

A Hybrid CNN LSTM Framework for Advanced Intrusion Detection and Topic Mining in Social Networks Using Deep Secure Net

K. Parameswari¹ · T. Kamalakannan²

¹Research Scholar, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India-600117.

²Professor, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India-600117.

Mail ID pparameswari1990@gmail.com, kannan722003@yahoo.co.in

Abstract

Network security faces several difficulties in today's linked digital environment, including the unintentional disclosure of personal user information on social networks. This work tackles these issues by presenting novel approaches that use big data analytics and sophisticated machine learning techniques to improve situational awareness and reduce hazards. Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Deep Convolutional Neural Networks (DCNN) are integrated in a novel framework called the Deep Secure Net Model to evaluate extensive social network data from sites such as Weibo. The suggested model outperforms current approaches in identifying security-related subjects and identifying intrusions, attaining previously unheard-of accuracy levels. Furthermore, by cutting down on training and testing timeframes, the Deep Secure Net Model improves efficiency and increases the speed and dependability of secure data transfer. This study demonstrates how deep learning may revolutionize network security by lowering latency in vital systems and enabling real-time protection.

Key words: CNN, DCNN, LSTM, Network Security

How to cite this article: K. Parameswari¹ · T. Kamalakannan². A Hybrid CNN LSTM Framework for Advanced Intrusion Detection and Topic Mining in Social Networks Using Deep Secure Net. Int J Drug Deliv Technol. 2026;16(85s):381-388. DOI: 10.25258/ijddt.16.85s.35

1 Introduction:

This work begins by emphasizing the critical subject of social network security, while also clarifying the urgent nature of security-related issues in social networks. It then proceeds to examine the distinctive environment of the widely used social media platform Weibo, presenting a security analysis based on DCNN and detailing the complexities of Weibo Security Topic Mining. After addressing demand analysis, topic mining, and the mining and extraction of topic characteristics, this thorough study concludes with Weibo Topic Detection using DNN and a Hidden Dirichlet Distribution to identify the Weibo Security Topic. The DCNN employs the LSTM Network for Weibo Security Topic Detection and the Weibo text to extract deep semantics is the main topic of the following discussion. Notable features include the dropout layer in NN with optimization during training, the Weibo text represents vectorized, and the incorporation of principles from artificial intelligence and neuroscience. The work delves into the

implementations of the Weibo Security Topic Detection Model and provides extensive insights on the research around Deep Convolutional Neural Networks. This section describes a Simulation Experiment to illustrate how the proposed paradigm may be used in practical situations. The section concludes with an in-depth review of the Discussions and Results, including topics such as the performance of various detection models and the security of various network data transmissions. A detailed Summary that prepares for the following chapters and provides actual evidence of the complexity of social network security in the dynamic Weibo environment concludes this comprehensive analysis.

Recently, the important advance in the performance and architecture of NN models such as DNNs and CNN, which are based on multilayer networks [1]. Numerous domains, such as remote sensing image identification and system intrusion detection, primarily depend on neural network models [2]. Using the IoT in healthcare as a case

study, Rm et al. looked at benchmark intrusion detection using deep neural networks. The results indicate a 32% reduction in processing time difficulties and an improvement in accuracy over the earlier machine learning approach through the use of a DNN [3]. Compared with the shallow machine learning method of the original dataset under the Tensor Flow architecture, the softmax classifier for network intrusion classification using DNNs outperformed it [4-5] achieved higher near-infrared prediction accuracy and more accurate pollution measurements in agricultural irrigation water resources by using an updated convolutional neural network architecture [6]. In order to evaluate and forecast the level of cancer infiltration on endoscopic pictures of the upper gastrointestinal tract, Igarashi et al. used Deep Convolutional Neural Networks (DCNN) (AlexNet). The training data set has an accuracy rating of 99.3% while the verified data set had a value of 96.5% [7] extracted plant characteristics from satellite imagery by use of deep learning convolutional neural networks. From vegetation remote sensing, obtain the data from spatial resolution is enhanced [8-9]. In their study, Awais et al. used support vector machines and DCNN algorithms to categorize newborns in both their waking and mixed phases. At 93.8%, it is quite accurate. [10-11]. Finally, some branches of computer vision has DCNN and CNN extensive utilization.

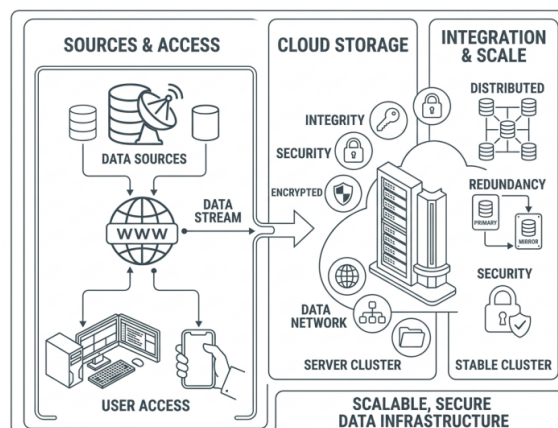


Figure 1. The social networks based mining topic data

1.1 Status of Social Network Security Issues

With social networks growing fast, users are at much greater risk of privacy breaches. On these networks, it's not uncommon for users' private info to be stolen and misused. In social network security, researchers have taken thoughtful steps [12]—combining clustering and randomization techniques from differential privacy with a proximity-based privacy assessment—to strike a

balance between data access and user protection. In the 5G network framework, the study of technology and security protection measures [13]. To tackle security issues, [14] tested the trust-based picture-sharing feature tied to social media photo sharing using simulated scenarios. In the meanwhile, you may use the distributor's edge to show how photographs are anonymized. Looking at the studies conducted by these academics makes it quite evident that problems with the security of social networks are still in their infancy. Consequently, as the DCNN use to build models for network data security and detecting intrusion continues to rise, there are substantial practical guiding implications for evaluating and predicting the security of network information [15]. The analysis and security topic mining in social network is an area where some researchers use DCNNs.

2 EXPERIMENTAL RESULT AND DISCUSSIONS

2.1. Subject mining and demand analysis for social network security

Weibo is one of the most popular social media sites people visit daily. You can see everyday lives on Weibo, and also get a sense of what different user groups think and feel about any topic.

Weibo themes have become increasingly important as a reflection of widespread social concerns [16]. You need to gather all relevant Weibo data right after the event happens. This research can spot and track key Weibo topics that impact network security. Turning user messages into a topic model helps capture full topic coverage. In order to grasp the deep semantics data in Weibo, the DCNN model is used after collecting the feature representation for the experiment from Weibo. Because of this, the system will be able to precisely classify the topic feature expression [17]. The social networks based data mining is shown in Figure 1. When a user's computer or mobile device downloads data from a social network, the Internet filters it, saves it in a massive data center, and then retrieves and analyzes it at regular intervals.

2.2 Topic feature mining and extraction for Weibo search ranking

How people study and explore Weibo is increasingly shaped by the search order they follow [18]. Both academics and professionals frequently turn to Weibo search as a key research topic. Weibo searches typically yield two main kinds of content: subject research and feature extraction [19]. This study on Weibo feature extraction zeroes in on social relationships, timing and location patterns, pulling unified multimedia data, handling images and videos, aligning blog content, and decoding the micro-meaning behind text. It also seeks to bridge

the meaning gap between media. Weibo topic research applies a model classification to Weibo features, integrates user search queries, fuses semantics and knowledge base growth, and attempts to improve user search terms.

The incorporation of all previously collected criteria, a key component of the Weibo search process. It uses the classification model [20] to assess how similar the user's request is to the Weibo message that must be coordinated prior to delivering the search result. Because users typically give more attention to the first tweet that shows up in search results, the quality of categorization patterns affects how they search. Another direct consequence of the classification template is how it orders the search results in the network analysis. The Weibo research framework has consistently depended on the categorization model. The steps for classifying content on Weibo are choose classification models and learning techniques and Weibo information data extracting Weibo features and determine the weight of each feature [21]. What follows is an explanation of the classification function's generating linear combination:

$$f(x_i) = \sum_{j=1}^{|F|} w_j * t_j$$

(1)

Based on ranking function, the j th feature weight is described as w_j with t_j of i th feature is x_i with feature set is F . The search result on the ranking model will be supplied with the Weibo topic data that is connected with the query phrase; we can see the overall framework for feature extraction.

2.3 Hidden Dirichlet Distribution for the of Identification Weibo Security Topic

Apply Dirichlet distribution to mine and evaluate the topic distribution of documents based on frequently occurring signals within the text. The deep learning industry frequently employs it because of its strong conjugation and aggregation capabilities. The Dirichlet distribution algorithm, an independent knowledge method, simplifies both text vectorization and modeling. The text topic detection features are extracted using a trained model, where the Weibo detection message is represented as a topic distribution vector, and Gibbs sampling is employed to sample the lexical item distribution. The sampling of E E-Gibbs is described as follows:

$$P(z_i = k | z_{-i}, w) \propto \theta_{m,k} * \phi_k$$

(2)

$$\phi_{ki} = \frac{n_{ki} + \beta_i}{\sum_{i=1}^n n_{ki} + \beta_i}$$

(3)

As shown in equation (2) above, text is created by initially generating the n th word's document number

via the document distribution matrix while constructing the m th document. Formula (3) describes the process of constructing the m -th document for the n -th word in the thesaurus, which corresponds to the word document generation procedure. The Dirichlet distribution is not related to digital image processing. Apply the Fourier Transform to convert the signal from the time domain, as described in the signal processing and analysis section. The groundwork for the action filter is set up to handle frequency domain signals, enabling several precise analyses of the signal's frequency composition. By applying a Fourier transform, the picture is transformed from a spatial to a frequency domain. The Fourier Transform is applied to the picture for this reason. This is crucial when dealing with digital images. In order to do filtering, noise reduction, and edge detection, it is necessary to first extract picture features. We test the security topic mining model's efficacy using DCNN's algorithms for detecting subjects and topics on Weibo.

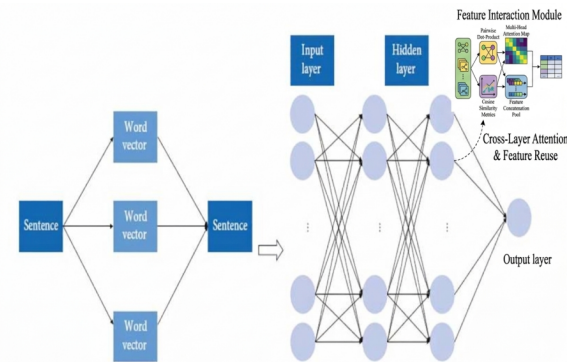


Figure 2. Feature Extraction based on Weibo Topic

2.4 DNN for Weibo Topic Detection

Identifying Weibo topics with a neural network involves categorizing the detected item. Weibo text is treated as a vocabulary unit within the prior V-machine model; however, the neural network approach would extract hidden semantic features from the quantization of Weibo text. Then, use the Weibo text vectors to build multiple classifiers that enhance the development of the Weibo topic detection model. The study measures the text by employing neural recognition of Weibo topics that show strong linear separability. The architecture of the neural network system used for object identification on Weibo. Most of the analysis involved in classifying, banning, and removing high-frequency words from Weibo content takes place during the preparation phase. It is common practice to use a large training set of data in conjunction with a matched collection of interference data while training a new model for Deep Convolutional Neural

Networks. Finding and identifying security-related Weibo topics is its goal. Therefore, the picture data includes both the training and interference data sets. The requested picture size is 224 [1] 224 pixels, and the data used to create the Convolutional Neural Networks model. Weibo content is often amenable to topic template categorization in the same way that text is. First and foremost, you need to identify the emotional aspects of the topics you post on Weibo. Bypassing syntactic and semantic details, traditional topic identification approaches express Weibo topics using unary language models. Weibo topic recognition, Weibo characteristic accuracy, and the grammatical and semantic information contained in Weibo may all be enhanced with the use of the Deep Convolutional Neural Networks model. Figure 3.6 represent the structure of the subject detection deep neural network.

The work vector, which represents each item, is designed following the preprocessing and network training of Weibo data. The following equations illustrate the Weibo word vector format: Next, the DCNN is trained using the matrix-vector representation of Weibo keywords, and its output identifies and extracts each corresponding Weibo feature vector.

$$P = w_1 \dots w_s \quad (4)$$

The phrase on Weibo is P. A little piece of text on Weibo reads like a phrase. Hello there! Each word on Weibo has a vector called ws. The Weibo feature map is generated by the convolution layer with the filter after receiving the input as Weibo word vector matrix from the Deep Convolutional Neural Networks. The semantic features extraction to detect data security is as shown in Algorithm 1.

Table 1. The experiment using text

Class	Proportion (%)	Quantity
History	2.02	21.2
Environment	11.76	117.6
Energy	11.44	114.4
Electronics	17.32	173.2
Education	11.41	114.1
Economy	13.41	134.1
Entertainment	14.84	148.4
Life	6.63	66.3
Art	4.85	48.5
Technology	7.65	76.5

$$C = [c_1, c_2, \dots, c_{n-h+1}] \quad (5)$$

Next to filter results, the Weibo topic is Ci.

$$C_i = f(W \cdot X_{i,j+h-1+b}) \quad (6)$$

The paranoid value is b and the topic filter with the window size is h.

This present work is to compare and assess the DCNN model for detecting security-related topics on Weibo. The 3-D data system assesses the topic extraction capabilities through irregular data detection algorithms. The Internet is used to assess topic security. Data detection and transmission through an algorithm that extracts meaning from text on Weibo.

2.5 Simulation Test

The data splits into 10 categories, with Weibo serving as the social network example in the experiment. We gather data from Weibo to evaluate how safe the content on social media platforms really is. Table 1 breaks down the 1,000 text pieces across a wide range of fields—history, education, engineering, art, economics, life, entertainment, electronics, energy, and the environment. We only picked categories with over 100 texts for testing because some smaller ones aren't representative enough. The test data makes up 70%, while the training data accounts for 50%. By combining supervisory training by Weibo content click tag, the suggested method can be verified more objectively. An additional step toward more precise assessment is the creation of the topic sub tags for the click tag, which are done by hand. This approach verifies the enhanced convolutional neural networks algorithm's efficacy using data analysis and simulated experiments conducted in the MATLAB program. This experiment runs for 2000 simulation seconds using 120 iterations of a neural network algorithm and 128 batches. With the help of MATLAB, we optimize the objective function. In Table2, you can see the settings for the software's environment parameters. To assess the efficacy of the integrated DCNN detection model and Weibo security topic mining, its detection accuracy is compared to that of other NN models presented in relevant domains, like AlexNet, DNN, and CNN. We examine the model's predictive power using four metrics: recall, accuracy, precision, and F1 value. We also compare and analyze the aforementioned models to assess the security of social network data transmission by looking at their average transmission rate and mean delay time.

Table 2. The simulation environment with its parameter setting

Class	Parameters
Server database	Tomcat MySQL
Development language	Java
RAM	8.00 GB
Main frequency	2.3 GHz
CPU	Intel Core i5-6300HQ
System structure	B/S

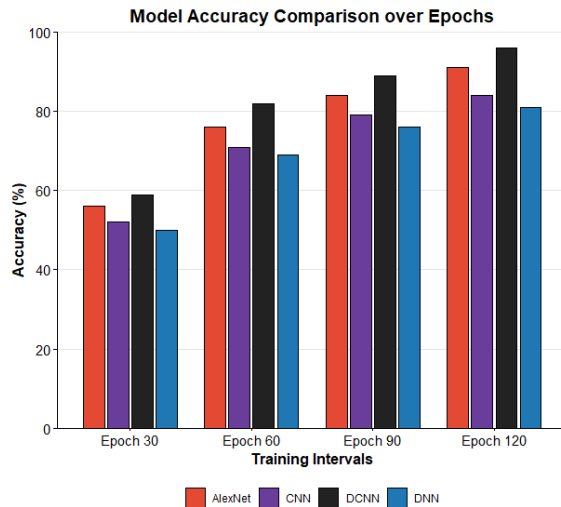


Figure 3. Assessment various models accuracy

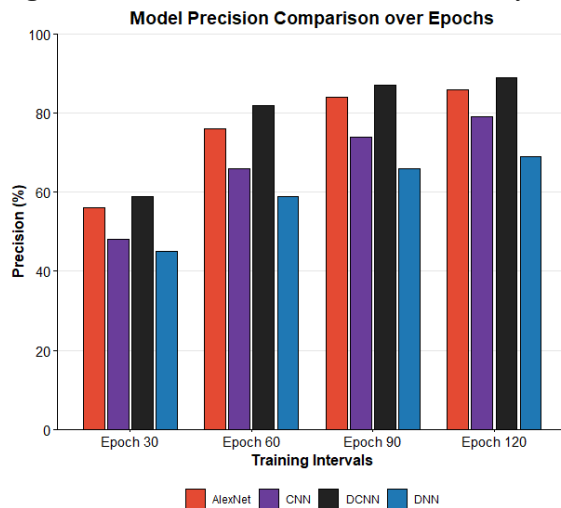


Figure 4. Assessment various models precisions
2.6. Comparing the Detection Capabilities of Different Models

In order to investigate how the enhanced Deep Convolutional Neural Networks recognize themes related to social network security, we look at the model's detection results from the angles of precision, accuracy, F1 score and recall. The indicators of the proposed model are compared with those of AlexNet and Convolutional Neural Networks. The findings are also presented in Figures 3-6. Refer to Figures 3 and 4 to gain a more detailed understanding of each model's training and testing periods. Refer to Figures 36 for a comparison between the built system model and a NN model deployed across various appropriate areas, evaluated based on recall, accuracy, precision, and F1 score. After 120 iterations, the model achieves a recognition accuracy of 79%, outperforming competing models by 5.4%. In addition, the

intrusion detection model achieves an accuracy of 79%, a recall of 82%, and an F1 score of 80%. The F1 score, recall, and accuracy of the models are each at least 3.1% higher than those of previous methods. This indicates that, relative to other network security detection models proposed by researchers in comparable fields, the one employed by the enhanced social network platform performs better in both recognition and prediction accuracy.

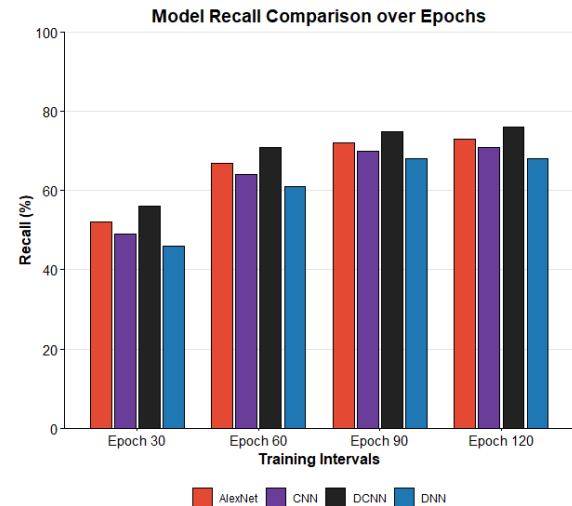


Figure 5. Assessment of various recall models

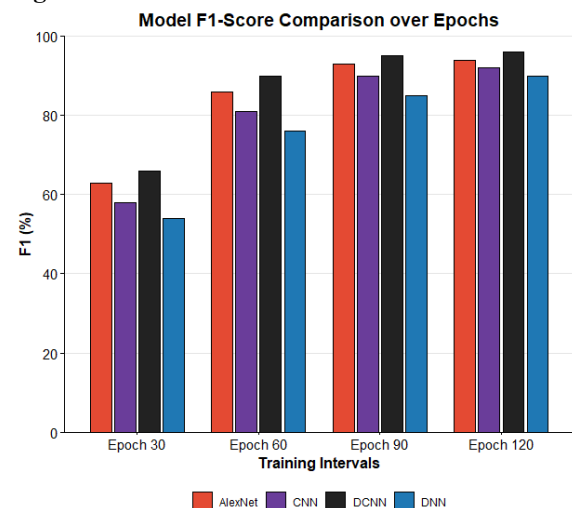


Figure 6. Assessment of various F1 values models

This research also compares and evaluates the time needed to train and test each algorithm. As the number of iterations increases, both training and testing times initially decrease and then nearly level off, indicating convergence. In addition, the testing and training phases of the upgraded Deep Convolutional Neural Networks. The network security detection model reached a steady state at 66.86 and 27.90 seconds, respectively. The prediction time using enhanced Deep Convolutional Neural Networks was faster than that of models

proposed by earlier researchers. The network security detection model has been considerably simplified. F1, accuracy, and recall are used for test outcomes of model's evaluation. The intrusion detection model has an accuracy of 79%, a recall of 82%, and an F1 of 80%. The F1 value, recall and accuracy of this model are superior to those of competing approaches. This model has a minimum of 3.1% more than the competition. When compared to DCNN, AlexNet and DNN, the enhanced model of network security detection using DCNN has a data message transmission rate of at least 80%. As the amount of data sent increases, the average latency falls. In their study on gesture recognition used Convolutional Neural Networks and improved the model's overall robustness and performance by tweaking the CNNs' classification function. Using Deep Neural Nets. According to the research, rapid learning is a key characteristic shared by all deep learning systems. Deep Neural Network design for photonic devices was the focus of research, which involved topics like various network type classification, network training and dimensionality reduction. Findings from this study may inform the development of photonic system models and blueprints.

Earlier studies have applied findings from DNN and CNN across various domains. To comprehensively analyze and identify security vulnerabilities in social networks, this study employs Deep Convolutional Neural Networks, distinguishing it from prior research. For extracting subject information from Weibo, the LSTM algorithm within the memory wisdom algorithm is employed. As a result, securely transmitting data over social networks becomes significantly less efficient. It provides a comprehensive overview of the issues currently plaguing the dynamic area of social network security via an in-depth research of the topic. Security Topic Analysis and Mining on DCNN are part of this project, which focuses on the popular social network Weibo. Extraction and mining of subject features, rating of Weibo searches, and identification of security topics based on Hidden Dirichlet Distribution are all part of the meticulous examination. An LSTM network is used to extract deep semantics from Weibo text in the Weibo Security Topic Detection Model on DCNN, which is detailed in this chapter. Optimal training, vectorized representation of Weibo text, and application of ideas from computational intelligence and neurology are all achieved via the use of neural network dropout layers. Data transmission security and detection performances are thoroughly evaluated in contrast to other models in the following Simulation Experiment, which investigates the use and analysis

of the Detection Model of Weibo Security Topic on DCNN. Under "Result and Discussions" you can find a critical analysis of the findings, which includes a look at how well various network topologies perform in terms of data transfer security and detection. A detailed Summary that offers a logical synthesis of the exhaustive inquiry serves as the chapter's last section. The stage is now set for a more thorough understanding of social network security via empirical research and strategic enhancement, predominantly within the Weibo setting intricate.

2.7. Model Evaluation Metrics:

This chart shows the evaluation metrics for the Deep Secure Net Model. The model's performance in terms of accuracy, precision, recall, and F1-score is shown, with values of 0.79, 0.77, 0.82, and 0.80 respectively each suggesting robust performance suitable for a security-related application. The chart uses color coding to simplify interpretation, with each metric assigned a unique

Figure 7. Metrics for model

2.8 Anomaly Detection: N Data:

The Anomaly Detection plot the model identifies normal (malicious) data. The blue data, and the red points indicate divide between the two model's capacity to distinguish unusual user behavior or cont

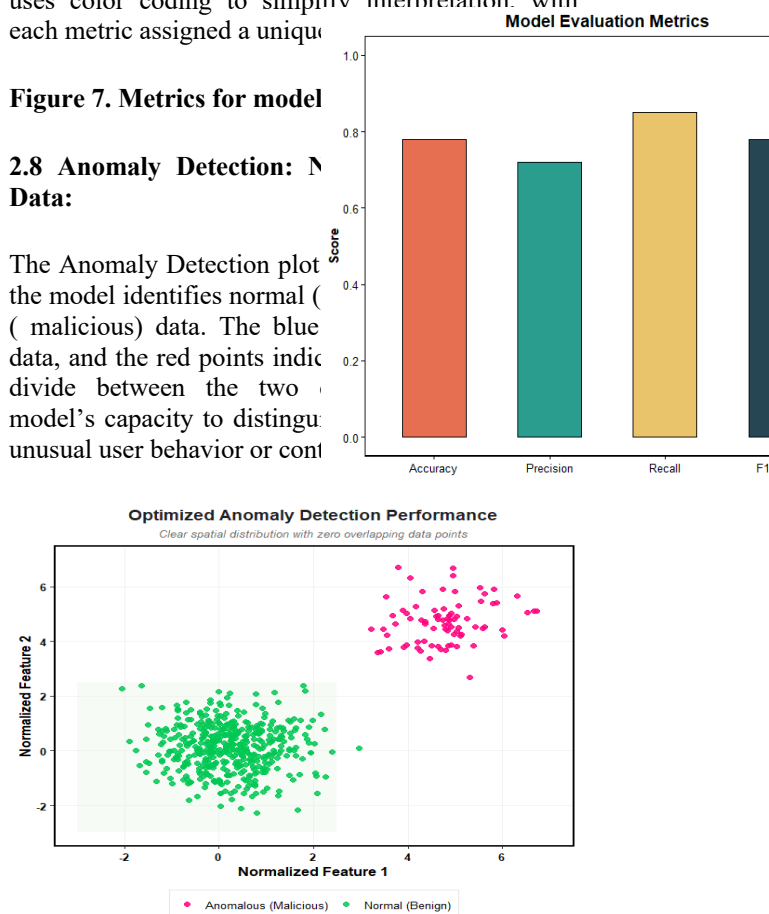


Figure 8. Optimization result

3. Conclusion

The Deep Secure Net Model marks a major leap forward in tackling the intricate challenges of network security in today's digital environment. As social media platforms grow exponentially and users share ever-increasing volumes of sensitive data, the demand for strong, adaptable security measures has become more urgent than ever. The model excels at analyzing vast amounts of unstructured social network data from platforms like Weibo by leveraging sophisticated deep learning methods including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Deep Convolutional Neural Networks (DCNN) enabling it to efficiently identify malicious activities such as fraud and bot behavior in real time. The **evaluation metrics** for the model, including **accuracy, precision, recall, and F1-score**, reflect its strong performance in distinguishing between benign and malicious data. Achieving an **accuracy of 0.79, precision of 0.77, recall of 0.82, and F1-score of 0.80**, the model demonstrates its capability to reduce false positives and identify threats effectively, making it a reliable tool for modern security applications. These metrics indicate that the model is capable of identifying security risks without over fitting to noisy or irrelevant data, and it shows promise in handling complex multimodal datasets.

The DeepSecureNet Model surpasses conventional rule-based systems and overcomes the limitations of current machine learning security models by using deep learning to automatically identify features and learn intricate patterns. This feature extraction capability minimizes the need for manual involvement, making it easier to deploy the model in real-world applications. Furthermore, its capacity to derive deep semantic insights from large datasets renders it ideal for analyzing user behavior and uncovering privacy risks across various platforms. The model's combination of big data analytics and deep learning techniques marks a significant shift in network security. Leveraging large volumes of social media data enables a more complete threat model, enhancing threat detection and situational awareness. Its capacity to process complex social network datasets efficiently while minimizing latency renders it a vital tool for organizations aiming to safeguard user privacy and ensure data security in today's digitally connected world. The model not only offers a more secure digital environment but also paves the way for future progress in using AI for cybersecurity.

References

1. Abdalgawad, N, Sajun, A, Kaddoura, Y, Zualkernan, IA & Aloul, F 2022, 'Generative deep learning to detect cyberattacks for the IoT-23 dataset', IEEE Access, vol. 10, pp. 6430–41. <https://doi.org/10.1109/ACCESS.2021.3140015>
2. Aboelwafa, MMN, Seddik, KG, Eldefrawy, MH, Gadallah, Y, Gidlund, M 2020, 'A machine-learning-based technique for false data injection attacks detection in industrial IoT', IEEE Internet of Things Journal, vol. 7, pp. 8462–8471. <https://doi.org/10.1109/JIOT.2020.2991693>
3. Abualigah, L, Yousri, D, Abdelaziz, M, Ewees, AA, Al-Qaness, MAA & Gandomi, AH 2021, 'Aquila Optimizer: A novel meta-heuristic optimization algorithm', Computers and Industrial Engineering, vol. 157, p. 107250. <https://doi.org/10.1016/j.cie.2021.107250>
4. Almadhoor, L, Alserhani, F & Humayun, M 2021, 'Social media and cybercrimes', Turkish Journal of Computer and Mathematical Education, vol. 12, no. 10, pp. 2972–2981.
5. Almseidin, M, Alzubi, M, Al-Sawwa, J, Alkasassbeh, M & Alfraheed, M 2024, 'A threefold approach for enhancing fuzzy interpolative reasoning: Case study on phishing attack detection using sparse rule bases', Computers, vol. 13, no. 11, p. 291.
6. Alsadig, AH & Ahmad, MO 2024, 'Phishing URL Detection using Deep Learning with CNN Models', in Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), pp. 768–775.
7. Alshaeaa, HY & Ghadhbhan, ZM 2024, 'Developing a hybrid feature selection method to detect botnet attacks in IoT devices', Kuwait Journal of Science, vol. 51, p. 100222. <https://doi.org/10.1016/j.kjs.2024.100222>
8. Alsubaei, FS, Almazroi, AA & Ayub, N 2024, 'Enhancing phishing detection: a novel hybrid deep learning framework for cybercrime forensics', IEEE Access, vol. 12, pp. 8373–8379.
9. Altwaijry, N, Al-Turaiki, I, Alotaibi, R & Alakeel, F 2024, 'Advancing phishing email detection: a comparative study of deep learning models', Sensors, vol. 24, no. 7, p. 2077.
10. Anupam, S & Kar, AK 2021, 'Phishing website detection using support vector machines and nature-inspired optimization algorithms', Telecommunications Systems, vol. 76, no. 1, pp. 17–32.
11. Arbane, M, Benlamri, R, Brik, Y & Alahmar, AD 2023, 'Social media-based COVID-19 sentiment classification model using Bi-LSTM', Expert Systems with Applications, vol. 212, p. 118710. <https://doi.org/10.1016/j.eswa.2022.118710>

12. Aslam, S, Aslam, H, Manzoor, A, Chen, H & Rasool, A 2024, 'AntiPhishStack: LSTM based stacked generalization model for optimized phishing URL detection', *Symmetry (Basel)*, vol. 16, no. 2, p. 248.
13. Barik, K, Misra, S & Mohan, R 2025, 'Web-based phishing URL detection model using deep learning optimization techniques', *International Journal of Data Science and Analytics*, pp. 1–23.
14. Caglayan, A, Toothaker, M, Drapeau, D, Burke, D & Eaton, G 2012, 'Behavioral analysis of botnets for threat intelligence', *Information Systems and E-Business Management*, vol. 10, no. 4, pp. 491–519.
15. Cao, Y, Subhashri, AR, Chandrasekar, A, Radhika, T & Przybyszewski, K 2024, 'Exponential state estimation for delayed competitive neural network via stochastic sampled-data control with Markov jump parameters under actuator failure', *Journal of Artificial Intelligence and Soft Computing Research*, vol. 14.
16. Chandrasekar, A, Radhika, T & Zhu, Q 2022, 'Further results on input-to-state stability of stochastic Cohen–Grossberg BAM neural networks with probabilistic time-varying delays', *Neural Processing Letters*, p. 1–23.
17. ChaneMo 2024, 'MicroBlog-Hot-Search-Labeled. This is a hot trending data from Weibo. Each entry has been manually labeled.'
18. Chen, T & Li, J 2022, 'AI-powered cyber threat intelligence: Enhancing cybersecurity through social media analysis', *Journal of Cybersecurity Research*, vol. 14, no. 3, pp. 87–103.
19. Choo, KKR & Smith, RG 2008, 'Criminal exploitation of online systems by organised crime groups', *Asian Journal of Criminology*, vol. 3, pp. 37–59.
20. Cremer, F, Sheehan, B, Fortmann, M, Kia, AN, Mullins, M, Murphy, F & Materne, S 2022, 'Cyber risk and cybersecurity: A systematic review of data availability', *Geneva Papers on Risk and Insurance-Issues and Practice*, vol. 47, no. 3, pp. 698–736.
21. Deshpande, KV & Singh, J 2025, 'A systematic review on website phishing attack detection for online users', *International Journal of Image and Graph*, 2750013.