International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I3P123

Volume 74 Issue 3, 336-352, March 2026
© 2026 Seventh Sense Research Group®

Original Article

Detection of Cyber Threats on Social Media using Optimized Sentiment-Aware Deep Learning Models

R. Pushpavalli[1*], Prabhu Rengaramanujam[2], I.Eugene Berna[3], D. Suseela[4], Dilli babu M[5], R.S.Vignesh[6]

[1]*Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamil Nadu, India.*
[2]*Senior Engineer, USA.*
[3]*Department of Artificial Intelligence and Machine Learning, Bannari Amman Institute of Technology, Erode, Tamil Nadu, India.*
[4]*Department of Artificial Intelligence and Data Science, Sri Krishna College of Engineering and Technology, Coimbatore. Tamil Nadu, India.*
[5]*Department of Information Technology, Panimalar Engineering College, Chennai, Tamil Nadu, India.*
[6]*Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, Tamil Nadu, India.*

[*]*Corresponding Author: pushpavallikumarapathy@gmail.com*

Received: 09 August 2025 Revised: 18 December 2025 Accepted: 06 February 2026 Published: 28 March 2026

Abstract - *In the modern age of digital society, the ramping up of cybercrime proves to be a severe issue that causes significant financial losses, emotional pain, and social impairment. Popularization of social media networking sites with possibilities of real-time communications and expressing oneself in society has seen an exponential increase in user content generated, which unfortunately has also led to the flourishing of negative actions like spreading fake news, cyberbullying, phishing, opinion spamming, and identity theft. These emerging threats are a very big threat to cyberspace security, privacy, and trust online, thus requiring smart and aggressive defense. To this end, this study proposes an exhaustive state of the cyber intelligence framework christened DSO-CAM-CDL that would identify/solve fake actions and threat-related sentiments that ensue on social network applications. The model also starts with the application of a new Dolphin-Sparrow Optimization method to acknowledge and pick the most relevant and high-impact features in large social media data. This refined set of features is then returned to the Customized Deep Learner (CDL), capable of doing sentiment analysis and behavioral prediction, using much higher precision and having much better computation speed. In order to further increase resilience and adaptive security, a Convoluted Auto-Encoding Memory (CAM) mechanism is added, which indicates that the system would learn complex patterns and anomalies that are specific to cyber threats. Experimental evaluation that is performed on a standard Twitter data demonstrates that the suggested DSO-CAM-CDL model performs extremely well, with accuracy of 99.1%, precision of 99%, recall of 98.9%, F1-score of 99% and specificity of 98.9%. The evaluation against other traditional classifiers like SVM, Naive Bayes, SVC, and CNN-LDA proves the evident advantage of the proposed model on all the assessment data.*

Keywords - *Cybercrime Detection, Sentiment Analysis, Social Media Security, Feature Optimization, Deep Learning, Auto-Encoding Memory Networks.*

1. Introduction

The fascination with the use of social media opinion research and sentiment mining for security scenarios has grown over time [1]. Social media networks offer useful information for sentiment analysis and opinion mining investigations. Maintaining public security remains a fundamental aspect of an independent nation. The notion of security has evolved to include a variety of fields and areas, notably social, conceptual, fiscal, and geopolitical [2, 3]. Furthermore, the idea of security has grown to include personal welfare and safety, rather than merely national or governmental security. Typically, security pertains to the operations associated with safeguarding a country, establishing, or person against assault and threat, as well as the condition of being joyful and free of danger or concern. Opinion mining, which is also referred to as sentiment analysis, is the study of how people communicate their opinions, feelings, assessments, mindsets, and moods about objects and their attributes in the form of words. The phrases "opinion" and "sentiment" are connected, although there is a minor gap between them. Opinion mining is largely concerned with an individual's actual perspective on something, whereas sentiment refers to a position or thought prompted by an emotion [4-6]. Opinion mining consists of two distinct types of detachment: just one viewpoint and a collection of opinions, whereas the analysis of sentiment is mostly concerned with opinions that illustrate or determine positive or negative sentiment. Figure 1 shows the typical social mining framework in public security.

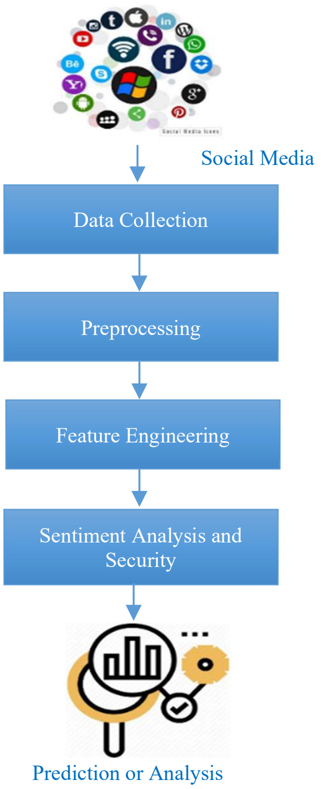

Fig. 1 Overview of the social mining framework in public security

However, the phrases "sentiment analysis" and "opinion mining" are often employed indiscriminately when describing multiple tasks, including opinion extraction, emotion mining, subjectivity analysis, effect analysis, mining operations, item mining, and sentiment evaluation [7]. Sentiment analysis and opinion mining initially served as tools for evaluations of goods, yet they have since been applied to a variety of other tasks such as financial markets, presidential elections, emergencies, medical services, and software development [8, 9]. In the field of public security, sentiment evaluation and opinion analysis have both been used to examine the sentiment and public perception surrounding an event or catastrophe in order to issue public warnings. In a broader sense, sentiment analysis is the examination of the feelings, sentiments, thoughts, and attitudes expressed by individuals towards happenings, issues, and specific crises [10, 11]. Sentiment analysis and opinion mining have been applied in a variety of sectors due to the abundance of sentiment and opinionated data available on social media.

Millions of people have benefited from the universal accessibility and low effort required of distant informal communication platforms like Facebook and Twitter, which have assisted them in maintaining relationships with loved ones. Like many technical revolutions, social networks have limitations as well. Based on security parameters, experts have found that general users of social networking platforms encounter numerous security-related problems. It covers factors such as isolation, lack of safety, and misuse of personal information due to internet threats. As a civilization reliant on technology, the communication network has been extended by including the electronic realm of the internet due to its widespread use. An essential component of social media cybersecurity and monitoring is sentiment analysis. It has proven to be quite useful in social media content analysis, uncovering a variety of security concerns and aiding in the development of effective solutions. The main focus of this study is the application of sentiment analysis in identifying opinion spam, malicious users, fraudsters, and online scammers. In addition, it addresses issues related to data provenance, mistrust of social networking sites, e-commerce security, forecasting of catastrophe relief events, risk evaluation, and other social media safety issues. Sentiment analysis is commonly employed in social media for studying user behavior and how they communicate with other users of the site.

1.1. Problem Statement

Currently, cybersecurity is constantly overflowing with technologies and online platforms in which people from varied backgrounds and knowledge contribute their views and ideas on a wide range of topics/events [12-14]. People often share information in a textual form. Sharing can be accomplished through any social platform, and as a result, people can voice their thoughts using a variety of online tools. This information is valuable in order to comprehend societal and customer opinions towards goods, campaigns, social occurrences, advertisements, firm strategies, and identity monitoring. Many people are uninformed that their ideas can negatively affect national security.

Negative opinions can disrupt a community and lead to divergent opinions among people from other countries, creating a threat to national security. To deal with this problem, researchers and intellectuals have been working hard on sentiment analysis over the past decade and a half. Sentiment analysis examines the sentiments, views, and emotions conveyed in texts targeted at an identifiable topic [15]. Sentiment analysis, also known as opinion mining, mining for thoughts, attitude analysis, or review processing, is the procedure of obtaining and grouping viewpoints, feelings, and perspectives from textual input. Opinion mining or sentiment analysis may be implemented to attain a variety of goals, including determining public opinion towards movements in politics, measuring consumer happiness, predicting movie revenue, and so on [16, 17]. Yet, the currently available opinion mining technology, which involves the use of a machine learning approach, is ineffective in determining and identifying people's thoughts and feelings in cyberspace.

1.2. Research Gap

Most of the Intelligence-based approaches have been developed to ensure the security of social media networks [18, 19]. However, past techniques struggle with the normal difficulties of computing cost in categorization, long forecast times, and inefficiency. Therefore, this study attempts to build a novel algorithm for maintaining security in social media networks.

1.3. Objectives of the Study

The main contributions of this work are listed below:

- To develop a novel hybrid Dolphin integrated Sparrow Optimization (DSO) technique that is used to identify important aspects from available social data.
- To introduce a Convoluted Auto-encoding Memory (CAM) model with a Customized Deep Learner (CDL) algorithm to improve the security of social networks with high efficiency, accuracy, and effective sentiment prediction.
- To evaluate the performance of the proposed DSO-CAM-CDL model against predominant metrics like accuracy, precision, FPR, F1-score, recall, and so on, to assess the effectiveness of the model.

1.4. Organization

The paper is organized into different sections: Section 2 provides a full literature overview on sentiment analysis, opinion mining, and security. It also examines the issues and limitations connected with conventional techniques. Section 3 provides a thorough explanation of the proposed security framework for defending social networks, including an overview model, algorithms, and descriptions. Section 4 compares the performance results and outcomes of the suggested model with various parameters. Finally, Section 5 summarizes the whole research endeavor, including the findings, outcomes, and future work.

2. Literature Review

This section presents the detailed literature review in the field of social data analysis, opinion mining, and security, where the problems and challenges behind the conventional methodologies are discussed. Deep learning has been employed to evaluate a wide range of real-world applications. Classification tasks require labelled datasets since they are capable of helping find data trends. Suhaimin et al. [20] investigated the recent trends, challenges, and some possible future directions for ensuring public security in social networks. This review discovered potential problems such as a lack of multi-class and distinct level examination methods, inadequate access to public security data, ineffective modelling on the basis of interval service, an absence of backing methods to deal with variations in languages, and restricted data accessibility. Sharma et al. [5] performed a detailed investigation to examine the different types of methodologies used for sentiment analysis and data security in social networks. Moreover, the authors discussed the major effects of adopting machine learning techniques in the field of social media security, which includes maximum entropy, Bayesian models, hidden markov models, cross-association, meta-modals and other forms of neural networks. In addition, different types of data including amazon user data, hotel review, stock market, restaurant data, and weibo data have been considered into account for analysis.

Alshaikh et al. [21] provided a conceptual view of the privacy and security issues in social media networks. Rahman et al. [22] developed a multi-tier sentiment analysis framework based on a supervised learning algorithm for social networks. This study looked at pre-processing approaches and machine learning models for categorizing sentiments across multiple categories. To improve effectiveness, a multi-layer classification model has been developed. Due to its similarity to social networking data, the movie reviews dataset has been used for deployment. Bengesi et al. [23] utilized a large dimensional dataset for analyzing the polarity of public opinion using tweets on Twitter. Previous research on monkeypox studies revealed that the majority of the data obtained for the application was confined to the original verified epidemic cases of the virus. They suggest that the circumstances surrounding monkeypox have altered due to the number of instances and general views expressed on online platforms. As a result, it is critical to conduct an analysis of prior instances.

Taherdoost et al. [24] did a thorough assessment of the literature to discover the primary consequences of using AI in sentiment analysis. Sentiment analysis determines how an individual and a customer feel about an identifiable subject matter. An expressive style reflects their opinions or emotions. Several algorithms have recently been created to interpret, anticipate, and determine feelings derived from textual information, such as products or consumer reviews. Sentiment analysis can significantly help with polarity recognition. Trillo et al. [25] introduced a large-scale group decision-making tool for sentiment analysis and opinion mining. The suggested approach determines the tenacity and optimism exhibited by the subject matter experts through their remarks during the debate. Sentiment analysis might be employed to attain this objective. This allows us to determine the level of positivity and hostility among the experts in the field. To begin, they employ the bag-of-words model to rate experts comments in accordance with the way they act and positive outlook. Saura et al. [7] looked into the privacy and security concerns in social networks. To ensure a successful sentiment analysis, textural analysis is used in this study's topic modelling. Shaik et al. [26] carried out a thorough study of the literature in the opinion mining and sentiment analysis fields. The main implications of using AI approaches for sentiment analysis in the education sector were covered by the writers of this research. A system for learning management is essential for providing both online and offline learners access to course materials and tracking their participation. Boukabous et al. [27]carried out a thorough assessment of the literature to look at the most recent learning-based prediction techniques for social network security and sentiment analysis. Because of the popularity of social media and its ease of use, authors have an interest in sentiment or opinion analysis from communications on social media that offers the most up-to-date and thorough information and trends.

Zucco et al. [28] carried out a thorough investigation of the various techniques and resources used in social network sentiment analysis. For sentiment prediction tasks, a number of data preprocessing, feature extraction, selection, and classification strategies are examined in this work. Jain et al. [29] carried out a thorough analysis to look at the security and privacy concerns in social media networks. Unlike techniques for sentiment analysis, various researchers have made reviews on different types of bio-inspired optimization techniques. Being different and advanced, we have reviewed the Particle Swarm Optimization (PSO), FireFly Optimization (FO), and Water Wave Optimization (WWO) that are predominant in improving the efficacy in solving difficult optimization problems [31-33].

Apart from these algorithms, some of the nature-inspired algorithms are reviewed as well, including Horse Herd optimization, Rainfall optimization, and Great Salmon Run optimization algorithms. Analyzing their advantages, limitations, and method of implementation, a novel Dolphin integrated Sparrow Optimization (DSO) is proposed in this approach.

Park and Kwon [34] proposed a hybrid detection framework integrating textual similarity analysis with community detection. Tested on the Twitter platform, an improved accuracy of 35% is encountered. Similarly, Marinho and Holanda [35] presented an end-to-end NLP model for the identification of profile emergency cyber-threats in Twitter. A F1-score of approximately 77% with a false alarm rate of 15% is observed as an outcome. Fang et al. [36] introduced a multi-task 1D-CNN + BiLSTM approach for performing cyber-threat detection. A 5-fold cross-validation technique was performed for evaluation, with 96.4% in F1-score. Zhao et al. [37] introduced “TIMiner” as an automated CTI extraction framework that categorizes CTI items and IOCs from social data. A domain-recognizer accuracy of 84% and IOC extraction accuracy of 94% is attained. Finally, Sufi et al. [38] provided a comprehensive survey of social-media-driven cyber-threat intelligence models and proposed a 12-block ETW/index system for threat indexing from Twitter.

Several of the most serious risks associated with social media are examined in this overview, including phishing, malware, cyberbullying, cyber espionage, cyber grooming, spam, and many more [39]. This study of the literature finds that earlier studies created a number of prediction techniques for security and sentiment analysis in social networks, as shown in Table 1. However, they face particular difficulties with greater computing load, longer processing times, reduced precision, and decreased efficiency. Thus, the goal of this research project is to apply new intelligence algorithms to provide a revolutionary security framework for social networks.

Table 1. Overview of existing research and their contribution

Author(s)	Research Focus	Key Contributions
Suhaimin et al. [20]	Public security challenges in social networks	Identified gaps such as a lack of multi-class methods, limited data access, language variation issues, and inadequate modelling techniques.
Sharma et al. [5]	Sentiment analysis and data security methods in social media	Reviewed ML techniques (Bayesian, HMM, neural networks, etc.) and analyzed multiple datasets, including Amazon, hotel reviews, stock market data, and Weibo.
Alshaikh et al. [21]	Privacy and security issues in social networks	Provided a conceptual overview of major privacy and security concerns in social media.
Rahman et al. [22]	Multi-tier sentiment classification in social networks	Developed a supervised multi-layer classification framework using pre-processing and ML models, validated with movie review data.
Bengesi et al. [23]	Public opinion polarity analysis using Twitter data	Analyzed large-scale tweets; emphasized the need to study evolving perspectives in contexts like monkeypox beyond initial outbreak data.
Taherdoost et al. [24]	AI applications in sentiment analysis	Conducted an extensive review of algorithms for interpreting and predicting textual sentiments, highlighting polarity detection.
Trillo et al. [25]	Group decision-making with sentiment and opinion mining	Proposed a tool using bag-of-words to measure positivity/negativity and expert attitudes during deliberations.
Saura et al. [7]	Security and privacy issues in social networks	Used textual analysis and topic modelling to support sentiment analysis related to privacy/security.
Shaik et al. [26]	Sentiment analysis in the education sector	Reviewed AI-based sentiment analysis approaches supporting learning management systems.
Boukabous et al. [27]	Prediction techniques for social network security and sentiment	Surveyed recent learning-based predictive models for security and opinion analysis on social platforms.

	analysis	
Zucco et al. [28]	Methods and tools for social network sentiment analysis	Reviewed preprocessing, feature extraction, and classification techniques for sentiment prediction.
Jain et al. [29]	Privacy and security challenges in social media	Provided a comprehensive review of issues in social network security
Park and Kwon [34]	Hybrid detection framework	The approach attained an improved accuracy by 35%.
Marinho and Holanda [35]	Presented an end-to-end NLP model	An F1-score of approximately 77% with a false alarm rate of 15% is seen.
Fang et al., [36]	Introduced a multi-task ID-CNN + BiLSTM model	Attained an F1-score of 96.4% in a 5-fold cross-validation approach.
Zhao et al., [37]	Introduced "TIMiner" as an automated CTI extraction framework	A domain-recognizer accuracy of 84% and IOC extraction accuracy of 94% is observed.

2.1. Limitations of Existing Study and Research Works

Through evaluation of previous literature works, the following research gaps or limitations are observed:

1. Existing models focus on a binary classification approach instead of multi-class security threat levels.
2. Most of the researchers have analyzed social media data without addressing privacy concerns, making them susceptible to ethical challenges.
3. Restricted access to real-time public security and sentiment data limits the reliability and generalizability of findings.

3. Proposed Methodology

This section offers a comprehensive explanation of the security architecture - DSO-CAM-CDL model and its detailed operation. This research work's original contribution is the use of cutting-edge algorithms to forecast user opinions and ensure security. The open-source social media dataset has been utilized in this framework for system analysis and design, with the first step of preprocessing and normalization operations being completed to enhance the quality of the data. Rigorous pre-processing is used, where the missing values in numerical features are handled using median imputation to prevent skewness, and textual data with negligible missing values are eliminated. The outliers are identified through Z-score and IQR methods, and the anomalies are flagged using Isolation Forests and the Local Outlier Factor (LOF) approach for preserving meaningful patterns.

The best subset of features from the provided data is chosen for the feature analysis using the innovative Dolphin integrated Sparrow Optimization technique, which guarantees an accurate classification. In the proposed approach, a mix of raw and engineered features is employed to detect spammers effectively. These include user activity metrics like posting frequency, time gaps between posts, and burstiness. Alongside, the engagement score derived from weighted likes, shares, and comments helps in distinguishing artificial amplification and organic interactions. Here, the Customized Deep Learner algorithm is used to do sentiment prediction. Based on selected features, the classifier model accurately predicts users' opinions. Therefore, in order to ensure higher security, the Convoluted Auto-encoding Memory model has been employed to forecast the anomalies from the social data. This work's novel idea is that it uses special approaches to achieve security and sentiment analysis goals in a single framework.

This work uses the Customized Deep Learner model for sentiment analysis and prediction, which incorporates the features collected from the earlier phase to make precise forecasts regarding users' views. This model merges convolutional neural network models with recurrent neural network models, incorporating Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) architectures in combination with Convolutional Neural Networks (CNN). In this architecture, GRU simplifies the LSTM structure by combining input and forget gates into one update gate while also merging the cell state together along with the hidden state into only one hidden state. The CDL algorithm first handles the input with an RNN layer. This layer collects the data sequence and feature representation. Then, the output from this RNN layer is taken and put into a CNN layer. The role of this CNN layer is to look at all data, noticing important pairs of characteristics within it. It combines both models' abilities: CNN can find significant parts in ordered word phrases, while RNN can remember the order of words. The CDL algorithm uses these complementary benefits to optimize the data learning process, effectively doing sentiment prediction by this complex categorization method. This algorithm is important for improving sentiment analysis and prediction. It helps to identify internet scammers, opinion spammers, malevolent users, and fraudsters. The Dolphin integrated Sparrow Optimization technique finds the best feature set for the CDL algorithm.

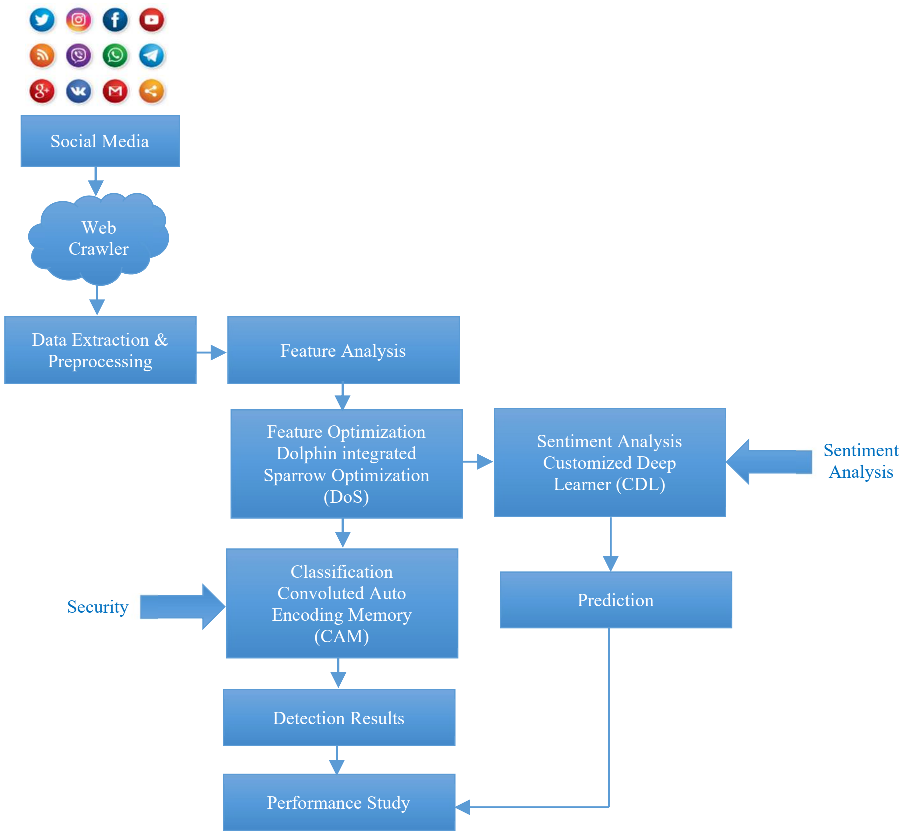
Social Media
Web Crawler
Data Extraction & Preprocessing
Feature Analysis
Feature Optimization Dolphin integrated Sparrow Optimization (DoS)
Sentiment Analysis Customized Deep Learner (CDL)
Sentiment Analysis
Security
Classification Convoluted Auto Encoding Memory (CAM)
Prediction
Detection Results
Performance Study

Fig. 2 Flow of the proposed DSO-CAM-CDL model

This is very important to discover the small emotional signals that scammers use, and the algorithm's arrangement is aiming for high precision and recall rates. It makes sure sentiments are classified correctly and finds relevant instances while lessening false positives. The sentiment predictions created by the CDL algorithm get combined with the CAM model, improving social network safety even more.

The DSO-CAM-CDL model works to make social networks more secure. It combines optimization methods using Dolphin integrated Sparrow Optimization technique, deep learning algorithms with Convoluted Auto-encoding Memory model, and sentiment analysis ability from Customized Deep Learner. The Dolphin integrated Sparrow Optimization technique helps to find the correct feature sets for identifying malicious activities such as internet scams and opinion spamming. The Convoluted Auto-encoding Memory model improves security by precisely recognizing patterns of fraudulent behavior, and the Customized Deep Learner algorithm does sentiment analysis to forecast user opinions and feelings accurately. The model, by being proactive, lets social media platforms take security actions quickly. These include things like moderating what is posted on the platform and checking if users are who they say they are. Such steps help to decrease how far harmful content spreads and protect people from online dangers.

3.1. Dolphin Integrated Sparrow Optimization (DSO) Method for Feature Analysis

In the proposed architecture, feature analysis is conducted using the innovative hybrid methodology, DSO, which considerably selects the optimal subset of features from the given data. The proposed DSO offers advantages over the previous optimization algorithms, namely: It is computationally efficient, converges quickly, requires little processing time, and is easy to apply. It is an adjustment to a brand-new figurative algorithm inspired by dolphin and sparrow behaviors. The searching and anti-predation habits of the dolphin and sparrows communities serve as a source of inspiration for the illustration of DSO. The application and discovery of the optimization space for searching are somewhat improved in lieu of applying the proposed DSO. When compared to other standard techniques, the proposed DSO performs better in terms of searching precision, uniformity, speed of convergence, and avoiding local ideal value. The primary method of implementing the DSO is by simulating the biological traits and lifestyle choices seen in the actual dolphin predatory system. The following is a list of the steps that make up this algorithm:

- Determination of echo location
- Cooperation & labor separation
- Information sharing

Like other very small birds, the sparrow has a strong sense of memory and is extremely perceptive. There are two kinds of hostage house sparrows: creators and scavengers. The following guidelines have been used in keeping with the previous illustration of the sparrows.

- Manufacturers typically have high energy levels and provide all borrowers with digging zones or bearings.
- Individuals start chirping as alarming indicators as soon as the sparrow recognizes the hunter. The producer is required to relocate all staff members to a safe area if the security risk is greater than the alert value.
- All sparrows have the potential to become breeders as long as they search for food. The share of scroungers and builders in the overall population does not change.
- Producers tend to the sparrows that are the busiest first. A tiny group of individuals would attempt to go to locations in order to refuel and survive because they were starving.
- Scroungers hunt for the best feed provider they know that provides the best food. Scavengers, on the other hand, search for food to proliferate, and some individuals go after those who produce food sources. In our attempt at recreation, they should be searching for food with virtual spades.

Algorithm 1 – DSO-based Feature Analysis

Input: Preprocessed social data;

Output: Selected subset of features;

Step 1: Initialize the set of population and fitness value for the dolphin swarms as shown below:

$$\mathbb{D} = \{\mathbb{D}_1, \mathbb{D}_2 \ldots \mathbb{D}_N\} \tag{1}$$

$$\text{ꞙ}X = \{\text{ꞙ}X_1, \text{ꞙ}X_2 \ldots \text{ꞙ}X_N\} \tag{2}$$

Where, $\mathbb{D}$ – set of dolphin population and $\text{ꞙ}X$ – Fitness value;

Step 2: //Look Phase

$$\mathcal{E}_{ijh} = \mathrm{Fit}\,(\mathbb{D}_i + \mathcal{Q}_{jh}) \tag{3}$$

Where, $\mathcal{E}_{ijh}$ - Fitness of the dolphin, $\mathcal{Q}_{jh}$ is the phase value;

Step 3: Compute $\text{ꞙ}Y$ using the following equation:

$$\text{ꞙ}Y = \{\min\mathcal{E}_{1jh}, \min\mathcal{E}_{2jh} \ldots \min\mathcal{E}_{Njh}\} \tag{4}$$

Where, $\text{ꞙ}Y$ – updated fitness;

Step 4: Calculate $\mathfrak{F}(s)$ using the following equation:

$$\mathfrak{F}(s) = \begin{cases} \text{ꞙ}Y_i \quad \text{if } \text{ꞙ}Y_i < fX_i \\ \text{ꞙ}Y_i, \exp\left[-\mathrm{Fit}(X_i) - \frac{\mathrm{Fit}(Y_i)}{M} > r[0,1]\right] \\ \text{ꞙ}X_i \quad \text{Otherwise} \end{cases} \tag{5}$$

In the above equation, $\mathfrak{F}(s)$ is the discovery of a suitable head;

Step 5: //Call Phase

$$\mathcal{J}_{ij} = \begin{cases} [\frac{\mathfrak{d}\mathfrak{d}_{ij}}{\mathfrak{V}\times\mathfrak{X}}] & \text{if} \text{ꞙ}X_i < fX_i \& \mathcal{J}_{ij} > [\frac{\mathfrak{d}\mathfrak{d}_{ij}}{\mathfrak{V}\times\mathfrak{X}}] \\ \mathcal{J}_{ij} & \text{Otherwise} \\ \mathcal{J}_{ij} & \text{Otherwise} \end{cases} \tag{6}$$

Where, $\mathcal{J}_{ij}$ – Sparrow population, $\mathfrak{X}$ – speed, and $\mathfrak{V}$ – Acceleration;

Step 6: //Reception Phase

$$\text{ꞙ}Y_i = \begin{cases} \text{ꞙ}X_i & if \text{ꞙ}X_i < fX_i \& \mathcal{J}_{ij} = 0] \\ \text{ꞙ}X_i & Otherwise \\ \mathcal{J}_{ij} & Otherwise \end{cases} \tag{7}$$

Step 7: //Predation Phase

Determine the value of $\mathfrak{d}X_i$ and $\mathfrak{d}XY_i$ based on the following models:

If $\mathfrak{d}X_i \leq G$

$$K_1 = \left(1 - \frac{2}{2}\right)\mathfrak{d}X \tag{8}$$

Else

$$\mathfrak{d}X_i \geq \mathfrak{d}XY_i \tag{9}$$

$$T_{ij}^{h+1} = T_{ij}^{h} + X \times \left(\frac{|T_{ij}^{h} - t_{wst}^{h}|}{(\mathfrak{F}_i - \mathfrak{F}_s) + \mathfrak{h}}\right) \tag{10}$$

End if;

Where, K_1 – Encompassing sweep, T_{ij}^{h+1} – updated position and t_{wst}^{h} - worst value;

Step 8: Update the fitness value $\text{ꞙ}X_i$;

Step 9: End while;

Step 10: Return the best optimal value X_i as the output;

Finally, the obtained optimal value can be used to pick the most required features for prediction operations.

3.2. Customized Deep Learner (CDL) Model for Sentiment Analysis

The proposed research uses the CDL model for sentiment analysis and prediction, which uses the features gathered from the earlier phase to accurately forecast users' opinions. Convolutional and recurrent neural network models are merged to form this sort of model. Both the Gated Recurrent Unit and Long Short-Term Memory with CNN models are mentioned in this architecture concept. The input and forget gates on an LSTM are put together into an update gate by GRU, which stands along with the addition of a reset gate. Furthermore, GRU creates a single hidden state by fusing the cell state and the hidden state, two LSTM states. To gain insight into the feature representation and data sequence, the input is initially processed using the RNN layer. The CNN layer continues to examine the data for pairs of significant characteristics using the output from the RNN layer as input. Each and every one of the common models offers benefits.

Whereas CNN can pick significant elements of ordered word phrases, RNN is more concerned with word order. Thus, it is anticipated that these benefits will optimize the process of data learning.

The proposed method efficiently performs sentiment prediction by utilizing this categorization technique. The CDL predicts better because it uses advanced neural network methods to study intricate social media data. It combines the strength from RNNs, GRUs, and LSTM networks along with CNNs. The RNN layer is in charge of understanding time-based connections as well as word sequences, which are crucial for understanding context very well. The CNN layer searches for local patterns and word phrases in the text that demonstrate certain feelings. The CDL model, its features sharpened by the DSO method, focuses on the most relevant information. This reduces noise and improves precision. Additionally, feature usage optimization enhances learning efficiency, leading to more accurate sentiment predictions. Moreover, it increases precision and recall while reducing false positives, ensuring that genuine users are not incorrectly identified as fake ones. Furthermore, in the CAM model as well, the CDL's forecasts are used. This adds more to the security system by aiding in recognizing and managing dangers from swindlers and dangerous users.

3.3. Convoluted Auto-Encoding Memory (CAM) Model for Security

The other objective of this work is to ensure the security of social networks with the use of the CAM model, which is used to identify anomalies in the network by analyzing the features of data. It uses a layer of flattening to convert the multi-dimensional latent field representation that the decoder subnet produces into a vector form, which is then fed through an MLP-based classifier. Two fully-connected layers, with a capacity of up to (or precisely), make up an MLP network design. Both levels of this model use the function that activates ReLU, and the final step in a neural network's processing of information is when the output layer generates a final decision. It is possible to keep gradient values calculated by back propagation during network training and sustain long-term temporal connections among inputs by considering the usage of memory cells (units) containing triple regulating gates for LSTMs structures.

When compared to other existing classification algorithms, the proposed CAM offers the main benefits of a simple architecture for learning, low time for training and validation, and high prediction accuracy. The CAM model is mainly developed for improving security by using intelligent deep learning methods to find and lessen dangers on social networks. It can recognize harmful activities like internet scams, opinion spamming, or fake behavior through studying patterns and irregularities in data from social media sites with great precision. The special structure of convolutional auto-encoding in CAM makes it good at capturing detailed relationships and understanding within the data. This helps to spot subtle signs that indicate a bad intention more effectively. Additionally, the CAM model functions in real-time. This ability to react straight away to security risks as they happen will improve the general safety level of social networks and protect users from possible dangers.

The CDL algorithm assists in making predictions better by enhancing feature selection. DSO model, this CDL algorithm understands and arranges features that are very helpful for doing prediction tasks - it focuses on these optimized characteristics to make sentiment predictions more accurate and quicker. The most significant characteristics that have been chosen for the CDL model are crucial in enhancing its performance and usefulness. As the CDL algorithm focuses more on these key features, it becomes better at capturing important signals and patterns within data, which leads to more accurate sentiment predictions. The chosen features also help in decreasing noise and repetition present in data, improving the model's effectiveness and capacity for scaling up. Usually, the characteristics of the CDL model are chosen to make its performance better and enhance how it does sentiment analysis. The CDL algorithm is significant for security because it can expose and examine sentiment patterns that could indicate harmful or dishonest actions. If the algorithm can forecast sentiment precisely, it might identify activities such as phishing attempts, social engineering attacks, or deceit schemes that are potentially dangerous for users on social networks. Furthermore, by incorporating sentiment analysis along with other safety features like anomaly detection and threat information gathering, we can enhance our overall security system to protect users from cyber dangers and bad actions.

4. Results and Discussion

The performance of the proposed and traditional prediction approaches for sentiment analysis and social network security is compared and validated in this section. To ensure reproducibility, the model is implemented and evaluated in a well-defined computational environment. A system with an Intel Core i7/i9 processor with 32GB RAM storage, and NVIDIA RTX with 10GB VRAM is used for DL training of the model. Regarding the software specifications, Python 3.8, including libraries like TensorFlow 2.8, Keras, Pytorch 11.1, and NLTK for language processing tasks, is used. For the optimization of the DSO algorithm, NumPy and SciPy are employed.

Table 2 provides a description of the open-source, large-dimensional Twitter dataset that is used for this assessment. Usually, a dataset from Twitter includes many kinds of data that are taken from the Twitter platform. This reflects the varied aspects of social media interactions. A basic type of such dataset is text-based data, which mainly consists of tweets made by users on Twitter. These tweets can have various types of content, from opinions and news updates to personal stories. Additionally, data from Twitter can contain information about the user's profile. This gives a look into the characteristics and groupings of Twitter users, along with network data that shows how complex connections between them are through relationships. They also help in understanding how people behave on social media within its ever-changing environment.

Table 2. Twitter dataset description

No of threats	No of non-threats	Total
1003 - 1st training	-	1003
1003 - 2nd training	1237	2240
100 - Testing	100	200
1103 - Threat	1337	2440

The model is verified by checking its results against ground truth data, usually through a process of learning and examination. The model starts with training on a marked dataset where the correct sentiment or classification for each example is given. This trained model then gets assessed using different parameters, including precision, recall, F1-score, and Area Under the ROC Curve (AUC). For this evaluation, we look at how well the model predicts positive and negative instances while also balancing between true positive cases and false ones.

The proposed model's performance is measured by recall, accuracy, precision, rate of false prediction, and F1-score. Recall, another name for sensitivity, calculates how well the model correctly identifies actual positive instances out of all positive instances in the dataset. In this instance, recall becomes very important because it shows the model's capacity to capture every single case of malicious activity, like internet scams or fraudulent behavior; this reduces false negatives and guarantees a complete identification of threats. However, accuracy calculates the total correctness of the model's predictions by comparing how many instances were predicted correctly to the total number of instances in the dataset. It gives a general view of performance, but it can be affected by class imbalance. F1-score, which is the harmonic average between precision and recall, works as an equal measure that takes into account both false positives and false negatives. This gives a more complete assessment of how well our model can identify malicious activities while keeping incorrect classifications as low as possible. By looking at many evaluation metrics, the method ensures strong evaluation performance for making knowledgeable choices about using it. The measurements that indicate a model's superiority in sentiment analysis and security tasks are accuracy, precision, recall (sensitivity), F1-score, and area under the ROC curve. A better model shows higher accuracy by more often making correct predictions about sentiment.

Moreover, several performance measures have been used to validate the prediction efficacy of the proposed DSO-CAM-CDL model, which includes the following:

$$\text{Accuracy} = \frac{\text{Tp+Tn}}{\text{Tp+Fp+Tn+F}} \tag{11}$$

$$\text{Precision} = \frac{\text{Tp}}{\text{Tp+Fp}} \tag{12}$$

$$\text{Recall} = \frac{\text{Tp}}{\text{Tp+Fn}} \tag{13}$$

$$\text{Specificity} = \frac{\text{Tn}}{\text{Fp+Tn}} \tag{14}$$

$$\text{FPR} = \frac{\text{Fp}}{\text{Fp+Tn}} \tag{15}$$

$$\text{FDR} = \frac{\text{Fp}}{\text{Fp+Tp}} \tag{16}$$

$$\text{FNR} = \frac{\text{Fn}}{\text{Fn+T}} \tag{17}$$

$$\text{F1} - \text{score} = \frac{\text{2Tp}}{\text{2Tp+Fp+Fn}} \tag{18}$$

Where Tp – true positives, Tn – true negatives, Fp – false positives, and Fn – false negatives. With the total samples of 200, among which 100 are threats, and 100 are non-threats, the model has successfully classified 99 as threats or Tp, 99 non-threats are correctly classified as Tn, 1 non-threat sample was misclassified as a threat or Fp, and 1 threat case is misclassified as non-threat or Fn. The resultant confusion matrix framed with the help of these values is given in Figure 3. By analyzing the misclassification pattern of the model, the results indicate that cyberbullying and phishing attacks are the most frequently misclassified ones, particularly when the language is ambiguous. To mitigate this issue, cost-sensitive learning will be adopted in future aspects for reducing Fn.

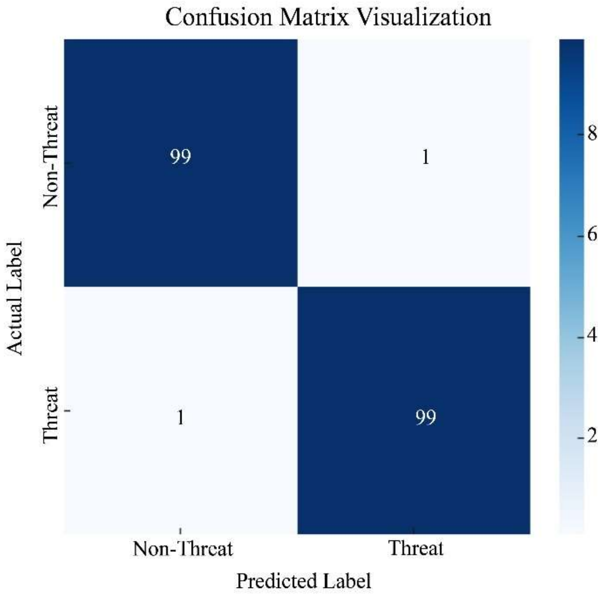

Fig. 3 Confusion matrix of DSO-CAM-CDL model

By using the Twitter dataset, Table 3 and Figure 4 validate the proposed DSO-CAM-CDL model with traditional machine learning [31]. Here, the most important characteristics used to assess the prediction effectiveness of the classification algorithm-precision, recall, and f1-score-are taken into account. The prediction system's overall efficiency is ascertained based on the enhanced values of these metrics. The comparison investigation reveals that the DSO-CAM-CDL model that has been suggested works better than all other machine learning techniques in terms of precision, recall, and F1-score values. The proposed approach is contrasted with the most popular machine learning techniques for threat identification in social networks in Table 4, and its appropriate graphical illustrations are given in Figure 5 and Figure 6. The Twitter Threat dataset was utilized in this investigation for the assessment [32]. The results show that the suggested model performs better than every other threat detection model that is currently in use, with excellent performance results. Given that the primary factor resulting in better prediction outcomes in the suggested framework is the deployment of the hybrid DSO algorithm.

Table 3. Comparative analysis with other classification methodologies using the Twitter dataset

Methods	Precision (%)	Recall (%)	F1-Score (%)
BERT	92	92	91
LR	90	84	87
SVM	92	76	83
RF	94	61	74
XGB	90	86	88
Proposed	99.1	98.9	99

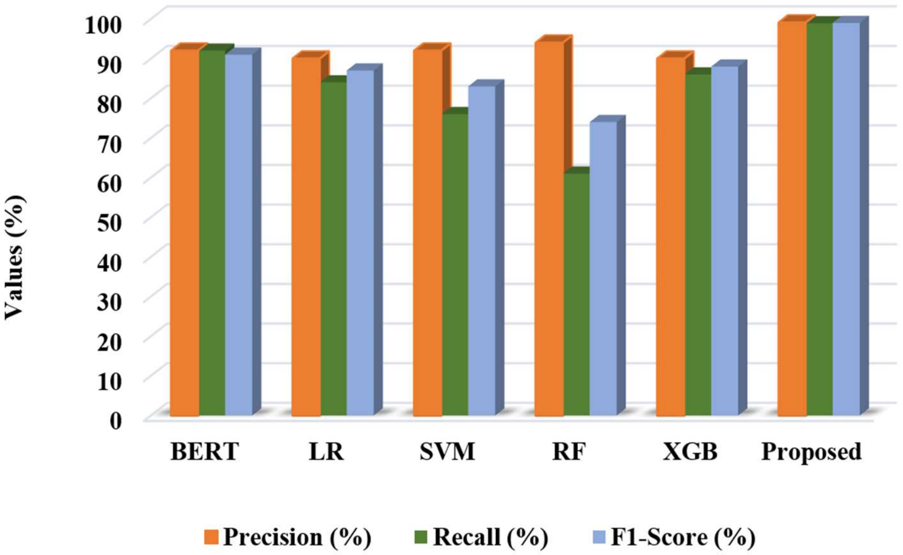

Fig. 4 Precision, recall, and f1-score analysis

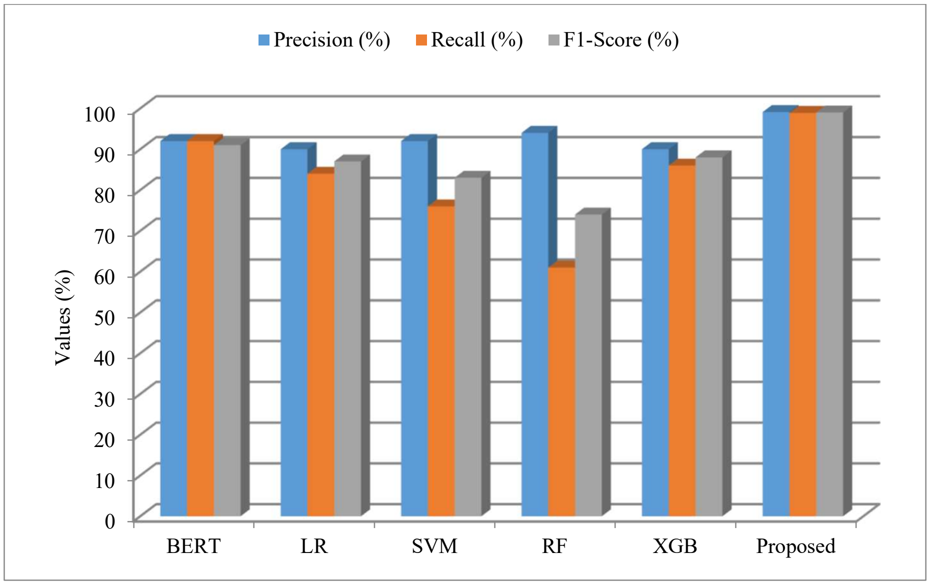

Fig. 5 Comparative analysis using the Twitter threat dataset

Table 4. Overall performance analysis using the Twitter threat dataset

Methods	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
NB	55	58	52	56
SVM	61	62	61	61
RF	63	63	63	63
LR	60	60	60	60
DT	53	54	53	54
XGB	55	57	54	56
KNN	55	59	48	55
DetThr	71	79	75	76
Proposed	99.1	99	98.8	98.8

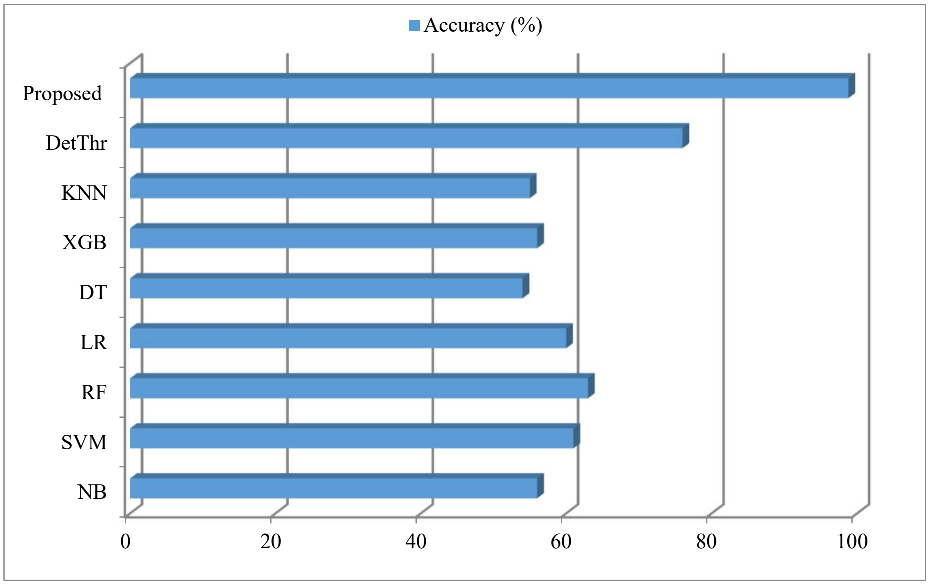

Fig. 6 Accuracy analysis using the Twitter threat dataset

The proposed prediction model is compared with a few traditional feature-fusion-integrated [33] classification approaches for social network security in Tables 5 and Figure 7. The metrics for accuracy, recall, and precision are also taken into account for analysis in this case. According to this study, the suggested DSO-CAM-CDL model achieves higher performance outcomes than the traditional feature fusion + classification approaches. Furthermore, as seen in Figure 8 and Table 8, the proposed security model is contrasted with the most advanced AI-based cyber intelligence algorithms utilizing Twitter data [34]. The suggested prediction methodology is contrasted with a few AI-based cyber intelligence tools to ascertain its efficacy and success rate. The results show that the suggested DSO-CAM-CDL outperforms the other approaches in terms of high recall (99%), f1-score (99.1%), and precision (99%) since the suggested security system's efficacy might be greatly enhanced with the addition of a hybrid DSO.

Table 5. Comparative analysis with other existing feature fusion-based classification methodologies

Methods	Accuracy (%)	Precision (%)	Recall (%)
BERT	82.42	84.61	79.21
Text GCN	75.88	76.75	76.56
BERT GCN	78.20	78.97	77.62
Text Level GCN	84.95	77.09	76.66
BERT – Text Level GCN	87.23	90.11	79.77
Proposed	99	98.8	98.8

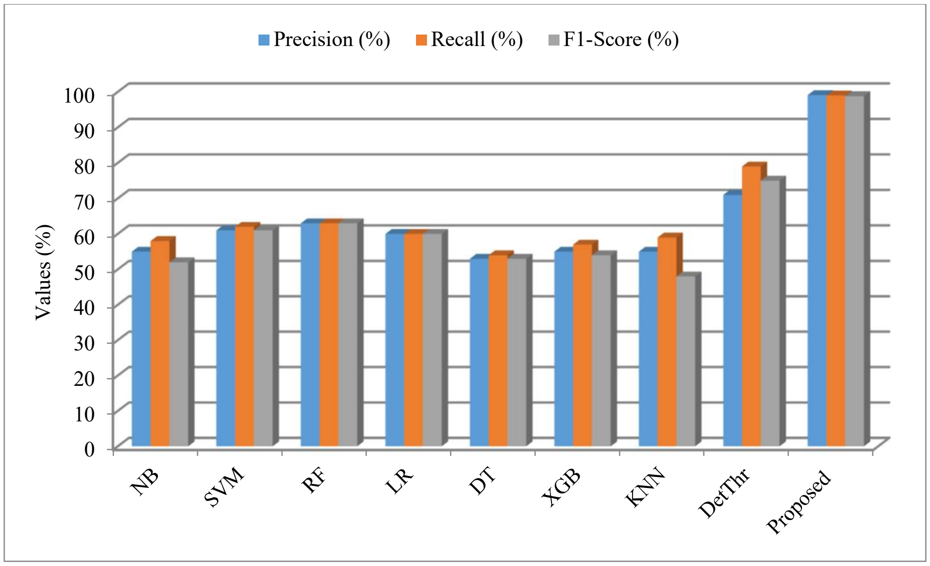

Fig. 7 Comparative analysis with conventional feature fusion-based classification models

Table 6. Comparative study among AI-based cyber-intelligence mechanisms

Methods	Precision (%)	Recall (%)	F1-score (%)
NB	94	91	93
SVM	95	94	95
ME	96	94	95
RF	94	61	74
SVC	73	96	83
LR	91	96	93
MNB	86	94	90
SGD	90	95	93
CNN-LDA	91	85	88
Proposed	99	99	99.1

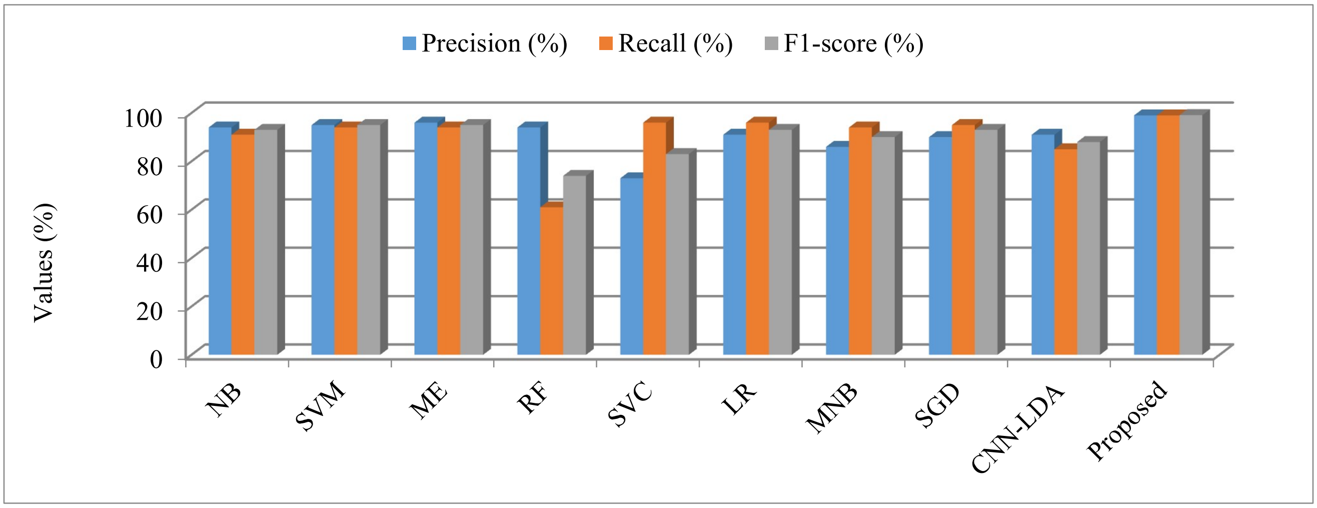

Fig. 8 Comparative analysis with other existing cyber intelligence mechanisms for social network security

Furthermore, Table 7 presents the validation and analysis of the suggested DSO-CAM-CDL model's overall performance. Figures 9 and 10 provide suitable graphical representations of the model. When compared to all other current methods, the suggested semantic analysis security framework performs well and yields excellent performance results, according to the overall findings.

Table 7. Overall performance analysis of the proposed model

Measure	Value (%)
Precision	99
Recall	98.9
Specificity	98.8
FDR	0.026
FPR	0.154
FNR	0.113
Accuracy	99.1
F1-score	99

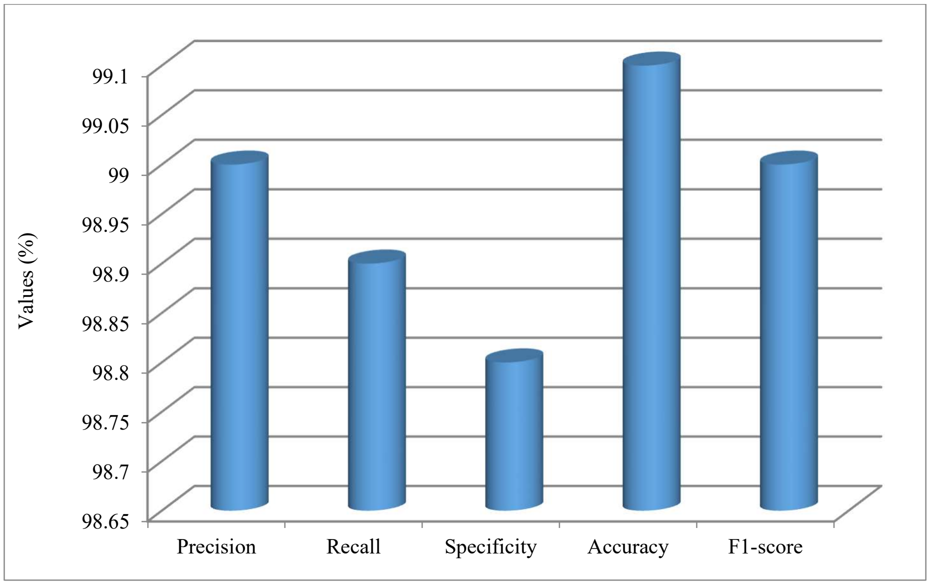

Fig. 9 Prediction performance

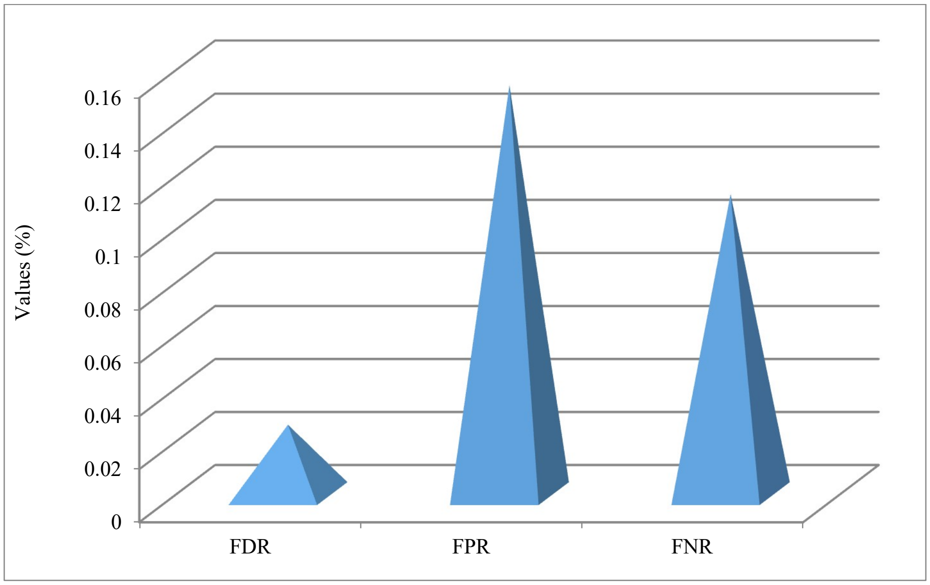

Fig. 10 False prediction analysis

To handle changeable situations, it is necessary to have adaptability and scalability in the infrastructure. To depict and analyze the scalability performance, Figure 11 showcases the scalability analysis with respect to training and inference time, which may be helpful. It can be seen that the training time increases linearly with an increase in the dataset size, indicating that the large datasets require more computation. Relatively, inference time remains stable, indicating the efficiency of the model to handle real-time predictions once the model is properly trained. Another factor that is considered critical in the development of the model is overhead complexity. As it can be seen that the model uses multiple modules like dolphin optimization and so on, we validate the approach to check for overfitting using the combination of regularization techniques and K-fold cross-validation. Figure 12 illustrates the comparative analysis in terms of computational overhead between traditional Ml approaches, DL approaches, and the proposed DSO-CAM-CDL framework. The chart takes into account different overhead types caused by factors like feature selection, training, memory, and inference time. It can be observed that the baseline-ML approaches possess minimal overhead due to their basic feature selection mechanism, followed by DL approaches with moderate overhead due to feature engineering mechanisms. But the DSO-CAM-CDL approach has the highest overhead because of the integration of advanced feature selection and multi-stage processing abilities.

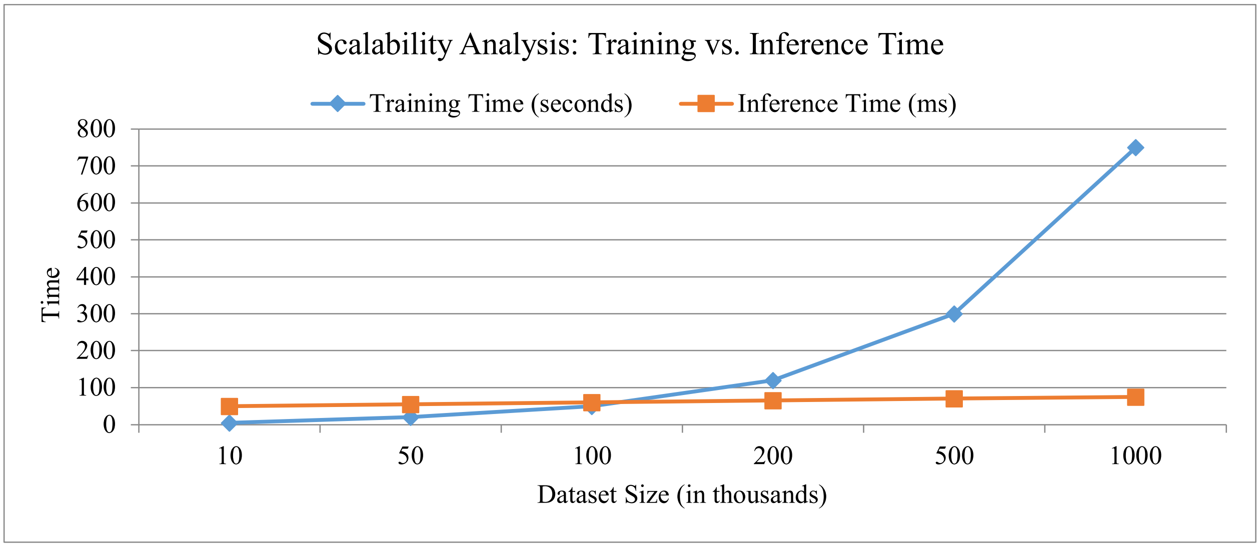

Fig. 11 Scalability analysis of DSO-CAM-CDL

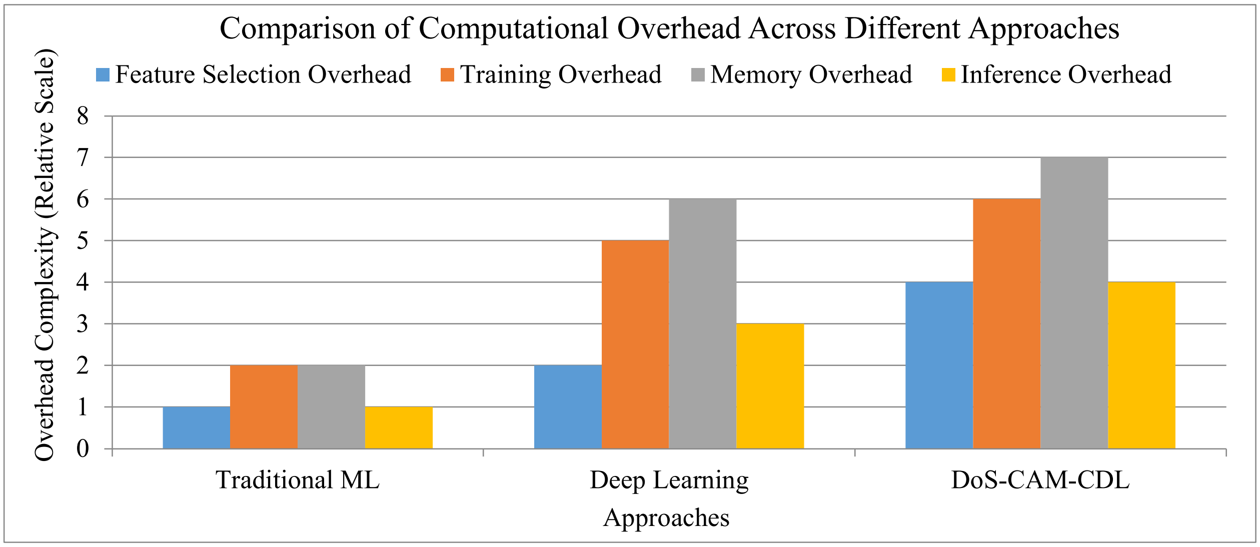

Fig. 12 Comparison of different methods based on computational overhead

To further prove the superiority of the proposed DSO-CAM-CDL approach compared to models in the literature section, a comparative analysis is carried out as part of the evaluation based on cyber-threat detection and accuracy. The results are tabulated in Table 8. Upon interpretation, it can be seen that a high accuracy of 99.1% and a cyber-threat detection score of 95 is attained by the DSO-CAM-CDL method. It is further followed by Rahman et al. [22] and Sharma et al. [5].

Table 8. Results

Model	Cyber-Threat Detection (0-100)	Accuracy (%)
Sharma et al. [5]	55	78
Saura et al. [7]	50	74
Suhaimin et al. [20]	40	65
Alshaikh et al. [21]	30	60
Rahman et al. [22]	60	82
Bengesi et al. [23]	50	75
Taherdoost et al. [24]	45	70
Trillo et al. [25]	35	68
Shaik et al. [26]	40	72
Boukabous et al. [27]	55	79
Zucco et al. [28]	52	77
Jain et al. [29]	35	62
Proposed DSO-CAM-CDL	95	99.1

4.1 Constraints and Limitations in Real-Time Feasibility

In the phase of implementation, there are a few difficulties that might occur. These could be related to the quality of data, the complexity of the model, its scalability, and also moral considerations. Checking and maintaining high-quality training data is very important because poor-quality or partial information can wrongly influence how well a model performs and its trustworthiness.

In addition, complicated deep learning algorithms like CDL can create obstacles due to the requirements for more computational power needed during the training process, along with a longer duration required for the training time frame, as well as issues related to understanding the model's interpretation ability involving many hidden layers' complexity, making it hard in some cases to understand what they do exactly.

Scalability worries can come up after putting the model into action in actual situations, especially when dealing with big data or a lot of user interactions. Moreover, thinking about ethics related to user privacy, keeping data safe, and algorithmic prejudice needs to be handled cautiously for using the model responsibly and ethically in social media platforms.

For handling these difficulties, it is necessary to take a full approach that includes strict preparation of data before processing large quantities of information; adjusting the architecture and settings of models; testing whether they are scalable enough; and following rules related to moral values as well as regulations required by law. The understanding of a model's predictions relies on different elements, like the intricacy of the model structure, the type of input data, and its use in an application.

For instance, with this suggested CDL algorithm, the interpretability level could be medium to low because it uses an effective deep learning model. Also, metadata connected with social media content, like hashtags or location labels, might offer some level of understanding by providing context and insights into the model's forecasting process. In a general sense, even though the CDL model's predictions may not be directly interpretable in a conventional way, as it is a black box type of model, efforts can still be put towards increasing transparency and comprehension through supplementary methods and features.

5. Conclusion

This study primarily focuses on the use of sentiment analysis to detect opinion spam, malevolent individuals, online scammers, and fraudsters. It also covers additional social media safety concerns, such as data provenance, mistrust of social networking sites, e-commerce security, catastrophe relief event forecasting, risk assessment, and others. Sentiment analysis is a popular tool used in social media research to examine user behavior and interactions with other users. The unique feature of this study is the use of state-of-the-art algorithms to predict user opinions and guarantee security.

This methodology has been applied to system analysis and design using the open-source social media dataset, after preliminary preprocessing and normalization operations were finished to improve the quality of the data. Using the novel DSO technique, the best subset of features from the given data is selected for the feature analysis, ensuring a precise categorization.

Here, sentiment prediction is accomplished using the CDL algorithm. The classifier model predicts users' opinions accurately based on a subset of features. Therefore, the CAM model has been used to forecast the anomalies from the social data in order to ensure improved security.

Additionally, the most widely used Twitter dataset is used to validate and evaluate the performance of the suggested framework. The DSO-CAM-CDL model proves to outperform the other methods in all metrics with an accuracy of 99.1%, a precision of 99%, a recall of 98.9%, an F1-score of 99%, and a specificity of 98.9%. Similarly, in the comparative analysis with existing techniques like SVM, NB, SVC, CNN-LDA, and so on, the proposed model performs with a superior score in all factors. Despite being an advanced technique in sentiment analysis, the architecture suffers from high computational overhead and accuracy issues if the dataset is imbalanced, noisy, and biased. So, future work focuses on optimizing the computational efficiency through the use of distributed computing techniques.

Additionally, expansion of the dataset, including multilingual & cross-platform data, and inclusion of explainable AI improves the factor of generalization and explainability.

Ethical Considerations

As the research used only publicly available anonymized social-media data, no personal or sensitive user information was collected. Hence, institutional ethical approval and informed consent are not applicable.

References

[1] Yanyan Wei et al., “Structural and Functional Abnormalities Across Clinical Stages of Psychosis: A Multimodal Neuroimaging Investigation,” *Asian Journal of Psychiatry*, vol. 99, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Wenqian Shang et al., “Aspect-Level Sentiment Analysis based on Aspect-Sentence Graph Convolution Network,” *Information Fusion*, vol. 104, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Kate Sherren et al., “Social Media and Social Impact Assessment: Evolving Methods in a Shifting Context,” *Current Sociology*, vol. 72, no. 4, pp. 630-648, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Muhammad Zulqarnain et al., “An Efficient Two-State GRU based on Feature Attention Mechanism for Sentiment Analysis,” *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 3085-3110, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Sanur Sharma, and Anurag Jain, “Role of Sentiment Analysis in Social Media Security and Analytics,” *Wiley Interdisciplinary Reviews: WIRE’s Data Mining and Knowledge Discovery*, vol. 10, no. 5, pp. 1-27, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] V. Ragu, and P. Jesu Jayarin, “Detecting Flooding Attacks in Distributed Denial of Service using Deep Neural Network Compared with Decision Tree,” *AIP Conference Proceedings*, vol. 3267, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jose Ramon Saura, Domingo Ribeiro-Soriano, and Daniel Palacios-Marqués, “Evaluating Security and Privacy Issues of Social Networks based Information Systems in Industry 4.0,” *Enterprise Information Systems*, vol. 16, no. 10-11, pp. 1694-1710, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Pratham Shah et al., “A Comprehensive Review on Sentiment Analysis of Social/Web Media Big Data for Stock Market Prediction,” *International Journal of System Assurance Engineering and Management*, vol. 15, no. 6, pp. 2011-2018, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] V. Ragu, and P. Jesu Jayarin, “Detecting Flooding Attacks in Distributed Denial of Service Attacks using Deep Neural Network Compared with Recurrent Neural Network,” *AIP Conference Proceedings*, vol. 3193, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Jose Ramon Saura, Daniel Palacios-Marqués, and Domingo Ribeiro-Soriano, “Using Data Mining Techniques to Explore Security Issues in Smart Living Environments in Twitter,” *Computer Communications*, vol. 179, pp. 285-295, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Hussain AlSalman, “An Improved Approach for Sentiment Analysis of Arabic Tweets in Twitter Social Media,” *2020 3rd International Conference on Computer Applications and Information Security (ICCAIS)*, Riyadh, Saudi Arabia, pp. 1-4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Anna Golebiowska et al., “Cybersecurity of Business Intelligence Analytics based on the Processing of Large Sets of Information with the Use of Sentiment Analysis and Big Data,” *European Research Studies Journal*, vol. 24, no. 4, pp. 850-871, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mohammed Al-Shabi, “Evaluating the Performance of the Most Important Lexicons Used to Sentiment Analysis and Opinions Mining,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 20, no. 1, pp. 51-57, 2020. [Google Scholar] [Publisher Link]

[14] Sheela Pitta, S. Gopalakrishnan, and S. Ravi Chand, “Securing WSN-IoT Networks using SwinAlert-GAN: A Deep Learning-based Intrusion Detection Framework,” *2025 Third International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, Trichy, India, pp. 211-218, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sulaiman Ainin et al., “Sentiment Analyses of Multilingual Tweets on Halal Tourism,” *Tourism Management Perspectives*, vol. 34, pp. 1-8, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kristian Bondo Hansen, and Christian Borch, “Alternative Data and Sentiment Analysis: Prospecting Non-Standard Data in Machine Learning-Driven Finance,” *Big Data and Society*, vol. 9, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Prajval Sudhir, and Varun Deshakulkarni Suresh, “Comparative Study of Various Approaches, Applications and Classifiers for Sentiment Analysis,” *Global Transitions Proceedings*, vol. 2, no. 2, pp. 205-211, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Wang Yue, and Lei Li, "Sentiment Analysis using Word2vec-CNN-BiLSTM Classification," *2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS)*, Paris, France, pp. 1-5, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Qianwen Ariel Xu, Victor Chang, and Chrisina Jayne, "A Systematic Review of Social Media-based Sentiment Analysis: Emerging Trends and Challenges," *Decision Analytics Journal*, vol. 3, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Mohd Suhairi Md Suhaimin et al., "Social Media Sentiment Analysis and Opinion Mining in Public Security: Taxonomy, Trend Analysis, Issues and Future Directions," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 9, pp. 1-25, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mansour Alshaikh et al., "Social Network Analysis and Mining: Privacy and Security on Twitter," *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, pp. 0712-0718, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Hameedur Rahman et al., "Multi-Tier Sentiment Analysis of Social Media Text using Supervised Machine Learning," *Computational and Mathematical Methods in Medicine*, vol. 74, no. 3, pp. 5527-5543, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Staphord Bengesi et al., "A Machine Learning-Sentiment Analysis on Monkeypox Outbreak: An Extensive Dataset to Show the Polarity of Public Opinion from Twitter Tweets," *IEEE Access*, vol. 11, pp. 11811-11826, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Hamed Taherdoost, and Mitra Madanchian, "Artificial Intelligence and Sentiment Analysis: A Review in Competitive Research," *Computers*, vol. 12, no. 2, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] José Ramón Trillo et al., "A Larg Scale Group Decision Making System based on Sentiment Analysis Cluster," *Information Fusion*, vol. 91, pp. 633-643, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Thanveer Shaik et al., "Sentiment Analysis and Opinion Mining on Educational Data: A Survey," *Natural Language Processing Journal*, vol. 2, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Mohammed Boukabous, and Mostafa Azizi, "Review of Learning-based Techniques of Sentiment Analysis for Security Purposes," *Innovations in Smart Cities Applications: The Proceedings of the 5th International Conference on Smart City Applications*, Safranbolu, Turkey, vol. 183, pp. 96-109, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] Chiara Zucco et al., "Sentiment Analysis for Mining Texts and Social Networks Data: Methods and Tools," *Wiley Interdisciplinary Reviews: WIRE's Data Mining and Knowledge Discovery*, vol. 10, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Ankit Kumar Jain, Somya Ranjan Sahoo, and Jyoti Kaubiyal, "Online Social Networks Security and Privacy: Comprehensive Review and Analysis," *Complex Intelligent Systems*, vol. 7, no. 5, pp. 2157-2177, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] Pradeep Mani, and Gopalakrishnan Subburayalu, "Enhancing Network Security with Memory-Augmented Visual Attention Networks and Predator-Prey Optimization Models," *Iran Journal of Computer Science*, vol. 8, no. 3, pp. 893-912, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[31] Nandita Pattnaik, Shujun Li, and Jason R.C. Nurse, "Perspectives of Non-Expert users on Cyber Security and Privacy: An Analysis of Online Discussions on Twitter," *Computers and Security*, vol. 125, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[32] Fethi Fkih, and Ghadeer Al-Turaif, "Threat Modelling and Detection using Semantic Network for Improving Social Media Safety," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 15, no. 1, pp. 39-53, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[33] Linli Wang, Hu Wang, and Hanlu Lei, "Public Sentiment Analysis of Social Security Emergencies based on Feature Fusion Model of BERT and TextLevelGCN," *Journal of Computer and Communications*, vol. 11, no. 5, pp. 194-204, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[34] Jeong-Ha Park, and Hyuk-Yoon Kwon, "Cyberattack Detection Model using Community Detection and Text Analysis on Social Media," *ICT Express*, vol. 8, no. 4, pp. 499-506, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[35] Renato Marinho, and Raimir Holanda, "Automated Emerging Cyber Threat Identification and Profiling based on Natural Language Processing," *IEEE Access*, vol. 11, pp. 58915-58936, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[36] Yong Fang et al., "Detecting Cyber Threat Event from Twitter using IDCNN and BiLSTM," *Applied Sciences*, vol. 10, no. 17, pp. 1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[37] Jun Zhao et al., "Timiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data," *Computers and Security*, vol. 95, pp. 1-27, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[38] Fahim Sufi, "A New Social Media-Driven Cyber Threat Intelligence," *Electronics*, vol. 12, no. 5, 1-21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[39] Fahim Sufi, "A New AI-based Semantic Cyber Intelligence Agent," *Future Internet*, vol. 15, no. 7, pp. 1-27, 2023. [CrossRef] [Google Scholar] [Publisher Link]