantity of user generated content makes it difficult to recognize CB. Current advancements in machine learning (ML), deep learning (DL), and natural language processing (NLP) tools enable to detect and classify CB in social networks. In this view, this study introduces a spotted hyena optimizer with deep learning driven cybersecurity (SHODLCS) model for OSN. The presented SHODLCS model intends to accomplish cybersecurity from the identification of CB in the OSN. For achieving this, the SHODLCS model involves data pre-processing and TF-IDF based feature extraction. In addition, the cascaded recurrent neural network (CRNN) model is applied for the identification and classification of CB. Finally, the SHO algorithm is exploited to optimally tune the hyperparameters involved in the CRNN model and thereby results in enhanced classifier performance. The experimental validation of the SHODLCS model on the benchmark dataset portrayed the better outcomes of the SHODLCS model over the recent approaches.

Keywords: Cybersecurity; cyberbullying; online social network; deep learning; spotted hyena optimizer

1 Introduction

Due to the expansion of the Internet, security is considered a significant factor. Though Web 2.0 offers interactive, simple, anywhere, and anytime accessibilities to the online societies, it additionally offers platform for cybercrimes namely cyberbullying (CB) [1]. Aggravating CB encounters amid adolescent persons was stated globally, therefore drafting interest in its negative influences. In the United States, the footprints of CB are extremely rising and it was formally recognized as a social risk [2]. CB has the same, if not a greater, adverse effect on the victims about conventional bullying since the predators generally assault a person concerning factors which an individual does not make any variation (e.g., physical appearance, religion, skin color, and ethnic background), allowing deep and long-lasting effects on the sufferer [3,4]. In a few cases, the related humiliation is adequate which may force the sufferer to harm or suicidal activities. Suicidal intention tends to raise in youth because of the exposure to various types of CB [5]. Still, preventive steps are conducted, and the rehabilitation of sufferers of CB cases is assumed as a challenging one for societies and families. Hypersensitivity, self-hate, and isolation prevailing in the socialization procedure results in depressed adults. In addition to this, the psychological disparity may build forthcoming bullies [6]. Amongst various difficulties which make the identification of CB in OSN very complicated, existing solutions to CB identification cannot indicate the scope of bullying forms in its identification method. Provided the various kinds of CB which could arise on the website, it is impossible to consider that a similar identification method will be effective in identifying each kind of bullying.

The computational identification CB can be performed on the basis of several classes of methods in the domains of machine learning (ML). Natural language processing (NLP) is assumed as another tool for social textual interaction examination [7]. The criteria of social interaction examination and sociolinguistics impose a focus on uniqueness, the presence of the effect, specificity, and the personality of the persons, and ascription to the society and their language utilization; whereas statistical supervised and unsupervised techniques highlight abstraction, generalization, and exploitation of patterns in the data [8]. The domains of social interaction interpretation and sociolinguistics have an important chasm and dissonance with the domains of ML and NLP. Various conventional ML methods needed clear feature extraction from input data [9]. NLP has extensive applications in this field, as authors have used various feature extraction methods for textual content. Fundamental attempts involve supervised categorization by utilizing bag-of-words at character-level representation through numerous conventional ML methods [10]. Deep learning (DL) methods were used for defeating the restrictions of conventional ML, reducing the manual feature extraction stage, and getting superior outcomes on large scale datasets.

Lu et al. [11] present a Character-level Convolutional Neural Network with Shortcuts (Char-CNNS) technique for identifying if the text from social media comprises CB. It can utilize character as the minimum unit of learning, allowing the method for overcoming spelling errors and intentional obfuscation from the real world corpora. The shortcuts were employed to stitch distinct levels of features for learning further granular bullying signals, and the focal loss function was implemented for overcoming the class imbalance problems. The authors in [12] purpose for addressing the computational challenge linked with harassment finding from the social media by establishing an ML structure with 3 distinguishing features. Chen et al. [13] presented a new deep method, HEterogeneous Neural Interaction Network (HENIN), to explainable CB recognition. The HENIN comprises the subsequent modules: comment encoded, post-comment co-attention sub-network, session-session, and post-post communication extractor. The authors in [14] discovered the issue of CB forecast and present MIIL-DNN, a multi-input integrative learning method on deep neural networks (DNNs). The MIIL-DNN integrates data in 3 sub-networks for detecting and classifying bully contents from the real time code-mix data. The authors in [15–18] tried for exploring this problem by compiling a global data set of 37,373 unique tweets on Twitter using seven ML models.

This study introduces a spotted hyena optimizer with deep learning driven cybersecurity (SHODLCS) model for OSN. The presented SHODLCS model intends to accomplish cybersecurity from the identification of CB in the OSN. For achieving this, the SHODLCS model involves data pre-processing and TF-IDF based feature extraction. In addition, the cascaded recurrent neural network (CRNN) model is applied for the identification and classification of CB. Finally, the SHO algorithm is exploited to optimally adjust the hyperparameters involved in the CRNN model and thereby resulting in enhanced classifier performance. The experimental validation of the SHODLCS model on the benchmark dataset portrayed the better outcomes of the SHODLCS model over the recent approaches.

2 The Proposed Model

In this study, a novel SHODLCS model has been developed to accomplish cybersecurity from the identification of CB in the OSN. The SHODLCS model involves data pre-processing and TF-IDF based feature extraction. Also, the SHO-CRNN model is applied for the identification and classification of CB. Fig. 1 offers the overall process of the SHODLCS technique.

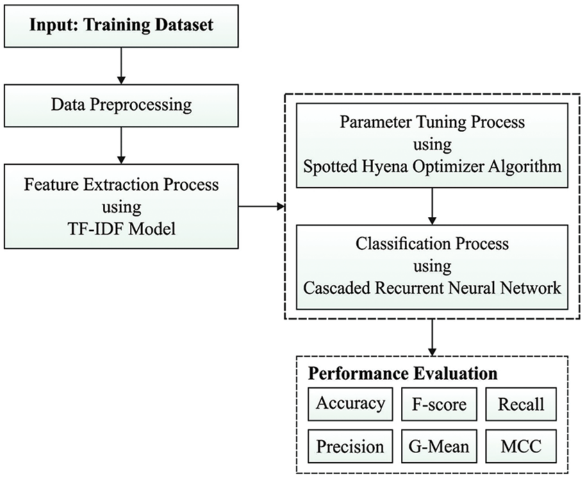

Input: Training Dataset
Data Preprocessing
Feature Extraction Process using TF-IDF Model
Parameter Tuning Process using Spotted Hyena Optimizer Algorithm
Classification Process using Cascaded Recurrent Neural Network
Performance Evaluation
Accuracy
F-score
Recall
Precision
G-Mean
MCC

Figure 1: Overall process of SHODLCS technique

2.1 Data Pre-processing

In this study, data preprocessing take place in different ways such as

- Discard empty rows,
- Convert characters into lowercase,
- Remove punctuation marks,
- Remove special characters,
- Remove numeral,
- Remove stopword,
- Tokenization, and
- Stemmization

2.2 Feature Extraction

Once the data is pre-processed, the term frequency-inverse document frequency (TF-IDF) model gets executed [19]. It is a statistical method which utilizes the occurrence of words as a measure to extract textual features. For a term w_j from the document x_j, whereas their existence is $n_{i,j}$ in x_j, it can compute the term-frequency TF is provided by Eq. (1).

$$TF_{i,j} = \frac{n_{i,j}}{\Sigma_k n_{k,j}} \tag{1}$$

At this point, $\Sigma_k n_{k,j}$ refers the sum of occurrences of a term w_i from the total document set. Afterward, it can calculate the IDF by adopting the logarithm of entire amount of documents separated by the amount of documents with term w_i as in Eq. (2).

$$IDF_i = log\left(\frac{|D|}{|\{i \cdot w_i \in xj\}| + 1}\right) \tag{2}$$

At this time, $|D|$ implies the entire amount of documents, and $\left|\{j : w_j \in x_j\}\right|$ signifies the amount of documents with term w_i. If it can reach the individual TF and IDF values, it can calculate the needed TF-IDF for the term w_i, provided by Eq. (3).

$$(TF - IDF)_{w_i} = TF_{i,j} \times IDF_i \tag{3}$$

2.3 Data Classification Module

Next to feature extraction, the CRNN model is applied for the identification and classification of CB [20]. For a provided dataset $\in \Re^k$, assume that a sequence where length represents k, hence recurrent neural network (RNN) is applied for learning features. This long-term sequence improves the training complexity because the gradient tends to explode or vanish. In order to overcome these shortcomings, one commonly applied methodology is to develop an increasingly complex activation function with the help of gating units namely the gated recurrent unit (GRU) and long short term memory (LSTM) units. In comparison with the LSTM unit, GRU has a lesser amount of variables that could be better for classifying data since it often contains a less amount training instances. The core component of GRU is two gating units, control the data flow within the unit. Rather than utilizing the activation of hidden state for band t is given in the following

$$h_t = (1 - u_t)h_{t-1} + u_t\tilde{h}_t \tag{4}$$

whereas u_t indicates the update gate, that is formulated as

$$u_t = \sigma(w_u x_t + v_u h_{t-1}) \tag{5}$$

In which σ denotes a sigmoid function, v_u indicates a weight vector, and w_u is represent a weight value. Likewise, $\tilde{h}$ is estimated as follows

$$\tilde{h} = tanh(wx_t + V(r_t \odot h_{t-1})) \tag{6}$$

Here, $\odot$ signifies an element-wise multiplication, and r_t represent the reset gate, that is given in the following

$$r_t = \sigma(w_r x_t + V_r h_{t-1}) \tag{7}$$

Especially, we split the spectral sequence x into l sub-sequences $= (z_1,\ z_2,\ \cdots,\ z_l)$, all of the comprises of adjacent spectral band. Moreover, the last sub-sequence represents z_l, the length of other sub-sequences indicates $d = floor(k/l)$, that represents the nearby integer lesser than or equivalent to k/l. Hence, for i-th sub-sequence $z_i, i \in, \{1, 2,\ \cdots,\ l\}$, it includes the subsequent bands. Fig. 2 depicts the structure of CRNN.

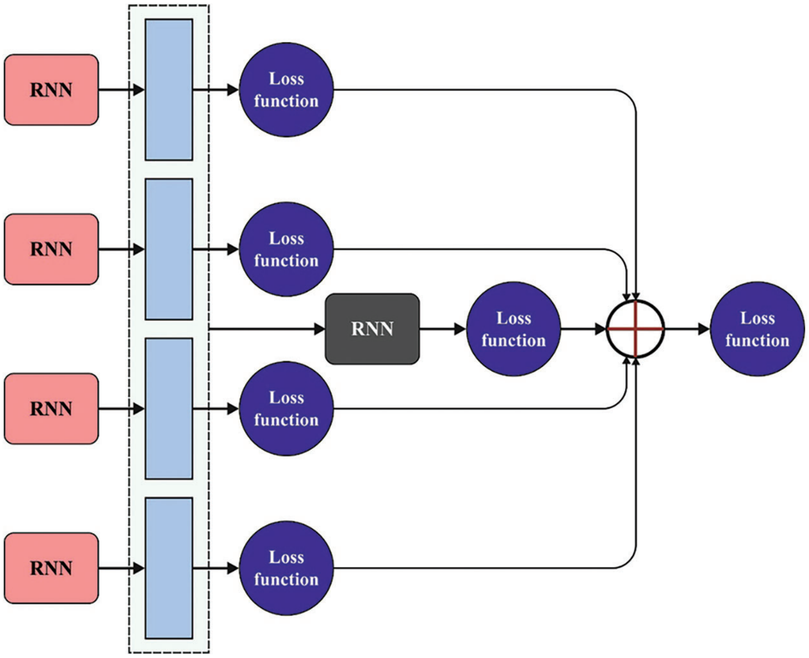


Figure 2: Structure of CRNN

$$z_i = \begin{cases} \left(x_{(i-1)\times d+1}, \ \cdots, \ x_{i\times d}\right), & \text{if } i \neq l, \\ \left(x_{(i-1)\times d+1}, \ \cdots, \ x_k\right), & \text{otherwise.} \end{cases} \tag{8}$$

At that time, we feed each sub-sequences into the initial-layer RNN correspondingly. This RNN has a shared parameter and similar architecture, thereby reducing the amount of variables for training. In sub-sequence z_i, all the bands have an output from GRU. Then, utilize output of the latter band as the last feature depiction for z_i, that is represented by $F_i^{(1)} \in \Re^{H_1}$, whereas H_1 indicates the size of hidden state in the initial-layer RNN. Next, integrates $F_i^{(1)}, i \in \{1, 2, \ \cdots, \ l\}$ with sequence for generating another sequence $F = \left(F_1^{(1)}, \ F_2^{(1)}, \ \cdots, \ F_l^{(1)}\right)$ that length represents l. The sequence is given to the next-layer RNN for learning the complementary data. Like the initial- layer RNN, we utilize the output of GRU at the final time l as the learned feature $F^{(2)}$. In order to attain a classifier outcome of x, then input $F^{(2)}$ is fed to the output layer that size equivalent to the amount of candidate class C.

2.4 SHO Based Hyperparameter Optimization

At the final stage, the SHO algorithm is exploited to tune the hyperparameter related to the CRNN model and thereby results in enhanced classifier performance [21–25]. SHO is stimulated by the social behavior of spotted hyenas. The major phases of the SHO procedure are from the hunting behavior. The mathematical model of the newly established SHO process is thoroughly discussed in the following.

Encircling prey: The mathematically modeling of these behaviors is given as follows:

$$D_h = \left| \ B. \vec{P}(x) - \vec{P}(x) \right| \tag{9}$$

$$\vec{P}(x+1) = \vec{P}_p(x) - \vec{E} \cdot \vec{D}_h \tag{10}$$

whereas $\vec{D}_h$ indicates distance among the prey and spotted hyena, x is the existing generation, $\vec{B}$ and $\vec{E}$ indicates coefficient vector, $\vec{P}_p$ is the location vector of prey, $\vec{P}$ shows the location vector of spotted hyenas. But, $||$ and $\cdot$ indicates the accurate value and vector multiplication symbol, correspondingly.

Now, B and E vectors are estimated in the following equations:

$$B = 2 \cdot \vec{rd}_1 \tag{11}$$

$$\vec{E} = 2\vec{h} \cdot \vec{rd}_2 - \vec{h} \tag{12}$$

$$\vec{h} = 5 - \left(Iteration \ \times \left(\frac{5}{\text{Max}_{Iteration}} \right) \right) \tag{13}$$

Here, $Iteration \ = 0, 1, 2, \ldots, \text{Max}_{Iteration}$

In which $\vec{h}$ is decreased linearly from 5 to 0, $\vec{rd}$ and $\vec{rd}$ vectors represent arbitrary vector within $[0, 1]$.

2) Hunting: The subsequent equation is suggested for hunting method:

$$\vec{D}_h = \left| \vec{B} \cdot \vec{P}_h - \vec{P}_k \right| \tag{14}$$

$$\vec{P}_k = \vec{P}_h - \vec{E} \cdot \vec{D}_h \tag{15}$$

$$\vec{C}_h = \vec{P}_k + \vec{P}_{k=1} + \ldots + \vec{P}_{k+N} \tag{16}$$

Here $\vec{P}_h$ represents the initial finest location of spotted hyena, $\vec{P}_k$ shows another searching agent viz., spotted hyenas, k indicates the location of searching agent, and N describes the amount of spotted hyenas that is estimated in the following:

$$N = count_{nos}\left(\vec{P}_h, \vec{P}_{h+1}, \vec{P}_{h+2}, \ \ldots, \ \left(\vec{P}_h + \vec{M} \right) \right) \tag{17}$$

Now $\vec{M}$ indicates an arbitrary value within [0.5,1], nos represents the amount of solutions, afterward adding $\vec{M}$, and $\vec{C}_h$ indicates a set of N amount of optimum solutions.

Attack prey (exploitation): The mathematical modeling for prey attack is probable for reducing the value of vector $\vec{h}$. The difference in vector $\vec{E}$ is answerable to altered the value in vector $\vec{h}$. The mathematical formula for prey attacking is defined in the following:

$$\vec{P}(x + 1) = \frac{\vec{C}_h}{N} \tag{18}$$

In the equation, $\vec{P}(x + 1)$ saves the optimal solution and updates the position of another searching agent (that is, spotted hyenas).

Searching for prey (exploration): purposefully requires vector B for exploration and offers arbitrary value in iteration method. This technique is useful for avoiding local optimal until final iteration and ending the process afterward fulfilling conditions.

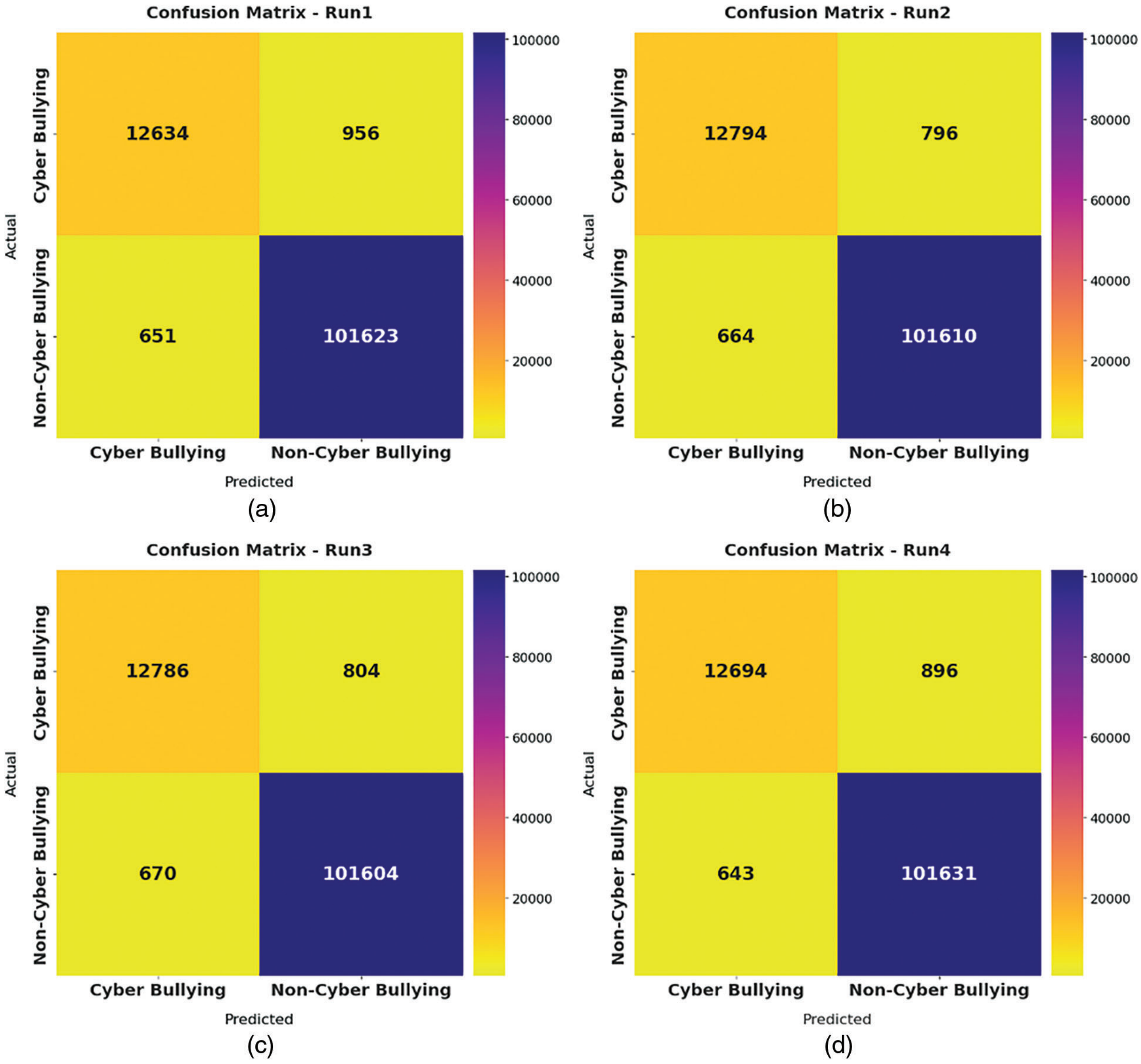
3 Performance Validation

The performance validation of the SHODLCS model is tested using the Wikipedia Attack Dataset [26] which contains 115,864 samples with 13,590 CB and 102,274 non-CB (NCB).

Fig. 3 exemplifies the confusion matrices formed by the SHODLCS model on test dataset. With run-1, the SHODLCS model has recognized 12634 samples into CB and 101623 samples into NCB. Meanwhile, with run-3, the SHODLCS technique has recognized 12786 samples into CB and 101604 samples into NCB.

Moreover, with run-5, the SHODLCS methodology has recognized 12805 samples into CB and 101562 samples into NCB. At the same time, with run-6, the SHODLCS approach has recognized 12858 samples into CB and 101487 samples into NCB.

Tab. 1 and Fig. 4 report the overall classification results of the SHODLCS model under distinct runs. On run-1, the SHODLCS model has offered average $accu_y$, $prec_n$, $reca_l$, F_{score}, Mathew Correlation Coefficient (MCC), and G_{mean} of 98.61%, 97.08%, 96.16%, 96.62%, 93.24%, and 96.11% respectively. Along with that, on run-3, the SHODLCS technique has accessible average $accu_y$, $prec_n$, $reca_l$, F_{score}, MCC, and G_{mean} of 98.73%, 97.12%, 96.71%, 96.91%, 93.83%, and 96.68% correspondingly. Moreover, on run-5, the SHODLCS system has offered average $accu_y$, $prec_n$, $reca_l$, F_{score}, MCC, and G_{mean} of 98.71%, 96.98%, 96.76%, 96.87%, 93.75%, and 96.73% respectively. Furthermore, on run-6, the SHODLCS algorithm has obtainable average $accu_y$, $prec_n$, $reca_l$, F_{score}, MCC, and G_{mean} of 98.69%, 96.76%, 96.92%, 96.84%, 93.68%, and 96.89% correspondingly.



(a) (b) (c) (d)

Figure 3: (Continued)

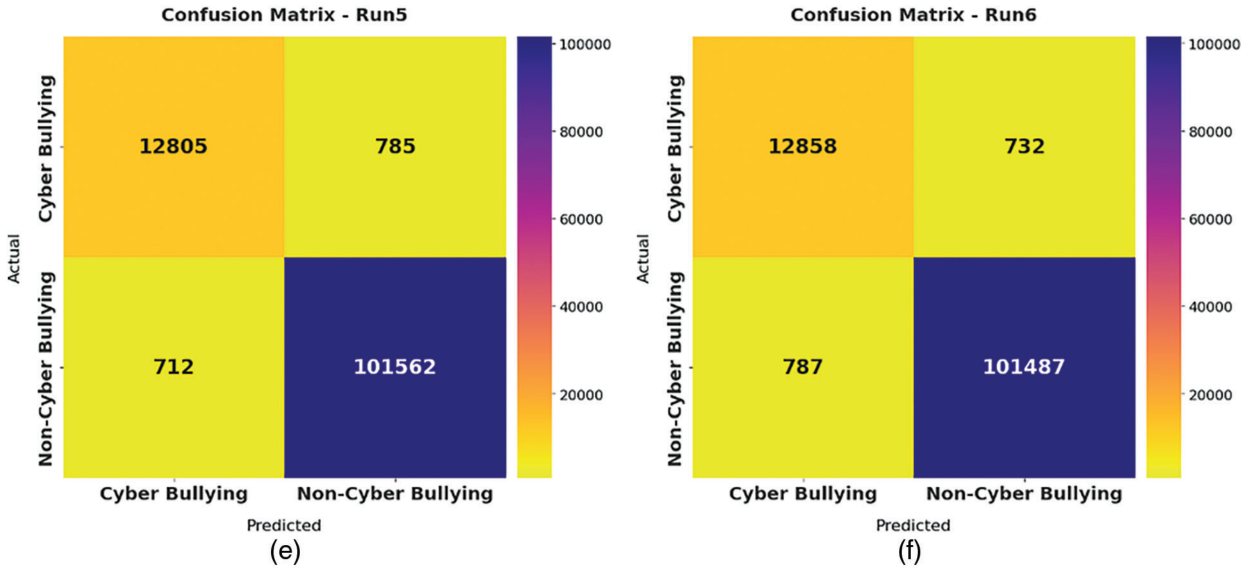


Figure 3: Confusion matrices of SHODLCS technique a) run-1, b) run-2, c) run-3, d) run-4, e) run-5, f) run-6

Table 1: Result analysis of SHODLCS technique with distinct measures and runs

Labels	Accuracy	Precision	Recall	F-Score	MCC	G-Mean
Run-1						
CB	98.61	95.1	92.97	94.02	93.24	96.11
NCB	98.61	99.07	99.36	99.22	93.24	96.11
Average	98.61	97.08	96.16	96.62	93.24	96.11
Run-2						
CB	98.74	95.07	94.14	94.6	93.89	96.71
NCB	98.74	99.22	99.35	99.29	93.89	96.71
Average	98.74	97.14	96.75	96.94	93.89	96.71
Run-3						
CB	98.73	95.02	94.08	94.55	93.83	96.68
NCB	98.73	99.21	99.34	99.28	93.83	96.68
Average	98.73	97.12	96.71	96.91	93.83	96.68
Run-4						
CB	98.67	95.18	93.41	94.28	93.54	96.34
NCB	98.67	99.13	99.37	99.25	93.54	96.34
Average	98.67	97.15	96.39	96.77	93.54	96.34
Run-5						
CB	98.71	94.73	94.22	94.48	93.75	96.73
NCB	98.71	99.23	99.3	99.27	93.75	96.73
Average	98.71	96.98	96.76	96.87	93.75	96.73
Run-6						
CB	98.69	94.23	94.61	94.42	93.68	96.89
NCB	98.69	99.28	99.23	99.26	93.68	96.89
Average	98.69	96.76	96.92	96.84	93.68	96.89

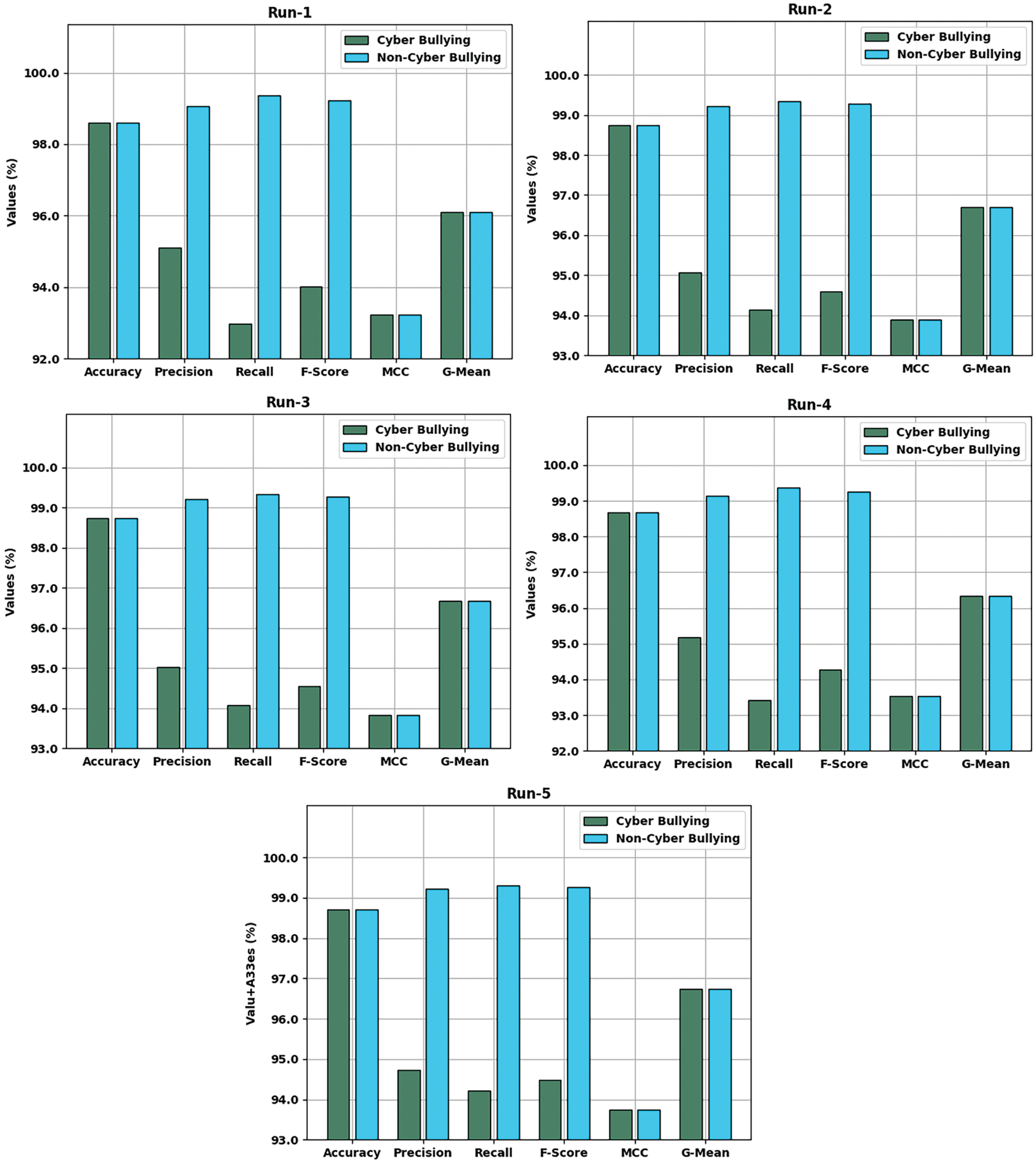


Figure 4: Result analysis of SHODLCS technique with distinct measures and runs

The training accuracy (TA) and validation accuracy (VA) attained by the SHODLCS model on test dataset is demonstrated in Fig. 5. The figure implied that the SHODLCS model has gained maximum values of TA and VA. In specific, the VA seemed to be higher than TA.

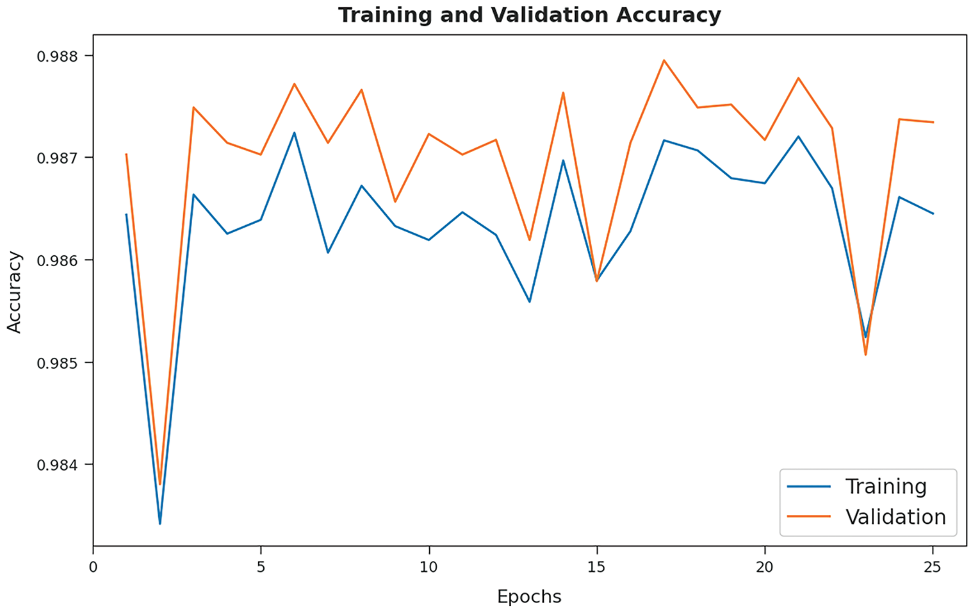


Figure 5: TA and VA analysis of SHODLCS technique

The training loss (TL) and validation loss (VL) achieved by the SHODLCS model on test dataset are established in Fig. 6. The results inferred that the SHODLCS model has been able least values of TL and VL. In specific, the VL seemed to be lower than TL.

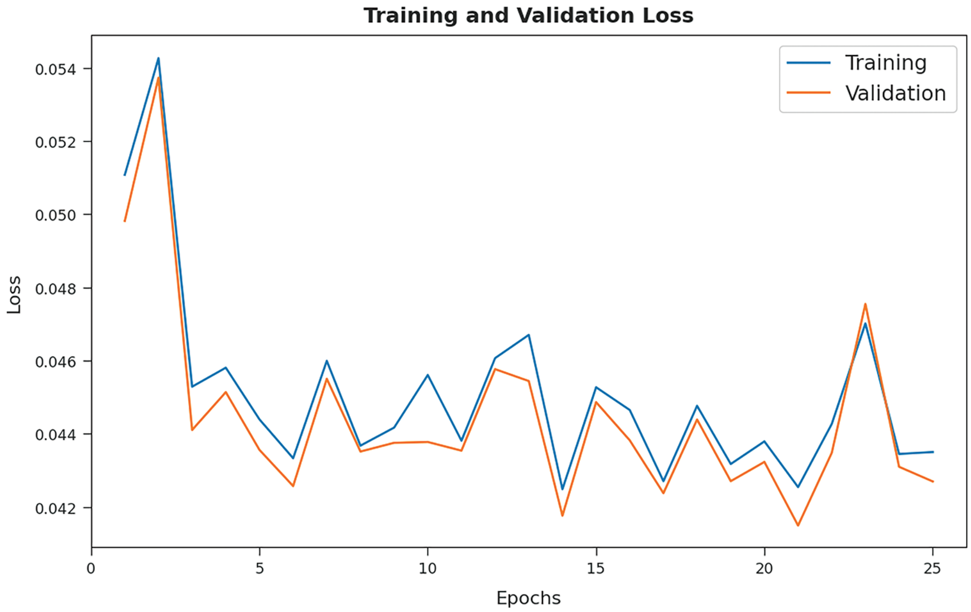


Figure 6: TL and VL analysis of SHODLCS technique

A brief precision-recall examination of the SHODLCS model on test dataset is portrayed in Fig. 7. By observing the figure, it is noticed that the SHODLCS model has accomplished maximum precision-recall performance under all classes.

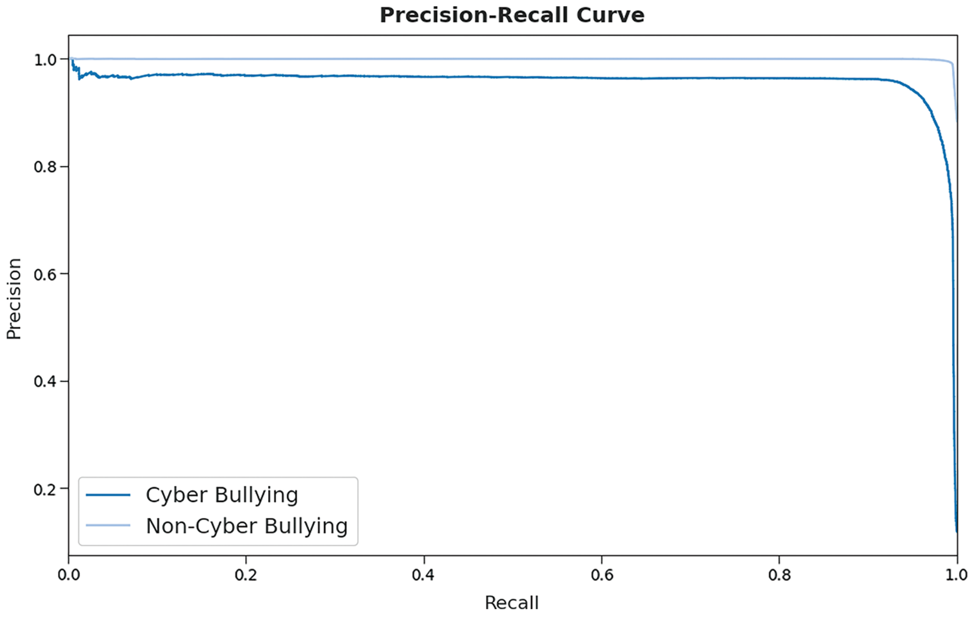


Figure 7: Precision-recall curve analysis of SHODLCS technique

A detailed receiver operating characteristic (ROC) curve investigation of the SHODLCS technique on test dataset is represented in Fig. 8. The results indicated that the SHODLCS model has exhibited its ability in categorizing two different classes such as cyberbullying and non-cyberbullying on the test dataset.

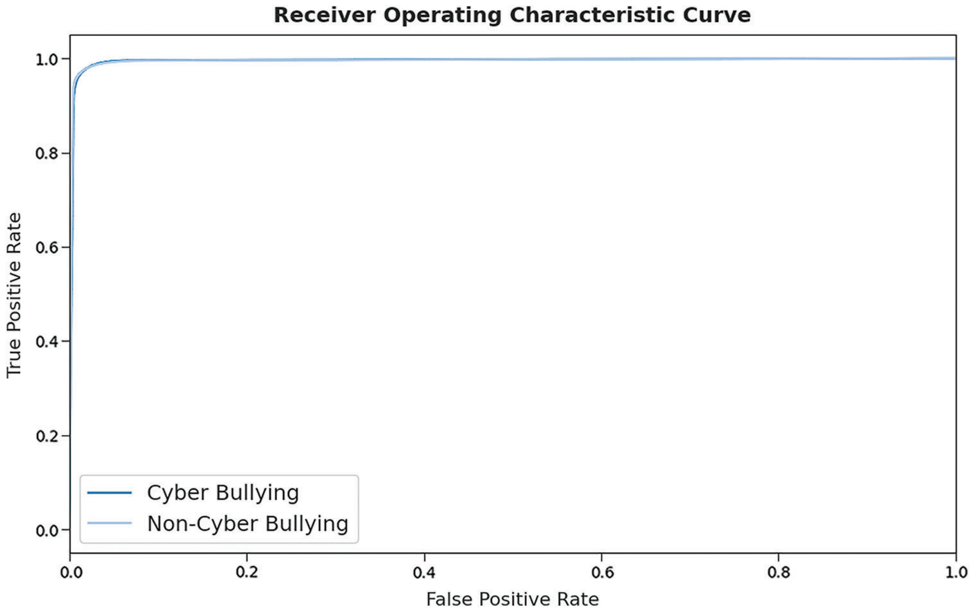


Figure 8: ROC curve analysis of SHODLCS technique

Tab. 2 reports a detailed comparative examination of the SHODLCS model with recent models. Fig. 9 illustrates a brief $prec_n$ and $recal_l$ investigation of the SHODLCS model with existing techniques. The figure reported that the support vector machine (SVM) model has shown least performance over the other methods with minimal $prec_n$ and $reca_l$ values of 95.90% and 94.24% respectively. At the same time, the DL-CNN, RNN-LSTM, RNN-GRU, and RNN-BLSTM models have obtained moderately closer values of $prec_n$ and $reca_l$. However, the SHODLCS model has surpassed existing models with maximal $prec_n$ and $reca_l$ of 97.14% and 96.75% respectively.

Table 2: Comparison study of SHODLCS with recent methods

Methods	Precision	Recall	Accuracy	F-Score
SVM Model	95.90	94.24	95.77	94.39
Deep Learning-CNN	96.02	93.13	95.08	94.50
RNN-LSTM	96.85	93.84	96.55	96.12
RNN-GRU	96.61	93.09	96.09	96.45
RNN-BLSTM	96.29	93.46	94.17	94.14
SHODLCS	97.14	96.75	98.74	96.94

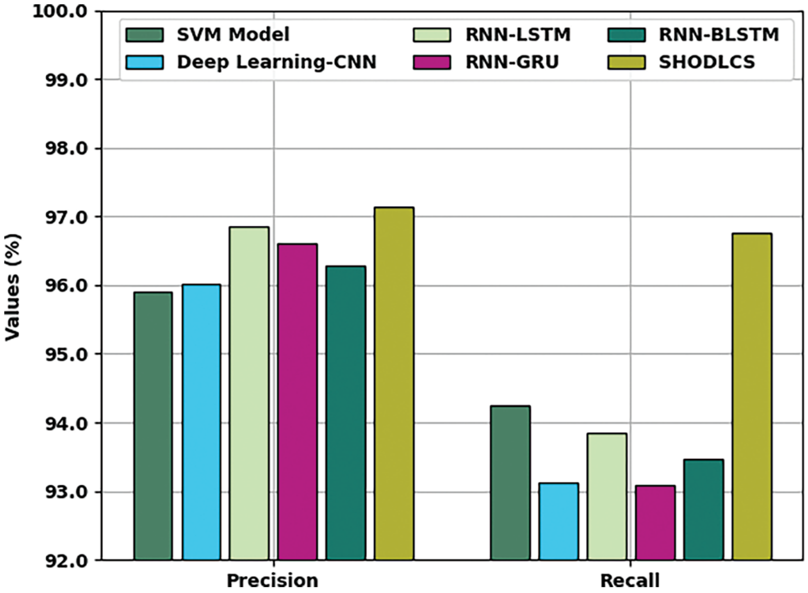


Figure 9: $Prec_n$ and $reca_l$ analysis of SHODLCS technique with existing approaches

Fig. 10 depicts a brief acc_y and F_{score} analysis of the SHODLCS model with existing techniques. The figure reported that the SVM technique has exhibited least performance over the other methods with minimal acc_y and F_{score} values of 95.77% and 94.39% correspondingly. Besides, the DL-CNN, RNN-LSTM, RNN-GRU, and RNN-BLSTM techniques have reached moderately closer values of acc_y and F_{score}. But, the SHODLCS system has outperformed the other methods with maximal acc_y and F_{score} of 98.74% and 96.94% correspondingly. From the results and discussion, it is apparent that the SHODLCS model has shown maximum performance over the other methods.

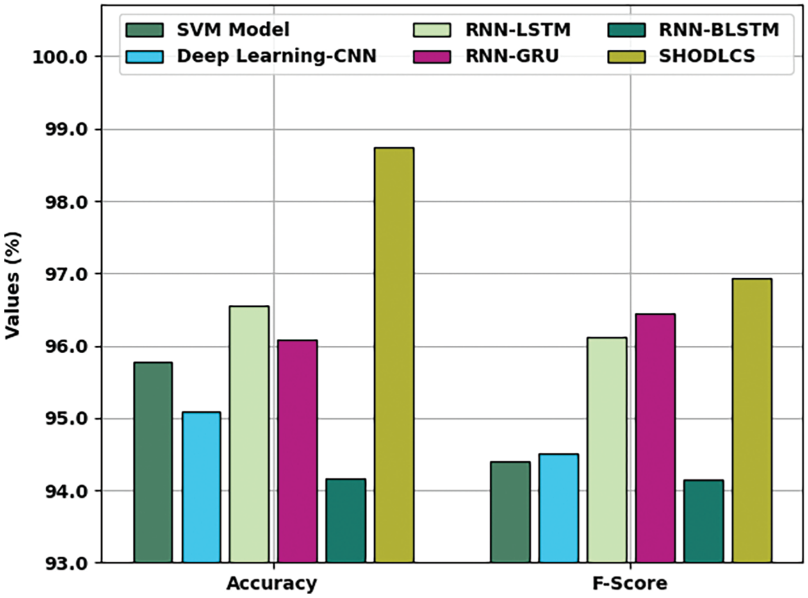


Figure 10: Acc_y and F_{score} analysis of SHODLCS technique with existing approaches

4 Conclusion

In this study, a novel SHODLCS model has been developed to accomplish cybersecurity from the identification of CB in the OSN. For achieving this, the SHODLCS model involves data pre-processing and TF-IDF based feature extraction. In addition, the CRNN model is applied for the identification and classification of CB. Finally, the SHO algorithm is exploited to effectually tune the hyperparameter related to the CRNN approach and thereby results in enhanced classifier performance. The experimental validation of the SHODLCS model on benchmark dataset portrayed the better outcomes of the SHODLCS model over the recent approaches. Thus, the SHODLCS model can be utilized as an effectual tool for CB detection and classification. In future, hybrid DL models can be exploited to improve the overall classification performance.

Funding Statement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R140), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: 22UQU4310373DSR15.

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

References

[1] Y. Fang, S. Yang, B. Zhao and C. Huang, “Cyberbullying detection in social networks using bi-gru with self-attention mechanism,” *Information*, vol. 12, no. 4, pp. 171, 2021.

[2] A. Bozyiğit, S. Utku and E. Nasibov, “Cyberbullying detection: Utilizing social media features,” *Expert Systems with Applications*, vol. 179, pp. 115001, 2021.

[3] M. Dadvar and K. Eckert, “Cyberbullying detection in social networks using deep learning based models,” in *Int. Conf. on Big Data Analytics and Knowledge Discovery, DaWaK 2020: Big Data Analytics and Knowledge Discovery, Lecture Notes in Computer Science book series*, Cham, Springer, vol. 12393, pp. 245–255, 2020.

[4] A. Abdulrahman Albraikan, S. Ben Haj Hassine, S. Mohamed Fati, F. N. Al-Wesabi, A. Mustafa Hilal *et al*., "Optimal deep learning-based cyberattack detection and classification technique on social networks," *Computers, Materials & Continua*, vol. 72, no.1, pp. 907–923, 2022.

[5] H. Rosa, J. P. Carvalho, P. Calado, B. Martins, R. Ribeiro *et al.,* "Using fuzzy fingerprints for cyberbullying detection in social networks," in *2018 IEEE Int. Conf. on Fuzzy Systems (FUZZ-IEEE)*, Rio de Janeiro, pp. 1–7, 2018.

[6] H. Rosa, N. Pereira, R. Ribeiro, P. C. Ferreira, J. P. Carvalho *et al.,* "Automatic cyberbullying detection: A systematic review," *Computers in Human Behavior*, vol. 93, pp. 333–345, 2019.

[7] A. Kumar and N. Sachdeva, "Multimodal cyberbullying detection using capsule network with dynamic routing and deep convolutional neural network," *Multimedia Systems*, vol. 15, no. 1, pp. 1–14, 2021.

[8] C. Iwendi, G. Srivastava, S. Khan and P. K. R. Maddikunta, "Cyberbullying detection solutions based on deep learning architectures," *Multimedia Systems*, vol. 25, no. 1, pp. 1–1, 2020.

[9] M. Alotaibi, B. Alotaibi and A. Razaque, "A multichannel deep learning framework for cyberbullying detection on social media," *Electronics*, vol. 10, no. 21, pp. 2664, 2021.

[10] A. Kumar and N. Sachdeva, "A Bi-GRU with attention and CapsNet hybrid model for cyberbullying detection on social media," *World Wide Web*, vol. 15, no. 1, pp. 1–14, 2021.

[11] N. Lu, G. Wu, Z. Zhang, Y. Zheng, Y. Ren *et al.,* "Cyberbullying detection in social media text based on character-level convolutional neural network with shortcuts," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 23, pp. 2999, 2020.

[12] E. Raisi and B. Huang, "Weakly supervised cyberbullying detection using co-trained ensembles of embedding models," in *2018 IEEE/ACM Int. Conf. on Advances in Social Networks Analysis and Mining (ASONAM)*, Barcelona, Spain, pp. 479–486, 2018.

[13] H. Y. Chen and C. T. Li, "HENIN: Learning heterogeneous neural interaction networks for explainable cyberbullying detection on social media," in *Proc. of the 2020 Conf. on Empirical Methods in Natural Language Processing (EMNLP)*, Dominican Republic, pp. 2543–2552, 2020.

[14] A. Kumar and N. Sachdeva, "Multi-input integrative learning using deep neural networks and transfer learning for cyberbullying detection in real-time code-mix data," *Multimedia Systems*, vol. 32, no. 1, pp. 1–15, 2020.

[15] A. Muneer and S. M. Fati, "A comparative analysis of machine learning techniques for cyberbullying detection on twitter," *Future Internet*, vol. 12, no. 11, pp. 187, 2020.

[16] F. Alrowais, A. S. Almasoud, R. Marzouk, F. N. Al-Wesabi, A. M. Hilal *et al.,* "Artificial intelligence based data offloading technique for secure mec systems," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2783–2795, 2022.

[17] A. A. Albraikan, S. B. Haj Hassine, S. M. Fati, F. N. Al-Wesabi, A. M. Hilal *et al.,* "Optimal deep learning-based cyberattack detection and classification technique on social networks," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 907–923, 2022.

[18] M. A. Hamza, S. B. Haj Hassine, I. Abunadi, F. N. Al-Wesabi, H. Alsolai *et al.,* "Feature selection with optimal stacked sparse autoencoder for data mining," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2581–2596, 2022.

[19] C. Raj, A. Agarwal, G. Bharathy, B. Narayan and M. Prasad, "Cyberbullying detection: Hybrid models based on machine learning and natural language processing techniques," *Electronics*, vol. 10, no. 22, pp. 2810, 2021.

[20] R. Hang, Q. Liu, D. Hong and P. Ghamisi, "Cascaded recurrent neural networks for hyperspectral image classification," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 57, no. 8, pp. 5384–5394, 2019.

[21] G. Dhiman and A. Kaur, "Spotted hyena optimizer for solving engineering design problems," in *2017 Int. Conf. on Machine Learning and Data Science (MLDS)*, Noida, India, pp. 114–119, 2017.

[22] M. N. A. Mhiqani, R. Ahmad, Z. Z. Abidin, K. H. Abdulkareem, M. A. Mohammed *et al.,* "A new intelligent multilayer framework for insider threat detection," *Computers & Electrical Engineering*, vol. 97, pp. 107597, 2022.

[23] R. Gopi, P. Muthusamy, P. Suresh, C. G. G. S. Kumar, I. V. Pustokhina *et al.,* "Optimal confidential mechanisms in smart city healthcare," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 4883–4896, 2022.

[24] A. Muthumari, J. Banumathi, S. Rajasekaran, P. Vijayakarthik, K. Shankar *et al.,* "High security for de-duplicated big data using optimal simon cipher," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1863–1879, 2021.

[25] I. V. Pustokhina, D. A. Pustokhin, E. L. Lydia, P. Garg, A. Kadian *et al.,* "Hyperparameter search based convolution neural network with Bi-LSTM model for intrusion detection system in multimedia big data environment," *Multimedia Tools and Applications*, vol. 13, no. 5, pp. 111, 2021.

[26] E. Wulczyn, N. Thain and L. Dixon, "Ex machina: Personal attacks seen at scale," in *Proc. of the 26th Int. Conf. on World Wide Web*, Perth, Australia, pp. 1391–1399, 2017.