iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72377

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 13 Issue VI June 2025- Available at www.ijraset.com

Dynamic Network Mapping and Traffic Intelligence for Cyber Simulations

Karthikeyan. S[1], Sarankumar N[2]
[1]*Assistant Professor, II MCA*
[1,2]*Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur*

Abstract: ***Ensuring seamless data flow while identifying irregularities is essential in network management. This project utilizes Long Short-Term Memory (LSTM) neural networks to predict network traffic patterns and applies the Isolation Forest algorithm to detect anomalies within the data. A synthetic dataset, designed to reflect fluctuations in traffic, is employed to train the LSTM model for forecasting upcoming traffic volumes. Simultaneously, the Isolation Forest algorithm flags unusual traffic behavior, which may signal network disruptions, cyber threats, or performance bottlenecks. This dual-method strategy strengthens network performance, boosts security, and optimizes resource distribution by delivering precise traffic forecasts and prompt anomaly alerts.***

Keywords: Isolation Forest , Anomaly Detection , Synthetic Dataset , Traffic Forecasting , Cyber Threats .

I. INTRODUCTION

The Framework for Network Topology Generation and Traffic Prediction Analytics for Cyber Exercises is an all-encompassing system designed to advance cybersecurity training. It facilitates the automated design of lifelike network architectures and models traffic behavior using predictive techniques. This empowers organizations to carry out more impactful cyber drills by replicating authentic network dynamics, uncovering potential vulnerabilities, and evaluating defense mechanisms in a realistic yet controlled environment. The framework enhances the effectiveness of cybersecurity preparedness through better planning, real-time monitoring, and performance assessment.

II. PROPOSED WORK

A. Overview

The proposed solution integrates Deep Learning, specifically Long Short-Term Memory (LSTM) networks, for predicting network traffic, and employs Machine Learning techniques like Isolation Forest to identify anomalies. This system offers an intelligent, real-time method for anticipating network bottlenecks, recognizing abnormal traffic behavior, and strengthening overall network defense.

B. Core Components of the System

1) Network Topology Simulation: A simulated network layout is built using a directed graph structure via the NetworkX library. Each link (edge) is assigned a randomized value to represent metrics such as latency or bandwidth. The architecture is easily adaptable, allowing it to scale according to various cybersecurity exercise sizes and specifications, while maintaining high predictive accuracy.

2) Traffic Data Creation and Preprocessing: Artificial network traffic is produced by combining sinusoidal trends with random noise, effectively simulating the variability seen in real-world traffic patterns. The generated data is then scaled using the MinMaxScaler technique to ensure consistent input ranges, and sequential datasets are structured to fit the requirements of the LSTM model.

3) LSTM-Powered Traffic Forecasting: A Long Short-Term Memory (LSTM) neural network is trained using the processed traffic sequences. The model captures historical data trends to estimate upcoming traffic volumes. This approach supports proactive management by reducing the risk of network congestion and enabling better utilization of network resources.

III. MODULES

A. Dataset Collection

Collects network traffic information from either simulated environments or existing datasets. This information serves as the core input for training machine learning models focused on traffic monitoring and cybersecurity analysis.

B. Dataset

Utilizes organized data formats such as CSV files, which include details like timestamps, traffic volume, source and destination addresses, and network protocols. This ensures that the data used for analysis is both relevant and of high quality.

C. Data Preparation

Processes the dataset by filling in incomplete values, applying normalization techniques, and segmenting the data into separate training and validation sets. This phase is essential to ensure reliable and precise outcomes from machine learning models.

D. Model Selection

Selects the most appropriate machine learning models for the given problem—for example, using LSTM networks for forecasting time-dependent data or applying Isolation Forest to identify anomalies in traffic patterns.

E. Analyze and Prediction

Utilizes the trained model on network traffic to uncover irregularities or anticipate surges in usage, aiding in the early detection of potential cybersecurity threats.

F. Accuracy on Test Set

Assesses the model's effectiveness by testing it on separate data, using evaluation metrics such as MAE, RMSE, and R^2 to gauge the accuracy and consistency of its predictions.

G. Saving the Trained Model

After successful validation, the model is stored for later use, enabling ongoing forecasting and anomaly identification without the need for repeated training.

IV. RESULT

The exploration of Dynamic Network Mapping and Traffic Intelligence in Cyber Simulations resulted in the creation of a system with the following key capabilities

Live Network Topology Tracking: The system dynamically maps network architecture and activity in real time, offering clear visibility into data flow and node connectivity as the network changes.

Advanced Traffic Analysis: By applying statistical techniques and machine learning algorithms, the system can examine traffic patterns, pinpoint irregularities, and forecast potential surges or malicious activities.

Support for Cyber Attack Simulations: It provides a flexible and realistic platform for modeling cyber-attacks, helping to evaluate defense mechanisms and refine response tactics effectively.

Enhanced Threat Detection: Techniques such as Long Short-Term Memory (LSTM) and Isolation Forest were employed to detect deviations from normal behavior, boosting the system's ability to recognize threats early.

Optimized Operational Efficiency: After being trained and validated, models were stored for ongoing use, enabling consistent traffic analysis and anomaly detection without the overhead of retraining.

V. CONCLUSION

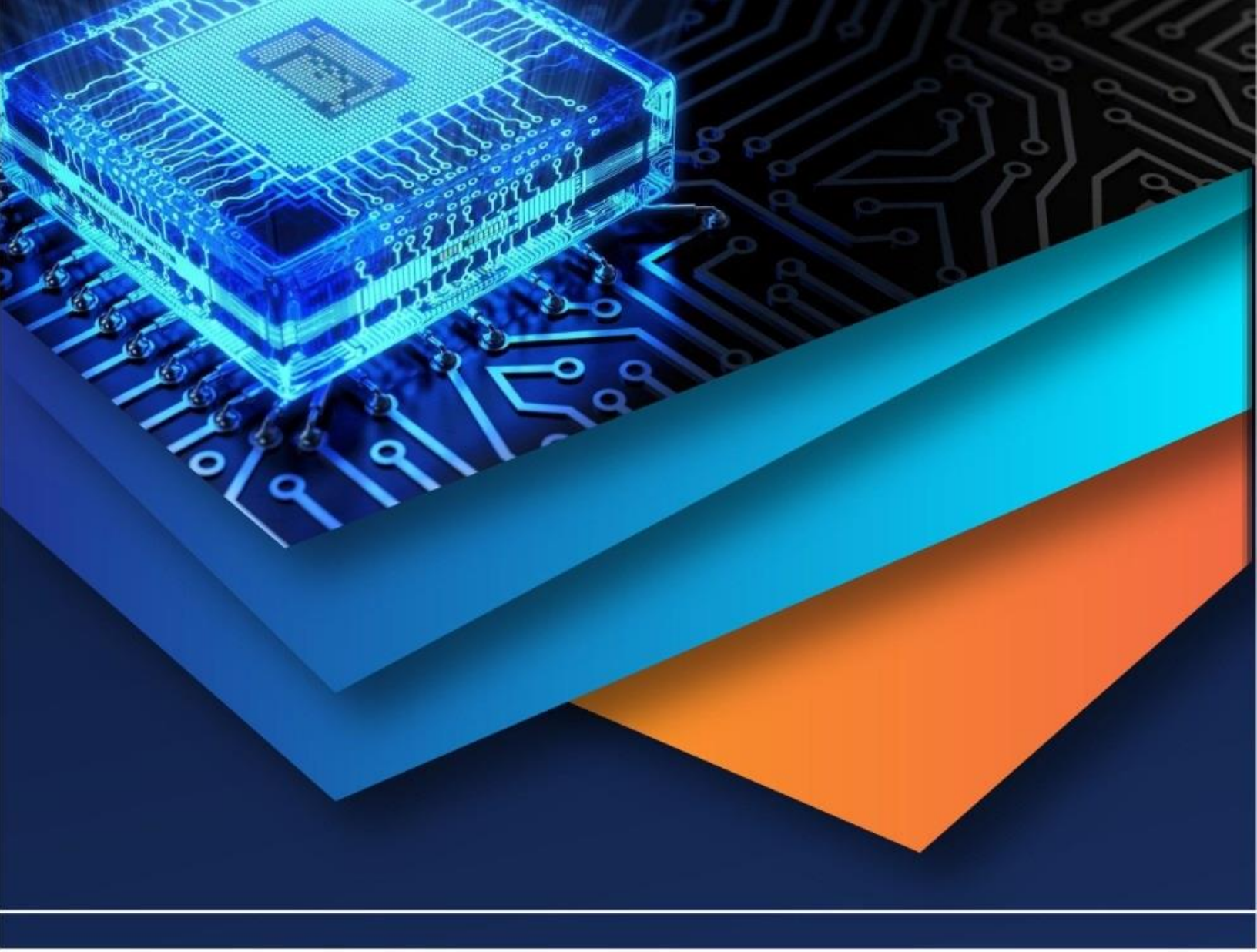
The framework designed for generating network topology and performing traffic prediction analytics significantly strengthens the cybersecurity stance of contemporary digital infrastructures. With the rise in advanced cyber threats, the ability to analyze and anticipate network activity is becoming crucial for proactively mitigating potential security breaches.

VI. ACKNOWLEDGMENT

The authors affirm that this study was conducted autonomously, without any external financial support or contributions requiring acknowledgment.

REFERENCES

[1] Barabási, A.-L. (2002). Linked: The New Science of Networks. Perseus Publishing.Offers essential knowledge on network science and the modeling of complex systems, forming a theoretical base for understanding network structures.
[2] Zhang, Y., & Paxson, V. (2000). Detecting Stepping Stones. USENIX Security Symposium.A key resource for grasping techniques used to detect intrusions by analyzing patterns within network traffic.
[3] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey.Provides an in-depth overview of various anomaly detection strategies that are highly relevant for cybersecurity data analysis.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY