CHAPTER 6

PHASE III-INTENTIONAL INSIDER MITIGATION (IIM)

CHAPTER 6

PHASE III - INTENTIONAL INSIDER MITIGATION (IIM)

6.1 INTRODUCTION

In the previous phase, only the unintentional insiders were mitigated. Intentional insiders detected in phase I and II are mitigated in this phase using a User Profiling mechanism. This chapter discusses the methodology for phase III-Intentional Insider Mitigation (IIM) which consists of three layers namely Data Preprocessing, Model Training and Evaluation, and User Profiling. The predicted user behavior from phase I and II contains categorical value that should be in numerical value. The Data Preprocessing is done to convert the data into a numerical format and to split the data for training and testing. The Model Training and Evaluation layer, detects and classifies the user risk into high and low. The User Profiling layer, profiles the user into an Allowlist and Denylist based on risk.

The following are the major contributions of the IIM phase:

- A Decision tree algorithm has been trained to detect and classify the user risk into high and low based on user behavior.
- The User Profiling has been employed to profile the users with low risk into Allowlist and users with high risk into Denylist for effective intentional insider mitigation.

The following section discusses the methodology of the IIM phase elaborately, along with the results obtained.

6.2 IIM METHODOLOGY OVERVIEW

The following Figure 6.1 depicts the methodology overview of the IIM phase. The IIM phase consists of three layers namely Data Preprocessing, Model Training and Evaluation, and User Profiling. In Data Preprocessing, label encoding and train test split are done to obtain a numerical representation and to evaluate the model performance. In Model Training and Evaluation, a Decision tree technique is trained to detect the user risk and classify it into high and low. In User Profiling, the high and low risk users are further profiled into Allowlist and Denylist.

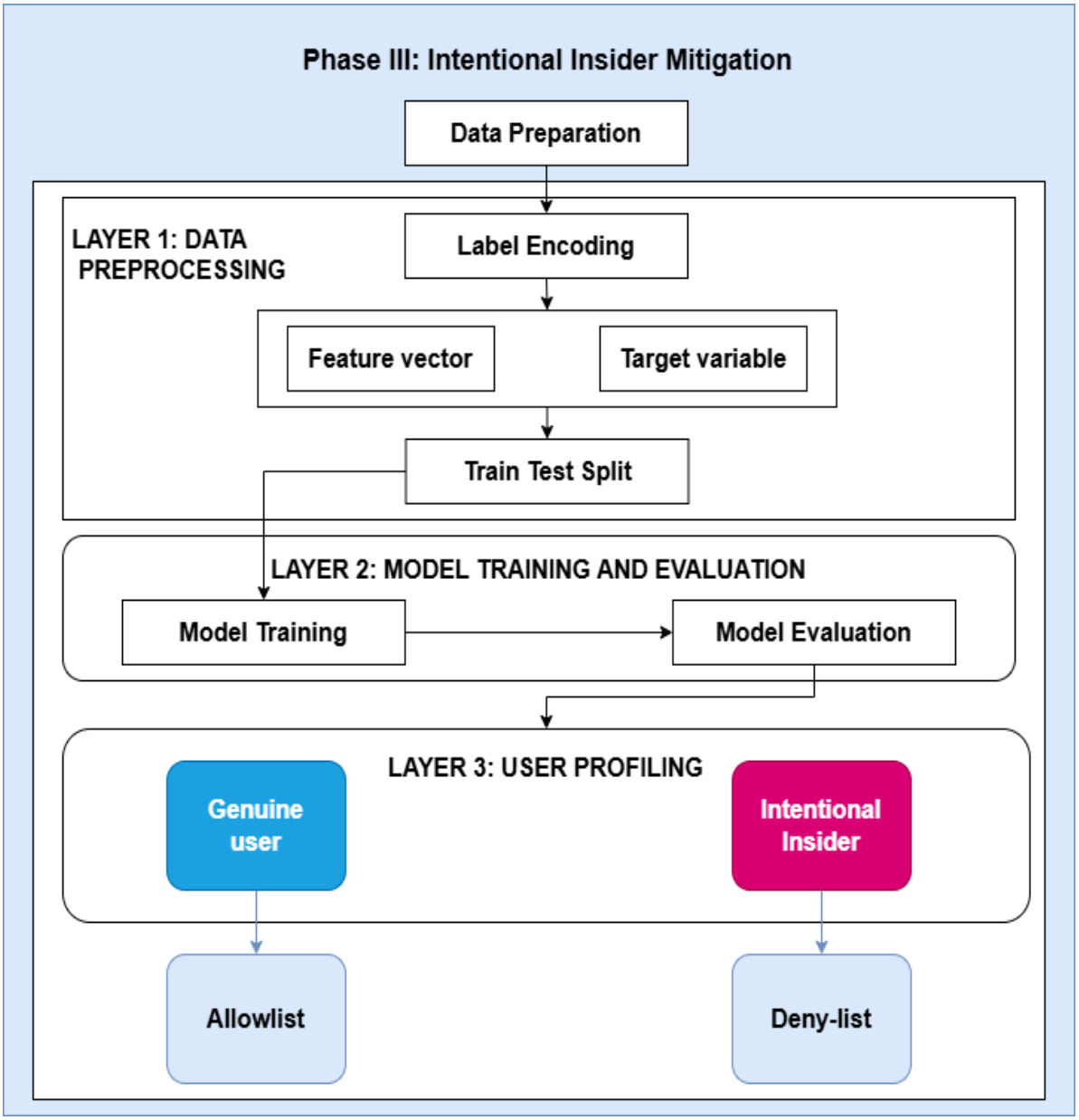

Figure 6.1: Methodology Overview of IIM Phase

6.2.1 DATASET PREPARATION

Log data with detected user behavior from the P&ID phase and UIM phase is necessary to profile and mitigate the intentional insiders for behavior-based User Profiling. P&ID phase incorporates insider detection and the outcome of P&ID phase is genuine, intentional, and unintentional insiders. In the UIM phase, the unintentional insiders are mitigated, and the outcome is genuine, and intentional insiders. The outcome obtained from the P&ID and UIM phase needs to be combined for User Profiling. Hence, dataset preparation is required.

The dataset preparation is done for two datasets:

- The CERT insider dataset for evaluating the proposed methodology, and
- CIC darknet dataset for validating the proposed methodology.

A. CERT Insider Dataset

The outcome obtained from the P&ID phase and UIM phase is integrated with log information in the CERT insider dataset. The sample of combined dataset in the CERT insider dataset is illustrated in Table 6.1

Table 6.1: Sample of Combined CERT Insider Dataset

Insider Threat	Source	User	Pc	Activity	Date	Detection Outcome	Mitigation Outcome
0	0	2702	3767	1	1.29E+09	Genuine User	Genuine
0	2	2702	3767	4	1.29E+09	Genuine User	Genuine
0	2	2702	3767	3	1.29E+09	Genuine User	Genuine
0	2	2702	3767	3	1.29E+09	Genuine User	Genuine
0	2	2702	3767	3	1.29E+09	Genuine User	Genuine
0	2	2702	3767	2	1.29E+09	Genuine User	Genuine
0	2	2702	3767	2	1.29E+09	Genuine User	Genuine
0	2	2702	3767	2	1.29E+09	Genuine User	Genuine
0	0	2702	3767	0	1.29E+09	Genuine User	Genuine
0	2	3779	1980	4	1.29E+09	Genuine User	Genuine
0	0	3564	1422	1	1.29E+09	Genuine User	Genuine
0	2	3564	1422	2	1.29E+09	Genuine User	Genuine
0	2	3564	1422	2	1.29E+09	Genuine User	Genuine
0	2	3564	1422	5	1.29E+09	Genuine User	Genuine
0	2	3564	1422	2	1.29E+09	Genuine User	Genuine
0	2	3564	1422	2	1.29E+09	Genuine User	Genuine
0	2	3564	1422	2	1.29E+09	Genuine User	Genuine
0	0	3564	1422	0	1.29E+09	Genuine User	Genuine
0	0	2702	3846	1	1.29E+09	Genuine User	Genuine
0	0	2702	3846	0	1.29E+09	Genuine User	Genuine
0	0	3779	2609	1	1.29E+09	Genuine User	Genuine

From table 6.1, it is evident that the combined CERT insider dataset determines six attributes related to the user behavior and two attributes related to their corresponding outcome from detection and mitigation phase. The dataset contains a simple-dimensional view and provides insight into genuine and insider behavior along with corresponding detection and mitigation strategies. The dataset description of the combined CERT insider dataset is listed in Table 6.2.

Table 6.2: Dataset Description of the Combined CERT Insider Dataset

Attribute	**Definition**
InsiderThreat (Binary Feature)	It indicates whether the activity is linked to an insider threat. Where '0' represents genuine user activities. '1' denotes activities related to potential insider threats.
Source	It represents the origin of the activity (e.g., http or device) associated with the user.
Date	It represents a timestamp indicating when the activity occurred, stored in epoch format.
User	It represents a unique identifier for individual users who perform a particular activity.
Pc	It denotes the personal computer or system ID used by the user while performing a particular activity.
Activity	It represents the type of action performed by the user and encodes the particular user performing activities.
Detection Outcome	It represents the outcome of insider detection in the P&ID phase in terms of 'Genuine User', 'Unintentional Insider', and 'Intentional Insider'.
Mitigation Outcome	It represents the outcome of unintentional insider mitigation in the UIM phase in terms of 'Genuine', and 'Intentional Insider'.

The dataset captures granular activity details along the detection and mitigation outcome. These outcome features is responsible for fine-grained user behavior profiling. It is utilized for evaluating the proposed research for mitigating intentional insiders.

B. CIC Darknet Dataset

In log data, the outcome obtained from P&ID phase and UIM phase is integrated in CIC darknet dataset. The combined CIC darknet dataset determines 85 attributes related to the darknet user behavior and two attributes related to their corresponding outcome from detection and mitigation phase. The dataset description of the combined CIC darknet dataset is listed in table 6.3.

Table 6.3: Dataset Description of the Combined CIC Darknet Dataset

Attribute(s)	Definition
'Flow ID', 'Flow Duration', 'Flow Bytes/s', and 'Flow Packets/s'	It represents the overall data transfer patterns to distinguish abnormal flows associated with potential insider threats.
'Total Fwd Packet', 'Total Bwd Packets', 'Total Length of Fwd Packet', and 'Total Length of Bwd Packet'	It represents the packet characteristics in both communication directions based on variations in packet flow.
'Flow IAT Mean', 'Flow IAT Std', 'Flow IAT Max', and 'Flow IAT Min'	It represents the unusual delays or bursts in network traffic.
'FIN Flag Count', 'SYN Flag Count', 'RST Flag Count', 'PSH Flag Count', 'ACK Flag Count', and 'URG Flag Count'	It denotes the packet functions in TCP protocols.
'Down/Up Ratio', 'Average Packet Size', 'Fwd Segment Size Avg', and 'Bwd Segment Size Avg'	It represents the abnormal traffic patterns.
'Subflow Fwd Packets', 'Subflow Fwd Bytes', 'Subflow Bwd Packets', and 'Subflow Bwd Bytes'	It represents the subflow of data packet.
'Active Mean', 'Active Std',	It represents the mean value, maximum value,

Attribute(s)	Definition
'Active Max', 'Active Min', 'Idle Mean', 'Idle Std', 'Idle Max', and 'Idle Min'	minimum value, and standard deviation value for active and inactive user activity.
Label	It provides a label of different types of traffic, such as Non-Tor, NonVPN, VPN, or Tor.
Detection Outcome	It represents the outcome of insider detection in the P&ID phase in terms of 'Genuine User', 'Unintentional Insider', and 'Intentional Insider'.
Mitigation Outcome	It represents the outcome of unintentional insider mitigation in the UIM phase in terms of 'Genuine', and 'Intentional Insider'.

The dataset captures granular activity details of darknet users along with the detection and mitigation outcome. It is utilized to evaluate the proposed research for mitigating the intentional insiders in the CIC darknet dataset.

6.2.2 INTENTIONAL INSIDER MITIGATION (IIM)

Mitigation of unintentional insiders is accomplished in the previous phase. The detected intentional insiders from the P&ID and UIM phases undergo mitigation in the IIM phase. The combined dataset is first preprocessed to obtain the numerical data for model training. Then, the data is trained using a Decision tree to classify the user risk into high and low. Users are profiled into Allowlist and Denylist based on their risk.

The proposed methodology for phase III (IIM) comprises of three layers. In the first layer, Data Preprocessing is encompassed using encoding and train test split to obtain numerical values for evaluating the model performance. In the second layer, the Decision tree technique is incorporated to detect and classify the user risk into high and low based on anomalous behavior. In the third layer, the users are profiled into Allowlist if the user possesses low risk, and profiled into Denylist if the user possesses high risk. The working procedure involved in the IIM phase is tabulated in Table 6.4.

Table 6.4: Working Procedure of the IIM Phase

Layer 1- Data Preprocessing
Step 1: Transform the features in categorical format into numerical values (Label encoding) Step 2: Split the data into train and test data (Train-test split)
Layer 2- Model Training and Evaluation
Step 3: The data is trained using the Decision tree technique to detect the risk and classify into high, and low (Model Training and Evaluation)
Layer 3-User Profiling
Step 4: The low risk users are profiled into Allowlist due to their authentic behavior pattern. The high risk users are profiled into Denylist due to their malicious activities (User Profiling)

Layer 1: Data Preprocessing

The combined log data from P&ID and UIM phase requires Data Preprocessing to obtain numerical value for train test split. Figure 6.2 illustrates the overview of Data Preprocessing layer.

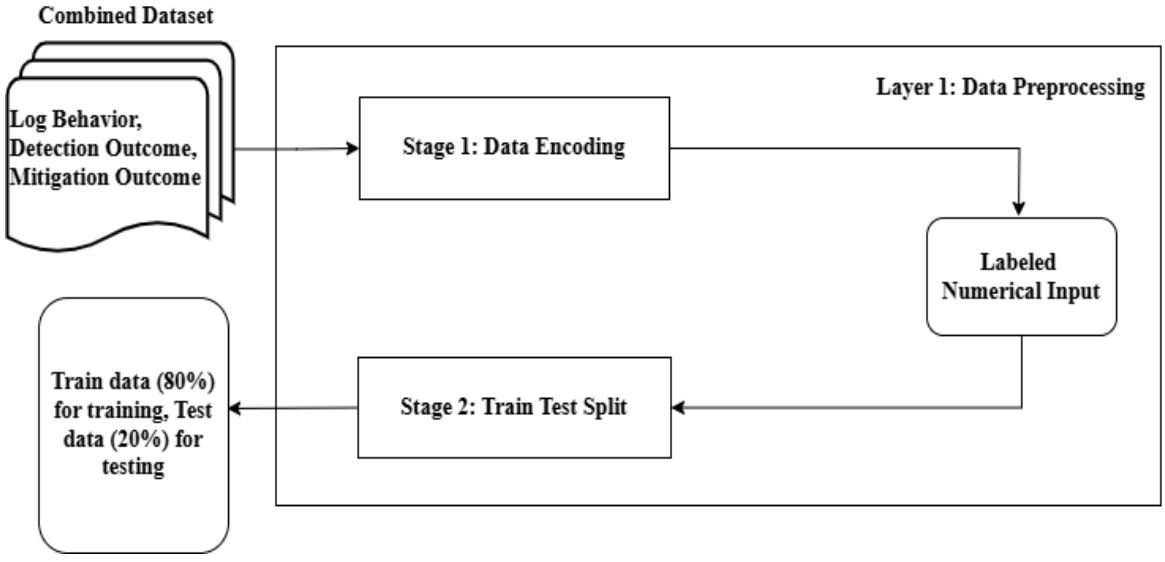

Figure 6.2. Overview of Data Preprocessing Layer

The combined dataset contains the categorical value. In data encoding, the combined categorical data is encoded to obtain the labelled numerical data. The numerical data is split into 80% train data and 20% test data for Model Training and Evaluation in layer 2.

The following subsection discusses the two stages of Data Preprocessing techniques: Data encoding that converts the categorical value, and the train test split, which splits the data into train and test data.

i) Data encoding

After Data Preparation, data encoding is performed. The combined data contains categorical features, it requires data encoding. Table 6.5 depicts the feature description of the combined data before data encoding.

Table 6.5. Feature Description of the Combined Data Before Data Encoding.

Feature(s)	**Description**
InsiderThreat	Integer
Source	Integer
Date	Integer
User	Integer
Pc	Integer
Activity	Integer
Detection Outcome	Categorical
Mitigation Outcome	Categorical

Every feature in the combined data is an integer, excluding Detection Outcome and Mitigation Outcome, which are categorical. Hence, data encoding is required to optimize the model's performance. If data encoding is not performed, the ML model will misinterpret results for intentional insider mitigation (Al-Shehari & Alsowail, 2021). Thus, data encoding is necessary to combat such challenges.

In this stage, the label encoding technique is used to address categorical features. It assigns a numerical value to every categorical feature. Table 6.6 displays the feature description of the combined data after data encoding.

Table 6.6. Feature Description of the Combined Data After Data Encoding.

Feature(s)	Description
InsiderThreat	Integer
Source	Integer
Date	Integer
User	Integer
Pc	Integer
Activity	Integer
Detection Outcome	Integer
Mitigation Outcome	Integer

ii) Train Test Split

After performing data encoding, train test split is done in this phase. The most relevant features, such as "InsiderThreat", "Source", "user", "pc", "activity", "Date", and "Detection Outcome", are selected as input features. The target variable is the 'Mitigation Outcome'. The dataset is split into a training and testing set with a ratio of 80:20, where 80% of the data is used for training, and 20% is reserved for testing. This division is critical to avoid overfitting.

Layer 2: Model Training and Evaluation

After Data Preprocessing, the Model Training and Evaluation is performed in this layer using train and test data obtained from train test split. This layer trains and evaluates the machine learning model for predicting the user risk. The following section discusses the Model Training and Evaluation to predict the user risk using Decision tree technique.

i) Decision Tree

The train and test data obtained using train test split that contains the user behavior and detection outcome, and is used for Model Training and Evaluation layer. The intentional insiders are individuals who deliberately perform malicious activities. These intentional insiders are detected in the P&ID phase, but are not mitigated which is crucial. Past research fails to incorporate the User Profiling mechanism to mitigate the intentional insiders. At first, the user risk is detected and classified into high risk and low risk using a Decision tree technique which is capable of profiling the users in a further section.

Decision tree is a supervised machine learning technique known for its simplicity, interpretability, and versatility in both classification and regression tasks (Le & Zincir-Heywood, 2018). A Decision tree is built by selecting features that maximize the information gain (IG) or minimize the Gini index or entropy. At each node, the technique evaluates all possible feature splits and chooses the one that best separates the data into distinct classes.

The overview of the Decision tree technique for Model Training and Evaluation to predict the user risk into high and low is illustrated in Figure 6.3.

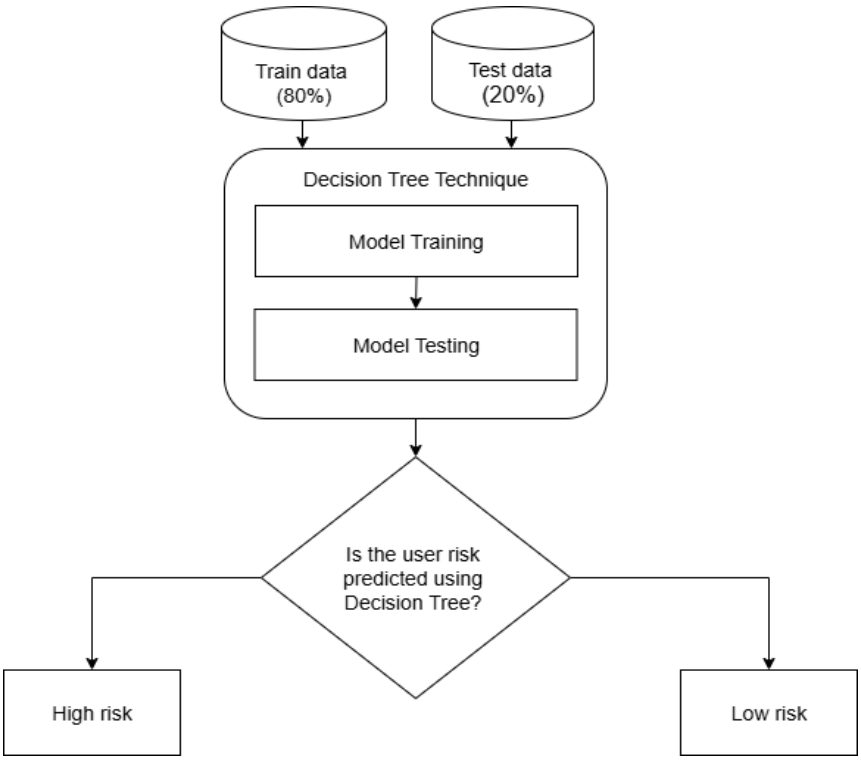

Figure 6.3. Overview of Decision Tree Technique for Model Training and Evaluation

The Decision Tree is trained using train data and tested using test data obtained from Data Preprocessing. Decision tree technique detects the unique user pattern and predicts the risk based on user behavior. Where it identifies the abnormal behavior that highly diverges from genuine behaviour is considered as high risk. It characterizes the minimal deviations in genuine behavior as low risk.

The working of a Decision tree technique for predicting user risk through Model Training and Evaluation are discussed below.

- *Model Training*: A Decision Tree is a supervised learning algorithm used for classification. It is trained using the dataset previously prepared to classify users based on their risk levels, either as low-risk or high-risk. Where low-risk denotes the genuine user and high-risk denotes the intentional insider.
- *Model Evaluation*: After model training, a Decision tree technique is used to generate the predictions for the likelihood of user behavior. It classifies the user, assigning them to either low risk or high risk based on the abnormality. The risk categories are:
    - *High-risk users*: These users exhibit behaviors that are associated with intentional insider threats, such as abnormal activity patterns, failed authentications, without proper clearance.
    - *Low-risk users*: Users who demonstrate normal behavior patterns that align with established user verification and do not pose a threat to the organization's assets.

A Decision tree is modeled and evaluated to predict the user risk by analyzing the user activity. The process of training and evaluation ensures users are classified into high risk and low risk, for further User Profiling.

Layer 3: User Profiling

After Model Training and Evaluation, users are profiled in this layer based on the risk predicted using a Decision tree technique. This layer profiles the users into Allowlist and Denylist based on the predicted risk. The following section discusses the User Profiling for intentional insider mitigation.

After predicting the user risk, the users are profiled into appropriate lists, known as the Allowlist and Denylist. These lists serve as preventive measures to mitigate risks and ensure that only trusted users are granted access to sensitive or critical systems and data (Peng et al., 2016).

- *Allowlist:* Genuine users performing less abnormal behavior is predicted as low-risk are further profiled into the Allowlist. Since, they are considered trustworthy, they are granted normal access to systems. The Allowlist essentially represents users who pose little to no threat, and their actions are in line with expected behavior.
- *Denylist:* Users predicted as high-risk are profiled into the Denylist. These individuals are flagged for suspicious behavior, and their access to certain systems and resources is either restricted or removed altogether. The Denylist serves as a security measure to proactively prevent malicious activities by insiders, ensuring they are prevented from executing any harmful actions.

By profiling users into these categories, it is helpful in organizations to address the intentional insider threats where the activities of intentional insiders are restricted.

The pseudo code for intentional insider mitigation is mentioned below.

```
BEGIN
# 1. Data Collection and Preparation
LOAD data from source
ENCODE categorical variables if any
NORMALIZE/scale features if needed
# 2. Feature Selection
SELECT relevant features (X)
SET target variable (y) to 'authentication_outcome'
# 3. Data Splitting
SPLIT data into training set (X_train, y_train) and testing set (X_test, y_test) with an 80-20 split
# 4. Model Training
INITIALIZE DecisionTreeClassifier with random_state=42
TRAIN classifier on X_train, y_train
# 5. Model Evaluation
```

PREDICT authentication outcomes on X_test using a trained classifier

CALCULATE accuracy score

PRINT accuracy score

PRINT classification report (precision, recall, F1-score)

PRINT confusion matrix

6. **Risk Classification**

PREDICT authentication outcomes for the entire dataset using trained classifier

Where '1' high risk, '0' low risk

#7. User Profiling

PROFILE users to 'Allowlist ' if predicted_outcome is 1

PROFILE users to 'Denylist' if predicted_outcome is 0

7. **Implementation and Integration**

OUTPUT lists of Allowlist user IDs and Denylist user IDs

END

6.3 EXPERIMENTAL RESULTS

6.3.1 PERFORMANCE METRICS FOR DECISION TREE

The train and test data obtained from Data Preprocessing is trained and evaluated using Decision Tree technique to predict risk for User Profiling. The performance of Decision Tree technique for predicting user risk and profiling them into Allowlist and Denylist is evaluated using four performance metrics. The metrics include Accuracy, Precision, Recall, and F-score.

Table 6.7 illustrates performance metrics for evaluating the performance of a Decision Tree to predict user risk.

Table 6.7. Performance Metrics to Evaluate a Decision Tree to Predict User Risk.

Performance Metrics	Definition	Formula
Accuracy	The ratio of correct predictions to the detected overall predictions.	$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$
Precision	The ratio of precisely predicted risk samples to the overall predicted risk samples.	$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$
Recall	The ratio of correctly predicted risk samples	$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$
F-score	A harmonic mean between precision and recall.	$\text{F} - \text{score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$

The present study applies all metrics mentioned above for a significant evaluation.

6.3.2 ELABORATIVE RESULT ANALYSIS OF IIM PHASE

The performance of IIM phase is evaluated using CERT insider dataset and the CIC darknet datasets. The following subsection discusses the experimental results of the IIM phase containing Data Preprocessing in layer 1, Model Training and Evaluation in layer 2, and User Profiling in layer 3.

Layer 1: Data Preprocessing

The performance of Data Preprocessing is evaluated using CERT insider and CIC darknet datasets. The following subsection explains the result obtained from two stages of Data Preprocessing techniques namely Data encoding and Train test split using both datasets.

i) Data Encoding

Data encoding is incorporated using the combined data obtained from Data Preparation. The result of data encoding in the CERT insider dataset the CIC darknet dataset using Label Encoding is explained below.

The Table 6.8 shows the results of data encoding using Label encoding in the CERT insider dataset.

Table 6.8. Result of Data Encoding in the CERT Insider Dataset.

Attribute(s)	Before encoding		After encoding	
	Datatype	Value	Datatype	Value
Insider Threat	Integer	0,1	Integer	0,1
Source	Integer	0,1,2	Integer	0,1,2
Date	Integer	1280707200	Integer	1280707200
User	Integer	4	Integer	4
Pc	Integer	128	Integer	128
Activity	Integer	750	Integer	750
Detection Outcome	Categorical	Genuine, Intentional Insider, Unintentional Insider	Integer	0,1,2
Mitigation Outcome	Categorical	Genuine, Intentional Insider	Integer	0,1

From the above Table 6.8, it is observed that every data in Detection Outcome and Mitigation Outcome are converted into a numerical representation. Meanwhile, others remained the same.

The following Table 6.9 shows the results of data encoding using label encoding in the CIC darknet dataset.

Table 6.9. Result of Data Encoding in the CIC Darknet Dataset.

Attribute(s)	Before encoding		After encoding	
	Datatype	**Value**	**Datatype**	**Value**
'Flow ID', 'Flow Duration', 'Flow Bytes/s', and 'Flow Packets/s'	Integer	20738	Integer	20738
‘Total Fwd Packet’, ‘Total Bwd Packets’, ‘Total Length of Fwd Packet’, and ‘Total Length of	Integer	3638	Integer	3638

Attribute(s)	Before encoding		After encoding	
	Datatype	**Value**	**Datatype**	**Value**
Bwd Packet’				
‘Flow IAT Mean’, ‘Flow IAT Std’, ‘Flow IAT Max’, and ‘Flow IAT Min’	Integer	359	Integer	359
‘FIN Flag Count’, ‘SYN Flag Count’, ‘RST Flag Count’, ‘PSH Flag Count’, ‘ACK Flag Count’, and ‘URG Flag Count’	Integer	0,1,2,3	Integer	0,1,2,3
‘Down/Up Ratio’, ‘Average Packet Size’, ‘Fwd Segment Size Avg’, and ‘Bwd Segment Size Avg’	Integer	0,1,2,3	Integer	0,1,2,3
‘Subflow Fwd Packets’, ‘Subflow Fwd Bytes’, ‘Subflow Bwd Packets’, and ‘Subflow Bwd Bytes’	Integer	371	Integer	371
‘Active Mean’, ‘Active Std’, ‘Active Max’, ‘Active Min’, ‘Idle Mean’, ‘Idle Std’, ‘Idle Max’, and ‘Idle Min’	Integer	1437765000927700	Integer	1437765 0009277 00
Label	Integer	0, 1, 2, 3	Integer	0, 1, 2, 3
Detection Outcome	Categorical	Genuine, Intentional Insider, Unintentional Insider	Integer	0,1,2
Mitigation Outcome	Categorical	Genuine, Intentional Insider	Integer	0,1

From Table 6.9, it is observed that two categorical features from the CIC darknet dataset, namely 'Detection Outcome' and 'Mitigation Outcome', were transformed into numerical values using label encoding techniques.

ii) Train test split

After data encoding, train test split is performed using the numerical data. The results obtained from train test split using both the CERT insider dataset and the CIC darknet dataset is discussed below.

The encoded data contains the numerical representation of log activities, detection outcome from phase I and mitigation outcome from phase II. In CERT insider dataset, the encoded data from data encoding is split into train and test data with the ratio of 80:20 in this phase. Where, 80% of train data is used for training and 20% of test data is used for testing.

In CIC darknet dataset, the encoded data obtained from data encoding is used to perform train test split. Train test split is employed to ensure a representative dataset for training and testing. Where, 80% of data used for training is considered as train data, and 20% of data used for testing is considered as test data.

Layer 2: Model Training and Evaluation

After train test split, the Model Training and Evaluation is performed using train and test data obtained from Data Preprocessing layer. Decision Tree technique is used to train and evaluate the model for predicting the high risk, and low risk users. The following section discusses the result obtained from Decision Tree technique for Model Training and Evaluation using both CERT insider and CIC darknet datasets.

The following Table 6.10 gives the performance evaluation of a Decision Tree in the IIM phase for intentional insider mitigation using CERT insider and CIC darknet datasets. It is evaluated based on precision, recall, f-score, and accuracy.

Table 6.10: Results of Model Training and Evaluation using CERT Insider and CIC Darknet datasets

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)	Predictions	
					Low Risk Users (in numbers)	High Risk Users (in numbers)
CERT Insider dataset	100	100	100	100	57	8
CIC Darknet dataset	100	100	100	100	5063	4647

From Table 6.10, the following are observed

- The methodology achieved exceptional results with 100% accuracy, precision, recall, and F1-score using Decision Tree for intentional insider mitigation.

- The performance underscores the capability of the proposed methodology to accurately predict every intentional insiders as high risk users and every genuine users as low risk users. i.e., 57 low risk users and 8 high risk users using CERT insider dataset. In CIC darknet dataset, 5063 users are predicted as low risk users, and 4647 users are predicted as high risk users.

Layer 3: User Profiling

After Model Training and Evaluation, the User Profiling is performed to profile high risk and low risk users obtained from the Model Training and Evaluation layer. The following section discusses the results obtained from User Profiling for intentional insider mitigation using both CERT insider and CIC darknet datasets.

The following Figure 6.4 gives the results of User Profiling in the IIM phase using CERT insider and CIC darknet datasets for intentional insider mitigation.

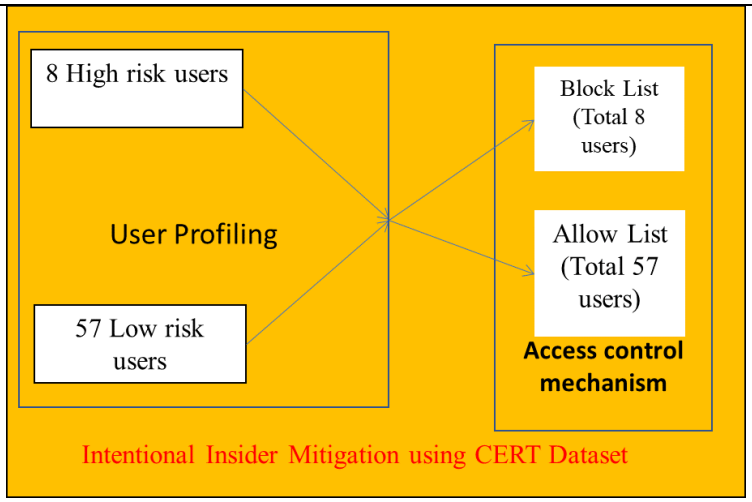

Figure 6.4 (a): Using the CERT Dataset

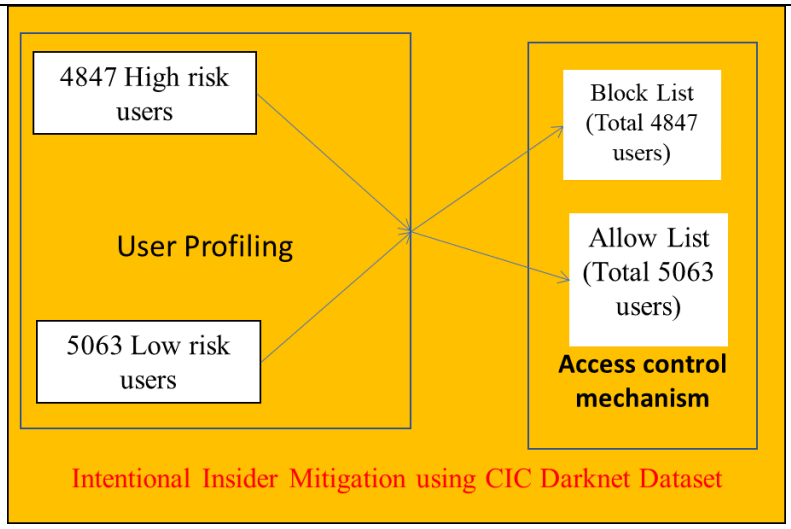

Figure 6.4 (b): Using the CIC Darknet Dataset

Figure 6.4: Performance of IIM Phase

From figure 6.4, the following are illustrated

- IIM phase profiled 57 low risk users performing genuine activities into the Allowlist and profiled 8 high risk users performing intentional malicious activities in the Denylist using the CERT insider dataset.
- The CIC Darknet dataset analysis demonstrated the scalability and robustness of the methodology. It profiled 5063 low risk users into the Allowlist and profiled 4847 high risk users into the Denylist.

- The Allowlist users comprises of low-risk users based on their consistent behavior that aligns with the baseline norms, indicating minimal likelihood of posing a threat. The Denylist user profiles users predicted as high-risk due to their potential malicious intention necessitate further scrutiny.

6.4 OUTCOME OF PHASE III

The outcome of the IIM phase is listed below.

- High-risk users in Denylist have limited access in sensitive systems to prevent potential exploitation. Thus, it mitigates intentional insiders.
- Intentional insiders are successfully mitigated using Decision tree with 100% accuracy for profiling high risk intentional insiders into Denylist and low risk genuine users into Allowlist. Thus achieving the stated secondary objective 3.

6.5 CHAPTER SUMMARY

The Intentional Insider Mitigation phase addresses the challenge of mitigating intentional insider threats. Initial Data Preparation is done by combining the log details with the detection and mitigation outcome. Then, Data Preprocessing including data encoding and train test split is done. Next to Data Preprocessing is Model Training and Evaluation. For Model Training and Evaluation, a Decision Tree technique is employed to predict the low-risk and high-risk users based on historical behavioral patterns. Next to Model Training and Evaluation is User Profiling. In User Profiling, low risk users are successfully profiled into Allowlist and high risk users are successfully profiled into Denylist.