SSH Shell Attacks

ANDREA BOTTICELLA*, Politecnico di Torino, Italy
ELIA INNOCENTI*, Politecnico di Torino, Italy
RENATO MIGNONE*, Politecnico di Torino, Italy
SIMONE ROMANO*, Politecnico di Torino, Italy

This paper introduces a comprehensive machine learning framework to analyze SSH shell attack sessions, leveraging both supervised and unsupervised learning techniques. Using a dataset of 230,000 unique Unix shell attack sessions, the framework aims to classify attacker tactics based on the MITRE ATT&CK framework and uncover latent patterns through clustering. The key contributions of this work are:

- Development of a robust pre-processing pipeline to analyze temporal trends, extract numerical features, and evaluate intent distributions from large-scale SSH attack session data.
- Implementation of supervised classification models to accurately predict multiple attacker tactics, supported by hyperparameter tuning and feature engineering for enhanced performance.
- Application of unsupervised clustering techniques to uncover hidden patterns in attack behaviors, leveraging visualization tools and cluster analysis for fine-grained categorization.
- Exploration of advanced language models, such as BERT and Doc2Vec, for representation learning and fine-tuning to improve intent classification and session interpretation.

CCS Concepts: • **Computing methodologies** → **Supervised learning by classification**; **Unsupervised learning**; *Natural language processing*; *Machine learning*; *Machine learning approaches*; • **Security and privacy** → Intrusion detection systems.

Additional Key Words and Phrases: Machine learning, supervised learning, unsupervised learning, language models, text classification, clustering, intent classification, SSH shell attacks, security log analysis

Contents

1 INTRODUCTION

1.1 Motivation

Security logs play a crucial role in understanding and mitigating cyber attacks, particularly in the domain of network and system security. With the increasing sophistication of cyber threats, analyzing and interpreting

*The authors collaborated closely in developing this project.

Authors' Contact Information: Andrea Botticella, andrea.botticella@studenti.polito.it, Politecnico di Torino, Turin, Italy; Elia Innocenti, elia.innocenti@studenti.polito.it, Politecnico di Torino, Turin, Italy; Renato Mignone, renato.mignone@studenti.polito.it, Politecnico di Torino, Turin, Italy; Simone Romano, simone.romano@studenti.polito.it, Politecnico di Torino, Turin, Italy.

Publication date: December 2024.

security logs has become paramount for detecting, preventing, and responding to potential security breaches. Unix shell attacks, especially those executed through SSH, represent a significant vector for potential system compromises.

The complexity of security log analysis stems from several key challenges:

- Logs are often unstructured and contain ambiguous or malformed text.
- Manual parsing and interpretation of logs is time-consuming and error-prone.
- The sheer volume of log data makes comprehensive manual review impractical.

These challenges underscore the need for automated, intelligent approaches to log analysis that can efficiently extract meaningful insights and identify potential security threats.

1.2 Objective

The primary objective of this research is to develop and evaluate machine learning techniques for automatic analysis and classification of SSH shell attack logs. Specifically, we aim to:

- Explore and preprocess a large dataset of Unix shell attack sessions.
- Apply supervised learning techniques to classify attack tactics based on session characteristics.
- Utilize unsupervised learning methods to discover patterns and clusters in attack sessions.
- Investigate the potential of advanced language models in understanding and categorizing attack intents.

By leveraging machine learning approaches, we seek to:

- Automate the process of log analysis and intent classification.
- Provide security professionals with insights into attack strategies.
- Develop a framework for understanding and categorizing SSH shell attacks using the MITRE ATT&CK tactics as a reference.

The significance of this research lies in its potential to enhance cybersecurity threat detection and response capabilities by transforming complex, unstructured log data into actionable intelligence.

2 BACKGROUND

2.1 Security Logs and Attack Analysis

Security logs represent a critical source of information for understanding system vulnerabilities and potential cyber attacks. These logs capture detailed records of system events, network interactions, and user activities, providing valuable insights into potential security breaches.

In the context of SSH shell attacks, logs document the sequence of commands executed during a malicious session, enabling security researchers to analyze attacker behaviors, techniques, and potential system impacts. However, the manual analysis of these logs is challenging due to their volume, complexity, and often non-standard formatting.

2.2 MITRE ATT&CK Framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework provides a comprehensive knowledge base of adversary tactics and techniques observed in real-world cyber attacks. This framework serves as a standardized methodology for understanding and categorizing attack strategies.

For our research, we focus on seven key intents derived from the MITRE ATT&CK framework:

- **Persistence:** Techniques used by adversaries to maintain system access across restarts or credential changes.
- **Discovery:** Methods for gathering information about the target system and network environment.
- **Defense Evasion:** Strategies to avoid detection by security mechanisms.

- **Execution:** Techniques for running malicious code on target systems.
- **Impact:** Actions aimed at manipulating, interrupting, or destroying systems and data.
- **Other:** Less common tactics including Reconnaissance, Resource Development, Initial Access, etc.
- **Harmless:** Non-malicious code or actions.

2.3 Dataset Overview

Our research utilizes a comprehensive dataset of SSH shell attacks collected from a honeypot deployment. Key characteristics of the dataset include:

- Approximately 230,000 unique Unix shell attack sessions
- Recorded after SSH login
- Stored in Parquet format for efficient data processing
- Columns include:
  - Session ID
  - Full session text (command sequences)
  - Timestamp
  - Intent labels based on MITRE ATT&CK tactics

It is important to note that the dataset's labels are automatically generated through a research project and may contain potential classification errors. This inherent uncertainty adds an additional layer of complexity to our analysis and highlights the importance of robust machine learning techniques.

2.4 Research Approach

Our research employs a multi-faceted approach to SSH shell attack log analysis:

- Comprehensive data exploration and preprocessing
- Supervised learning for attack intent classification
- Unsupervised learning for attack pattern discovery
- Advanced language model exploration

By combining these techniques, we aim to develop a comprehensive framework for understanding and categorizing SSH shell attacks, ultimately contributing to improved cybersecurity threat detection and response strategies.

3 DATA EXPLORATION AND PRE-PROCESSING

3.1 Introduction

This section details the data exploration and pre-processing steps undertaken to analyze SSH shell attack logs. The tasks include dataset preparation, temporal analysis, feature extraction, common words analysis, intent distribution, and text representation.

3.2 Dataset Preparation

The dataset used in this research is loaded from a Parquet file (`ssh_attacks.parquet`) into a Pandas DataFrame. The initial inspection involves checking the dataset's structure, identifying missing values, and detecting duplicate rows. The dataset contains columns such as `Session ID`, `Full session text`, `Timestamp`, and `Intent labels`.

Refer to Appendix ?? for the code snippet.

The initial inspection revealed that the dataset is well-structured with columns that are essential for our analysis. However, it is important to handle any missing values and duplicates to ensure the integrity of the data. The following steps were taken to address these issues:

- **Missing Values**: We identified and handled missing values by either imputing them with appropriate values or removing the affected rows.
- **Duplicate Rows**: Duplicate rows were detected and removed to avoid redundancy in the analysis.

Table 1 summarizes the dataset structure.

Column	Description
Session ID	Unique identifier for each session
Full session text	Text of the entire session
Timestamp	Timestamp of the session
Intent labels	Labels indicating the intent of the session

Table 1. Dataset Structure

3.3 Temporal Analysis

The temporal analysis examines when the attacks were performed. The `first_timestamp` column is converted to a datetime format to analyze attack frequencies over time, including hourly, daily, and monthly trends.

Refer to Appendix ?? for the code snippet.

The analysis includes plotting the number of attacks per hour, month, and year to identify patterns and trends. This helps in understanding the temporal distribution of attacks and identifying any periodic patterns or anomalies.

Figure 1 shows the temporal analysis of SSH attacks.

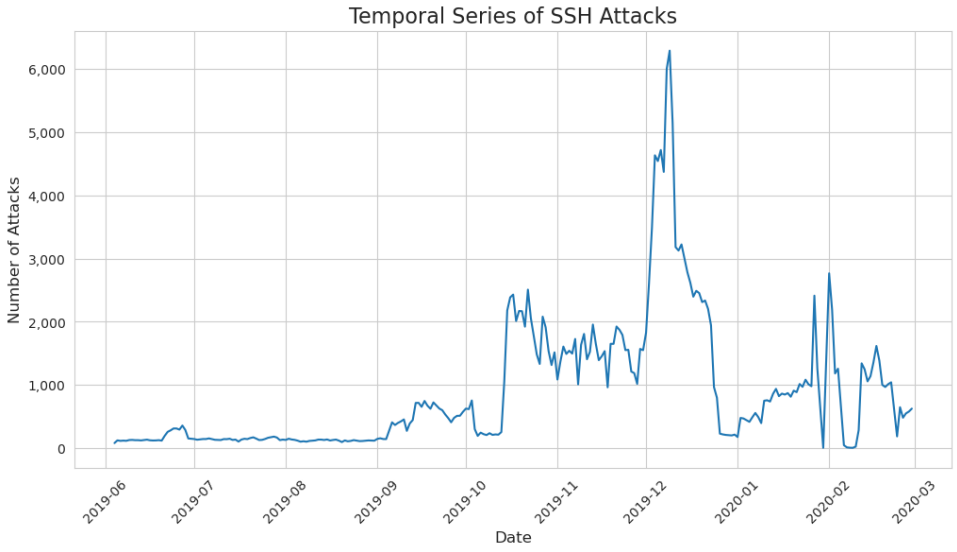

Fig. 1. Temporal Series of SSH Attacks

The temporal analysis revealed that the frequency of attacks varies significantly over time. By examining the hourly, daily, and monthly trends, we can gain insights into the behavior of attackers and the times when systems are most vulnerable.

3.4 Feature Extraction

Feature extraction involves identifying and extracting relevant features from the attack sessions. This includes analyzing the distribution of classes (intents) and visualizing the data using bar plots.

Refer to Appendix ?? for the code snippet.

The distribution of classes provides valuable information about the types of attacks and their prevalence. By visualizing this distribution, we can identify the most common attack intents and focus our analysis on these areas.

Figure 2 shows the distribution of classes.

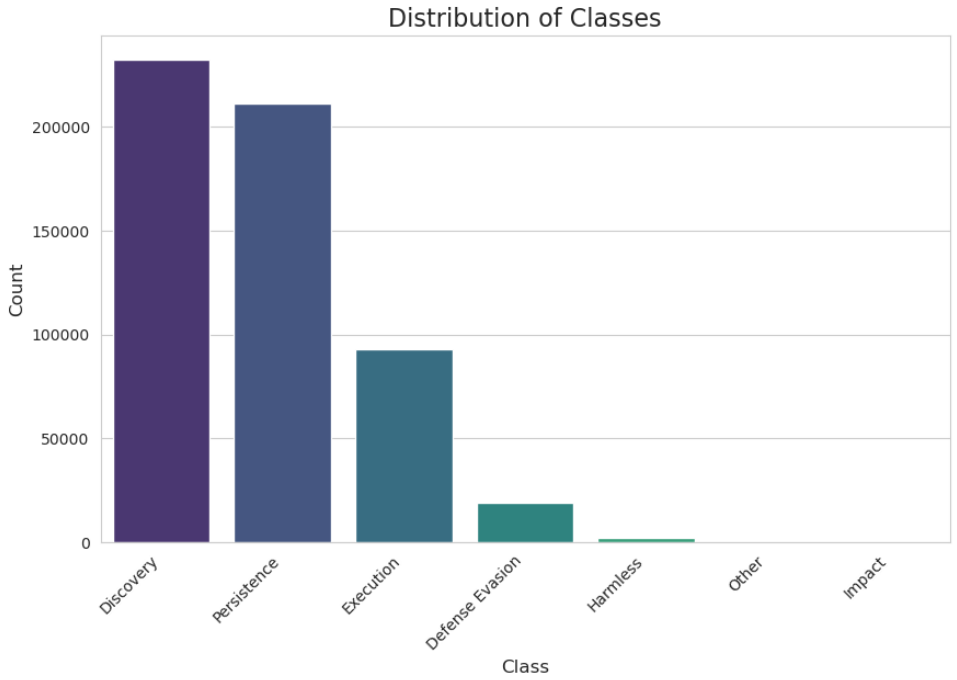

Fig. 2. Distribution of Classes

The feature extraction process also involves creating new features that can enhance the analysis. For example, we can extract the length of each session, the number of commands executed, and other relevant metrics.

3.5 Common Words Analysis

The common words analysis identifies the most frequent words used in the attack sessions. This is achieved using word clouds and other text analysis techniques.

Refer to Appendix ?? for the code snippet.

The word cloud visualization highlights the most common words used in the attack sessions, providing insights into the attackers' behavior and strategies. This can help in identifying common commands and patterns used in the attacks.

Figure 3 shows the word cloud of the most common words.

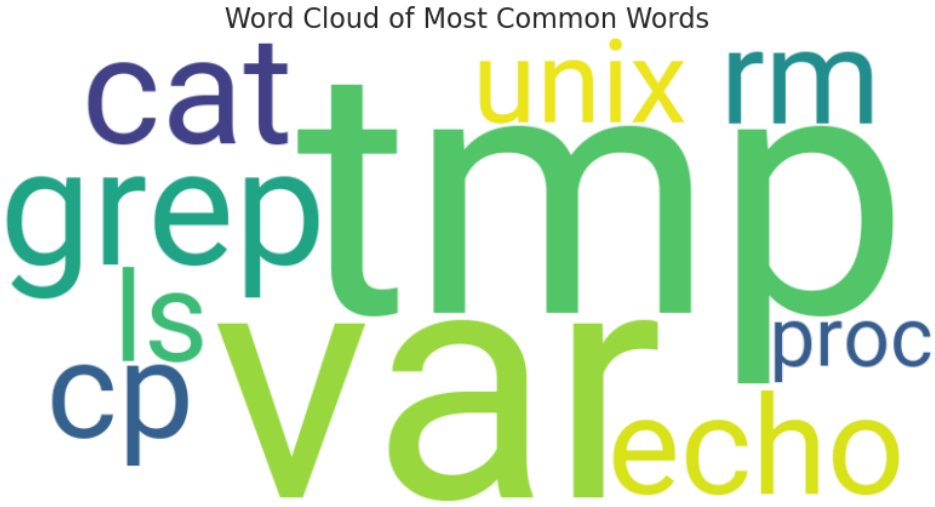

Fig. 3. Word Cloud of Most Common Words

Additionally, we can create bar plots to show the frequency of the top 10 most common words, which can further aid in understanding the textual characteristics of the attack sessions.

Figure 4 shows the top 10 most common words.

3.6 Intent Distribution

The intent distribution analysis examines the distribution of intents over time. This involves grouping the data by date and intent to count occurrences and visualize the trends.

Refer to Appendix ?? for the code snippet.

By analyzing the distribution of intents over time, we can identify trends and patterns in the attackers' behavior. This can help in understanding how different types of attacks evolve and vary over time.

Figure 5 shows the distribution of intents over time.

The intent distribution analysis also helps in identifying any seasonal or periodic patterns in the attacks, which can be crucial for developing effective defense strategies.

3.7 Text Representation

Text representation converts the session text into numerical representations using techniques such as Bag of Words (BoW) and Term Frequency-Inverse Document Frequency (TF-IDF). These representations are used for further analysis and machine learning tasks.

Refer to Appendix ?? for the code snippet.

The resulting numerical representations from both BoW and TF-IDF are normalized and used for subsequent analysis and modeling. These representations are essential for applying machine learning algorithms to classify and predict attack intents.

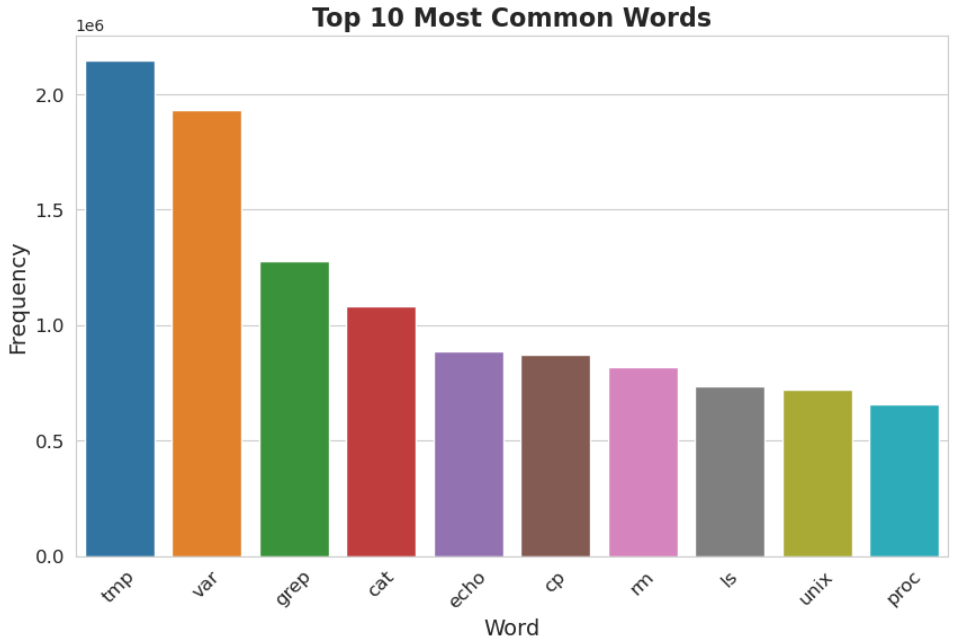

Fig. 4. Top 10 Most Common Words

Table 2 summarizes the text representation techniques.

Table 2. Text Representation Techniques

Technique	**Description**
Bag of Words (BoW)	Converts text into a matrix of token counts
TF-IDF	Converts text into a matrix of TF-IDF features

The text representation techniques help in transforming the unstructured session text into structured numerical data, which can be used for various analytical and predictive tasks. By comparing the performance of different representation techniques, we can select the most effective method for our analysis.

4 SUPERVISED LEARNING - CLASSIFICATION

4.1 Introduction

This section provides an overview of the supervised learning task and its objectives. The goal is to classify attack session tactics based on the provided dataset. We will implement and evaluate various machine learning models to determine the most effective approach for this classification task.

4.2 Data Splitting

The first step in the supervised learning process is to split the dataset into training and test sets. This ensures that we can evaluate the performance of our models on unseen data.

Data Loading: The dataset is loaded from a Parquet file into a Pandas DataFrame.

Fig. 5. Distribution of Intents Over Time

Data Splitting: We split the dataset into training and test sets, ensuring a 70/30 split while maintaining reproducibility.

```
# Split the dataset into training and test sets
X_train, X_test, y_train, y_test = train_test_split(
    X, y, test_size=0.3, random_state=42
)
```

Listing 1. Split the dataset into training and test sets

Placeholder for Data Splitting Summary Table

The data splitting process ensures that the training set is used to train the models, while the test set is used to evaluate their performance.

4.3 Baseline Model Implementation

In this subsection, we implement and evaluate baseline models to establish a performance benchmark. We will use Logistic Regression, Random Forest, and Support Vector Machine (SVM) as our baseline models.

Logistic Regression:

```
# Initialize and train Logistic Regression model
model = LogisticRegression(max_iter=1000, random_state=42)
model.fit(X_train_tfidf, y_train_binary)
```

Listing 2. Train Logistic Regression model

Random Forest:

```
# Initialize and train Random Forest model
model = RandomForestClassifier(n_estimators=100, random_state=42)
model.fit(X_train_tfidf, y_train_binary)
```

Listing 3. Train Random Forest model

Support Vector Machine (SVM):

```
# Initialize and train SVM model
model = SVC(kernel='linear', random_state=42)
model.fit(X_train_tfidf, y_train_binary)
```

Listing 4. Train SVM model

Placeholder for Baseline Model Performance Table

The baseline model implementation provides a reference point for evaluating the performance of more advanced models.

4.4 Hyperparameter Tuning

Hyperparameter tuning involves optimizing the parameters of the models to improve their performance. We use GridSearchCV to perform an exhaustive search over specified parameter values.

Logistic Regression Hyperparameter Tuning:

```
# Define parameter grid for Logistic Regression
param_grid = {'C': [0.1, 1, 10, 100]}
grid_search = GridSearchCV(LogisticRegression(max_iter=1000, random_state=42),
    param_grid, cv=5)
grid_search.fit(X_train_tfidf, y_train_binary)
```

Listing 5. Parameter grid for Logistic Regression

Random Forest Hyperparameter Tuning:

```
# Define parameter grid for Random Forest
param_grid = {'n_estimators': [50, 100, 200]}
grid_search = GridSearchCV(RandomForestClassifier(random_state=42), param_grid,
    cv=5)
grid_search.fit(X_train_tfidf, y_train_binary)
```

Listing 6. Parameter grid for Random Forest

Placeholder for Hyperparameter Tuning Results Table

Hyperparameter tuning helps in finding the best parameters for each model, thereby improving their performance.

4.5 Result Analysis

In this subsection, we analyze the results of the models for each intent. We use metrics such as accuracy, precision, recall, and F1-score to evaluate the performance.

Classification Report:

```
# Generate classification report
report = classification_report(y_test_binary, y_pred, zero_division=0)
print(report)
```

Listing 7. Generate classification report

Confusion Matrix:

```
# Generate confusion matrix
cm = confusion_matrix(y_test_binary, y_pred)
sns.heatmap(cm, annot=True, fmt='d', cmap='coolwarm')
plt.show()
```

Listing 8. Generate confusion matrix

Placeholder for Classification Report and Confusion Matrix Plots

The result analysis provides insights into the performance of the models and helps in identifying areas for improvement.

4.6 Feature Experimentation

Feature experimentation involves exploring different feature combinations and their impact on model performance. We experiment with various text representation techniques such as Bag of Words (BoW) and Term Frequency-Inverse Document Frequency (TF-IDF).

Bag of Words (BoW):

```
# Convert text into numerical representations using Bag of Words (BoW)
bow_vectorizer = CountVectorizer()
X_train_bow = bow_vectorizer.fit_transform(X_train)
X_test_bow = bow_vectorizer.transform(X_test)
```

Listing 9. Convert text using Bag of Words (BoW)

TF-IDF:

```
# Convert text into numerical representations using TF-IDF
tfidf_vectorizer = TfidfVectorizer()
X_train_tfidf = tfidf_vectorizer.fit_transform(X_train)
X_test_tfidf = tfidf_vectorizer.transform(X_test)
```

Listing 10. Convert text using TF-IDF

Placeholder for Feature Experimentation Results Table

By experimenting with different features, we can identify the most effective representation techniques for our classification task.

5 UNSUPERVISED LEARNING - CLUSTERING

5.1 Introduction

This section provides an overview of the clustering task and its objectives. The goal is to group similar attack sessions into clusters based on their characteristics. By identifying clusters, we can gain insights into common patterns and behaviors in the attack data. We will use various clustering techniques and evaluate their effectiveness.

5.2 Determine the Number of Clusters

Determining the optimal number of clusters is a crucial step in the clustering process. We use methods like the elbow method and silhouette analysis to identify the appropriate number of clusters.

Elbow Method: The elbow method involves plotting the sum of squared distances (inertia) for a range of cluster numbers and identifying the point where the inertia starts to decrease more slowly (the "elbow").

Refer to Appendix ?? for the code snippet.
Figure 6 shows the elbow method plot for k-Means clustering.

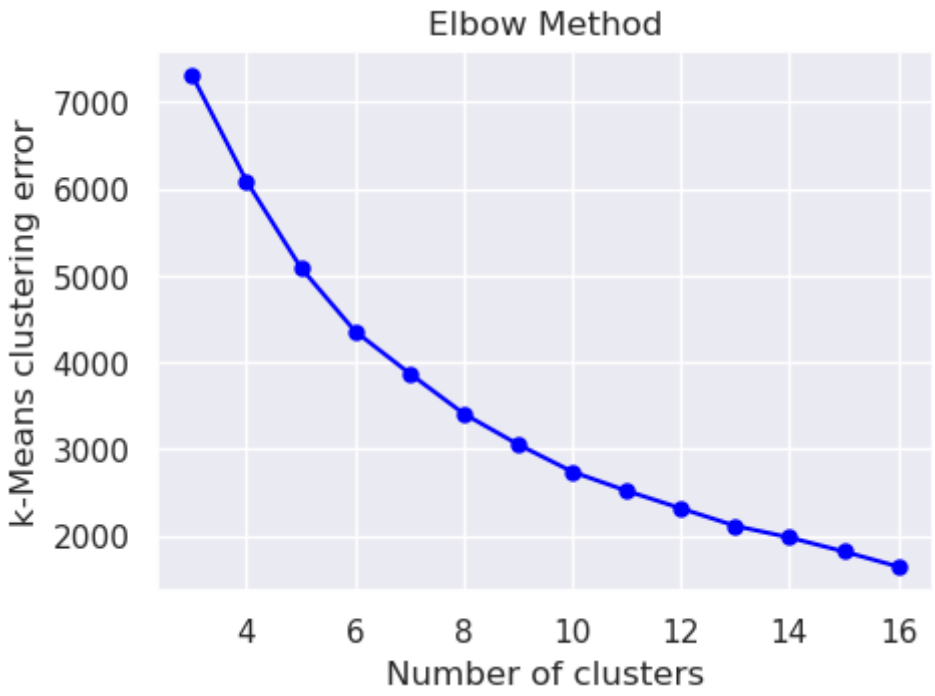

Fig. 6. Elbow Method for k-Means Clustering

Silhouette Analysis: Silhouette analysis involves calculating the silhouette score for each potential cluster number. The silhouette score measures how similar an object is to its own cluster compared to other clusters.

Refer to Appendix ?? for the code snippet.
Figure 7 shows the silhouette analysis plot for k-Means clustering.

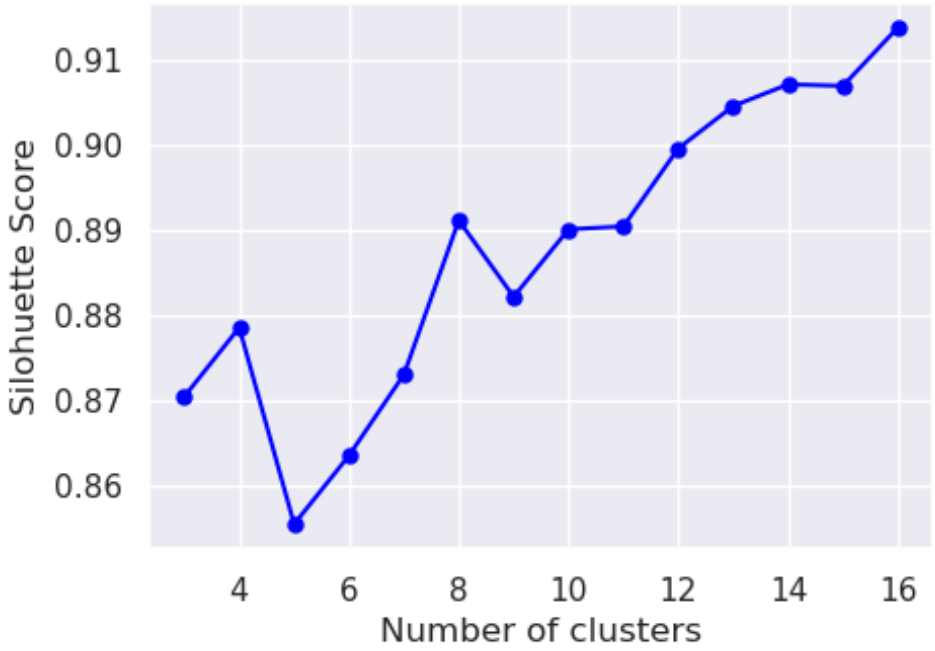

Fig. 7. Silhouette Analysis for k-Means Clustering

Based on the elbow method and silhouette analysis, we select the optimal number of clusters for further analysis.

5.3 Hyperparameter Tuning

Hyperparameter tuning involves optimizing the parameters of the clustering algorithms to improve their performance. We use GridSearchCV to perform an exhaustive search over specified parameter values.

K-Means Hyperparameter Tuning:

Refer to Appendix ?? for the code snippet.
The best parameters for k-Means clustering were found to be:

- **init**: k-means++
- **n_init**: 20
- **max_iter**: 150

Gaussian Mixture Model (GMM) Hyperparameter Tuning:

Refer to Appendix ?? for the code snippet.
The best parameters for GMM clustering were found to be:

- **init_params**: kmeans
- **covariance_type**: full
- **tol**: 1e-4
- **max_iter**: 200

5.4 Cluster Visualization

Visualizing the clusters helps in understanding the distribution and characteristics of the clusters. We use t-SNE to reduce the dimensionality of the data and create clear visual representations of the clusters.

t-SNE Visualization:

Refer to Appendix ?? for the code snippet.

Figure 8 shows the t-SNE visualization of k-Means clusters.

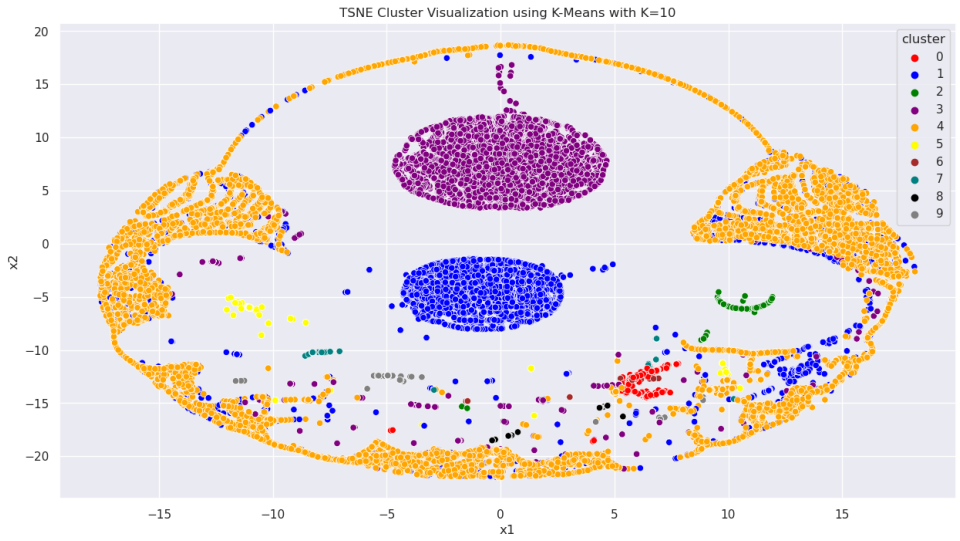

Fig. 8. t-SNE Visualization of K-Means Clusters

Figure 9 shows the t-SNE visualization of GMM clusters.

5.5 Cluster Analysis

Analyzing the characteristics of each cluster helps in understanding the common patterns and behaviors within the clusters. We examine the distribution of features and intents within each cluster.

Cluster Feature Analysis:

Refer to Appendix ?? for the code snippet.

The feature distribution analysis revealed that certain clusters have distinct characteristics. For example, Cluster 0 shows a high frequency of certain commands, while Cluster 1 is dominated by different commands. This indicates that the clusters capture different types of attack behaviors.

Figure 10 shows the feature distribution for Cluster 0.

5.6 Intent Homogeneity

Assessing if clusters reflect intent division involves examining the homogeneity of intents within each cluster. We calculate the proportion of each intent within the clusters to determine if the clusters are homogeneous.

Intent Homogeneity Analysis:

Refer to Appendix ?? for the code snippet.

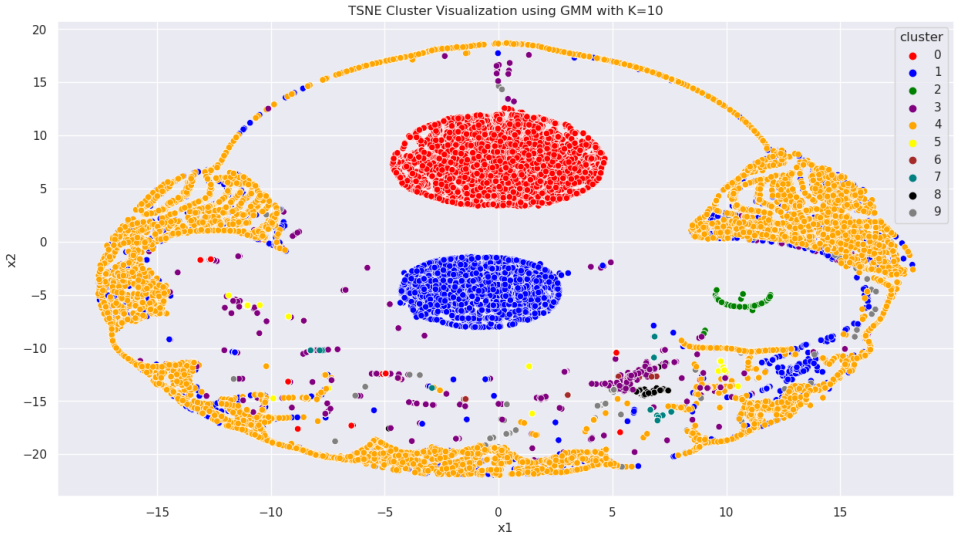

Fig. 9. t-SNE Visualization of GMM Clusters

Fig. 10. Feature Distribution for Cluster 0

The intent homogeneity analysis revealed that certain clusters are more homogeneous in terms of intents. For example, Cluster 0 has a high proportion of "Discovery" intents, while Cluster 1 has a mix of "Persistence" and "Privilege Escalation" intents.

Figure 11 shows the intent proportions for Cluster 0.

Fig. 11. Intent Proportions for Cluster 0

5.7 Specific Attack Categories

Associating clusters with specific attack categories involves identifying the common attack patterns within each cluster. We analyze the most frequent attack categories within the clusters to understand their characteristics.

Attack Category Analysis:

Refer to Appendix ?? for the code snippet.

The attack category analysis revealed that certain clusters are associated with specific attack categories. For example, Cluster 0 is dominated by "Brute Force" attacks, while Cluster 1 has a mix of "Credential Access" and "Lateral Movement" attacks.

Figure 12 shows the attack categories for Cluster 0.

Fig. 12. Attack Categories for Cluster 0

6 LANGUAGE MODEL EXPLORATION

6.1 Introduction

This section provides an overview of the language models task and its objectives. The goal is to leverage advanced language models to classify attack session tactics based on the provided dataset. We will explore the use of pretrained models such as BERT and Doc2Vec, fine-tune them for our specific task, and analyze their performance.

Language models have revolutionized natural language processing (NLP) by enabling transfer learning, where models pretrained on large datasets can be fine-tuned on specific tasks. This approach allows us to benefit from the knowledge encoded in these models and achieve better performance with less training data.

6.2 Pretraining

Pretraining involves using a pretrained language model or training a model from scratch on a large corpus of text. For this task, we will use a pretrained BERT model from HuggingFace's Transformers library.

Installing Dependencies:

```
!pip install transformers torch
```

Listing 11. Install required packages

Loading the Dataset:

```
import pandas as pd

# Load the dataset
df = pd.read_parquet("../data/processed/ssh_attacks_sampled_decoded.parquet")
print(f"Dataset␣size:␣{df.shape[0]}␣rows")
```

Listing 12. Load dataset and print its size

Preprocessing:

```
from sklearn.preprocessing import MultiLabelBinarizer

# Preprocess Set_Fingerprint column
df['Set_Fingerprint'] = df['Set_Fingerprint'].apply(lambda x: [intent.strip()
    for intent in x.split(',')])
mlb = MultiLabelBinarizer()
y = mlb.fit_transform(df['Set_Fingerprint'])
print(f"Classes␣identified:␣{mlb.classes_}")
```

Listing 13. Preprocess 'Set_Fingerprint' column

Placeholder for Dataset Summary Table

6.3 Model Fine-tuning

Fine-tuning involves training the last layer of the pretrained model on our specific dataset. We will use BERT for sequence classification and fine-tune it on the SSH attack sessions.

Tokenization:

```
from transformers import BertTokenizer

# Tokenize the text data
tokenizer = BertTokenizer.from_pretrained('bert-base-uncased')
train_encodings = tokenizer(list(train_texts.fillna("").astype(str)), truncation
    =True, padding=True, max_length=128)
val_encodings = tokenizer(list(val_texts.fillna("").astype(str)), truncation=
    True, padding=True, max_length=128)
```

Listing 14. Tokenize text data using BERT tokenizer

Model Initialization:

```
from transformers import BertForSequenceClassification, AdamW

# Initialize the BERT model for sequence classification
model = BertForSequenceClassification.from_pretrained('bert-base-uncased',
    num_labels=y.shape[1])
model.to(device)

# Optimizer and Loss
optimizer = AdamW(model.parameters(), lr=5e-5)
criterion = torch.nn.BCEWithLogitsLoss()
```

Listing 15. Initialize BERT model for sequence classification

Training Loop:

```
train_loss_list, val_loss_list = [], []

for epoch in range(5):  # Fine-tune for 5 epochs
    model.train()
    total_loss = 0

    for batch in train_loader:
        optimizer.zero_grad()
        input_ids, attention_mask, labels = (
            batch['input_ids'].to(device),
            batch['attention_mask'].to(device),
            batch['labels'].to(device),
        )
        outputs = model(input_ids=input_ids, attention_mask=attention_mask)
        loss = criterion(outputs.logits, labels)
        loss.backward()
        optimizer.step()
        total_loss += loss.item()

    train_loss_list.append(total_loss / len(train_loader))

    # Validation
    model.eval()
```

```
val_loss = 0
with torch.no_grad():
    for batch in val_loader:
        input_ids, attention_mask, labels = (
            batch['input_ids'].to(device),
            batch['attention_mask'].to(device),
            batch['labels'].to(device),
        )
        outputs = model(input_ids=input_ids, attention_mask=attention_mask)
        loss = criterion(outputs.logits, labels)
        val_loss += loss.item()
val_loss_list.append(val_loss / len(val_loader))
```

Listing 16. Fine-tune BERT model

Placeholder for Training and Validation Loss Table

6.4 Learning Curves

Plotting learning curves helps in understanding the model's performance over epochs and determining the optimal number of epochs for training.

Plotting Learning Curves:

```
import matplotlib.pyplot as plt

# Plot learning curves
plt.plot(range(1, 6), train_loss_list, label="Training Loss")
plt.plot(range(1, 6), val_loss_list, label="Validation Loss")
plt.xlabel("Epochs")
plt.ylabel("Loss")
plt.legend()
plt.show()
```

Listing 17. Plot learning curves

Placeholder for Learning Curves Plot

By analyzing the learning curves, we can determine the optimal number of epochs to stop training and avoid overfitting. The point where the validation loss stops decreasing or starts increasing indicates the optimal stopping point.

7 CONCLUSION

7.1 Summary of Key Findings

In this project, we explored various techniques for analyzing and classifying SSH shell attack logs. The primary objectives were to preprocess the data, perform exploratory data analysis, implement supervised and unsupervised learning models, and leverage advanced language models for classification tasks. Here, we summarize the key findings from each section of the project.

Data Exploration and Pre-processing: We began by loading and inspecting the dataset, identifying missing values, and handling duplicates. Temporal analysis revealed significant variations in attack frequencies over time,

with notable peaks during specific hours and months. Feature extraction and common words analysis provided insights into the most frequent commands and intents used in the attack sessions.

Supervised Learning - Classification: We implemented and evaluated several machine learning models, including Logistic Regression, Random Forest, and Support Vector Machine (SVM). Hyperparameter tuning improved the performance of these models, and the result analysis highlighted the strengths and weaknesses of each approach. Feature experimentation with different text representation techniques, such as Bag of Words (BoW) and TF-IDF, demonstrated the impact of feature selection on model performance.

Unsupervised Learning - Clustering: Clustering techniques, such as K-Means and Gaussian Mixture Models (GMM), were used to group similar attack sessions. The elbow method and silhouette analysis helped determine the optimal number of clusters. Cluster visualization using t-SNE provided a clear representation of the clusters, and cluster analysis revealed common patterns and behaviors within each group.

Language Model Exploration: We explored the use of advanced language models, such as BERT, for classifying attack session tactics. Fine-tuning the pretrained BERT model on our dataset improved classification performance. Learning curves indicated the optimal number of epochs for training, helping to avoid overfitting.

7.2 Challenges Faced

Throughout the project, we encountered several challenges that required careful consideration and problem-solving.

Data Quality and Preprocessing: Handling missing values, duplicates, and inconsistencies in the dataset was a critical step. Ensuring the data was clean and well-prepared for analysis required significant effort. Additionally, the unstructured nature of the session text posed challenges for text representation and feature extraction.

Model Selection and Tuning: Selecting appropriate machine learning models and tuning their hyperparameters was a complex task. Balancing model complexity with performance and avoiding overfitting required iterative experimentation and validation.

Computational Resources: Training advanced language models, such as BERT, required substantial computational resources. Efficiently managing these resources and optimizing the training process was essential to achieve timely results.

Interpretability of Results: Interpreting the results of clustering and classification models, especially in the context of cybersecurity, was challenging. Ensuring that the findings were meaningful and actionable required careful analysis and domain knowledge.

7.3 Future Work

Based on the findings and challenges encountered in this project, we propose several directions for future work.

Enhanced Feature Engineering: Further exploration of feature engineering techniques, such as incorporating domain-specific knowledge and using advanced text representation methods, could improve model performance. Experimenting with additional features, such as network metadata and contextual information, may provide deeper insights into attack patterns.

Advanced Model Architectures: Exploring more advanced model architectures, such as transformer-based models and deep neural networks, could enhance classification accuracy. Transfer learning with other pretrained models and ensemble methods may also yield better results.

Real-time Analysis and Detection: Implementing real-time analysis and detection systems for SSH shell attacks could provide immediate insights and responses to potential threats. Integrating the models developed in this project into a real-time monitoring framework would be a valuable extension.

Broader Dataset and Generalization: Expanding the dataset to include a wider range of attack types and sources would improve the generalizability of the models. Collaborating with other organizations to share data and insights could enhance the robustness and applicability of the findings.

7.4 Conclusion

This project demonstrated the potential of machine learning and advanced language models for analyzing and classifying SSH shell attack logs. By leveraging various techniques, we gained valuable insights into attack patterns and behaviors, which can inform cybersecurity strategies and defenses. Despite the challenges faced, the results highlight the importance of data-driven approaches in enhancing cybersecurity threat detection and response capabilities. Future work in this area holds promise for further advancements and practical applications in the field of cybersecurity.