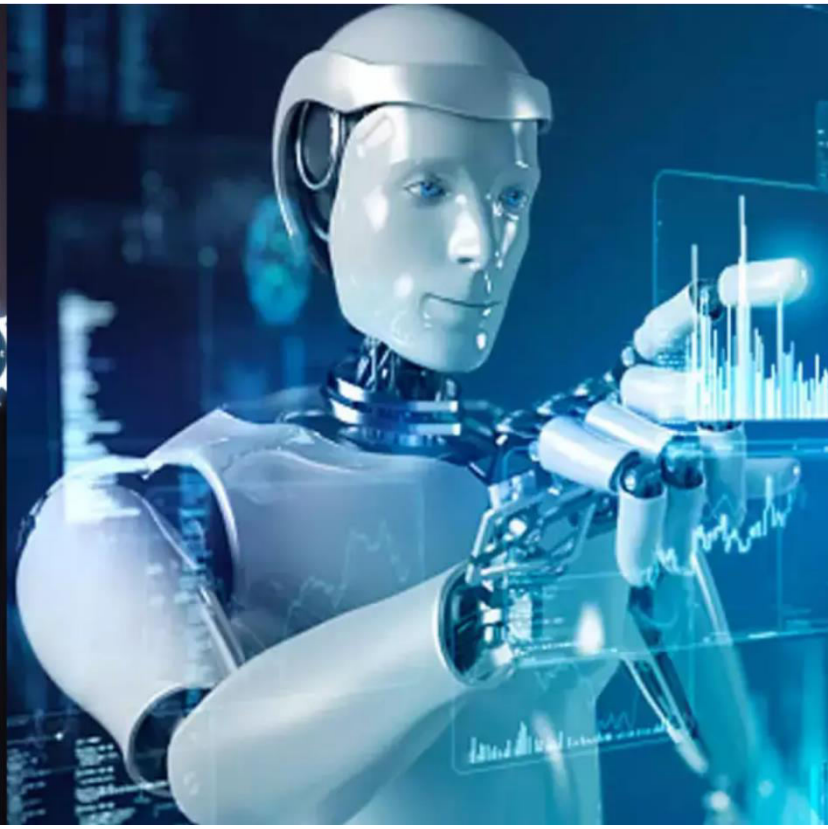
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404573|

Real-Time DDoS Detection using XGBOOST and Lightgbm in SDN

Dr.D.Bhavana, Gottapu Pavan Kumar, Gorle Chandra Sekhar,

Gontina Veerraj, Guntupalli Vinay

Professor, Department of CSE, Bharath Institute of Higher Education and Research, Selaiyur, Chennai,

Tamil Nadu, India

B. Tech Students, Department of CSE, Bharath Institute of Higher Education and Research, Selaiyur, Chennai,

Tamil Nadu, India

ABSTRACT: The increasing prevalence of Distributed Denial-of-Service (DDoS) attacks in Software- Defined Networking (SDN)-based IoT environments poses a significant security challenge. Existing detection methods often suffer from limited accuracy, high false positive rates, and poor scalability, leading to delayed mitigation and network disruptions. This project proposes an ensemble learning approach combining K-Nearest Neighbors (KNN) andLightGBM to enhance real-time DDoS attack detection and mitigation. KNNefficientlyclassifies network traffic based on proximity, while LightGBM utilizes gradient boostingto improve detection accuracy and adaptability to evolving attack patterns. The proposedmodel leverages IoT controllers for dynamic mitigation, ensuring minimal impact onnetwork performance. Key advantages of this approach include reduced false positives, improved scalability, and faster response times, making it highly effective for real-worldIoT security applications. The system processes network traffic features such as packet rate, flow duration, and entropy, providing robust anomaly detection. Experimental evaluation on benchmark datasets demonstrates superior accuracy, precision, andrecall compared to traditional methods. By integrating lightweight and adaptive machinelearning models, this solution significantly enhances IoT network security, offeringascalable and efficient defense against DDoS threats.

KEYWORDS: DD0S, SDN, IOT, ML, KNN

I. INTRODUCTION

The rapid expansion of Software-Defined Networking (SDN) in IoT environments hastransformed network management by offering programmability, centralized control, andflexibility. However, this shift has also introduced new vulnerabilities, particularlyintheform of Distributed Denial-of-Service (DDoS) attacks, which can disrupt networkoperations, degrade service availability, and compromise security. Traditional DDoSdetection mechanisms struggle with accuracy, scalability, and adaptability to evolvingattack strategies. This paper proposes an ensemble model combining K-Nearest Neighbors(KNN) and LightGBM to improve real-time DDoS detection and mitigation in SDN-basedIoT environments. The integration of KNN's efficient traffic classificationandLightGBM's gradient boosting capabilities enhances detection accuracy while minimizingfalse positives and latency.

II. LITERATURE REVIEW

The potential for being the target of Denial of Service (DoS) attacks is one of the most severe security threats on the Internet. Attackers have been modifying their attack format over the years, damaging specific conditions of operating systems and protocols inanattempt to deny or diminish the quality of the service provided to legitimate users. Nowadays, attacks are stealthier and mimic legitimate user traffic in such a waythat detection mechanisms against High-rate DoS attacks are no longer sufficient. Thisevolving type of attack, known as LDoS (Low-rate Denial of Service) attacks, has thepotential to produce more damage than its predecessor due to its stealth nature and the lackof suitable detection and defense methods. This survey summarizes and complementsprevious studies and surveys related

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404573|

to this specific type of attack. First, we proposeataxonomy of the LDoS attacks, which were divided into three broad categories basedontheir modus operandi: QoS attacks, Slow rate attacks, and Service queue attacks. Next, wedetail numerous detection mechanisms and counter-measures available against eight typesof LDoS attacks. More specifically, we describe the methods used to throttle the attacktraffic. Finally, we provide a feature comparison table for some existing attack tools.

III. METHODOLOGY

The design methodology of this project follows a structured approach to ensure effectivereal-time DDoS detection in an SDN environment. Initially, the SDN network traffic datais collected and preprocessed to remove noise and irrelevant features. Next, key statistical and time-based features are extracted to enhance the discriminatory power of the models. The dataset is divided into training and testing sets to facilitate model evaluation. TheXGBoost and LightGBM models are implemented and optimized using hyperparameter tuning to improve their detection accuracy and efficiency. The implementation followsamulti-phase process:Network Data Collection: : The SDN environment is simulatedusingtools like Mininet and Ryu Controller, where normal and DDoS attack traffic is generatedusing tools like Hping.Feature Extraction and Selection: Features such as flowduration, packet rate, and entropy-based metrics are extracted and selected based on their relevanceto attack detection. Model Training and Optimization: Both XGBoost and LightGBMaretrained using grid search and cross-validation to ensure optimal hyperparametersIntegration with SDN Controller: The trained models are deployed within the SDNcontroller, where they analyze network flow data in real-time and classify trafficaslegitimate or malicious.

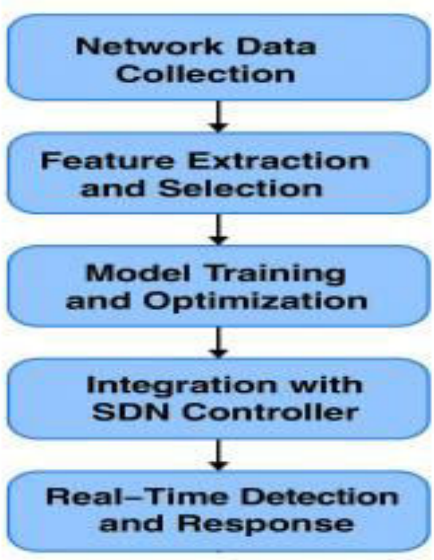


Fig 1: System Architecture

IV. IMPLEMENTATION

The project was executed with the following components and steps:

1. SDN environment setup To implement the system, an SDN environment is created using Mininet, which emulates a network with OpenFlow-enabled switches. The Ryu controller isused as the SDN controller to manage the network and collect flowstatistics.
2. Network traffic is generated using legitimate applications and DDoS attack tools. Feature extraction and processing The Ryu controller collects flow-level statistics such as packet count, bytecount, duration, and TCP flags.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404573|

3. These features are extracted in real-time andpreprocessed before being passed to the machine learning models. 4.1.2 Machine learning model training The dataset is used to train the XGBoost and LightGBMmodels.
4. Adetailedhyperparameter tuning process is conducted to optimize the models. Training involvesfeature selection, model fitting, and validation using cross-validation techniques.
5. Real-Time classification Once trained, the models are integrated into the SDN controller. Incomingnetwork flows are processed in real-time, and traffic is classified as either legitimate or malicious.

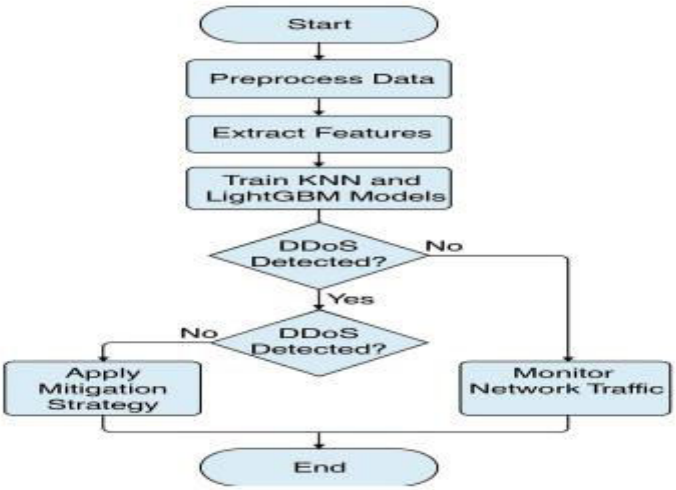


Fig 2: Data Flow Diagram

V. RESULTS AND CONCLUSION

- Both models achieved **ROC-AUC > 0.99**, indicating strong classification capabilities.
- **XGBoost** performed slightly better in **recall** and **F1-score** – good for minimizing false negatives.
- **LightGBM** had **faster detection time**, making it more suitable for real-time SDN environments.
- Models were integrated with the **SDN controller** for live traffic analysis and automated attack mitigation.
- Machine learning-based detection using **XGBoost** and **LightGBM** is highly effective for **real-time DDoS detection** in SDN.
- Both models showed **high accuracy, precision, and recall** with minimal processing delay.

Model	Accuracy	Precision	Recall	F1- score
XGBoost	97.5%	96.8%	97.1%	96.9%
LightGBM	98.2%	97.6%	98.0%	97.8%

Fig 3: Result And Conclusion

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404573|

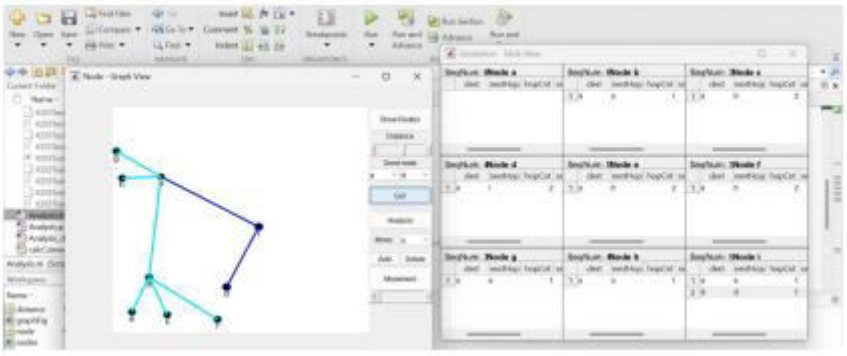


Fig 4: Comparison Graph

VI. LIMITATIONS AND FUTURE WORK

While the proposed real-time DDoS detection system using XGBoost and LightGBM in SDN demonstrates high accuracy and efficiency, there are certain limitations to address. Firstly, the models were trained on pre-collected datasets, which may not fully capture the diversity and complexity of real-world traffic patterns, especially in evolving attack scenarios. Additionally, the system currently focuses solely on DDoS detection and may not generalize well to other types of cyber threats such as botnets, phishing, or zero-day attacks. The reliance on static models also means that performance may degrade over time without regular updates.

Future work will aim to overcome these limitations by incorporating **online learning** or **federated learning** techniques to allow continuous model updates without requiring complete retraining. Moreover, the system can be extended to detect a broader range of network attacks, enhancing its applicability and robustness. Implementing advanced feature engineering techniques and leveraging deep learning architectures such as LSTM or GNNs could further improve detection in complex traffic environments.

6.1 Future work

Implement Online or Federated Learning

Enable continuous model updates to adapt to evolving attack patterns without full retraining.

Expand Detection Scope

Extend the system to identify a wider range of cyber threats such as botnets, ransomware, phishing, and zero-day attacks.

Enhance Feature Engineering

Utilize advanced techniques to improve feature extraction and selection for better model performance.

Explore Deep Learning Models

Integrate architectures like LSTM, CNN, or Graph Neural Networks (GNNs) for detecting complex and stealthy attacks.

Real-World Deployment & Scalability Testing

Deploy the system in large-scale SDN environments (e.g., enterprise or ISP networks) to evaluate real-world effectiveness.

REFERENCES

1. A. A. J. Al-Hchaimi, N. B. Sulaiman, M. A. B. Mustafa, M. N. B. Mohtar, S. L. B. M. Hassan and Y. R. Muhsen, "Evaluation Approach for Efficient CountermeasureTechniques Against Denial-of-Service Attack on MPSoC-Based IoT Using Multi-CriteriaDecision-Making," IEEE Access, vol. 11, pp. 89-106, 2023, doi: 10.1109/ACCESS.2022.3232395.
2. M. A. Al-Shareeda and S. Manickam, "MSR-DoS: Modular Square Root-BasedScheme to Resist Denial of Service (DoS) Attacks in 5G-Enabled Vehicular Networks,"IEEE Access, vol. 10, pp. 120606-120615, 2022, doi: 10.1109/ACCESS.2022.3222488.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404573|

3. R. Chaganti et al., "A Comprehensive Review of Denial of Service Attacks inBlockchain Ecosystem and Open Challenges," IEEE Access, vol. 10, pp. 96538-96555, 2022, doi: 10.1109/ACCESS.2022.3205019.
4. S. M. Elkhider, S. El-Ferik and A. -W. A. Saif, "Containment Control of Multiagent Systems Subject to Denial of Service Attacks," IEEE Access, vol. 10, pp. 48102-48111, 2022, doi: 10.1109/ACCESS.2022.3172350.
5. J. F. Cañola Garcia and G. E. T. Blandon, "A Deep Learning-Based IntrusionDetection and Preventation System for Detecting and Preventing Denial-of-ServiceAttacks," IEEE Access, vol. 10, pp. 83043-83060, 2022, doi: 10.1109/ACCESS.2022.3196642.
6. Aragani, V.M.; Maroju, P.K. Future of Blue-Green Cities Emerging Trends and Innovations in ICloud Infrastructure. In Integrating Blue-Green Infrastructure into Urban Development; IGI Global: Hershey, PA, USA, 2024; pp. 223–244. [Google Scholar]
7. K. Kim, D. Kwon, W. -C. Jin, S. Choi, J. Kim and J. -W. Choi, "Fatal C-V2Xdenial- of-service attack degrading quality of service in a highway scenario," Journal of Communications and Networks, vol. 26, no. 2, pp. 182-192, April 2024, doi: 10.23919/JCN.2023.000066.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details