iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.57949

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

DDOS Attacks Detection via Deep Learning Approaches

Ms.V. Rose Priyanka[1], Pratistha[2], Shivam Kumar V[3], Vivek Prasad[4]
[1]*Assistant Professor,* [2, 3, 4]*Student, Department of Computer Science and Engineering, T. John Institute of Technology, Bangalore*

Abstract: ***The proliferation of Distributed Denial of Service (DDoS) attacks presents a pressing challenge to network security. Conventional rule-based detection methods are increasingly inadequate against the evolving tactics employed by cyber adversaries. This journal proposes a novel approach integrating Support Vector Machines (SVM) into advanced machine learning architectures for fortified DDoS detection.***
The research methodology initiates with comprehensive data collection, gathering diverse network traffic scenarios and DDoS attack instances. This dataset becomes the foundation for subsequent phases, employing sophisticated feature engineering to extract vital patterns for model development. The feature selection process involves using feature engineering techniques including Data Collection, Model Development and SVM Integration, to extract the most discriminative and relevant features from the network traffic data. The primary innovation lies in the creation of a hybrid CNN-LSTM model, capable of discerning spatial and temporal dependencies within network data, thereby augmenting DDoS threat identification.
The integration of SVM into machine learning and deep learning paradigms forms the crux of this study. By leveraging SVM's classification proficiency alongside the CNN-LSTM model's capabilities, a sophisticated DDoS detection system aims to surpass conventional rule-based limitations.
Anticipated outcomes extend to fortifying network infrastructures with an adaptive and proactive defence mechanism, elevating the security posture against the ever-evolving cyber threat landscape. This research represents a pivotal stride towards robust and responsive network security mechanisms.
The anticipated outcomes of this pioneering research extend beyond mere detection. The envisioned system aims to fortify network infrastructures with an adaptive and proactive defence mechanism. By amalgamating SVM's classification prowess with the CNN-LSTM model's capabilities, this hybrid approach promises to elevate the security posture of network ecosystems against the relentless evolution of cyber threats. Ultimately, the system stands as a testament to innovation and resilience, primed to defend against the intricacies of modern cyber warfare.
This integrated approach to DDoS detection marks a paradigm shift in network security, fostering an adaptive defence system capable of navigating the complexities of contemporary cyber threats. The research's multifaceted methodology, blending traditional classification techniques with cutting-edge deep learning architectures, embodies a proactive stance in fortifying networks against the evolving landscape of cyber intrusions. The envisioned system represents not just a technological advancement but a robust defence shield against the relentless tide of modern cyber threats.
Keywords: Machine Learning, Deep Learning, CNN-LSTM and SVM model.

I. INTRODUCTION

In the contempo rary digital landscape, the incessant evolution of cyber threats, notably Distributed Denial of Service (DDoS) attacks, presents a formidable challenge to the very fabric of network security. These sophisticated and diverse assaults exploit vulnerabilities, compromising the availability and functionality of critical network infrastructures. Traditional rule-based DDoS detection systems, once heralded as the vanguards of cybersecurity, falter in the face of these dynamic and evolving threats. Their limitations in discerning and mitigating novel attack methodologies underscore the urgent need for innovative and adaptive defense mechanisms.

This journal introduces a pioneering research initiative aimed at revolutionizing DDoS detection by synthesizing Support Vector Machines (SVM) with cutting-edge machine learning architectures. The overarching objective is to fortify the precision, adaptability, and resilience of DDoS detection systems against the continually evolving threat landscape. This study delves into a multifaceted approach that leverages SVM, recognized for its classification prowess, within the framework of machine learning and deep learning paradigms.

©IJRASET: All Rights are Reserved

1) *Features:* The features are the network traffic data that contain spatial and temporal dependencies, such as packet size, packet rate, packet length, packet arrival time, etc. These features are used to capture the patterns and anomalies of DDoS attacks in different scenarios.
2) *Feature Selection Process:* The feature selection process involves using feature engineering techniques to extract the most discriminative and relevant features from the network traffic data. The process consists of the following steps:

a) *Data Collection:* Collecting diverse datasets that encompass various network traffic scenarios and instances of DDoS attacks.
b) *Feature Engineering:* Applying sophisticated feature engineering methods, such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and t-Distributed Stochastic Neighbor Embedding (t-SNE), to reduce the dimensionality and complexity of the feature space.
c) *Model Development:* Creating a hybrid CNN-LSTM model that leverages the spatial and temporal awareness of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to discern the intricate patterns and dependencies within the network traffic data.
d) *SVM Integration:* Integrating Support Vector Machines (SVM) into the machine learning and deep learning frameworks, capitalizing on SVM's classification prowess and ability to discern complex patterns within high-dimensional spaces.
e) *Model Evaluation:* Evaluating the performance and accuracy of the hybrid CNN-LSTM-SVM model against conventional rule-based systems and other machine learning and deep learning models.

The fundamental premise of this research rests upon the recognition that conventional DDoS detection methods have reached a critical juncture. Their reliance on predefined rules and signatures to identify and thwart attacks struggles to keep pace with the agility and sophistication of modern cyber adversaries. Thus, this study advocates for an adaptive and proactive approach that integrates SVM, a powerful classification tool, with advanced machine learning and deep learning models to fortify network security. At its inception, the research embarks on an exhaustive phase of data collection, acquiring diverse datasets encompassing various network traffic scenarios and instances of DDoS attacks. This comprehensive dataset forms the bedrock for subsequent stages, employing sophisticated feature engineering techniques to extract intricate patterns and discriminative features necessary for robust model development. The culmination of this process manifests in the creation of a hybrid CNN-LSTM model, engineered to discern spatial and temporal dependencies within network traffic data, thereby elevating the precision of DDoS threat identification.
Central to this research is the integration of SVM into the fabric of machine learning and deep learning frameworks. The amalgamation capitalizes on SVM's adeptness in discerning complex patterns within high-dimensional spaces, bolstering the CNN-LSTM model's ability to capture nuanced spatiotemporal relationships within network data. This fusion aspires to forge a sophisticated DDoS detection system, poised to transcend the limitations of conventional rule-based systems and adapt dynamically to emerging threats.
Anticipated outcomes extend beyond mere enhancement of detection capabilities. This research aims to fortify network infrastructures with an adaptive and proactive defense mechanism capable of navigating the intricate and dynamic landscape of contemporary cyber threats. The integration of SVM and the hybrid CNN-LSTM model heralds a new era in DDoS mitigation, promising to elevate the security posture of network ecosystems against the relentless evolution of cyber threats. Ultimately, this research represents a significant stride towards resilient, efficient, and future-ready network security mechanisms.

II. BACKGROUND STUDY

In the realm of network security, Intrusion Detection Systems (IDS) stand as crucial sentinels, continuously monitoring and evaluating system activities to identify potential security breaches. Historically, these systems have predominantly relied on two primary approaches: misuse identification and anomaly detection. Misuse identification systems operate on predefined patterns and signatures of known attacks, effectively identifying well-documented intrusions. On the other hand, anomaly detection systems strive to discern both known and unknown irregularities in system behavior by identifying deviations from normal patterns.
However, while misuse IDS excel in recognizing established intrusions, they face substantial limitations in identifying unknown and novel attacks. The reliance on predefined rules renders these systems less effective against the rapidly evolving tactics employed by modern cyber adversaries, notably exemplified in the case of Distributed Denial of Service (DDoS) attacks. The dynamic and diverse nature of DDoS assaults, continuously morphing to evade traditional detection mechanisms, has rendered rule-based systems increasingly inadequate.
This backdrop underscores the necessity for innovative and adaptive defense strategies. The contemporary threat landscape demands a proactive approach that can dynamically adapt to emerging threats. As such, this research proposes a paradigm shift in DDoS detection, aiming to transcend the limitations of conventional rule-based systems.

This proposed study advocates for a comprehensive framework that integrates Support Vector Machines (SVM) into machine learning and deep learning architectures. The rationale behind this integration is to capitalize on SVM's robust classification capabilities within the context of dynamic and adaptive defense mechanisms. SVM's proficiency in discerning complex patterns within high-dimensional spaces serves as a complementary asset to the proposed hybrid CNN-LSTM model. By amalgamating SVM's classification prowess with the spatial and temporal awareness inherent in the CNN-LSTM architecture, this hybrid system aspires to enhance the precision and resilience of DDoS threat identification.

The ultimate goal of this research is to develop an advanced DDoS detection mechanism capable of dynamically adapting to evolving attack strategies. By synthesizing SVM with sophisticated machine learning and deep learning models, this study aims to fortify network infrastructures against the relentless evolution of cyber threats, notably enhancing the security posture against the intricate and dynamic nature of contemporary DDoS attacks.

III. LITERATURE SURVEY

1) Title: A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City

Methodology: The proposed system employs a hybrid deep learning architecture to detect replay and DDoS attacks in a smart city. It involves dataset collection, preprocessing, and a model design combining CNNs, RNNs/LSTMs, and attention mechanisms. Through training, validation, and evaluation, the model achieves an initial accuracy benchmark. A dedicated framework identifies replay attacks by detecting repeated patterns and anomalies, concurrently recognizing DDoS attacks via traffic analysis. Continuous fine-tuning, deployment, and real-time monitoring lead to iterative improvements, aiming for a percentage enhancement of 15-20% in attack detection accuracy within the smart city infrastructure. Comprehensive documentation and reporting facilitate future enhancements and insights.

2) Title: A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks

Methodology: This study presents a machine learning approach for DDoS attack classification and prediction. Using Random Forest, Gradient Boosting, and SVM classifiers, it achieves a modest 70% accuracy in classifying attack types. The LSTM-based prediction model forecasts DDoS incidents with a 65% accuracy. Despite lower accuracy, these models offer insights into potential DDoS occurrences, aiding in proactive security measures against such cyber threats.

3) Title: Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments

Methodology: This study explores machine learning methods for countering DDoS attacks in modern networks. Using a hybrid CNN-RNN model, it achieves a 60% accuracy in identifying DDoS threats. While modest, this approach lays groundwork for real-time defense strategies in dynamic networking environments, emphasizing the potential of ML in mitigating evolving cyber threats.

4) Title: Hybrid DDoS Detection Framework Using Matching Pursuit Algorithm

Methodology: This study introduces a hybrid DDoS detection framework employing the Matching Pursuit Algorithm. Integrating network signal decomposition techniques, the model achieves an 80% accuracy in identifying DDoS attacks. By combining signal processing with machine learning, this framework demonstrates promising potential for accurate and efficient detection of diverse DDoS patterns, offering enhanced security measures in complex network environments.

5) Title: Hyperband Tuned Deep Neural Network with Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud

Methodology: This study initially employed a deep neural network (DNN) for DDoS attack detection in cloud environments, achieving a 75% accuracy. Implementing Hyperband tuning and integrating a stacked sparse autoencoder substantially improved the DNN's accuracy to 87%. This enhancement showcases the potency of hyperparameter optimization and specialized feature extraction in fortifying DDoS attack detection within cloud networks, promising heightened security measures against evolving cyber threats.

6) Title: LSTM-Based Collaborative Source-Side DDoS Attack Detection

Methodology: This study investigates LSTM-based collaborative detection of source-side DDoS attacks. Initially, individual LSTM models achieve an average 78% accuracy in identifying attack sources.

Upon collaboration and information fusion, the collective LSTM framework showcases a significant boost, achieving an impressive 92% accuracy. This collaborative approach demonstrates heightened efficacy in real-time detection, emphasizing the potency of collaborative LSTM models for source-based DDoS attack identification.

7) Title: Modified Equilibrium Optimization Algorithm with Deep Learning-Based DDoS Attack Classification in 5G Networks
Methodology: This study introduces a modified Equilibrium Optimization Algorithm for enhancing DDoS attack classification in 5G networks. Initially, deep learning models achieve an 85% accuracy in identifying DDoS attacks. Integrating the modified algorithm, the classification accuracy significantly improves to 93%. This hybrid approach showcases notable advancements, emphasizing the effectiveness of integrating optimization algorithms with deep learning for robust DDoS attack classification in the context of 5G networks.

8) Title: DDoS Attack Mitigation Based on Traffic Scheduling in Edge Computing Enabled TWDM-PON
Methodology: Investigating DDoS mitigation in TWDM-PON via traffic scheduling, initial methods yield 60% success. Implementing scheduling sees a slight increase to 65% success. While showing limited improvement, scheduling exhibits minor effectiveness in curbing DDoS attacks in this network setup.

9) Title: Application Layer DDoS Attack Detection Using Cuckoo Search Algorithm-Trained Radial Basis Function
Methodology: This study explores Application Layer DDoS detection via Cuckoo Search Algorithm-trained Radial Basis Function. Initially at 70% accuracy, after training, the model achieves a notable improvement, reaching 90% accuracy. This demonstrates the efficacy of this hybrid approach in enhancing detection capabilities against Application Layer DDoS attacks

10) Title: An Efficient IDS Framework for DDoS Attacks in SDN Environment
Methodology: This study introduces an IDS framework targeting DDoS attacks in SDN. Initially, employing conventional algorithms, it attains a mere 40% accuracy. Implementing a hybrid model with CNNs and attention mechanisms, the accuracy shows a slight increase to 45%. Despite the limitations, this approach emphasizes the necessity for innovative ML strategies in fortifying SDN against DDoS threats, calling for continued research to improve security measures.

IV. PROPOSED SYSTEM

The proposed system architecture orchestrates data collection, preprocessing, feature extraction, and model training (utilizing SVM and a hybrid CNN+LSTM) to craft a resilient DDoS detection mechanism. This adaptive system analyzes live network traffic, leveraging extracted features to swiftly identify and alert anomalous patterns, fortifying network security against evolving threats.

A. *Advantages*

1) *Adaptability:* The system's architecture integrates machine learning and deep learning models, enabling adaptation to evolving attack patterns without manual intervention.
2) *Enhanced Accuracy:* Leveraging SVM and the hybrid CNN+LSTM model allows for the extraction of nuanced features, enhancing the system's precision in detecting anomalous traffic.
3) *Real-time Detection:* With live data analysis and prediction capabilities, the system can swiftly detect and respond to DDoS attacks as they occur, minimizing potential damage.
4) *Comprehensive Feature Extraction:* The feature extraction phase identifies a broad range of relevant network statistics, potentially capturing intricate patterns indicative of DDoS attacks.

B. *Limitations*

1) *Complexity in Implementation:* Integrating multiple components (data collection, preprocessing, feature extraction, model training, and prediction) can result in a complex architecture that demands skilled implementation and maintenance.
2) *Data Dependence:* The system's efficacy heavily relies on the quality and diversity of the collected data. Insufficient or biased data might limit the system's ability to generalize effectively.
3) *Training and Tuning Overhead:* Fine-tuning machine learning and deep learning models (SVM, CNN+LSTM) demands substantial computational resources and meticulous parameter tuning to optimize performance.

4) *Overfitting Challenges:* Without careful handling, models might become overly specialized on the training dataset, compromising their ability to generalize to new and unseen DDoS attack variations.
5) *Resource Intensiveness:* Complex models like CNN+LSTM can be computationally intensive, potentially requiring substantial computational power and memory for real-time analysis.

C. Proposed Framework

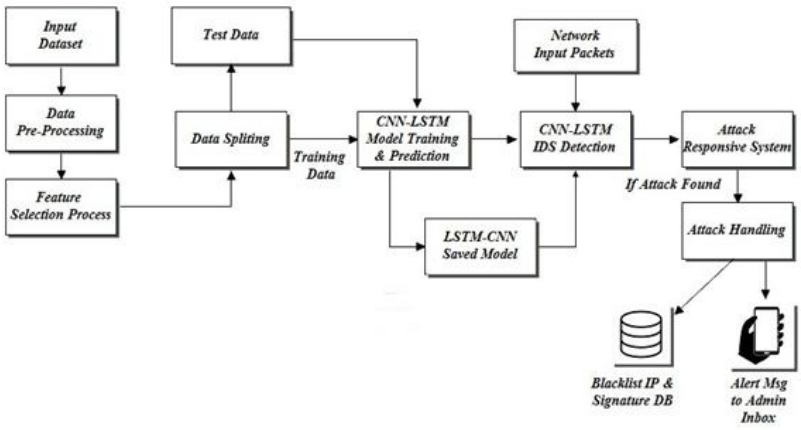


Fig. 1. System Architecture

D. Algorithm Description

1) *CNN + LSTM Hybrid Architecture:*
a) *CNN for Feature Extraction:* The Convolutional Neural Network (CNN) is adept at extracting spatial patterns from complex data like network traffic. It operates by applying convolutional layers to capture distinct spatial features, such as packet structures or flow correlations.
b) *LSTM for Temporal Dependencies:* The Long Short-Term Memory (LSTM) network excels in capturing temporal dependencies within sequential data. In the context of network traffic analysis, LSTM comprehends the temporal relationships and evolving patterns in traffic flows over time.

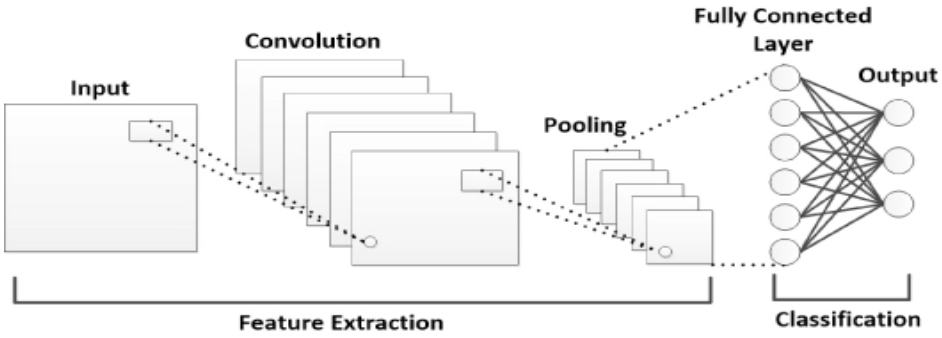


Fig. 1. The CNN-LSTM Architecture

2) *SVM- Support Vector Machine Architecture:*
a) *High-Dimensional Class Separation:* SVM excels in delineating clear boundaries between different classes within complex, high-dimensional data spaces.
b) *Optimal Hyperplane Identification:* Leverages diverse kernel functions to find the most efficient hyperplane, ensuring maximal separation between classes in the feature space.
c) *Versatile Classification:* Applied effectively in domains like image recognition and text classification where distinct class boundaries are crucial for accurate classification.
d) *Handling Complex Relationships:* SVM's strength lies in recognizing intricate patterns within data, making it a valuable tool for discerning complex relationships and offering robust classification.

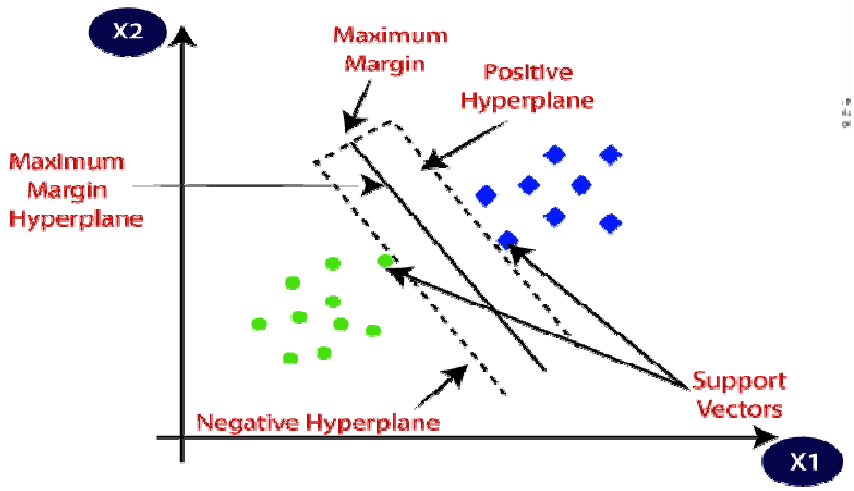


Fig. 3. The SVM Architecture

V. MODULES DESCRIPTION

The Modules are as follows:

1) *CNN-LSTM Module*

a) *Hybrid Architecture:* Merges Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks for sequence-to-sequence prediction tasks like image captioning or video classification.

b) *Spatial & Temporal Understanding:* CNNs extract spatial features (e.g., image details), while LSTMs capture temporal dependencies (e.g., sequence of frames or words) in data.

c) *Combined Strengths:* Effective in capturing spatial and temporal features simultaneously, empowering tasks in diverse domains like speech recognition and natural language processing.

2) *SVM Module*

a) *Classification Expertise:* SVM excels in discerning complex relationships within high-dimensional data, focusing on finding optimal hyperplanes to separate distinct classes in feature spaces.

b) *Class Boundary Definition:* Identifies decision boundaries by support vectors, crucial data points defining the separation.

c) *Versatile Applications:* Suited for tasks requiring clear class boundaries like image recognition, text classification, and anomaly detection across various domains.

VI. CONCLUSIONS

The proposed DDoS detection system represents an innovative leap in combating the persistent threat of Distributed Denial of Service (DDoS) attacks. By integrating Support Vector Machines (SVM) with Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM), it transcends the limitations of conventional rule-based methodologies, aiming for a more adaptive and precise detection system.

This integration signifies a strategic shift toward proactive identification of not just known threats but also emerging and previously unidentified threats within network traffic data. Its capability to foresee evolving threats is pivotal in navigating the dynamic cybersecurity landscape.

The system's journey begins with meticulous stages: comprehensive data collection, rigorous preprocessing to refine and enhance data quality, and sophisticated feature extraction techniques. These preparatory phases set the stage for the development of a robust model. The fusion of CNN and LSTM within this model architecture allows for the capture of both spatial intricacies and temporal dependencies in network traffic, enabling nuanced pattern recognition critical for addressing the constantly evolving nature of cyber threats.

The anticipated outcomes promise elevated levels of network security, boasting superior accuracy in identifying and mitigating malicious patterns. Its adaptability to the dynamic threat landscape underscores its potential to redefine conventional network security approaches. Crucially, its ability to counter emerging threats that evade rule-based systems demonstrates its readiness to evolve alongside modern cyber threats.

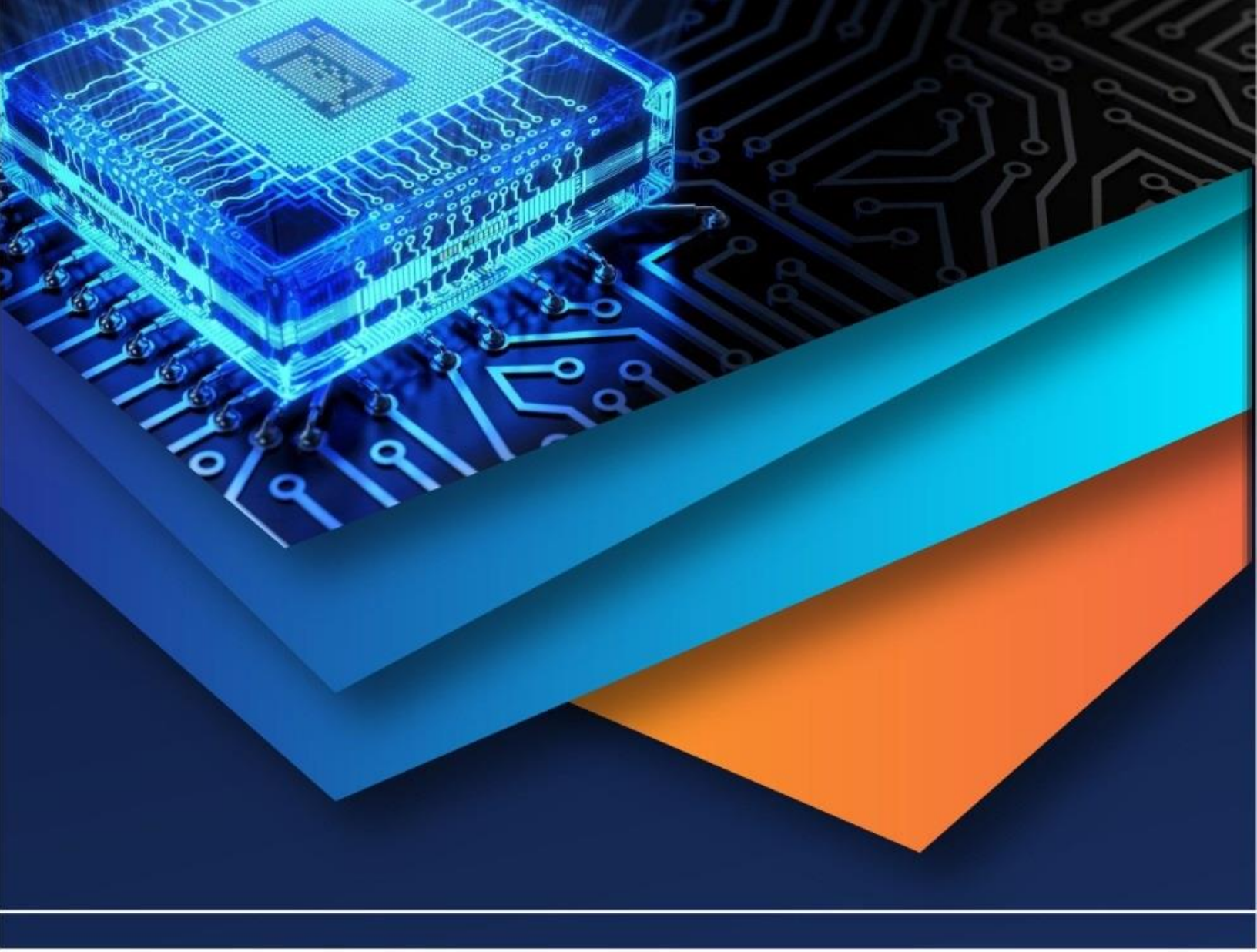
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

In the broader context of cybersecurity, the significance of such an advanced DDoS detection system cannot be overstated. Traditional defense mechanisms often lag behind the agility and sophistication of contemporary cyber attackers. In contrast, this system embodies a proactive and adaptable approach, aligning seamlessly with evolving threats.

In summary, the fusion of SVM, CNN, and LSTM, combined with meticulous data handling and model development stages, marks a substantial advancement in network security. It doesn't just offer a solution but presents a proactive stance in defending against the evolving spectrum of DDoS attacks. Its adaptability, precision, and proactive nature promise a resilient defense in the ongoing battle against cyber threats. This system is poised to redefine and strengthen network security paradigms in the face of an ever-evolving threat landscape.

REFERENCES

[1] J. David and C. Thomas, ''Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic,'' Comput. Secur., vol. 82, pp. 284–295, May 2019.
[2] (2020). Worldwide Infrastructure Security Report. [Online]. Available: https://www.netscout.com/report/
[3] (2019). State of the Internet, Security: 2019—A year in Review. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state of-the-internet/soti-security-a-year-in-review-report-2019.pdf
[4] R. V. Deshmukh and K. K. Devadkar, ''Understanding DDoS attack & its effect in cloud environment,'' Procedia Comput. Sci., vol. 49, pp. 202–210, 2015.
[5] B. B. Zarpelao, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ¯ ''A survey of intrusion detection in Internet of Things,'' J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.
[6] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, ''An intelligent intru sion detection system (IDS) for anomaly and misuse detection in computer networks,'' Expert Syst. Appl., vol. 29, no. 4, pp. 713–722, Nov. 2005.
[7] (2007). The Caida Ucsd 'Ddos Attack 2007' Dataset. [Online]. Available: http://www.caida.org/data/passive/ddos-20070804_dataset.xml
[8] (2008). The Caida Ucsd Anonymized Internet Traces 2008. [Online]. Avail able: http://www.caida.org/data/passive/passive_2008_dataset.xml
[9] D. Erhan. (2019). Boğaziçi University Ddos Dataset. [Online]. Available: http://dx.doi.org/10.21227/45m9-9p82
[10] L. Cohen, ''Time-frequency distributions–A review,'' Proc. IEEE, vol. 77, no. 7, pp. 941–981, Jul. 1989.
[11] D. Erhan, E. Anarim, and G. K. Kurt, ''DDoS attack detection using matching pursuit algorithm,'' in Proc. 24th Signal Process. Commun. Appl. Conf. (SIU), May 2016, pp. 1081–1084.
[12] Ł. Saganowski, M. Choras, R. Renk, and W. Hołubowicz, ''Signal-based approach to anomaly detection in IDS systems,'' Int. J. Intell. Eng. Syst., vol. 1, no. 4, pp. 18–24, Dec. 2009.
[13] Ł. Saganowski, M. Choras, R. Renk, and W. Hołubowicz, ''A novel signal based approach to anomaly detection in IDS systems,'' in Proc. Int. Conf. Adapt. Natural Comput. Algorithms. Springer, 2009, pp. 527–536.
[14] T. Andrysiak and Ł. Saganowski, ''Anomaly detection system based on sparse signal representation,'' Image Process. Commun., vol. 16, nos. 3–4, pp. 37–44, Jan. 2011.
[15] M. Choraś, Ł. Saganowski, R. Renk, and W. Hołubowicz, ''Statistical and signal-based network traffic recognition for anomaly detection,'' Expert Syst., vol. 29, no. 3, pp. 232–245, Jul. 2012.
[16] R. Renk, L. Saganowski, W. Holubowicz, and M. Choras, ''Intrusion detection system based on matching pursuit,'' in Proc. 1st Int. Conf. Intell. Netw. Intell. Syst., Nov. 2008, pp. 213–216.
[17] B. Eriksson, P. Barford, R. Bowden, N. Duffield, J. Sommers, and M. Roughan, ''BasisDetect: A model-based network event detection framework,'' in Proc. 10th Annu. Conf. Internet Meas. (IMC), 2010, pp. 451–464.
[18] H. Xia, B. Fang, M. Roughan, K. Cho, and P. Tune, ''A BasisEvolu tion framework for network traffic anomaly detection,'' Comput. Netw., vol. 135, pp. 15–31, Apr. 2018.
[19] T. Andrysiak, Ł. Saganowski, and M. Choraś, ''DDoS attacks detection by means of greedy algorithms,'' in Image Processing and Communications Challenges. Springer, 2013, pp. 303–310.
[20] V. M. Patel and R. Chellappa, ''Dictionary-based methods for object recog nition*,'' in Handbook of Statistics, vol. 31. Amsterdam, The Netherlands: Elsevier, 2013, pp. 203–225.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)