International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 10, Issue 5, May-2025, http://ijmec.com/, ISSN: 2456-4265

Online Bus Ticketing Application

Kolli Chiranjivi Venu Gopal
PG scholar, Department of MCA, CDNR collage, Bhimavaram, Andhra Pradesh.
K.Venkatesh
(Assistant Professor), Master of Computer Applications, DNR collage, Bhimavaram, Andhra Pradesh.

Abstract

The proliferation of web-based applications and services has led to a significant rise in the frequency and sophistication of cyberattacks. From SQL injections to cross-site scripting (XSS) and denial-of-service (DoS) attacks, these threats can cause serious disruptions and data breaches. The need for intelligent, scalable, and accurate detection systems is more urgent than ever. This project aims to conduct a comprehensive performance analysis of various Machine Learning (ML) and Deep Learning (DL) algorithms to detect web-based attacks effectively. By leveraging well-established datasets and evaluation metrics, we assess each algorithm's capacity to identify different categories of web threats. The models explored include both classical ML algorithms—such as Support Vector Machines (SVM), Decision Trees, and Random Forests—and advanced DL models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. Each of these is evaluated under consistent data and performance metrics.

Through comparative analysis, this research seeks to recommend the most efficient models for real-time implementation, balancing performance, scalability, and interpretability. The insights gained will contribute to the design of more robust intrusion detection systems for modern web infrastructure.

Introduction

In recent years, the internet has become integral to daily life and commerce, making it a primary target for cyberattacks. Web-based applications often hold sensitive data and serve critical services, which makes securing them a top priority for organizations.

Web attacks exploit vulnerabilities in applications and protocols, which, if undetected, can result in data leaks, financial losses, and service downtime. Traditional intrusion detection systems (IDS), which rely on fixed rules and known signatures, often fail to detect novel or obfuscated attack patterns.

Machine Learning and Deep Learning technologies offer dynamic and adaptive mechanisms for web attack detection. These methods can generalize from known patterns and identify unknown attacks based on statistical anomalies and behavioral changes in web traffic.

The objective of this project is to investigate how different ML/DL models perform in the context of web attack detection. By identifying their strengths and weaknesses, we can guide the selection and deployment of suitable models in real-time web environments.

Literature Survey

1. Several studies have employed ML techniques for network intrusion detection. For instance, SVM and Random Forests

have demonstrated high accuracy when classifying network traffic as benign or malicious, particularly using datasets like NSL-KDD and CICIDS2017.

2. Deep learning models such as CNNs have been used to automatically extract spatial features from raw input data, eliminating the need for manual feature engineering. This makes them suitable for complex tasks like detecting polymorphic web attacks.

3. LSTM and GRU networks, known for their ability to model sequential data, have been used to detect attacks that unfold over time. Their ability to learn long-term dependencies makes them ideal for identifying advanced persistent threats.

4. Hybrid models combining traditional ML with DL elements are gaining traction. For instance, CNN-LSTM networks have achieved superior accuracy in classifying multi-step attacks. These models also offer better adaptability and lower false-positive rates.

Existing Method

1. Traditional intrusion detection systems can be broadly categorized into signature-based and anomaly-based detection systems. Signature-based methods detect known threats by matching patterns, but they fail against zero-day and evolving attacks.

2. Anomaly-based systems monitor the baseline behavior of network traffic and flag deviations as potential threats. While capable of detecting new attacks, they tend to produce higher false positives due to the variability in web behavior.

3. Classical ML approaches have been adopted to enhance these systems. Algorithms like Decision Trees, Naïve Bayes, and k-NN rely on structured features from traffic logs but often lack the ability to detect complex, high-dimensional patterns.

4. Though these models serve as good baselines, their performance plateaus with increasing data complexity. Additionally, they require manual feature selection, which is time-consuming and may overlook critical information hidden in raw traffic data.

Proposed Method

1. The proposed system involves a comparative study using both ML and DL models to identify which algorithms are most effective in detecting web attacks. Benchmark datasets such as CICIDS2017 and UNSW-NB15 will be used for training and evaluation.

2. Data preprocessing includes steps like feature normalization, label encoding, and balancing using Synthetic Minority Over-sampling Technique (SMOTE) to ensure fairness across all models. All models are trained on identical training-test splits for valid comparisons.

3. The selected models include SVM, Random Forest, Decision Tree, CNN, LSTM, and hybrid CNN-LSTM. These are evaluated using metrics such as Accuracy, Precision, Recall, F1-Score, and AUC.

Confusion matrices and ROC curves are used for visual analysis.

4. Based on empirical results, the best-performing models will be recommended for real-time detection scenarios. The goal is to achieve high detection accuracy with minimal false positives while maintaining computational efficiency and scalability.

RESULT

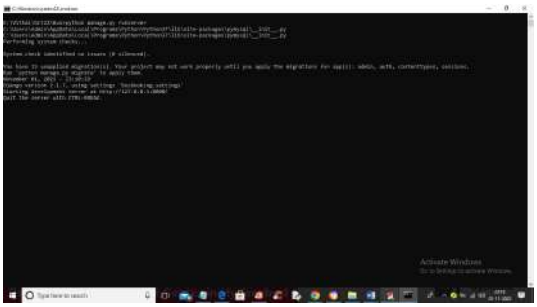
Here we are designing online Bus Ticket Booking system which can be used by any user to search busses and can make booking and can cancel booking.

To implement this project we have design following modules

1) Admin Module: using this module admin can login to application by using username and password as 'admin' and 'admin'. After login admin can add new buses travel from source to destination and can view all bookings made by user
2) User Module: user can signup with the application and then can login and then can search for buses and can make booking or cancel existing booking

To run project install MYSQL database and give its password as 'root' while installation and now open MYSQL command line console and copy content from 'DB.txt' file and paste in MYSQL to create database.

Now double click on 'run.bat' file to start python WEB SERVER and get below screen (note: after deployment on amazon no need to do this steps we will give you one URL and by using that URL you can execute code)



In above screen python WEB server started and now open browser and enter URL as 'http://127.0.0.1:8000/index.html' and press enter key to get below page

In above screen click on 'Admin Login' link to login as admin and get below screen

In above screen admin is login and after login will get below admin option

In above screen admin can click on 'Add New Bus Routes' link to add new buses details screen like below screen

In above screen admin will add bus details travel from source to destination and add fare details with sitting capacity and then press button to get below output

In above screen in red colour text we can see bus details added and now click on 'View Bookings' which allow admin to view all bookings

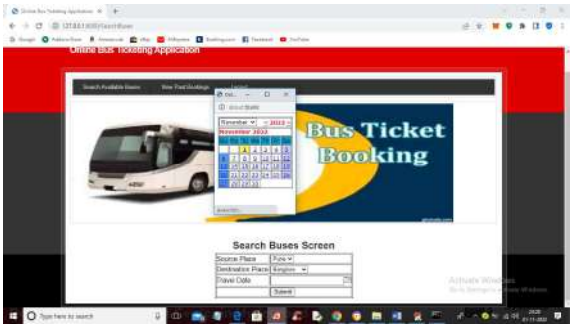
In above screen admin can view all bookings done by the user and now logout and signup new user to make booking

In above screen new user is signing up and after signup will get below output

In above screen user signup completed and now login as user in below screen

In above screen user is login and after login will get below screen which contaisn user modules

In above screen user can click 'Search Available Buses' link to get below screen



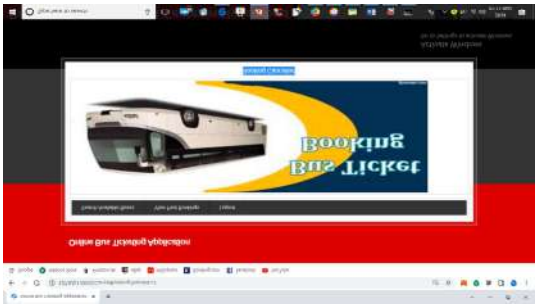
In above screen user will select source place and destination place and then choose travel date and press button to get available busses like below screen

In above screen user can view available buses and then click on 'Click Here to Book' link to make booking like below screen

In above screen user can select desired number of seats and then click on 'Submit' button to complete booking and get below confirmation

In above screen we can see user booking is confirmed with booking ID 2 and now user can click on 'View Past Bookings' link to view all past bookings and can cancel advanced booked tickets only for upcoming days

In above screen user can view all bookings details and at any time by clicking on 'Click Here to Cancel' link to cancel booking and get below output



In above screen in blue colour text we can see booking is cancelled. Similarly you can add buses and can make and cancel bookings

Conclusion

1. This study highlights the importance of intelligent systems in the detection of web attacks. ML and DL algorithms provide an edge over traditional systems by learning from data and adapting to new threat patterns.
2. Among the tested algorithms, DL models—particularly CNN and LSTM—demonstrated superior performance in detecting complex and sequential attacks. However, their higher computational requirements make them less suitable for lightweight environments.
3. Random Forest and SVM stood out among ML models for their balance between detection capability and efficiency. These are ideal for quick deployment and real-time alerting in resource-constrained environments.
4. Future research can focus on real-time stream analysis, adversarial attack resilience, and the deployment of these models in hybrid cloud-edge architectures. Combining multiple models using ensemble or federated learning could further enhance security in dynamic web environments.

References

1. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). *A Deep Learning Approach to Network Intrusion Detection*. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

2. Moustafa, N., & Slay, J. (2015). *UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems*. Military Communications and Information Systems Conference (MilCIS), IEEE.

3. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). *A Detailed Analysis of the KDD CUP 99 Data Set*. IEEE Symposium on Computational Intelligence for Security and Defense Applications.

4. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). *A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks*. IEEE Access, 5, 21954–21961.

5. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). *A Deep Learning Approach for Network Intrusion Detection System*. EAI International Conference on Bio-inspired Information and Communications Technologies.

6. Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). *Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection*. IEEE Access, 6, 33789–33795.

7. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). *Applying Convolutional Neural Network for Network Intrusion Detection*. International Conference on Advances in Computing, Communications and Informatics (ICACCI).

8. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). *Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization*. Proceedings of ICISSP.

9. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). *A Survey of Deep Learning Methods for Cyber Security*. Information, 10(4), 122.

10. Kwon, D., Kim, J., & Kim, J. (2019). *Deep Learning-Based Anomaly Detection System for Discovering Web Attacks*. IEEE Access, 7, 183527–183536.

11. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

12. Lippmann, R. P., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). *The 1999 DARPA Off-Line Intrusion Detection Evaluation*. Computer Networks, 34(4), 579–595.

13. Kim, Y., Kim, W., & Kim, H. K. (2020). *A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection*. Expert Systems with Applications, 186, 115002.

14. Sommer, R., & Paxson, V. (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*. IEEE Symposium on Security and Privacy.

15. Khan, L., Awad, M., & Thuraisingham, B. (2007). *A New Intrusion Detection System Using Support Vector Machines and Hierarchical Clustering*. The VLDB Journal, 16(4), 507–521.