IJRDET

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 3, March 2026)

Predicting Cyber Attacks with Machine Learning Intelligence

M. Elakiya[1], Ms.C. Durga devi [2],

[1],Second year M.Sc. Computer Science, School of Computer Studies, A.V.P. College of Arts and Science (Autonomous), Tirupur, Tamil Nadu, India.
[2]Assistant Professor, School of Computer Studies, A.V.P. College of Arts and science (Autonomous), Tirupur, Tamil Nadu, India.

Abstract-* The rapid growth of cyber threats has made traditional manual intrusion detection methods inefficient and error-prone modern cyber-attacks such as DoS, R2L, U2R, and Probe attacks require intelligent and automated detection mechanisms this study proposes a machine learning-based framework for predicting cyber-attacks in Software Defined Network (SDN) environments a large-scale SDN dataset containing 1.18 million network traffic records with 79 features was used for classification a multiple supervised learning algorithms, including Decision Tree, Support Vector Classifier (SVC), Random Forest, and Multi-Layer Perceptron (MLP), were implemented and compared Performance was evaluated using accuracy, precision, recall, and F1-score. Experimental results show that the Random Forest classifier achieved the highest accuracy of 93.6% and demonstrating superior performance in detecting and classifying the network intrusions and the proposed system enhances proactive cyber defence through automated and scalable threat detection.

***Keywords-* Cyber Security, Machine Learning, Intrusion Detection System (IDS), Software Defined Network (SDN), Random Forest, Classification, Network Traffic Analysis**

I. INTRODUCTION

The increasing dependency on a digital network has significantly elevated the risk of cyber-attacks traditional security mechanisms such as firewalls and signature-based intrusion detection systems are largely a reactive and fail to address evolving attack patterns. Machine Learning (ML), a subset of Artificial Intelligence (AI), offers data-driven techniques and capable of identifying complex patterns in network traffic and predicting potential threats before severe damage occurs this research models cyber-attack prediction as a supervised classification problem the dataset, is collected from an SDN environment, consists of 79 quantitative and qualitative features and representing network flow characteristics it includes both benign traffic and various attack types such as DDoS, XSS, Brute Force, and SQL Injection.

The main objective of this work is to develop an efficient automated cyber-attack detection system and compare multiple ML algorithms to identify the most accurate model of a flask-based web application is also developed to enable real-time prediction and visualization of attack patterns.

II. LITERATURE REVIEW

The recent research in cyber security emphasizes the importance of machine learning techniques for intrusion detection traditional methods rely heavily on predefined rules and signature databases, making them ineffective against zero-day attacks and evolving threats the supervised learning models such as Support Vector Machines (SVM), Decision Trees, Logistic Regression, and Neural Networks have been widely applied for attack classification it ensemble learning methods like Random Forest have shown improved accuracy due to their ability to reduce overfitting and enhance generalization the several studies highlight the challenge of class imbalance in intrusion datasets, which affects the detection of rare but critical attack types the recent advancements include hybrid models and deep learning approaches such as CNNs and RNNs for capturing complex traffic patterns.

However, computational complexity and scalability remain concerns in real-time environments this study builds upon existing work by performing a comparative evaluation of multiple classifiers and identifying the most efficient model for SDN-based intrusion detection.

III. METHODOLOGY

This research adopts a supervised machine learning approach to detect cyber-attacks in Software Defined Networks (SDN).

The dataset consists of 1,188,333 labeled network traffic records with 79 features, including both benign and malevolent traffic such as DDoS, XSS, Brute Force, and SQL Injection attacks. Initially, data preprocessing was performed to handle missing and infinite values, followed by standardization to ensure uniform feature scaling. Exploratory Data Analysis (EDA) was showed to understand class distribution and detect imbalance in attack categories. Feature selection techniques were applied to remove redundant attributes and retain significant network flow features that contribute to intrusion detection. Four sorting algorithms were applied: Decision Tree, Support Vector Classifier (SVC), Random Forest, and Multi-Layer Perceptron (MLP). The dataset was divided into 80% training and 20% testing data. Models were estimated using accuracy, precision, recall, F1 score, and confusion matrix analysis to measure detection performance and generalization capability.

IV. RESULTS AND DISCUSSION

Experimental results indicate that ensemble-based learning methods outstrip single classifiers. Random Forest achieved the highest precision of 93.6% and F1 score of 0.93, signifying strong capability in detecting both common and rare attack types. MLP and SVC also produced competitive results, while Decision Tree showed comparatively lower performance due to overfitting tendencies. The analysis confirms that Random Forest well reduces false positives and false negatives, making it more reliable for real-world intrusion detection. The integration of the trained model into a Flask-based web application further enhances usability by enabling visualization and automated attack prediction

Table 1

Experimental Results of Machine Learning Models

Model	Accuracy (%)	F1 Score
Random Forest	93.6	0.93
MLP	91.8	0.91
SVC	90.7	0.90
Decision Tree	88.5	0.88

V. CONCLUSION AND FUTURE WORK

This study demonstrates the effectiveness of machine learning techniques for detecting cyber-attacks in Software Defined Networks. By analyzing large-scale network traffic data, the system successfully classified many attack types including DDoS, Brute Force, XSS, and SQL Injection.

Among the evaluated models, Random Forest achieved the highest accuracy and overall performance, showing strong ability in handling high-dimensional network traffic data and falling prediction errors. The addition of machine learning models with a Flask-based web application enables automated cyber-attack prediction and visualization, providing a practical solution for network administrators to monitor potential threats. The outcomes confirm that machine learning-based intrusion detection systems can significantly improve cybersecurity by enabling early detection and rapid response to malicious actions.

Future improvements can focus on addressing class inequality issues, particularly for rare attacks such as SQL Injection, by applying innovative resampling techniques such as SMOTE. Additionally, mixing deep learning copies such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) may further enhance detection accuracy by capturing complex network traffic patterns. Present intrusion detection using streaming data and online learning algorithms can also be explored to improve system responsiveness in dynamic network environments. Furthermore, deploying the system in cloud-based or edge computing environments will enhance scalability and enable real-time protection for large-scale enterprise networks.

References

[1] Lutz, M. (2013). Learning Python, 5th Edition (5 edition). Beijing: O'Reilly Media.

[2] Tibbits, S., van der Harten, A., & Baer, S. (2011). Rhino Python Primer (3rd ed.).

[3] Downey, A. B. (2015). "Think Python: How to Think Like a Computer Scientist (2 edition)". Sebastopol, CA: O'Reilly Media.

[4] Greg Wilson. "Data crunching: solve everyday problems using Java, Python and more. The pragmatic programmers", Pragmatic Bookshelf, Raleigh.

[5] Guido van Rossum and Fred L. Drake, Jr. "The Python Tutorial — An Introduction to Python". Network Theory Ltd., Bristol,

[6] Michael Dawson. "Python programming for the absolute beginner". Premier Press Inc., Boston, MA, USA, 2003.

[7] Harvey M. Deitel, Paul Deitel, Jonathan Liperi, and Ben Wiedermann "Python How To Program". P T R Prentice-Hall, Englewood Cliffs.

[8] Brad Dayley. "Python phrasebook: essential code and commands. Developer's library". SAMS Publishing, Indianapolis,

[9] Liza Daly. "Next-generation web frameworks in Python". O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol.

[10] Mike Dawson. "Python programming for the absolute beginner". Thomson Course Technology, Boston,

[11] Peter Norton, Alex Samuel, David Aitel, Eric Foster-Johnson, Leonard Richardson, Jason Diamond, Aleatha Parker, Michael Roberts, "Begining Python", 2005.