BRUTE-FORCE ATTACK DETECTION USING LOG DATA

TEAM: NIKHIL VISHNU CHOWDARY VADLAMUDI, SAI SUMANTH REDDY KACHI, SAI TARUN DANTULURI, SUSHANTH REDDY MANDAPURAM, VAGBHAT DWIBHASHYAM

UMBC

INTRODUCTION

- In today's digital world, protecting user authentication from cyber attacks has become extremely important.
- Brute force login attempts pose a major threat among various cyber attacks strategies since they continuously try different combinations in order to gain unauthorized access.
- Our project aims to mitigate risk by developing an effective machine learning model to analyze log data. It uses features like login attempts count, IP reputation scores and access patterns and this data is used to train the model.
- The goal is to create an accurate, scalable and adaptable to evolving attack strategies to prevent unauthorized access effectively.
- Studies had begun on brute force attacks when WhitField Diffie and Martin Hellman released a paper in 1977, specifically in the context of cryptography of the Data Encryption Standard (DES).

OBJECTIVE:

To develop a machine learning model which can detect brute-force login attempts by analyzing log data from authentication systems. The model can identify any abnormal login behaviors (such as sudden spikes in login attempts, or login attempt at unusual time) and classify the attempt as normal attempt or brute-force attack.

Dataset Description:

The dataset contains 11 attributes and 9537 instances. Out of the 11 attributes 5 are numerical, 5 categorical, and 1 text. There are no redundant or duplicate rows and even no missing values in the dataset. Total attributes: session_id, network_packet_size, protocol_type, login_attempts, session_duration, encryption_used, ip_reputation_score, failed_logins, browser_type, unusual_time_access and attack_detected.

Important Attributes:
login_attempts, ip_reputation_score, failed_logins, and unusual_time_access, encryption_used.

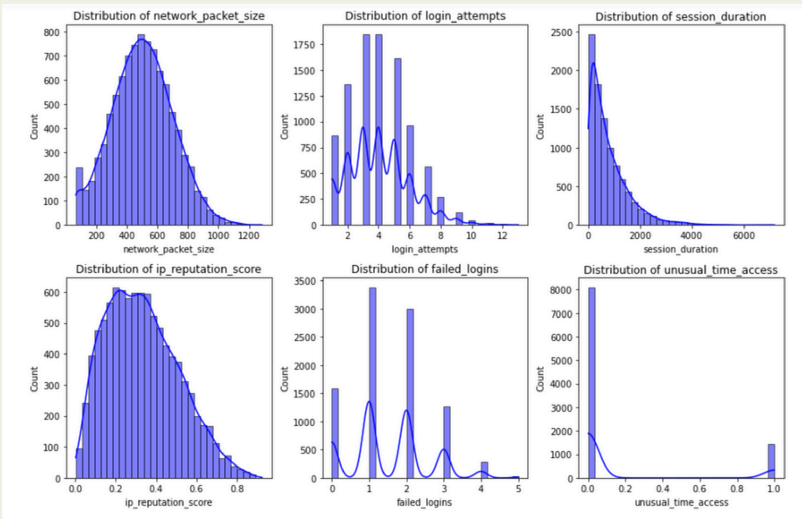
DATA PREPROCESSING:

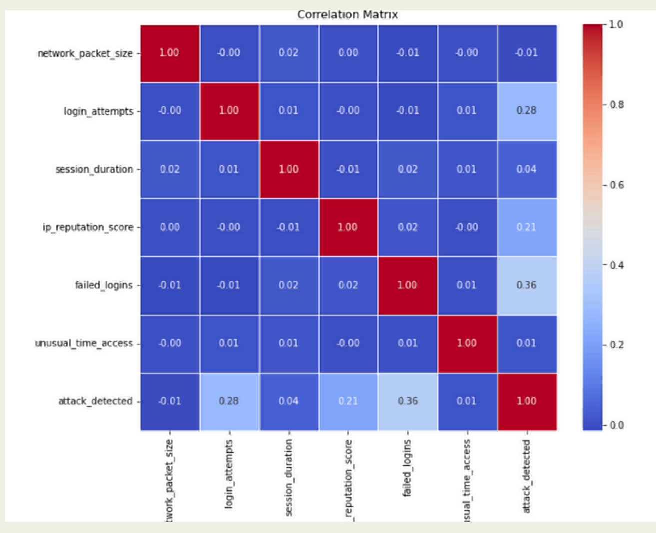
- **Feature Redundancy:** The session_id, network_packet_size and browser_type attributes are dropped.
- **Improving Data Clarity:** The 'None' value present in the encryption_used column has been changed to 'No encryption' for better understanding.
- **Categorical Encoding:** Binary columns for each category of categorical variables have been created using one-hot encoding.
- **Feature Scaling:** Numerical attributes like network_packet_size, login_attempts, session_duration, etc., have been scaled to a range between 0 and 1 using MinMax scaling.

EXPLORATORY DATA ANALYSIS

EDA played a crucial role in understanding the dataset and preparing it for modeling. Key techniques included:

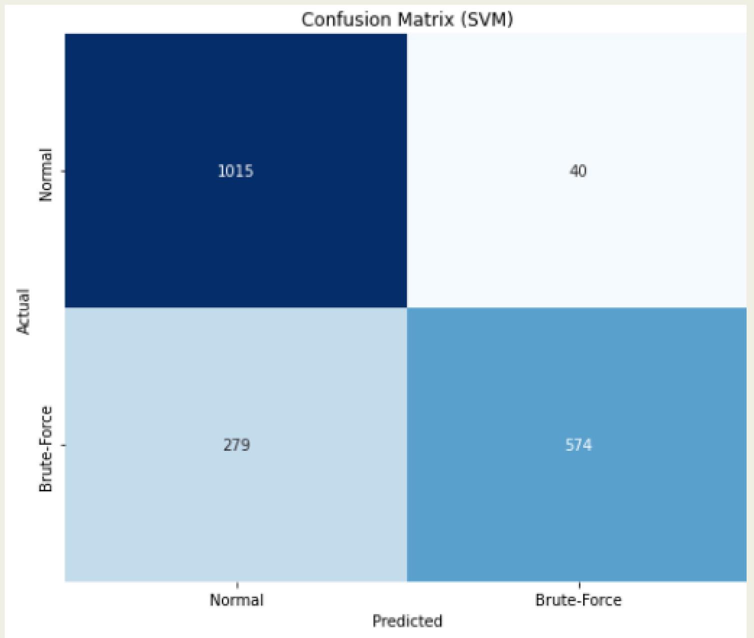
- **Correlation Matrices:** These helped identify relationships between features, highlighting attributes with strong positive or negative correlations to the target variable.
- **Distribution Plots:** Used to examine the spread of numerical features, detect outliers, and understand patterns in data distributions.
- **Feature Engineering Insights:** Insights from EDA informed the transformation of features better interpretability.





IMPLEMENTED MODELS WITH RESULTS:

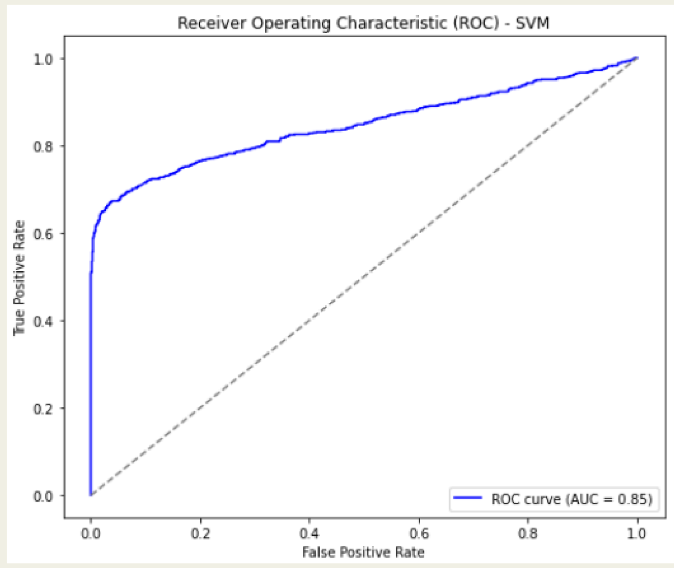
SVM



Accuracy: 0.833
Classification Report:

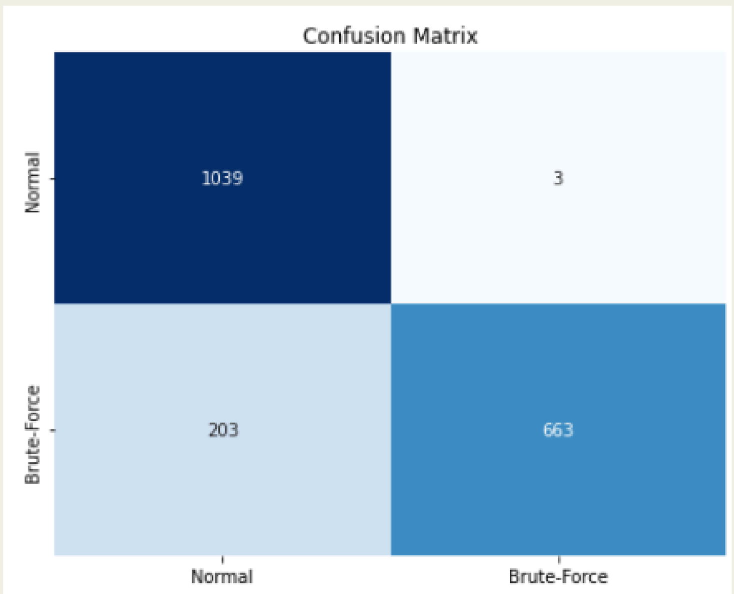
	precision	recall	f1-score	support
0	0.78	0.96	0.86	1055
1	0.93	0.67	0.78	853
accuracy			0.83	1908
macro avg	0.86	0.82	0.82	1908
weighted avg	0.85	0.83	0.83	1908

AUC: 0.8456298650428096



- The SVM model achieved 83.3% accuracy and an AUC of 0.85, with high precision for brute-force attacks (0.93) but lower recall (0.67), meaning more attacks were missed compared to other models.
- Despite solid performance, the model struggles to capture all brute-force attempts, indicating the need for further tuning or advanced models to improve recall.

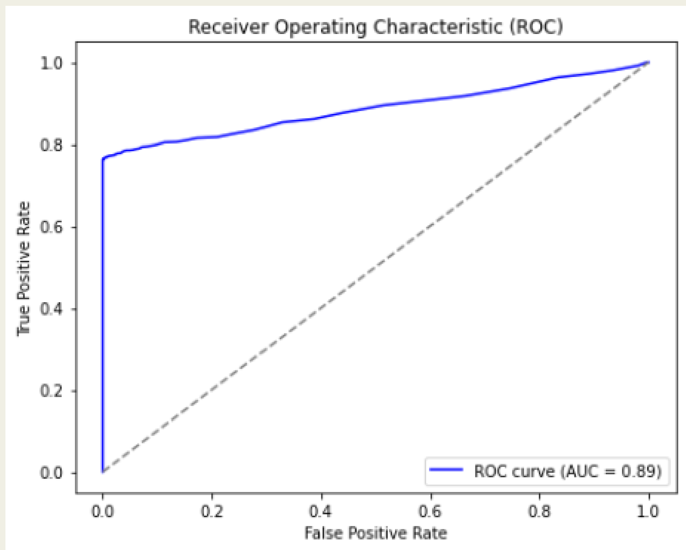
Random Forest



Accuracy: 0.8920335429769392
Classification Report:

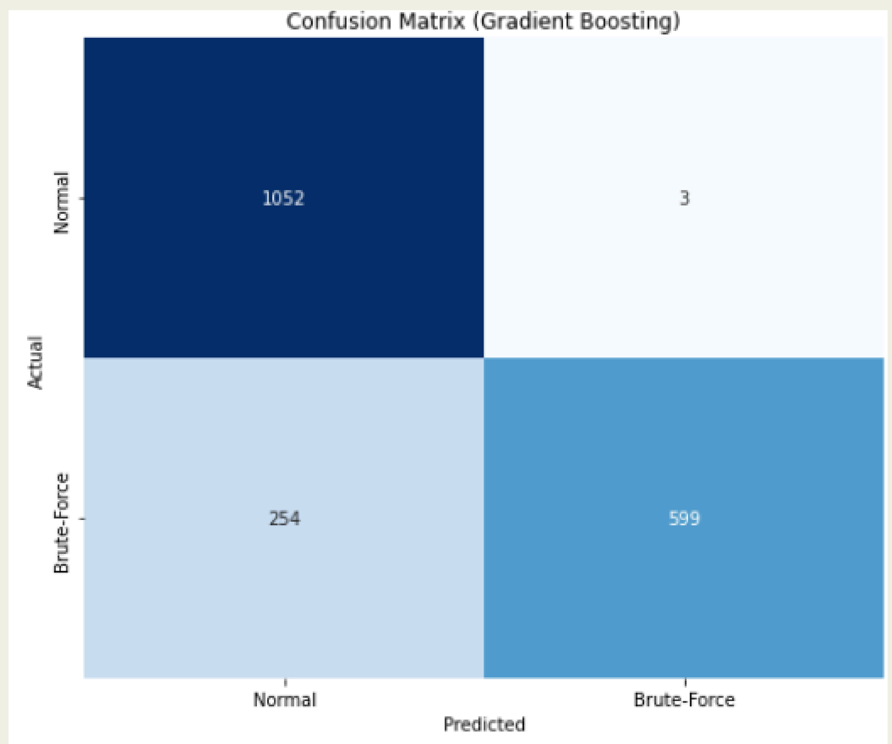
	precision	recall	f1-score	support
0	0.84	1.00	0.91	1042
1	1.00	0.77	0.87	866
accuracy			0.89	1908
macro avg	0.92	0.88	0.89	1908
weighted avg	0.91	0.89	0.89	1908

AUC: 0.886079687756269



- The Random Forest model achieved 89% accuracy with perfect precision (1.0) for brute-force attack detection, though recall for brute-force was slightly lower at 0.77, indicating some attacks were missed.
- The model's performance is strong overall, demonstrated by a ROC AUC of 0.89, confirming its high capability to distinguish between normal and brute-force login attempts.

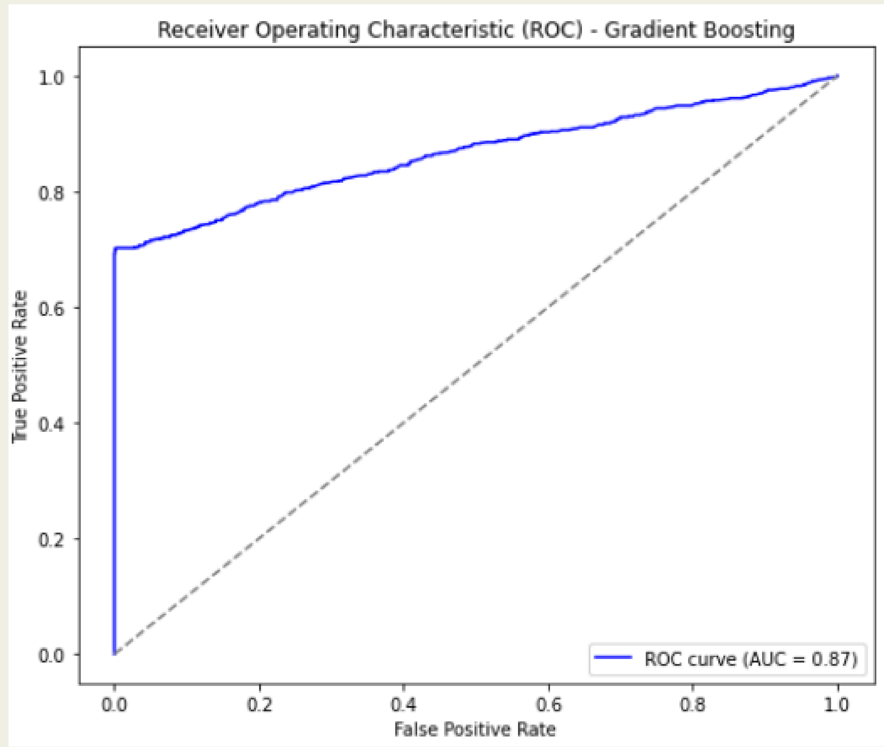
Gradient Boosting



Accuracy: 0.865
Classification Report:

	precision	recall	f1-score	support
0	0.81	1.00	0.89	1055
1	1.00	0.70	0.82	853
accuracy			0.87	1908
macro avg	0.90	0.85	0.86	1908
weighted avg	0.89	0.87	0.86	1908

AUC: 0.8650800353366705



- The Gradient Boosting model achieved 86.5% accuracy and an AUC of 0.87, with perfect precision (1.0) but lower recall (0.70) for brute-force attack detection.
- While highly precise in classifying brute-force attempts, the model missed more attacks compared to Random Forest, showing room for improvement in recall.

Best Model:

Out of all the models, Random Forest performed best with an accuracy of 89%, and with a perfect precision of 1.

FUTURE WORK :

In the future, the team plans to train more advanced models, such as Neural Networks, to further improve both accuracy and recall. After identifying the most effective model, efforts will be directed towards optimizing and thoroughly testing it to ensure robustness and prevent overfitting. The ultimate objective is to deploy this model in real-time environments, enabling the active detection of brute-force attacks as they occur. In addition to detection, the system is intended to incorporate preventive measures, including rate limiting, CAPTCHA, and IP blocking, to stop attacks before they succeed. Furthermore, the team aims to expand the dataset and introduce more meaningful features, enhancing the model's ability to adapt to evolving attack patterns and improving its overall intelligence and flexibility.

CONCLUSION:

In this project, machine learning models were developed to detect brute-force login attempts by analyzing authentication log data. Multiple models, including Logistic Regression, Random Forest, Gradient Boosting, and Support Vector Machines (SVM), were implemented and evaluated based on their performance in terms of accuracy, precision, recall, and AUC. Among all the models tested, Random Forest provided the best overall balance, achieving a high accuracy of 89% and perfect precision. However, the model's recall indicated some room for improvement, as not all brute-force attempts were identified. Gradient Boosting and SVM also demonstrated strong performance, but faced greater challenges in recall, leading to more missed brute-force attacks. The results highlight that machine learning approaches are highly effective for detecting brute-force login attempts. Nevertheless, enhancing recall without compromising precision remains an important objective. Future work will focus on exploring more advanced models and incorporating additional features to increase the system's robustness and enable real-time deployment. This project establishes a solid foundation for building automated brute-force attack detection systems, which can significantly strengthen organizational cybersecurity and minimize risks associated with unauthorized access.

QR CODE