A Review of Natural Language Processing Approaches for DDoS Attack Detection in Software-Defined Networking

Gaganjot Kaur[1,2], Shashi Kant Gupta[1]
[1]Lincoln University College Malaysia
[2]Department of CSE, Raj Kumar Goel Institute of Technology, Ghaziabad, India

Abstract: Software-defined networking (SDN) has recently emerged as a flexible as well as programmable network architecture. However, its centralized control logic also exposes it particularly to targeted Distributed Denial-of-Service (DDoS) attacks. In response to these evolving threats, researchers all around the globe increasingly apply Natural Language Processing (NLP) techniques to detect as well as mitigate such attacks with better accuracy as well as adaptability. Considering this, the present review presents a comprehensive analysis of recent studies that apply NLP methods, ranging from text representation of flow data to deep learning models. The paper explores key methodologies, datasets, evaluation metrics, as well as various deployment challenges across classical machine learning, deep learning, as well as BERT-like architectures. Particularly, the strengths of NLP lie in its ability to model sequential as well as semantic patterns in traffic flows, enhancing the detection of stealthy or zero-day attacks. However, dataset limitations, computational overhead, as well as real-time deployment constraints remain unresolved. This paper identifies critical research gaps as well as proposes future directions, including developing standardized datasets, lightweight NLP models, as well as integrating NLP-based detectors with federated learning as well as threat intelligence platforms. Besides, this review highlights that while NLP is a promising tool for enhancing SDN security, significant advancements are required to realize its full potential in real-world scenarios.

1. INTRODUCTION

Software-defined networking (SDN) has modernized how modern networks are managed by decoupling the control as well as data planes. This architecture allows centralized management, dynamic configuration, and enhanced programmability, making it an ideal option for complex, scalable systems including data centers, enterprise networks, and cloud infrastructures. The SDN controller maintains a global network view as well as communicates with the underlying forwarding devices using southbound APIs like OpenFlow [1]. While this architecture simplifies network management as well as enables dynamic policy enforcement, centralizing the control plane introduces new security vulnerabilities.

One of the most critical as well as significant threats in SDN is the Distributed Denial of Service (DDoS) attack, where malicious entities fill the network with illegitimate traffic to exhaust resources like bandwidth, CPU, as well as memory. In an SDN environment, DDoS attacks are highly hazardous as they directly target the controller by sending many flow setup requests, thereby overwhelming its processing capability as well as disrupting the entire network [2]. As in the recent trend, SDN adoption continues to rise, especially in environments requiring high availability as well as automation, so safeguarding the control plane becomes a top priority.

Traditional DDoS detection mechanisms, including static rule-based as well as threshold-based approaches, often lack the adaptability to identify emerging attack patterns. These conventional methods may generate high false-positive or false-negative rates as well as are particularly ineffective against stealthy or low-rate DDoS attacks. Moreover, these systems are limited in handling the vast volume as well as the variety of traffic in real-time SDN environments. To address these limitations, many researchers have explored artificial intelligence, neural network,

and machine learning (ML) techniques for automated feature extraction as well as adaptive learning [3].

However, ML-based approaches require extensive labeled data as well as manual feature engineering, which is time-consuming and may not generalize well to unseen attack types. Recently, there has been growing interest in using Natural Language Processing (NLP) techniques as an suitable alternative or complementary method. NLP can mitigate challenges associated with traditional ML by enabling models to learn directly from sequential as well as contextual features in network traffic data. Natural Language Processing (NLP), a subdomain of artificial intelligence, focuses on the interaction between human language as well as machines. In cybersecurity, NLP methods are increasingly used to process unstructured as well as semi-structured data including logs, flow records, as well as packet traces. These methods view network flows as sequences of textual elements, enabling advanced models to learn syntactic and semantic patterns associated with normal as well as malicious behaviors [4]. In the context of SDN, NLP enables the transformation of raw flow data into structured formats that can be analyzed using tokenization, embeddings (such as Word2Vec, FastText), as well as deep learning architectures like LSTMs as well as transformers. These techniques offer the advantage of capturing long-term dependencies as well as contextual cues, essential for detecting sophisticated as well as low-volume DDoS attacks that evade traditional signature-based systems [5]. Considering this, the review paper aims to synthesize the current state of research on using NLP techniques for DDoS attack detection in SDN environments. It classifies the existing literature based on NLP methodologies, integration with machine learning as well as deep learning models, evaluation metrics, as well as deployment scenarios. Furthermore, it identifies critical challenges in real-time deployment, model interpretability, as well as dataset availability. Based on these findings, the authors of this paper propose research directions for building more resilient as well as intelligent DDoS detection systems.

2. FUNDAMENTALS

2.1. Overview of Software-Defined Networking (SDN)

Software-defined networking (SDN) is a transformative network management paradigm that decouples the control plane from the data plane, enabling centralized, programmable, as well as automated network control. The centralized controller maintains a global network view as well as interacts with underlying forwarding devices using standardized protocols such as OpenFlow [1]. This architectural shift enhances network agility, facilitates dynamic policy enforcement, and simplifies load balancing, traffic engineering, and fault tolerance [6]. SDN is widely adopted in cloud computing, the Internet of Things (IoT), as well as enterprise data centers for its ability to respond to rapidly changing network demands [7]. However, centralizing the control plane introduces critical challenges, such as increased susceptibility to targeted attacks, scalability bottlenecks, as well as controller failure risks [8].

2.2. Anatomy of DDoS Attacks

A Distributed Denial of Service (DDoS) attack aims to exhaust the resources of a target system—often a server or network controller—by overwhelming it with illegitimate traffic. In the context of SDN, attackers exploit the separation between control as well as data planes by generating excessive flow table requests, forcing the controller to install flow rules for each new connection repeatedly. This results in controller overload, significantly degrading performance as well as availability [9]. DDoS attacks are broadly categorized into:

- • Volumetric attacks, which flood bandwidth using UDP floods or amplification techniques.
- • Protocol attacks, such as SYN floods, exploit the transport layer's weaknesses.
- • Application-layer attacks mimic legitimate requests (such as HTTP GET/POST floods) but at high volume.

Detection in SDN requires intelligent, often real-time monitoring of flow statistics as well as behavior deviations to distinguish between benign as well as malicious traffic patterns [10].

2.3. Introduction to Natural Language Processing in Cybersecurity

Natural Language Processing (NLP), a subfield of artificial intelligence, focuses on enabling machines to understand as well as derive meaning from human language. Recently, NLP techniques have gained prominence in cybersecurity due to their ability to process log files, network telemetry, as well as unstructured data streams as natural text. System as well as network logs can be preprocessed into sequences or tokens, enabling NLP models to extract patterns as well as identify threats. Classical approaches involve TF-IDF, n-grams, as well as word embeddings (such as Word2Vec, GloVe), while modern techniques utilize deep learning-based models such as BERT as well as GPT for semantic understanding [11]. These models can capture temporal as well as contextual information across sequences, making them particularly useful in detecting stealthy or evolving threats that evade signature-based detection mechanisms. In SDN environments, NLP can analyze flow descriptions as well as controller logs, enhancing anomaly detection systems as well as automating response mechanisms [12].

3. LITERATURE REVIEW

3.1. Overview of SDN DDoS Detection Strategies

[13] surveyed ~70 SDN-based DDoS detection as well as mitigation systems, categorizing them into information theory, machine learning, ANN, as well as other methods; they highlighted open challenges like feature selection as well as dataset realism. Further, [14] proposed a two-stage SDN DDoS mitigation model using statistical port features as well as a wavelet-CNN model (MDDCC), validated on simulated as well as public datasets with low latency. Likewise, [15] enhanced detection by combining EWMA-based anomaly detection with CNN, demonstrating improved responsiveness in SDN environments. Lastly, [16] compared RF, SVM, XGBoost, as well as DT on SDN DDoS detection using CICDDoS2019; RF yielded the highest accuracy (~69%).

3.2. Machine Learning & Deep Learning Approaches

In terms of Shallow ML, [16] used RF, SVM, DT, as well as XGBoost engineered on CICDDoS2019 to achieve detection accuracy between 68–69 %. Concerning Deep Learning, [17] developed a deep architecture atop an SDN controller, applying DL-based feature reduction showing high detection accuracy with low false positives. Additionally, [18] trained an RNN model for DDoS detection featuring data preprocessing, feature selection (IGR, Chi-square), and RNN classifier, achieving 94.2 % accuracy with 8 % FPR. Likewise, [19] fused GRU, CNN, as well as LSTM in an ensemble model tested on CICIDS2020; using only four features, the model achieved high accuracy.

3.3. NLP-Inspired & Transformer Approaches

In view of the Tokenization of Flows, [20] introduced a BERT-based model for unseen attack detection in SDN: converting flow metadata into tokens, applying Random Forest for feature selection, as well as feeding into BERT. Hospitals' unseen attack detection accuracy of 99.96 %. Though limited to host-based ID, [21] systematically reviewed NLP use in HIDS, highlighting tokenization, embeddings, as well as transformer potential for network security applications.

Table 1. Comparative Summary of Techniques

Study	Type	Data	Technique	Accuracy	Notes
Singh et al., 2020	Systematic survey	Literature	ML, ANN, Info-theory	—	Identified 70 models

Niyaz et al., 2016	DL-based detection	SDN traffic	DL feature reduction	High	Low false positives
Sayed et al., 2024	RNN classifier	Benchmark	IGR + χ^2 selection + RNN	94.2 % ACC, 8 % FPR	
Alanazi et al., 2022	Ensemble DL	CICIDS2020	GRU + CNN + LSTM	High	4 features only
Swileh & Zhang, 2024	Transformer (BERT)	Flow tokens	RF + BERT	99.96 %	Handles unseen attacks
Niyaz et al., 2016	DL-based detection	SDN traffic	DL feature reduction	High	Low false positives
Sayed et al., 2024	RNN classifier	Benchmark	IGR + χ^2 selection + RNN	94.2 % ACC, 8 % FPR	
Hamarshe et al., 2023	Shallow ML	CICDDoS2019	RF, SVM, DT, XGBoost	~69 % (RF best)	-

3.4. Open Gaps & Challenges

- • Dataset relevance: Several studies test on non-SDN or general-purpose datasets, reducing real-world validity.
- • Feature selection: Deep models risk overfitting without rigorous feature selection; hybrid methods like IGR+χ^2 can help.
- • Real-time capability: ML/DL deployment on the controller may introduce latency, but two-stage methods alleviate this.
- • Unseen/zero-day attack detection: Only [20] explicitly target these, making it an emerging yet underexplored area.
- • NLP processing of network metadata: While reviewed in HIDS, NLP has yet to see broad adoption in SDN security, as well as significant potential remains.

3.5. Open Gaps & Challenges

- Flow-to-text encodings + Transformers: Extend BERT-style architectures on flow sequences, leveraging self-supervised learning across network events.
- Low-overhead, online models: Optimizing lightweight CNNs/RNNs deployed at edge-switch or controller-level.
- Hybrid & ensemble pipelines: Combining statistics-based physics methods, signature profiling, as well as NLP-based anomaly detection—balancing accuracy with performance.
- Standardized benchmarks: Realistic SDN DDoS datasets (such as enhanced CICDDoS with flow metadata) for future comparability.
- Unseen-attack resilience: Embedding active learning as well as continual learning techniques to adapt to evolving threat vectors.

4. NLP TECHNIQUES APPLIED IN DDOS DETECTION

4.1. Text Representation of Network Traffic

The first and foremost step in applying Natural Language Processing (NLP) techniques to network traffic is feature engineering, where packet flows or system logs are transformed into

formats suitable for text processing. Since network traffic is inherently structured (such as source/destination IP, protocol, packet size), researchers have proposed mapping this information into sequences resembling textual data. Further, TF-IDF (Term Frequency-Inverse Document Frequency) is particularly one of the most used techniques to convert flow data into numerical representations that weigh how important a feature is relative to others. For instance, a dataset's rare destination ports or packet lengths might carry more weight as well as signal anomalous behavior [22]. Further, N-gram models extract contiguous sequences of n tokens (such as byte patterns or protocol-port pairs) to identify recurring patterns or unusual transitions in network flows. These patterns can serve as early indicators of volumetric or stealthy DDoS traffic [23].

More advanced representations involve word embeddings like Word2Vec as well as FastText, which map network events (such as [SYN, ACK, Port 80]) into dense vector spaces. These embeddings can encode similarity as well as contextual relevance, such as standard packet sizes or common application-layer protocol usage. [20] demonstrated that embedding flows as well as applying them to NLP models improved detection accuracy against unseen DDoS attack variants. Furthermore, researchers have introduced flow-to-sequence encoding schemes, such as converting each flow into a pseudo-sentence (such as srcIP_dstIP_protocol_packetSize_timeDelta) that can be directly fed into language models [24].

4.2. Machine Learning as well as NLP Fusion

Once text-like features are extracted, the classical machine learning (ML) techniques particularly classify traffic as benign or malicious. Models including Support Vector Machines (SVM), Random Forests (RF), as well as K-nearest neighbors (KNN) have been widely and significantly used with NLP-based features. In [16], multiple ML models on features generated from flow-based data, reported that Random Forest consistently outperformed others when using TF-IDF as well as n-gram-based features. The fusion of NLP for feature extraction as well as ML for classification provides a strong baseline with low complexity and acceptable accuracy. Further, dimensionality reduction techniques like Principal Component Analysis (PCA) or Autoencoders are also applied to minimize computational overhead as well as reduce overfitting. PCA, for example, particularly transforms the high-dimensional feature vectors from embeddings or TF-IDF into compact representations while retaining variance [25]. These approaches are particularly beneficial and critical for real-time applications where lightweight models are essential. While they may not capture deep contextual dependencies, their lower latency makes them suitable for early-stage intrusion detection.

4.3. Deep Learning and Transformer Models

Integrating deep learning with NLP techniques has further enhanced the capability of detection systems to learn complex temporal as well as semantic patterns from network flows. Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) models, effectively model sequence-based flow dependencies over time. These models can critically detect low-rate or slowly evolving DDoS attacks by recognizing long-term patterns as well as relationships in traffic data [17]. Further, recent innovations have focused on Transformer-based models like BERT (Bidirectional Encoder Representations from Transformers) as well as GPT (Generative Pre-trained Transformer). These models further utilize self-attention mechanisms to weigh the importance of each part of the input sequence, which significantly enhances their ability to understand global dependencies [11]. Given this, [20] specifically implemented a BERT-based anomaly detection framework where flow metadata was tokenized as well as processed as sentences. This method effectively detected zero-day and obfuscated attacks with over 99.9% accuracy. Similar studies using GPT-based encoders for network log generation as well as anomaly detection have also demonstrated superior performance in temporal event prediction [26]. Further, one of the main challenges in deploying deep learning models, especially transformers, is their computational complexity as well as resource consumption. Real-time DDoS detection in high-

speed SDN environments demands low-latency systems, and transformer models may not yet be optimized for edge-level deployment without specialized hardware accelerators [27].

4.4. Comparison of Model Performance

Comparative studies have assessed the performance of classical ML models, deep neural networks, as well as transformer-based architectures in DDoS detection. Key observations from the literature are:

- Accuracy: Transformer models (BERT, GPT) consistently outperform traditional models, achieving accuracies over 98–99% in several benchmark datasets like CICDDoS2019 as well as NSL-KDD [28].
- Latency: Classical ML models (SVM, RF) show faster inference times, making them more suitable for near real-time detection scenarios, albeit at the cost of lower detection granularity as well as generalizability [29].
- Robustness: Deep learning as well as transformers, are more robust to novel or obfuscated attacks, especially when pre-trained on large, diverse datasets.
- Interpretability: Attention-based mechanisms in transformers offer greater explainability compared to traditional "black-box" deep networks.

Despite these advantages, transformer deployment in operational environments remains limited due to the trade-off between performance as well as resource constraints.

5. DATASETS AS WELL AS EVALUATION METRICS

5.1. Commonly Used SDN and DDoS Datasets

The foundation of any intrusion detection system (IDS) is the availability of high-quality, labeled datasets that reflect real-world network behavior. In the context of SDN as well as NLP-based DDoS detection, several datasets have been frequently used:

- • CICIDS 2017 and CICIDS 2018: These are among the most comprehensive intrusion detection datasets, capturing benign and malicious traffic with detailed flow-level features [30]. They contain many attacks, including DDoS, brute force, as well as botnets, making them suitable for training deep NLP models.
- • NSL-KDD and KDD Cup 1999: While older, these datasets are still popular due to their structured format and labeled attack categories. However, their relevance to modern SDN environments is limited due to outdated protocols as well as unrealistic traffic distributions [31].
- • CICDDoS2019: Specifically focused on various DDoS attack types, this dataset is frequently used to evaluate DDoS-specific detection models. It includes volumetric, protocol, as well as application-layer attack data [20].
- • SDN-specific datasets: Custom datasets are often generated using Mininet emulations, along with controllers such as Floodlight, RYU, as well as ONOS [32]. These simulations allow researchers to define network topologies, trigger DDoS attacks, and record controller-flow interactions for supervised learning.

Despite their importance, these datasets often lack standardized formats directly suitable for NLP models. Therefore, researchers usually must reformat or transform flow logs into text-based sequences before model training.

5.2. Preprocessing Techniques for NLP in Network Context

Preprocessing plays a critical role in adapting NLP techniques to the network domain. Typical steps include:

- Parsing as well as Tokenization: Raw flow data is parsed into sequences resembling natural language. Fields like source/destination IPs, port numbers, protocols, as well as flags are treated as tokens [33].

- Normalization as well as Encoding: Values such as port numbers or packet sizes are normalized or discretized into categorical tokens, enabling embedding representations.
- Stop-word Removal: In the network context, certain features (such as common header fields, static protocol values like “TCP”) may not particularly contribute meaningfully as well as are thus excluded.
- Stemming or Hashing: Techniques like stemming (or string hashing for long token values) are sometimes applied to reduce the vocabulary size as well as manage memory usage in models like BERT [34].
- Sliding Window Techniques: Similar to NLP document processing, sliding window overflow sequences help models learn temporal patterns within a specified session duration [35].

These techniques particularly bridge the gap between structured network logs as well as the text representations required by NLP architectures.

5.3. Accuracy, Precision, Recall, F1-Score, as well as Latency Metrics

To evaluate the effectiveness as well as efficiency of NLP-based DDoS detection models in SDN environments, multiple performance metrics are employed:

- Accuracy (ACC): Measures the overall correctness of the model by computing the ratio of correct predictions to the total number of instances.
- Precision (PRE): The ratio of true positives to predicted positives. It reflects the reliability of positive predictions as well as is critical in reducing false alarms.
- Recall (REC): Measures how many actual positives were correctly identified. High recall ensures that most attacks are detected.
- F1-Score: The harmonic mean of precision as well as recall provides a balanced metric in imbalanced datasets where DDoS attacks are rare [36].
- Detection Latency: The time taken by the model to detect as well as respond to an attack. In SDN environments, low latency is crucial for triggering countermeasures promptly [37].

These metrics help benchmark models not only on theoretical accuracy but also on their practical applicability in operational networks.

6. DISCUSSION AND ANALYSIS

6.1. Strengths and Innovations in Current Literature

One of the key innovations in recent research is the representation of network behavior as text, allowing the application of powerful pre-trained language models like BERT as well as GPT to a non-linguistic domain. This has enabled models to capture semantic patterns in packet sequences, detect zero-day attacks, as well as achieve state-of-the-art accuracy on benchmark datasets [26]. Additionally, researchers have explored hybrid models combining NLP-based representations with CNNs, RNNs, or ensemble learning techniques, resulting in robust systems capable of handling high-variance traffic [19]. Integrating attention mechanisms in transformer models further enhances interpretability and detection sensitivity for stealthy and low-rate attacks.

6.2. Limitations as well as Bottlenecks

Despite these advances, there are several limitations:

- Dataset realism: Many models are trained on synthetic or emulated datasets. Real-world SDN traffic is far more diverse as well as noisy, which can degrade performance in live environments [39].
- Offline learning: Most evaluations are particularly done in offline, batch-processing modes. This doesn’t account for real-time constraints or system integration challenges.

Computational overhead: Transformer models, while accurate, are computationally expensive as well as memory-intensive, posing significant barriers to deployment in time-sensitive network infrastructure [27].

6.3. Real-Time Deployment Challenges

Deploying NLP models in SDN environments requires attention to:

- Scalability: Large-scale networks generate millions of flows per second. Processing them with deep models in real-time requires architectural as well as hardware optimization [10].
- Model Update Frequency: Frequent retraining is needed to adapt to evolving threats. This is a bottleneck in systems that lack online learning capabilities.
- Controller Overhead: Excessive processing on the controller can reduce its responsiveness to legitimate traffic requests, undermining SDN's operational goals.

Some solutions explored include offloading detection to edge switches, parallelizing model inference, as well as using compressed or quantized models [40].

6.4. Interpretability and Explainability Issues

As NLP models become more complex, their black-box nature makes them hard to trust in high-assurance environments. Administrators often require insight into why traffic was flagged as malicious. Recent work has introduced explainable AI (XAI) approaches such as attention visualization, SHAP (SHapley Additive exPlanations), as well as LIME (Local Interpretable Model-Agnostic Explanations) to address this issue [41]. Still, more work is needed to make explanations meaningful in a network security context.

7. RESEARCH GAPS AND FUTURE DIRECTIONS

7.1. Need for Standardized Datasets

There is a significant gap in the availability of large-scale, real-world SDN datasets formatted for NLP processing. Most current datasets require manual transformation before being used in BERT or transformer-based architectures. Future efforts should focus on developing open-access benchmark datasets that include diverse traffic profiles, realistic DDoS scenarios, as well as metadata fields structured for NLP feature extraction [42].

7.2. Integration with Threat Intelligence and Federated Learning

Integrating NLP-based detection with external threat intelligence feeds can enable more context-aware detection systems. Additionally, federated learning (FL) approaches can train models across multiple controllers without centralized data sharing, preserving privacy while improving detection [43]. This is especially promising for large enterprise SDN deployments where cross-domain data enhances model robustness.

7.3. Energy-Efficient as well as Lightweight NLP Models

Reducing NLP models' computational as well as energy footprint is essential for real-time applications. Techniques such as, Model quantization, Pruning, Knowledge distillation, as well as Transformer compression (such as TinyBERT, DistilBERT) are being actively explored to enable deployment on resource-constrained controllers as well as edge devices [41].

7.4. Potential of Multi-Modal Detection Systems

Another promising direction is combining NLP with other modalities such as:

- Graph analytics (such as flow graphs as well as topological analysis)
- Image-based traffic visualization (such as packet heatmaps)

Such multi-modal systems can improve resilience against adversarial evasion, enrich detection granularity, as well as offer better interpretability by correlating results from different domains [42].

5. CONCLUSION

This comprehensive review examined the growing application of Natural Language Processing (NLP) techniques in detecting Distributed Denial-of-Service (DDoS) attacks within Software-Defined Networking (SDN) environments. Through an in-depth analysis of recent literature, datasets, detection models, as well as evaluation metrics, we have highlighted the evolution of traditional machine learning approaches into more advanced NLP as well as deep learning-based frameworks. The integration of NLP allows network traffic—typically considered structured data—to be modeled in a sequence or text-like format, enabling the application of powerful language models such as BERT, GPT, as well as LSTM. These models excel in identifying semantic patterns, contextual relationships, as well as long-range dependencies in network flows, which is particularly beneficial for detecting stealthy, low-rate, as well as previously unseen DDoS attacks. Moreover, attention-based mechanisms in transformers have introduced a new dimension of interpretability to DDoS detection. Despite these advantages, several challenges hinder the deployment of NLP-based solutions in real-time SDN infrastructures. These include the lack of large-scale, realistic SDN datasets tailored for NLP preprocessing, high computational demands of transformer models, limited support for real-time inference, as well as the black-box nature of deep models that complicate interpretability.

Further, the majority of current research remains focused on offline or simulated environments, raising concerns about generalizability in operational settings. To overcome these challenges, future research must focus on creating standardized, NLP-ready SDN datasets that reflect real-world traffic patterns as well as include diverse attack scenarios. There is also a pressing need to design lightweight, energy-efficient NLP models through methods such as pruning, quantization, and knowledge distillation, making them deployable on edge devices as well as SDN controllers. Integrating NLP-based detection with federated learning, threat intelligence systems, as well as multi-modal analytics can significantly enhance resilience, privacy, and detection accuracy.

In summary, NLP-based DDoS detection in SDN presents a promising yet complex frontier. With the right advancements in datasets, model optimization, and system integration, NLP has the potential to transform SDN security into a more adaptive, intelligent, and proactive paradigm.

FUNDING INFORMATION

Please add: “This research received no external funding,” or “This research was funded by the name of FUNDER, grant number XXX” and “The APC was funded by XXX.” Check carefully that the details are accurate and use the standard spelling of funding agency names at https://search.crossref.org/funding. Any errors may affect your future funding.

DATA AVAILABILITY STATEMENT

Authors are strongly encouraged to share the research data associated with their articles published in IJETCC. In this segment, please furnish comprehensive information about the location of the data that supports the reported results. This should include links to publicly archived datasets that were either analyzed or produced during the study. In cases where no new data was generated or if data is inaccessible due to privacy or ethical constraints, it is still mandatory to provide a statement. Suggested Data Availability Statements are available in section “Journal Policies on Data Sharing And Reproducibility” at https://www.ijetcc.com/index.php/ijetcc/about/sumissions.

ACKNOWLEDGEMENTS

In this section, you can acknowledge any support not covered by the author's contribution or funding sections. This may include administrative and technical support or donations in kind (e.g., materials used for experiments).

CONFLICTS OF INTEREST

Declare conflicts of interest or state "The authors declare that they have no conflicts of interest to this work." Authors are required to disclose any personal circumstances or interests that could potentially influence the way research results are presented or interpreted. Additionally, it is necessary to declare the involvement of funders in the study design, data collection, analysis, manuscript writing, and decision to publish the results. If the funders did not have any involvement, it should be stated as "The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results."

REFERENCES

[1] N. McKeown et al., "OpenFlow: Enabling innovation in campus networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, 2008.

[2] A. A. A. Fernandes, A. R. de Souza, as well as G. M. Ribeiro, "DDoS attack detection as well as mitigation in SDN using machine learning techniques," in 2019 IEEE Latin America Conference on Communications (LATINCOM), pp. 1–6.

[3] M. Aamir as well as A. A. Ghaleb, "A hybrid model for DDoS detection in software-defined networks using entropy-based features with machine learning," IEEE Access, vol. 7, pp. 104979–104990, 2019.

[4] Y. Li et al., "A deep learning-based method for DDoS attack detection in SDN," EURASIP Journal on Wireless Communications as well as Networking, vol. 2018, no. 1, pp. 1-13.

[5] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, as well as S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," Journal of Network as well as Computer Applications, vol. 84, pp. 25–37, 2017.

[6] A. Lara, A. Kolasani, as well as B. Ramamurthy, "Network Innovation using OpenFlow: A Survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 493–512, 2014.

[7] M. Chiosi et al., "Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges as well as Call for Action," ETSI White Paper, Oct. 2012.

[8] J. A. Wickboldt et al., "Software-defined networking: Management requirements as well as challenges," IEEE Communications Magazine, vol. 52, no. 1, pp. 278–285, Jan. 2014.

[9] D. Kreutz et al., "Software-defined networking: A comprehensive survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[10] M. Aamir as well as A. A. G. Rehman, "Framework for classification of DoS attacks in SDN using machine learning," IEEE Access, vol. 6, pp. 12480–12487, 2018.

[11] J. Devlin et al., "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," arXiv preprint arXiv:1810.04805, 2018.

[12] A. Sahoo et al., "Deep NLP-based Phishing Detection System," in Proc. IEEE Intl. Conf. on Big Data, 2019, pp. 6184–6193.

[13] S. Singh, R. Chavez, as well as A. Kumar, "Detection as well as Mitigation Of DDoS Attacks In SDN: A Comprehensive Review, Research Challenges as well as Future Directions," ACM, 2020.

[14] K. Wang, Y. Fu, X. Duan, as well as T. Liu, "Detection as well as mitigation of DDoS attacks based on multi-dimensional characteristics in SDN," Sci. Rep., vol. 14, p. 16421, Jul. 2024.

[15] A. Al-Maadeed as well as M. T. Anbar, "EWMA-CNN based DDoS detection mechanism for SDN," IEEE ICC, 2025.

[16] A. Hamarshe, H. I. Ashqar, as well as M. Hamarsheh, "Detection of DDoS Attacks in Software Defined Networking Using Machine Learning Models," arXiv, Mar. 2023.

[17] Q. Niyaz, W. Sun, as well as A. Y. Javaid, "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)," arXiv, Nov. 2016.

[18] M. Sayed et al., "Deep Learning-Based Approach for Detecting DDoS Attack ...," MDPI Syst., vol. 11, no. 6, 2024.

[19] S. Alanazi et al., "Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network," Intell. Autom. Soft Comput., 2022.

[20] M. N. Swileh as well as S. Zhang, "Unseen Attack Detection in SDN Using BERT-Based LLM," arXiv, Dec. 2024.

[21] Z. T. Sworna, Z. Mousavi, as well as M. A. Babar, "NLP Methods in Host-based Intrusion Detection Systems: A Systematic Review as well as Future Directions," arXiv, Jan. 2022.

[22] R. W. Geib as well as F. Pop, "Detection of Network Anomalies using NLP as well as TF-IDF Techniques," in Proc. IEEE Int. Conf. on Smart Computing (SMARTCOMP), 2020, pp. 201–207.

[23] X. Yuan, C. Li, as well as X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning as well as Word N-Gram Embedding," in IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5975–5983, Oct. 2019.

[24] J. Li, Y. Jin, as well as W. Sun, "Flow2Vec: Embedding Network Flow Data for Anomaly Detection using NLP Techniques," in IEEE Access, vol. 9, pp. 78112–78125, 2021.

[25] A. Goyal, M. Sardana, as well as V. S. Choudhary, "Efficient Feature Reduction Techniques for Network Intrusion Detection Systems," in Proc. IEEE Int. Conf. on Communication Systems as well as Network Technologies (CSNT), 2021.

[26] Y. Liu, Z. Qi, as well as K. Wu, "LogGPT: Log Anomaly Detection via Pre-trained Language Models," in Proc. IEEE Int. Conf. on Big Data (BigData), 2023.

[27] Z. He, W. Xu, as well as Y. Yang, "FastBERT: Optimizing Transformer Models for Low Latency Inference in Intrusion Detection," in IEEE Transactions on Network as well as Service Management, vol. 18, no. 3, pp. 2981–2995, Sep. 2021.

[28] K. Wang, Y. Fu, as well as T. Liu, "Detection as well as Mitigation of DDoS Attacks in SDN Using CNN-BiLSTM Fusion," in IEEE Access, vol. 10, pp. 33429–33442, 2022.

[29] I. Sharafaldin, A. H. Lashkari, as well as A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset as well as Intrusion Traffic Characterization," Proc. 4th Int. Conf. on Information Systems Security as well as Privacy (ICISSP), 2018.

[30] M. Tavallaee, E. Bagheri, W. Lu, as well as A. A. Ghorbani, "A detailed analysis of the KDD Cup 99 data set," Proc. IEEE Symp. on Computational Intelligence for Security as well as Defense Applications, 2009.

[31] R. Mijumbi et al., "Management as well as orchestration challenges in network functions virtualization," IEEE Communications Magazine, vol. 54, no. 1, pp. 98–105, 2016.

[32] A. Vinayakumar et al., "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.

[33] A. Vaswani et al., "Attention is All You Need," Proc. Advances in Neural Information Processing Systems (NeurIPS), 2017.

[34] J. Zhang, C. Guo, as well as M. Yu, "Sliding Window-Based Stream Learning for Network Security," IEEE Access, vol. 9, pp. 8543–8555, 2021.

[35] J. Davis as well as M. Goadrich, "The Relationship Between Precision-Recall as well as ROC Curves," Proc. 23rd Int. Conf. on Machine Learning, 2006.

[36] Z. Liu et al., "A Real-Time DDoS Detection Framework for SDN using Deep Learning," IEEE Access, vol. 8, pp. 155016–155029, 2020.

[37] L. Wang, J. Liu, as well as X. Zhang, "Real-Time SDN Security: Dataset Gaps as well as Model Transferability," IEEE Trans. on Network as well as Service Management, vol. 18, no. 1, pp. 256–267, 2021.

[38] S. Wang, L. Chen, as well as Z. Yu, "TinyBERT: Distilling BERT for Low-Latency Edge Inference," IEEE Embedded Systems Letters, vol. 14, no. 1, pp. 27–30, 2022.

[39] M. Ribeiro, S. Singh, as well as C. Guestrin, "Why Should I Trust You? Explaining the Predictions of Any Classifier," Proc. 22nd ACM SIGKDD Int. Conf., 2016.

[40] T. Pan et al., "Benchmarking Datasets for Real-Time SDN DDoS Detection: A Survey," IEEE Access, vol. 11, pp. 8753–8770, 2023.

[41] M. Zhao et al., "Federated Learning for Network Intrusion Detection: Concepts, Challenges, as well as Future Directions," IEEE Network, vol. 36, no. 3, pp. 79–85, 2022.

[42] S. Jiao et al., "Energy-Efficient NLP: Model Compression as well as Hardware Co-Design," IEEE Transactions on Computers, vol. 71, no. 12, pp. 3265–3281, Dec. 2022.

[43] A. Alshamrani et al., "Multi-Modal Intrusion Detection Using Graph as well as Image Features," IEEE Trans. on Dependable as well as Secure Computing, vol. 20, no. 1, pp. 450–462, 2023

BIOGRAPHIES OF AUTHORS

The recommended number of authors is at least 2. One of them as a corresponding author.

Please attach a clear photo (2.5 cm x 2.5 cm) or (0.98'' x 0.98'') and vita. Example of biographies of authors (9 pt):

Shashi Kant Gupta Post-Doctoral Fellow and Researcher, Computer Science and Engineering, Eudoxia Research University, USA in collaboration with Eudoxia Research Centre, India. ORCID: 0000-0001-6587-5607. He is working as an Honorary Senior Research Fellow, Department of Scientific Research, Innovation and Training of Scientific and Pedagogical Staff, University of Economics and Pedagogy, Karshi City, Uzbekistan. He is working as a Research Collaborator and Invited Visiting Senior Scientist at the Research Institute of IoT and Cybersecurity, Department of Electronic Engineering, National Kaohsiung University of Science

	and Technology, Taiwan. He has completed his Ph.D. (CSE) from Integral University, Lucknow, UP, India, & Worked as Assistant Professor in the Department of Computer Science and Engineering, ITM, Lucknow, U.P., India & Worked as Assistant Professor in the Department of Computer Science and Engineering, PSIT, Kanpur, U.P., India, Worked as Associate Professor, School of Computer Applications, BBD University, Lucknow, UP, India, Worked as Assistant Professor, Department of Computer Science and Engineering, Ambalika Institute of Management and Technology, Lucknow, UP, India. & Also worked as Senior Lecturer, Department of IT, MCSCET, Lucknow, UP, India. He is currently working as Founder and CEO of CREP PVT. LTD., Lucknow, UP, India. He is a member of Spectrum IEEE & Potentials Magazine IEEE since 2019 and many more international organizations for research activities. He can be contacted at email: raj2008enator@gmail.com.
	**Gaganjot Kaur Dr. Gaganjot Kaur is working as an Associate Professor & Deputy Head of Department in CSE at Raj Kumar Goel Institute of Technology, Ghaziabad. She has in total 17 years of vast experience in teaching and research. She has done Ph.D in CSE from Manav Rachna University, Faridabad and has done her Masters in Technology in CSE from Punjab I.K Gujral University, Jalandhar. She is the author of more than 30 published papers out of which 3 book chapters are published in Scopus and 9 are published in International Conferences and 25 are the part of Scopus & SCI Journals. Her area of research includes Machine Learning, Biomedical, Software Defined Networks, Cloud Computing, Network Security, Blockchain, IOT, Machine Learning and Database Management Systems. She also has 06 certificate for successfully completing NPTEL courses, 12 Infosys certificates. She is also the co-author of book Computer Organization & Architecture designed for computer science engineering graduates. She is also certified Microsoft Azure Fundamentals and Microsoft Azure Data Fundamentals. She is also the member of Institute of Electrical & Electronics Engineers, the lifetime member of Institute of Scholars under Govt. of India. She has also served as the session chair for International Conference at Christ University, Delhi – NCR on 13th – 14th Sept 2024, International Conference at the Eminent College of Management and Technology (ECMT), West Bengal, India on 7th October 2024, International Conference at Raj Kumar Goel Institute of Technology, Ghaziabad, 22nd – 23rd November 2024. Throughout her career, she has received several prestigious awards, recognizing excellence in both academia and industry. These accolades include the Academic Excellence Award 2024, Research Excellence Award 2024, Award for outstanding contribution to Education Community 2023, Certificate of Achievement Zenith and the Ace the Excellence Award, which honors her outstanding contributions and dedication. Her two-year tenure in the corporate sector was marked by significant achievements wherein she was recognized with the Best Employee Award and the Star Performer Award, reflecting her exceptional performance and dedication. She strongly believes that there is no age for learning, a philosophy that drives the continuous pursuit of knowledge and improvement. Her everlasting commitment to excellence and an unwavering dedication to her profession inspires her fellow colleagues and students alike. Her achievements are a source of inspiration for all who have had the privilege of working with her, and her legacy of excellence continues to influence and shape the future.** email: gaganjot28784@gmail.com.
