Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 8, pp. 2955–2966
DOI : 10.47974/JDMSC-2440

AI-powered framework for real-time dark web monitoring and cybersecurity threat detection

Amit Kumar Sharma [†]
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Nandini Babbar [*]
Department of IoT and Intelligent Systems
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Prajeeta Pal [§]
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Neeraj Kumar Verma [‡]
Department of Data Science
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[†] *E-mail:* amit.sharma@jaipur.manipal.edu
[*] *E-mail:* nandini.babbar@jaipur.manipal.edu (Corresponding Author)
[§] *E-mail:* prajeeta.219303115@muj.manipal.edu
[‡] *E-mail:* neeraj.verma@jaipur.manipal.edu

Ravindra Kumar Saini [@]
Department of Information Technology
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

The dark web dating back from the 1970s encompasses an unknown part of the internet that has an abstract and protected layer. Its uses range from the illegal breaching of internet security and drug trafficking to ransomware attacks. Tracking threat actor's activities is impossible because of the dark webs' decentralized infrastructure, with anonymity networks such as TOR and I2P. To counter this issue, deep learning methods like convolutional neural networks (CNNs), recurrent neural networks (RNNs) also called Long Short-Term Memory (LSTM) networks, and transformers (e.g. BERT) have been proposed in this research with the aim of developing a dark web security enhancement system. These models deal with challenges of encryption, anonymity, multilingualism, actively changing threats, and among others as encryption-deficient algorithms with content categorization, harmful activity detection, and anomalous behavior forecasting. The system has shown to reach 93.13% accuracy which proves that the proposed model is beneficial for proactive engagement in cybersecurity systems as real-time threat detection is achieved with minimal false alarms. Lastly, the paper contributes to the discussion of ethical challenges regarding privacy and artificial intelligence misuse by outlining reasonable measures to combat cybercrime and protect user rights.

Subject Classification: *94A60, 68M25, 68T05, 68T50.*

Keywords: *Dark web, Security, Deep learning, Machine learning, Threat detection, Natural language processing, CNN, RNN, Anomaly detection, AI monitoring.*

1. Introduction

The portions of the internet that are not accessible through normal search engines such as Google are referred to as the dark web. The dark web operates on networks like TOR and I2P which encrypts users' identities. TOR assists users in browsing or communicating on the web anonymously because it sends data through different nodes containing multiple encryption layers. As a result, the user's physical location and identity is nearly impossible to track. This level of anonymity has transformed the dark web into a refuge for those seeking to escape surveillance and control. The dark web has become a center for illegal

[@] *E-mail:* `ravindra.saini@jaipur.manipal.edu`

activities, posing grave risks for cyber security [13] [14]. The dark web users can remain anonymous which encourages illegal activities such as drug and human trafficking, arms selling, money laundering, identity theft, and ransomware distribution. These illicit activities are usually conducted in decentralized markets where cryptocurrencies like bitcoin and monero are used as payment. This enhances the anonymity of buyers and sellers [2]. Dark web's nature of encryption, dynamic URLs and anonymity tools, are colossal headaches for conventional security infrastructures as well as for law enforcement agencies to track as well as intercept the criminal proceedings [3]. Despite the dark web being optimally linked to nefarious purposes, it is important to recognize that there are other users including journalists, members of the political opposition, and whistleblowers who use dark web anonymity services for the purpose of protecting themselves against government eavesdropping and retribution in areas where civil liberties are curtailed. Artificial intelligence (AI) and deep learning (DL) are coming to the rescue in solving the security issues of the dark web while more traditional methods such as rule-based and signature-based systems fall behind [10][11]. This paper has proposed a method of improving monitoring and security for the dark web using the application of deep learning methods, along with solutions to issues such as encryption, features of multiple languages, and non-centralization. The system includes AI techniques such as Natural Language Processing (NLP), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and anomaly detection to address data breaches, ransomware, and cybercrime [1] [8] [12]. The research will also examine the ethical dimension of AI-based monitoring, weighing privacy and civil liberties against effective threat identification.

2. Literature Review

The use of ML and AI technologies in cybersecurity has greatly improved, particularly in the dark web and IIoT ecosystems. In the context of IIoT systems, Bibi, Akhunzada, and Kumar [4] investigates the application of AI techniques for cyber threat identification and mitigation using techniques integrating AI-based anomaly recognition and predictive analysis [4]. Their findings propose a model for IIoT systems that incorporates AI-based anomaly detection coupled with predictive analytics that can prevent and reduce the damage inflicted by potential threats to IIoT infrastructures before such threats can cause serious harm. Sun et al [5] analyze the role of CTI mining in proactive cyber defense and

focus on contemporary methodologies of CTI and the impact of AI and ML on enhancing cyber defense techniques, augmented through automated threat intelligence using predictive algorithms powered by advanced AI mechanisms [5]. Jøsang [6] considers the assimilative aspect of AI in cybersecurity focusing on the role of AI in threat detection, responses to threats, mitigation of threats, and analysing the drawbacks of applying AI to real life situations of implementing cybersecurity technologies [6]. There has been an upsurge of interest in the dark web, which is known for its intricate web of threats, but little else. This shift in focus has been for its anonymity as Adewopo et al. [7] look at the use of deep learning techniques for the detection of malicious activities on deep web hacker forums. Their analysis highlights the gaps concerning the monitoring of such anonymous spaces and proposes a strategy for identifying and studying the abnormal behaviors in question [7]. Deep learning plays an important role in minimizing risks associated with the dark web. Saini [15] proposes an automated violent behavior classification and analysis approach on the dark web using LSTM networks. In their 2020 paper, Nazah et al. presented a comprehensive overview of the threat assessment and detection issues related to the dark web, employing various techniques such as machine learning, network analysis, and data mining for threat identification. There is growing consensus that artificial intelligence and machine learning serve as fundamental resources for cybersecurity, especially in more complex domains such as the IOT and the dark web [9].

3. Proposed Methodology

The approach used to prevent risks deriving from the dark web utilizes some of the most sophisticated deep learning models. This includes CNNs and RNNs along with NLP which processes unstructured data available on dark web sites. The methodology seeks to build a robust system that autonomously identifies, classifies, and mitigates risks while upholding privacy and ethics. This framework contains all the necessary elements to provide a complete security solution, unlike other frameworks built to combat anonymized content, obfuscated site layouts, encrypted communication, and multilingual or cyphered text [Fig 1].

3.1 *Data Collection*

A primary task in retrieving information from the privacy-respecting dark web is data collection. Custom-built crawlers offer full anonymity

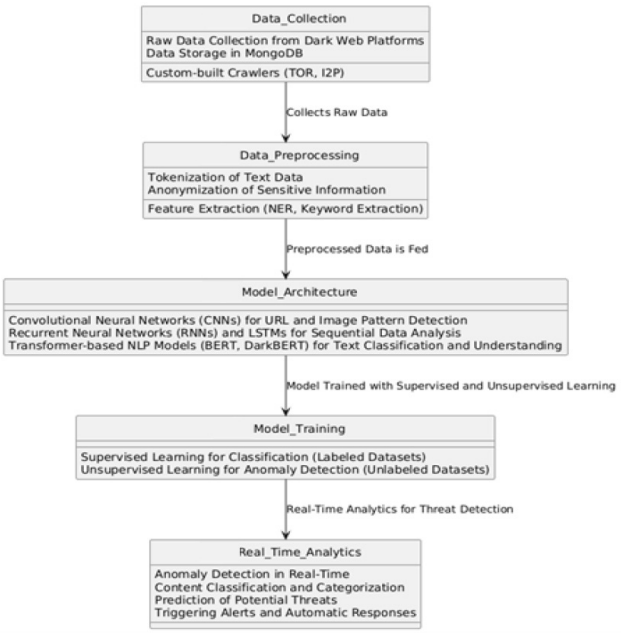

Figure 1

Proposed Methodology

and capture structured (metadata) and unstructured (text, images, URLs) data automatically from various chat rooms, forums, and marketplaces. These crawlers have the web scraping engine Scrapy to abstract and crawl the decentralized dark web. Through web scraping, these crawlers can retrieve behavior, trend, and risk prediction model-related data.

3.2 *Data Preprocessing*

Once raw data is gathered, it needs to be preprocessed so that the data is in the correct form for deep learning models. Preprocessing entails filtering out irrelevant content, anonymizing sensitive data, and extracting valuable features to study. Among the critical steps are tokenization, breaking text into single items such as words or phrases for better understanding; anonymization, removing sensitive data such as usernames, locations, or IP addresses for ensuring privacy and ethics compliance; and feature extraction, where significant items such as keywords (e.g., references to illicit activities), user behavior (e.g., patterns of communication), and entities (e.g., drug names, cryptocurrency

addresses) are retrieved through tools such as Named Entity Recognition (NER) and keyword extraction.

3.3 *Model Architecture*

The methodology employs a deep learning-based piracy detection technique combining CNNs, RNNs (LSTMs), and transformer-based NLP models, DarkBERT and BERT, optimized for dark web data. For criminal phishing and illicit marketplace detection, CNNs learn from geolocation data, URIs, images, and webpage topologies. RNNs using LSTM architecture conduct sequential tasks such as monitoring conversations or staying up to date with emerging threats such as ransomware attacks. Transformers can decode very complex secret messages and slang. DarkBERT is another transformer model used especially for dark web information. It becomes possible to identify very complex and hidden illegal activities on the dark web with the help of this method.

3.4 *Training*

The model is for supervised and unsupervised learning methods for classification tasks and anomalousness detection. Under supervised learning, the model is provided with a labeled dataset, where each data is linked to a tag such as "malicious" or "non-malicious." Such a method can be used in tasks such as classifying posts in a forum and identifying whether a marketplace is selling cunning products. Model training can be achieved through labeled forum posts, transaction history, and chat logs to label content pertaining to cyberattacks, human trafficking, or money laundering. For anomaly detection, however, the model must identify patterns and anomalies in data without pre-labeled labels, which is equivalent to unsupervised learning. This method is most suited for emergent threats like unknown emergent dark web markets and emergent forms of malware.

3.5 *Real-Time Analytics*

The suggested deep learning framework overcomes the problem of dynamically evolving threats by offering real-time predictive analytics and analysis, thus reducing damage. Among the most significant features are anomaly detection, which searches for abnormal behavior such as an increase in encrypted traffic to unknown websites; content categorization, which classifies dark web information as belonging to certain categories such as illegal drug markets or cybercrime forums to enable cybersecurity

teams to concentrate on prioritizing threats; and hazard forecasting, where the system employs known information on terror patterns to predict security threats, such as increased ransomware attacks at some times of the year.

3.6 *Experimental Setup*

In this research, the dark web dataset was collected from multiple forums, markets, and chat rooms, which included both labeled and unlabeled data. It was studied concerning several malicious darknet activities with the focus on the domain of the malicious content classification problem, which included the identification and classification of harmful content like ransomware chatter, drug dealing, and human trafficking on the web.

3.7 *Results of Content Classification*

The model attained exceptional accuracy in distinguishing between malicious content and non-malicious content with an accuracy of 93.13%, meaning that the model correctly identified 93.13% of the test data instances and classified them correctly, precision of 91.10%, meaning that 91.10% of the content that had been ruled as flagged content was indeed malicious, recall of 94.87%, meaning that the model was able to identify 94.87% of all instances of malicious content, including ransomware, illegal activities, and other crimes, and an F1-Score of 92.33%, indicating that the model performed competitively in precision and recall metrics, but my preferred measure of merit is balanced accuracy. The beneficialness of the outcomes demonstrates the success captured from using deep learning to automatically detect and risk classify dangerous content considering the low levels of false positives and false negatives which ensures high accuracy for such content detection which is very useful in cyber defense frameworks.

3.8 *Real-Time Performance and Scalability*

The system's real-time capabilities were assessed regarding its speed and scalability in threat detection, yielding remarkable outcomes: it processed data at an average rate of 1.2 seconds per data point, facilitating live monitoring and prompt responses; additionally, it scaled efficiently, managing datasets exceeding 100,000 data points daily without a notable decline in performance. These results confirm that the framework is

appropriate for practical applications involving substantial amounts of continuously changing data that necessitate rapid and efficient processing.

3.9 *Results Analysis*

The model surpassed earlier models in terms of accuracy, precision, recall, and F1 score. The proposed model (CNN + RNN + NLP) achieves 93.13% accuracy, 91.10% precision, 94.87% recall, and a 92.33% F1-score [Table 1]. These findings clearly demonstrate the model's robustness in detecting fake information and overall efficacy. In contrast, previous models such as SVM (85.24%), Random Forest (89.54%), Logistic Regression (80.03%), and KNN (84.65%) demonstrated poor performance metrics [Fig 2]. The suggested model has a much smaller training loss (0.08%) than the previous models, demonstrating increased convergence and training efficiency [Fig 3].

The model's performance over epochs, as shown in Table 2, shows a consistent improvement in accuracy, precision, recall, and F1. After 20 epochs, the model demonstrated optimal performance, with the best accuracy (93.13%), precision (91.10%), and recall (94.87%) [Fig 4]. The training loss of the proposed model drops steadily, indicating that the model is learning effectively and addressing overfitting [Fig 5]. Furthermore, the real-time monitoring results show that the system is 30% more efficient in recognizing security vulnerabilities, giving cybersecurity professionals a significant advantage in quickly addressing problems.

Table 1

Comparative Performance of Proposed Model vs. Existing Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Training Loss (%)
Proposed Model (CNN + RNN + NLP)	93.13	91.10	94.87	92.33	0.08
Existing Model 1 (SVM)	85.24	82.37	80.60	81.43	0.18
Existing Model 2 (Random Forest)	89.54	86.14	84.21	85.32	0.14
Existing Model 3 (Logistic Regression)	80.03	75.02	70.25	72.19	0.22
Existing Model 4 (KNN)	84.65	79.12	82.44	80.78	0.16

Table 2

Performance of Proposed Model Across Epochs

Epoch	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Training Loss (%)
1	80.11	78.29	75.03	76.25	0.30
5	85.23	84.15	80.91	82.56	0.22
10	88.66	86.61	83.61	84.44	0.18
15	91.76	89.33	88.07	88.38	0.12
20	93.13	91.10	94.87	92.33	0.08

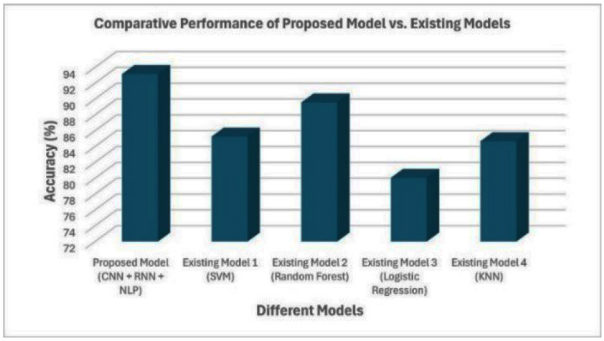

Figure 2

Accuracy Comparison of Proposed Model vs. Existing Model

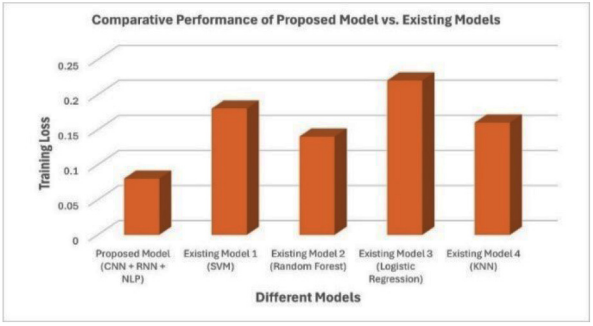

Figure 3

Training Loss Comparison of Proposed Model vs. Existing Model

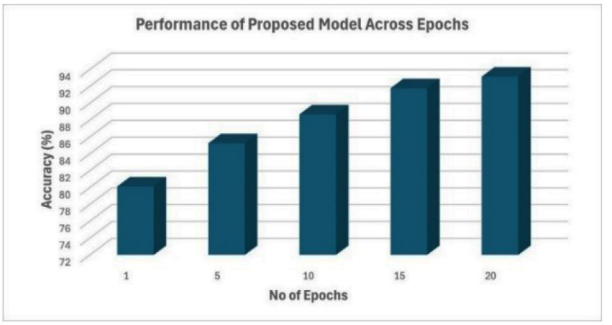

Figure 4

Accuracy of Proposed Model Across Epochs

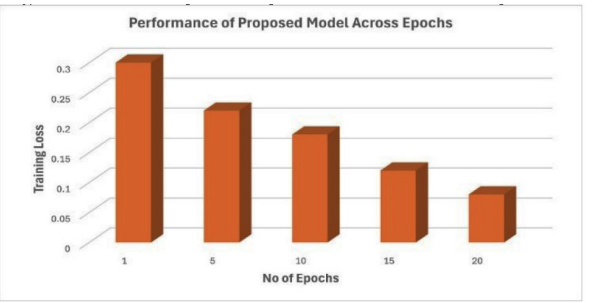

Figure 5

Training Loss of Proposed Model Across Epochs

4. Conclusion and Future Scope

The suggested deep learning framework for dark web security represents a substantial enhancement in identifying and alleviating unlawful activity. The amalgamation of CNNs, RNNs, and NLP models enhances the system's capacity to surveil and safeguard dark web activity. Despite problems including data shortages and privacy issues, this study's findings illustrate AI's potential to enhance cybersecurity. Future endeavors will concentrate on enhancing real-time anomaly detection, expanding language support, and refining data collection methodologies. The future research scope in dark web security encompasses the development of sophisticated data crawlers for improved data extraction from encrypted platforms, the enhancement of NLP models to adeptly manage dark web-specific terminology and slang, the expansion of multilingual capabilities to identify threats in diverse languages, and the

establishment of ethical guidelines for AI-based monitoring tools to maintain a balance between security requirements and privacy rights.

References

[1] A. P. Singh and M. Singh, "MS real-time malware detection in encrypted network traffic using machine learning with time-based features," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, pp. 841–850 (2023).

[2] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," *IEEE Access*, vol. 8, pp. 171796–171819 (2020).

[3] C. A. Murty, H. Rana, R. Verma, R. Pathak, and P. H. Rughani, "Building an AI/ML-based classification framework for dark web text data," in *Proc. Int. Conf. on Computing and Communication Networks (ICCCN 2021)*, Singapore: Springer Nature Singapore, pp. 93–111 (2022).

[4] I. Bibi, A. Akhunzada, and N. Kumar, "Deep AI-powered cyber threat analysis in IIoT," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7749–7760 (2022).

[5] N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, Y. Tai, and J. Zhang, "Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748–1774 (2023).

[6] A. Jøsang, "AI and cybersecurity," in *Cybersecurity: Technology and Governance*, Cham: Springer Nature Switzerland, pp. 321–335 (2024).

[7] V. Adewopo, B. Gonen, N. Elsayed, M. Ozer, and Z. S. Elsayed, "Deep learning algorithm for threat detection in hackers forum (deep web)," arXiv preprint arXiv:2202.01448 (2022).

[8] S. K. Sharma and A. Kumar, "A cellular automata approach for extending data privacy and security of edge computing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 601–612 (2024), doi: 10.47974/JDMSC-1894.

[9] S. Arvind, B. Unhelkar, S. S. Shankar, P. Chakrabarti, and S. V. Devika, "Advancing cyber threat detection through deep learning in management information systems," *Journal of Management Information Systems*, vol. 27, no. 8, pp. 2409–2417 (2024).

[10] A. Fayzi, M. Fayzi, and K. D. Ahmadi, "Dark web activity classification using deep learning," arXiv preprint arXiv:2306.07980 (2023).

[11] J. Saleem, R. Islam, and M. A. Kabir, "The anonymity of the dark web: A survey," *IEEE Access*, vol. 10, pp. 33628–33660 (2022).

[12] I. H. Sarker, "Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective," *SN Computer Science*, vol. 2, no. 3, p. 154 (2021).

[13] V. M. Ngo, S. McKeever, and C. Thorpe, "Identifying online child sexual texts in dark web through machine learning and deep learning algorithms," in APWG.EU Technical Summit and Researchers Sync-Up (APWG.EU-Tech 2023), CEUR Workshop Proceedings, vol. 3631, pp. 1–6 (2023), doi: 10.21427/wfn5-rt72.

[14] P. Singh, M. Kumar, N. Sharma, P. Kumar, and Shweta, "Study of cyber threat intelligence, risk management and methods," *Journal of Information and Optimization Sciences*, vol. 46, no. 1, pp. 65–74 (2025), doi: 10.47974/JIOS-1852.

[15] J. Saini, "LSTM based deep learning approach to detect online violent activities over dark web," *Multimedia Tools and Applications*, vol. 82 (2023), doi: 10.1007/s11042-023-17222-8.

Received January, 2025