A

Mini Project

On

ROBUST AND SECURE DATA TRANSMISSION USING ARTIFICIAL INTELLIGENCE TECHNIQUES IN AD-HOC NETWORKS

(Submitted in partial fulfillment of the requirements for the award of Degree)

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

A. Amulya(217R1A05K8)

AJV. Swaroop(217R1A05K7)

P. Arun Teja(217R1A05P5)

Under the Guidance of

DR. G. MADHUKAR

(Associate Professor)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CMR TECHNICAL CAMPUS

UGC AUTONOMOUS

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, New Delhi)

Recognized Under Section 2(f) & 12(B) of the UGCAct.1956,

Kandlakoya (V), Medchal Road, Hyderabad-501401.

2021-25

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project titled "**ROBUST AND SECURE DATA TRANSMISSION USING ARTIFICIAL INTELLIGENCE TECHNIQUES IN AD-HOC NETWORKS"** being submitted by **A.AMULYA(217R1A05K8), AJV.SWAROOP(217R1A05K7) & P.ARUN TEJA(217R1A05P5)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, is a record of Bonafide work carried out by them under our guidance and supervision during the year 2024-25.

The results embodied in this project have not been submitted to any other University or Institute for the award of any degree or diploma.

Dr. G. Madhukar
Associate Professor
INTERNAL GUIDE

Dr. A. Raji Reddy
DIRECTOR

Dr. N. Bhaskar
HOD

EXTERNAL EXAMINER

Submitted for viva voice Examination held on _____

ACKNOWLEDGEMENT

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project.

We take this opportunity to express our profound gratitude and deep regard to our guide **Dr. G. Madhukar,** Associate Professor for his exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him shall carry me a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to Project Review Committee (PRC) Coordinators : **Dr. J. Narasimha Rao, Dr. K. Maheshwari , Mr. K .Ranjith Reddy, Mrs. K. Shilpa** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. N. Bhaskar,** Head Of The Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative throughout the course of this project. We would like to express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairman for providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

A. AMULYA (217R1A05K8)

AJV. SWAROOP (217R1A05K7)

P. ARUN TEJA (217R1A05P5)

ABSTRACT

This project is titled as “Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks”. It presents a new security aspect for a Mobile Ad-Hoc Network (MANET)-based IoT model using the concept of artificial intelligence. The Black Hole Attack (BHA) is considered one of the most affecting threats in the MANET in which the attacker node drops the entire data traffic and hence degrades the network performance. Therefore, it necessitates the designing of an algorithm that can protect the network from the BHA node. This project introduces Ad-hoc On-Demand Distance Vector (AODV), a new updated routing protocol that combines the advantages of the Artificial Bee Colony (ABC), Artificial Neural Network (ANN), and Support Vector Machine (SVM) techniques. The combination of the SVM with ANN is the novelty of the proposed model that helps to identify the attackers within the discovered route using the AODV routing mechanism. Here, the model is trained using ANN but the selection of training data is performed using the ABC fitness function followed by SVM. The role of ABC is to provide a better route for data transmission between the source and the destination node.

LIST OF FIGURES

LIST OF SCREENSHOTS

TABLE OF CONTENTS

1. INTRODUCTION

1.INTRODUCTION

1.1 PROJECT SCOPE

This project is titled as “Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks”. This project involves the development of Innovative solutions to enhance the security and reliability of data communication in decentralized, dynamic environments. Ad-hoc networks, characterized by their self-configuring nature and lack of fixed infrastructure, are leads to various security threats such as data interception, unauthorized access, and malicious attacks. Additionally, this project will focus on improving the robustness of data transmission to ensure minimal packet loss and latency, even in the presence of interference or unstable connections.

1.2 PROJECT PURPOSE

The purpose of this project is to improve the security and reliability of data transmission in ad-hoc networks by using AI techniques. It aims to protect the network from threats like unauthorized access, data tampering, and malicious attacks, while ensuring efficient and stable communication. It will optimize network performance by adapting routing paths and managing network resources efficiently By combining robust security with efficient data delivery, the project seeks to provide a reliable solution for critical applications, such as emergency response and mobile communications.

1.3 PROJECT FEATURES

Real-Time Threat Detection: Utilizes machine learning algorithms to identify and respond to security threats, such as packet drops and unauthorized access, as they occur.

Adaptive Routing Protocols: Implements AI-driven routing algorithms that dynamically adjust communication paths based on network conditions and detected threats, ensuring optimal data delivery.

Data Integrity Verification: Ensures the authenticity and integrity of transmitted data using encryption and protecting against tampering.

Self-Configuring Network: Supports automatic formation and allowing nodes to join or leave.

2. SYSTEM ANALYSIS

2.SYSTEM ANALYSIS

SYSTEM ANALYSIS

System Analysis is the important phase in the system development process. The System is studied to the minute details and analyzed. The system analyst plays an important role of an interrogator and dwells deep into the working of the present system. In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done. A key question considered here is, "what must be done to solve the problem?" The system is viewed as a whole and the inputs to the system are identified. Once analysis is completed the analyst has a firm understanding of what is to be done.

2.1 PROBLEM DEFINITION

A detailed study of the process must be made by various techniques like Image processing, feature recognition etc. The data collected by these sources must be scrutinized to arrive to a conclusion. The conclusion is an understanding of how the system functions. This system is called the existing system. Now the existing system is subjected to close study and problem areas are identified. The designer now functions as a problem solver and tries to sort out the difficulties that the enterprise faces. The solutions are given as proposals. The proposal is then weighed with the existing system analytically and the best one is selected. The proposal is presented to the user for an endorsement by the user. The proposal is reviewed on user request and suitable changes are made. This is loop that ends as soon as the user is satisfied with proposal.

2.2 EXISTING SYSTEM

In the Existing system The CL-PRE(certificateless proxy re-encryption) scheme, the data owner encrypts the data with the symmetric key. Subsequently, the symmetric key is encrypted with the public key of the data owner. Both the encrypted data and the key are uploaded to the cloud. The encrypted key is re-encrypted by the cloud (that acts as a proxy re-encryption agent) that becomes decryptable by the user's private key. The public–private keys generated in the proposed scheme are not based on the certificates. The user's identity is used to generate the public–private key pair. The proxy re-encryption is based on bilinear pairing and the BDH that makes the CL-PRE scheme computationally intensive. The computational cost of the bilinear pairing is high as compared with the standard operations in finite fields.

2.2.1 LIMITATIONS OF EXISTING SYSTEM

- Energy Consumption
- Trust and privacy issues
- Cost of Deployment
- Slow Decision Making
- Difficulty in Training

2.3 PROPOSED SYSTEM

The aim of proposed system is to develop a system of improved facilities. The proposed system can overcome all the limitations of the existing system. The proposed system has optimized route, suggested by ABC, is then passed to the SVM model along with the node's properties. Based on those properties, ANN decides whether the node is a normal or an attacker node. The simulation analysis performed in software application shows that the proposed work exhibits an improvement in terms of Packet Delivery Ratio (PDR), throughput, and delay. To validate the system efficiency, a comparative analysis is performed against the existing approaches such as Decision Tree and Random Forest that indicate that the utilization of the SVM with ANN is a beneficial step regarding the detection of BHA attackers in the MANET-based IoT networks.

2.3.1 ADVANTAGES OF THE PROPOSED SYSTEM

The system is very simple in design and to implement. The system requires very low system resources and the system will work in almost all configurations. It has got following features

- Real-Time decision making
- Energy efficiency
- Load Balancing
- Security
- Self Learning capabilities
- Improved Reliability
- Robust against attacks
- Improved user privacy

2.4 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. Three key considerations involved in the feasibility analysis are

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

2.4.1 ECONOMIC FEASIBILITY

The developing system must be justified by cost and benefit. Criteria to ensure that effort is concentrated on project, which will give best, return at the earliest. One of the factors, which affect the development of a new system, is the cost it would require.

The following are some of the important financial questions asked during preliminary investigation:

- The costs conduct a full system investigation.
- The cost of the hardware and software.
- The benefits in the form of reduced costs or fewer costly errors.

Since the system is developed as part of project work, there is no manual cost to spend for the proposed system. Also all the resources are already available, it give an indication of the system is economically possible for development.

2.4.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

2.4.3 BEHAVIORAL FEASIBILITY

This includes the following questions:

- Is there sufficient support for the users?
- Will the proposed system cause harm?

The project would be beneficial because it satisfies the objectives when developed and installed. All behavioral aspects are considered carefully and conclude that the project is behaviorally feasible.

2.5 HARDWARE & SOFTWARE REQUIREMENTS

2.5.1 HARDWARE REQUIREMENTS:

Hardware interfaces specifies the logical characteristics of each interface between the software product and the hardware components of the system. The following are some hardware requirements.

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40GB
- RAM : 4GB

2.5.2 SOFTWARE REQUIREMENTS:

Software Requirements specifies the logical characteristics of each interface and software components of the system. The following are some software requirements.

- Operating system : Windows 8 or above
- Coding Language : Python 3.7.0

3. ARCHITECTURE

3.ARCHITECTURE

3.1 PROJECT ARCHITECTURE

This project architecture shows the procedure followed for breed detection using machine learning, starting from input to final prediction.

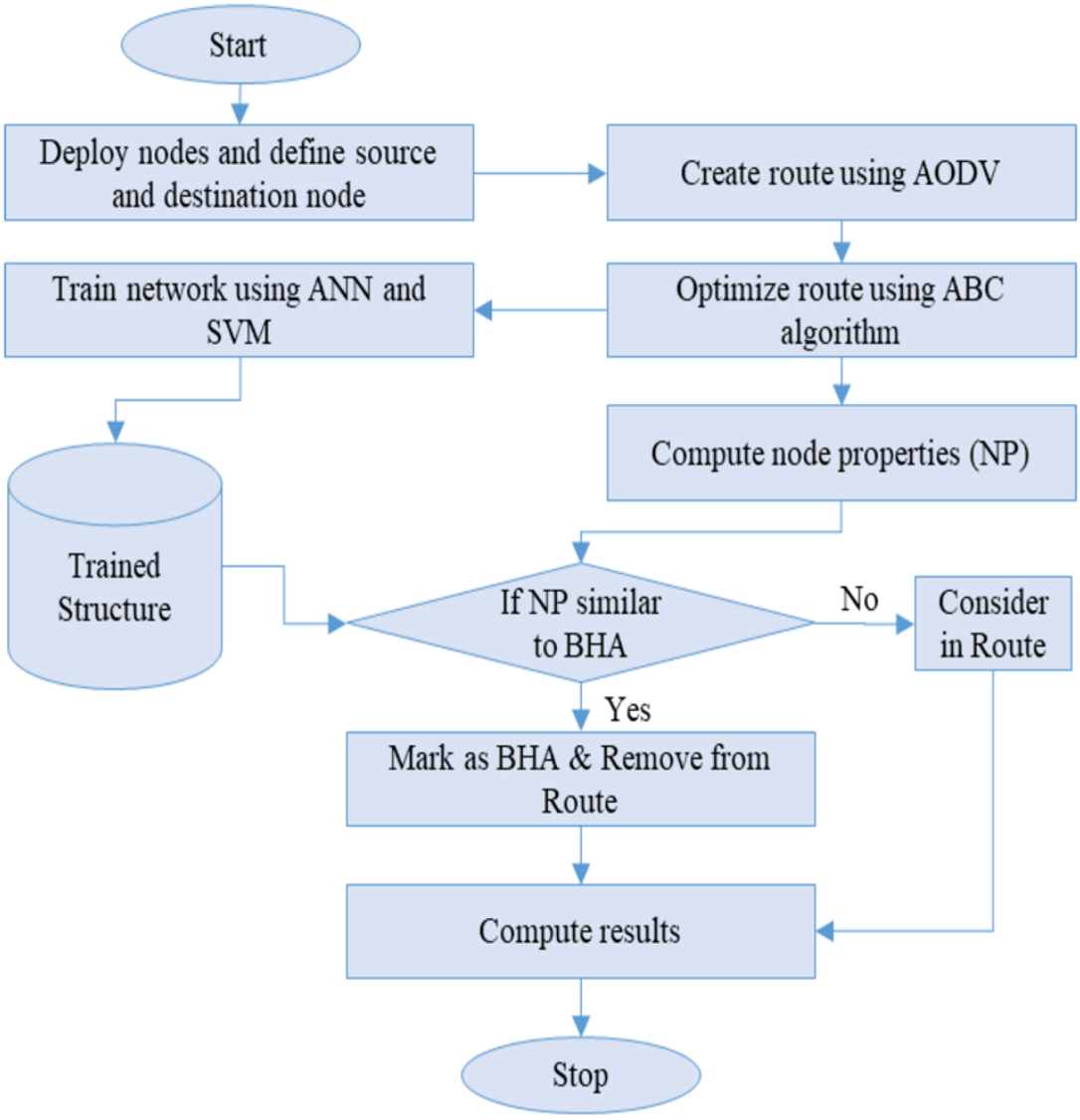


Figure 3.1: Project Architecture of Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks

3.2 DESCRIPTION

Start: The process begins.

Deploy Nodes and Define Source and Destination Node: Nodes are deployed in the network, and the source and destination nodes are defined for communication.

Create Route Using AODV: The route is created using the AODV routing protocol, which is commonly used in mobile ad hoc networks.

Optimize Route Using ABC Algorithm: The route is further optimized using the ABC algorithm, which is inspired by the foraging behaviour of honeybees and is used to optimize search processes.

Compute Node Properties: The properties of the nodes involved in the network (such as connectivity, energy levels, etc.) are computed.

Train Network Using ANN and SVM: The network is trained using machine learning algorithms such as ANN and SVM, which help in predicting or classifying the nodes based on their behaviour.

Trained Structure: The trained model or structure is stored and can be used for future decision-making regarding node selection.

If NP Similar to BHA:

Yes: If the node properties are similar to those seen in a black hole attack, the node is marked as BHA and removed from the route. The black hole attack is a type of security attack where malicious nodes drop all packets.

No: If no similarity is detected, the node is considered in the route.

Compute Results: Once the nodes are selected and routes are optimized, the final results are computed.

Stop: The process ends.

3.3 USE CASE DIAGRAM

In the use case diagram we have basically two actors who are the user and the Database. The user upload AODV Dataset, Preprocess Dataset, Run purpose ABC SVM ANN Model, Run Random Forest Algorithm, Run Decision Tree Algorithm, Comparision Graph, Attack Detection from Test Data. Whereas Database Processes all those and returns Output.

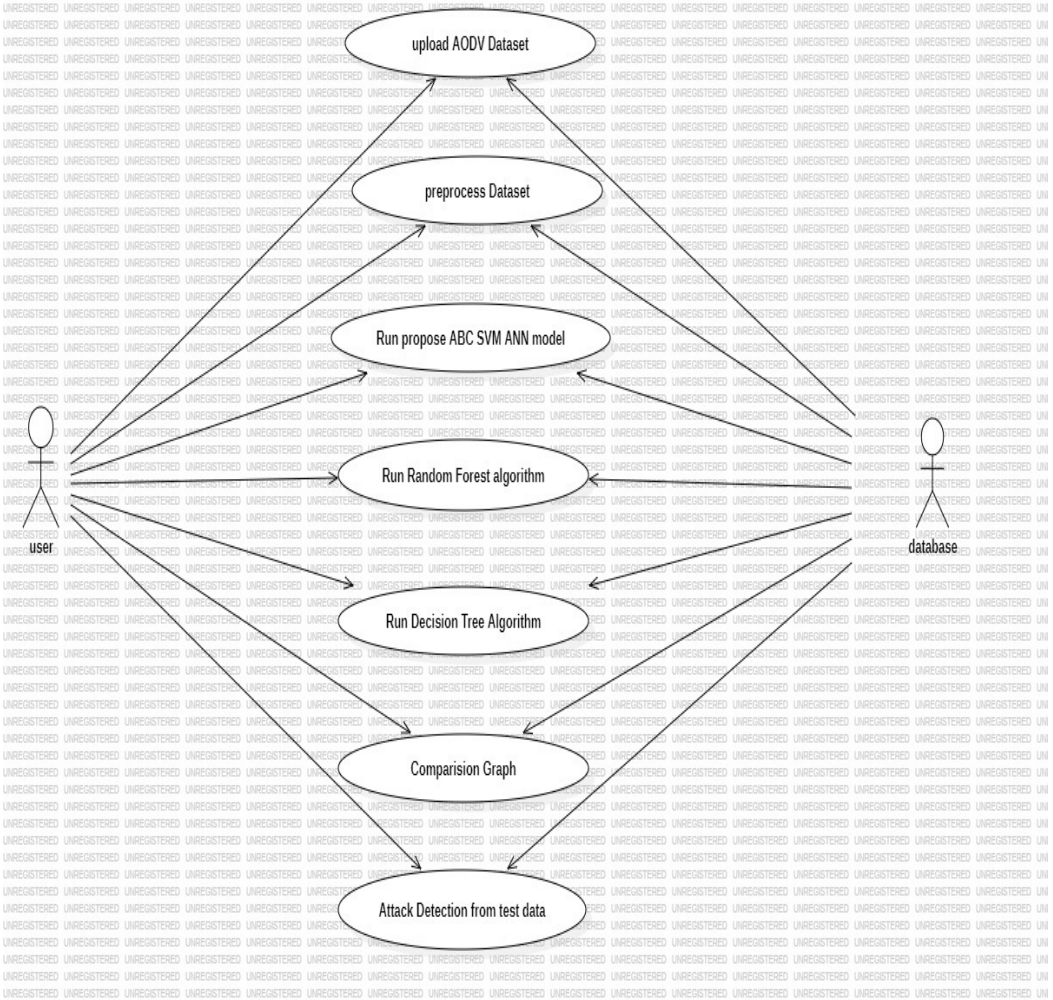


Figure 3.2 Use Case Diagram for Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks

3.4 CLASS DIAGRAM

Class Diagram is a collection of classes and objects.

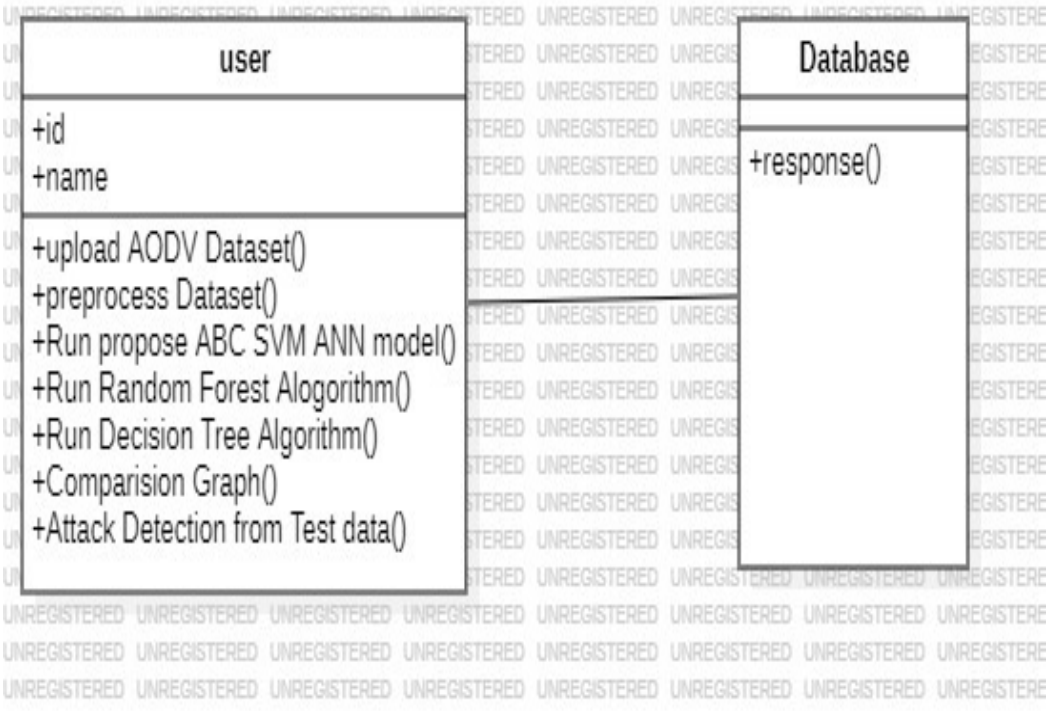


Figure 3.3: Class Diagram for Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks

3.5 SEQUENCE DIAGRAM

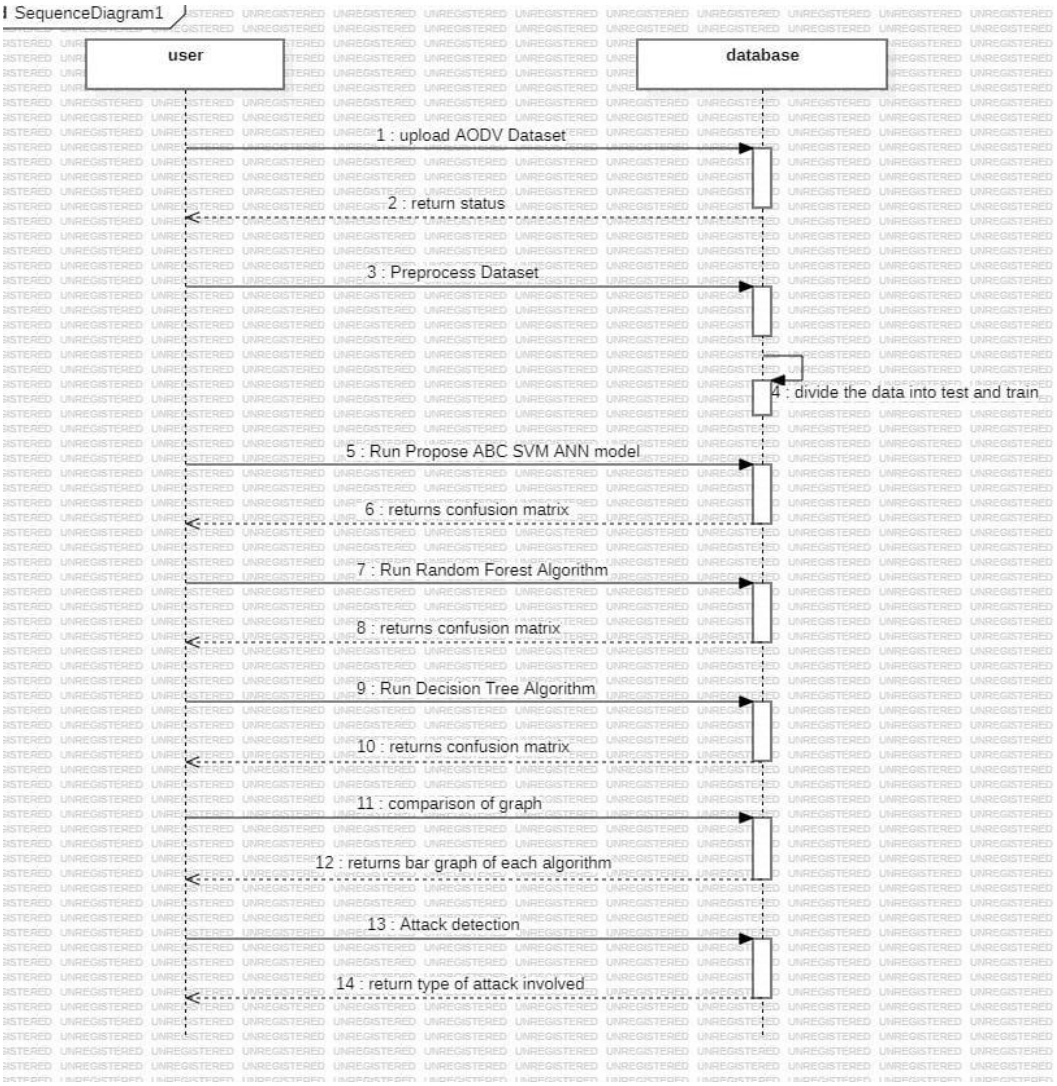


Figure 3.4: : Sequence Diagram for Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks

3.6 ACTIVITY DIAGRAM

It describes about flow of activity states.

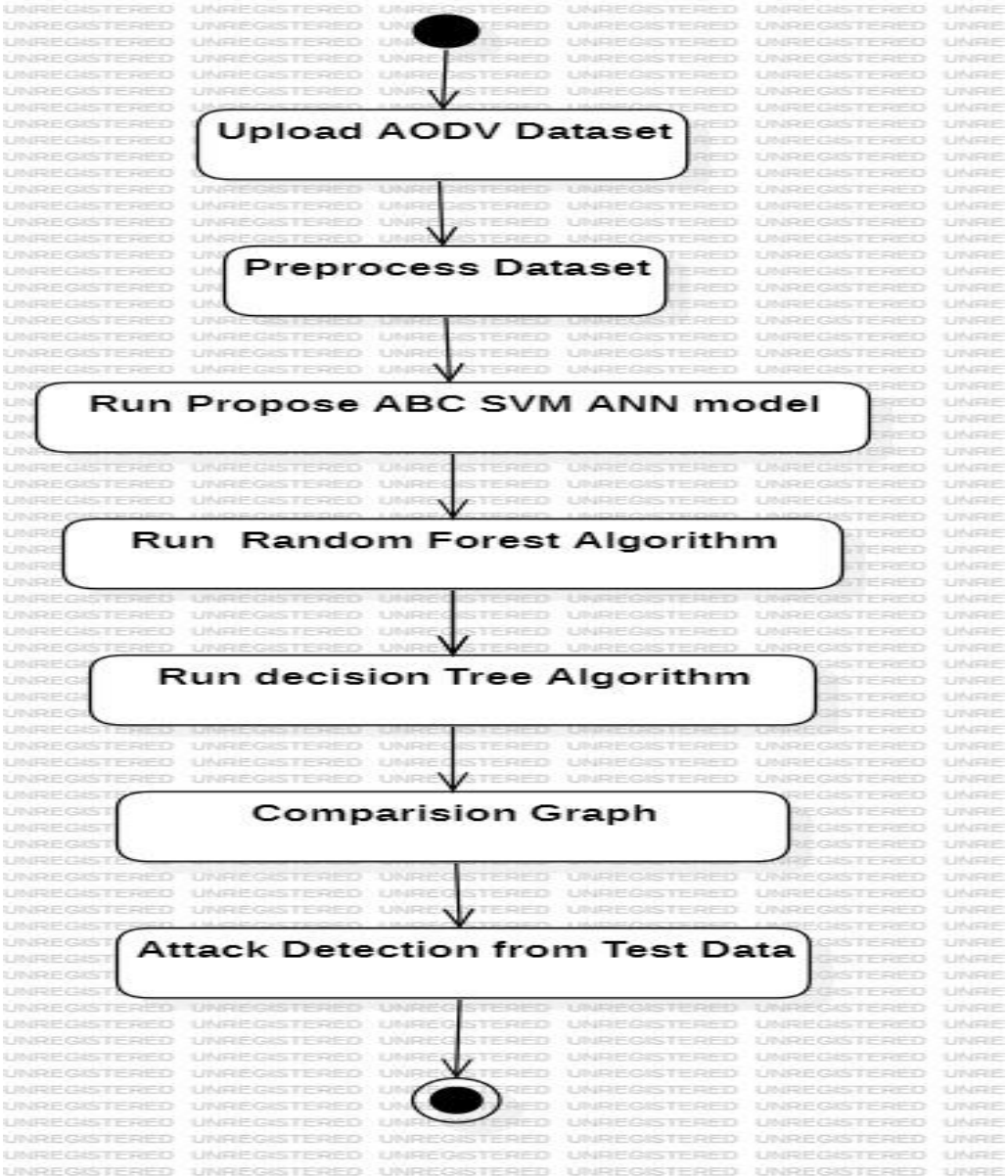


Figure 3.5: Activity Diagram for Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks

4. IMPLEMENTATION

4. IMPLEMENTATION

4.1 SAMPLE CODE

```
from tkinter import *
import tkinter
from tkinter import filedialog
from tkinter.filedialog import askopenfilename
import seaborn as sns
from sklearn.metrics import accuracy_score
from sklearn.model_selection import train_test_split
from sklearn.metrics import precision_score
from sklearn.metrics import recall_score
from sklearn.metrics import f1_score
from sklearn.metrics import confusion_matrix
from sklearn.ensemble import RandomForestClassifier
from sklearn.tree import DecisionTreeClassifier
import os
import pandas as pd
import numpy as np
from sklearn.preprocessing import LabelEncoder
from sklearn.preprocessing import MinMaxScaler
from sklearn.model_selection import train_test_split
import matplotlib.pyplot as plt
from ABC import ABC
from SwarmPackagePy import testFunctions as tf
from sklearn.svm import SVC
from keras.models import Sequential
from keras.layers.core import Dense,Activation,Dropout, Flatten
from keras.utils.np_utils import to_categorical
from keras.callbacks import ModelCheckpoint
import os
import pickle
main = tkinter.Tk()
main.title("Robust and Secure Data Transmission Using Artificial Intelligence Techniques in
Ad-Hoc Networks")
main.geometry("1200x1200")
global filename
global X, Y
global X_train, X_test, y_train, y_test
global throughput
global pdr
global delay
```

```
global classifier, class_labels, dataset, label_encoder, scaler
def uploadDataset():
global filename, class_labels, dataset
filename = filedialog.askopenfilename(initialdir="AODVDataset")
pathlabel.config(text=filename)
text.delete('1.0', END)
text.insert(END,filename+" loaded\n\n")
dataset = pd.read_csv(filename)
text.insert(END,str(dataset))
class_labels = np.unique(dataset['Label'])
label = dataset.groupby('Label').size()
label.plot(kind="bar")
plt.title("Different Attacks Found in Dataset Graph")
plt.xlabel("Attack Name")
plt.ylabel("Count")
plt.show()
def preprocessDataset():
global dataset, label_encoder, X, Y, X_train, X_test, y_train, y_test, scaler
text.delete('1.0', END)
dataset.fillna(0, inplace = True)
label_encoder = []
columns = dataset.columns
types = dataset.dtypes.values
for i in range(len(types)):
name = types[i]
if name == 'object': #finding column with object type
le = LabelEncoder()
print(columns[i])
dataset[columns[i]]
= pd.Series(le.fit_transform(dataset[columns[i]].astype(str)))#encode all str columns
to numeric
label_encoder.append(le)
text.insert(END,str(dataset)+"\n\n")
dataset = dataset.values
X = dataset[:,0:dataset.shape[1]-1]
Y = dataset[:,dataset.shape[1]-1]
scaler = MinMaxScaler(feature_range = (0, 1)) #use to normalize training features
X = scaler.fit_transform(X)
#function which will calculate all metrics and plot confusion matrix
def calculateMetrics(predict, y_test, algorithm):
global class_labels
p = precision_score(y_test, predict,average='macro') * 100
r = recall_score(y_test, predict,average='macro') * 100
a = accuracy_score(y_test,predict)*100
conf_matrix = confusion_matrix(y_test, predict)
throughput.append(a)
```

```
pdr.append(p)
delay.append(100 - r)
text.insert(END,algorithm+' Throughput    : '+str(a)+"\n")
text.insert(END,algorithm+' PDR   : '+str(p)+"\n")
text.insert(END,algorithm+' Delay      : '+str(100 - r)+"\n\n")
plt.figure(figsize =(6, 4))
ax = sns.heatmap(conf_matrix, xticklabels = class_labels, yticklabels = class_labels,
annot = True, cmap="viridis" ,fmt ="g");
ax.set_ylim([0,len(class_labels)])
plt.title(algorithm+" Confusion matrix")
plt.ylabel('True class')
plt.xlabel('Predicted class')
plt.show()
def runPropose():
text.delete('1.0', END)
global X, Y, throughput, pdr, delay
delay = []
throughput = []
pdr = []
alh = ABC(X, tf.easom_function, -10, 10, 2, 20)
Gbest = np.asarray(alh.get_Gbest())
in_mask = [True if i > 0 else False for i in Gbest]
in_mask = np.asarray(in_mask)
X_selected_features = X[:,in_mask==1]
svm_cls = SVC(probability=True)
svm_cls.fit(X_selected_features, Y)
Y1 = to_categorical(Y)
X_selected_features = np.reshape(X_selected_features, (X_selected_features.shape[0],
X_selected_features.shape[1], 1))
X_train, X_test, y_train, y_test = train_test_split(X_selected_features, Y1, test_size=0.2)
ann_model = Sequential()
ann_model.add(Flatten(input_shape=[X_train.shape[1],X_train.shape[2]]))
ann_model.add(Dense(300, activation="relu"))
ann_model.add(Dense(100, activation="relu"))
ann_model.add(Dense(y_train.shape[1], activation="softmax"))
 ann_model.compile(loss='categorical_crossentropy',optimizer='adam',
 metrics=['accuracy'])
 if os.path.exists("model/model_weights.hdf5") == False:
 model_check_point = ModelCheckpoint(filepath='model/model_weights.hdf5',
 verbose = 1, save_best_only = True)
 hist = ann_model.fit(X_train, y_train, batch_size = 32, epochs = 350,
 validation_data=(X_test, y_test), callbacks=[model_check_point], verbose=1)
 f = open('model/history.pckl', 'wb')
 pickle.dump(hist.history, f)
 f.close()
 else:
```

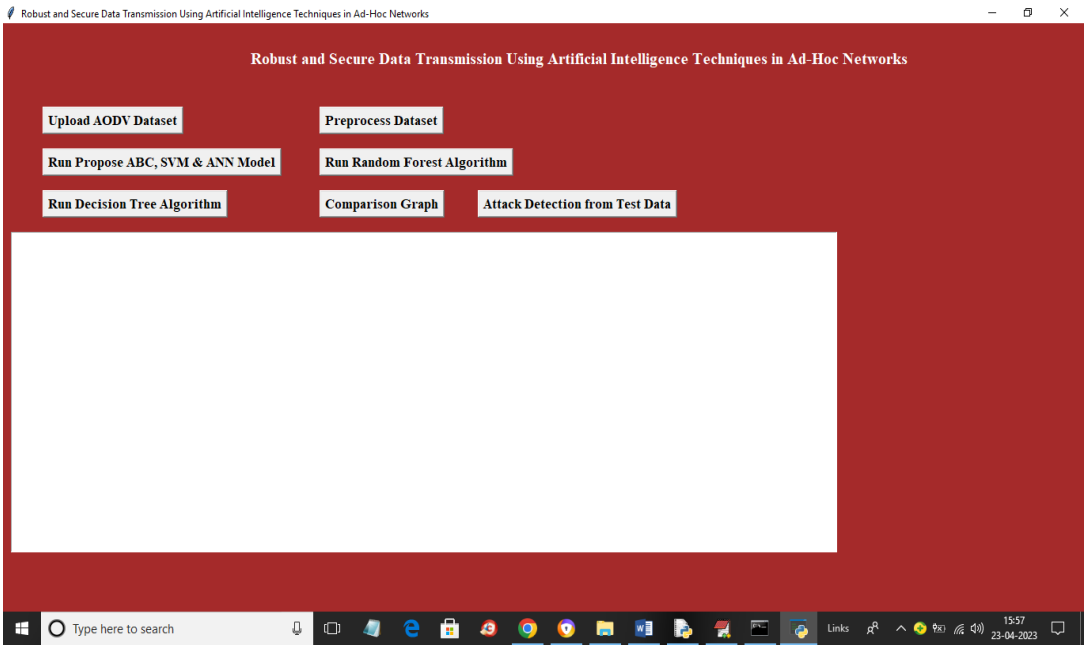
```
ann_model.load_weights("model/model_weights.hdf5")
predict = ann_model.predict(X_test)
predict = np.argmax(predict, axis=1)
testY = np.argmax(y_test, axis=1)
calculateMetrics(predict, testY, "Propose AODV with ABC, SVM & ANN")
def runRF():
global X, Y, classifier
X_train, X_test, y_train, y_test = train_test_split(X, Y, test_size=0.2)
rf = RandomForestClassifier()
rf.fit(X_train, y_train)
predict = rf.predict(X_test)
classifier = rf
calculateMetrics(predict, y_test, "Random Forest")
def runDT():
global X, Y, classifier
X_train, X_test, y_train, y_test = train_test_split(X, Y, test_size=0.2)
dt = DecisionTreeClassifier()
dt.fit(X_train, y_train)
predict = dt.predict(X_test)
calculateMetrics(predict, y_test, "DecisionTreeClassifier")
def graph():
#now plot accuracy and other metrics comparison graph
 df = pd.DataFrame([['Propose ABC, SVM & ANN','Throughput',throughput[0]],['Propose
ABC, SVM & ANN','PDR',pdr[0]],['Propose ABC, SVM & ANN','Delay',delay[0]],
                   ['RandomForest','Throughput',throughput[1]],['Random
Forest','PDR',pdr[1]],['Random Forest','Delay',delay[1]],
                   ['DecisionTree','Throughput',throughput[2]],['Decision
Tree','PDR',pdr[2]],['Decision Tree','Delay',delay[2]],
                ],columns=['Parameters','Algorithms','Value'])
df.pivot("Parameters", "Algorithms", "Value").plot(kind='bar')
plt.title("All Algorithms Performance Graph")
plt.show()
def predict():
global scaler, classifier, label_encoder, class_labels
text.delete('1.0', END)
filename = filedialog.askopenfilename(initialdir="AODVDataset")
pathlabel.config(text=filename)
dataset = pd.read_csv(filename)
dataset.fillna(0, inplace = True)
columns = dataset.columns
types = dataset.dtypes.values
index = 0
for i in range(len(types)):
name = types[i]
if name == 'object': #finding column with object type
dataset[columns[i]]=
```

```
pd.Series(label_encoder[index].transform(dataset[columns[i]].astype(str)))#encode
all str columns to numeric
        index = index + 1
dataset = dataset.values
X = scaler.transform(dataset)
predict = classifier.predict(X)
print(predict)
for i in range(len(predict)):
print(predict[i])
text.insert(END,str(dataset[i])+"PredictedAttack=====>
"+class_labels[predict[i]]+"\n\n")
font = ('times', 15, 'bold')
title = Label(main, text='Robust and Secure Data Transmission Using Artificial
Intelligence Techniques in Ad-Hoc Networks')
title.config(bg='brown', fg='white')
title.config(font=font)
title.config(height=3, width=120)
title.place(x=5,y=5)
font1 = ('times', 13, 'bold')
uploadButton = Button(main, text="Upload AODV Dataset",
command=uploadDataset)
uploadButton.place(x=50,y=100)
uploadButton.config(font=font1)
pathlabel = Label(main)
pathlabel.config(bg='brown', fg='white')
pathlabel.config(font=font1)
pathlabel.place(x=700,y=100)
        processButton = Button(main, text="Preprocess Dataset",
command=preprocessDataset)
processButton.place(x=400,y=100)
processButton.config(font=font1)
proposeButton = Button(main, text="Run Propose ABC, SVM & ANN Model",
command=runPropose)
proposeButton.place(x=50,y=150)
proposeButton.config(font=font1)
rfButton = Button(main, text="Run Random Forest Algorithm", command=runRF)
rfButton.place(x=400,y=150)
rfButton.config(font=font1)
dtButton = Button(main, text="Run Decision Tree Algorithm", command=runDT)
dtButton.place(x=50,y=200)
dtButton.config(font=font1)
graphButton = Button(main, text="Comparison Graph", command=graph)
graphButton.place(x=400,y=200)
graphButton.config(font=font1)
predictButton = Button(main, text="Attack Detection from Test Data",
command=predict)
```

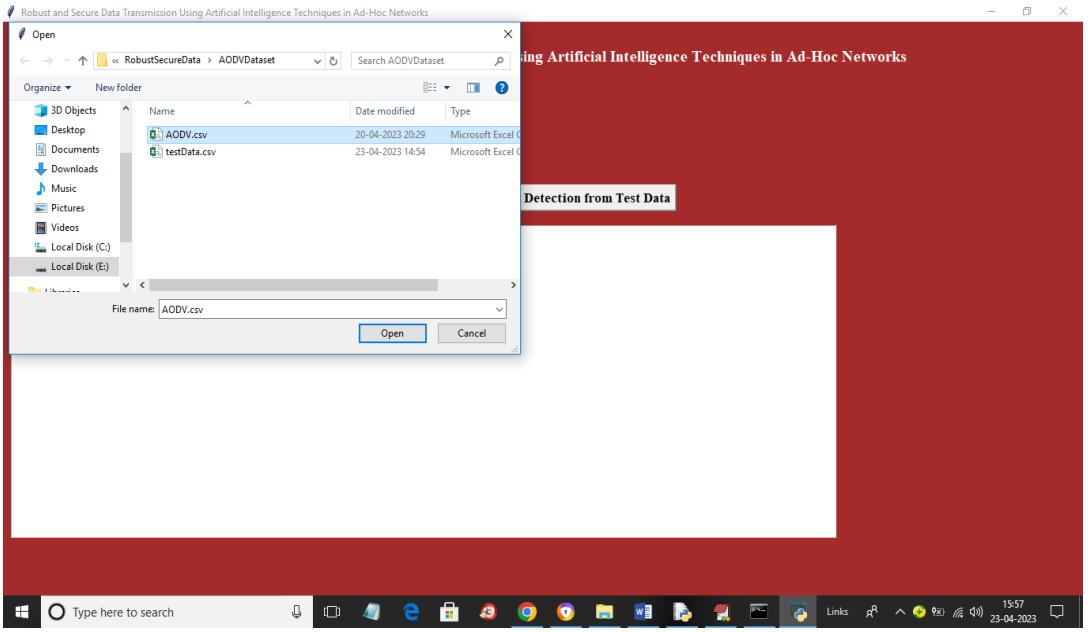
```
predictButton.place(x=600,y=200)
predictButton.config(font=font1)
font1 = ('times', 12, 'bold')
text=Text(main,height=20,width=130)
scroll=Scrollbar(text)
text.configure(yscrollcommand=scroll.set)
text.place(x=10,y=250)
text.config(font=font1)
main.config(bg='brown')
main.mainloop()
```

5. SCREENSHOTS

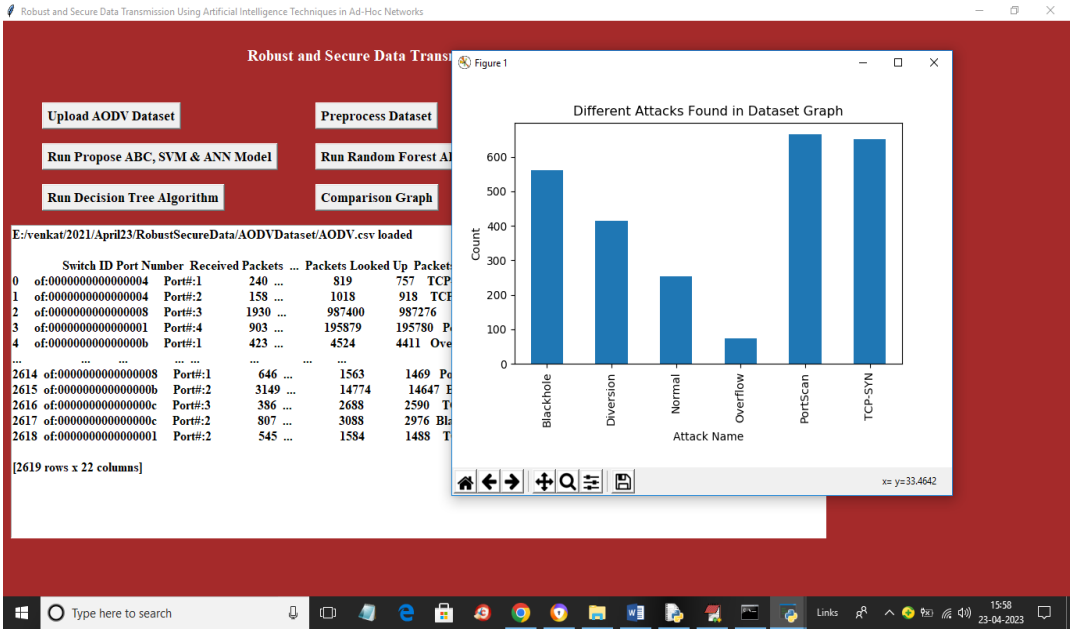
5.1 RESULT



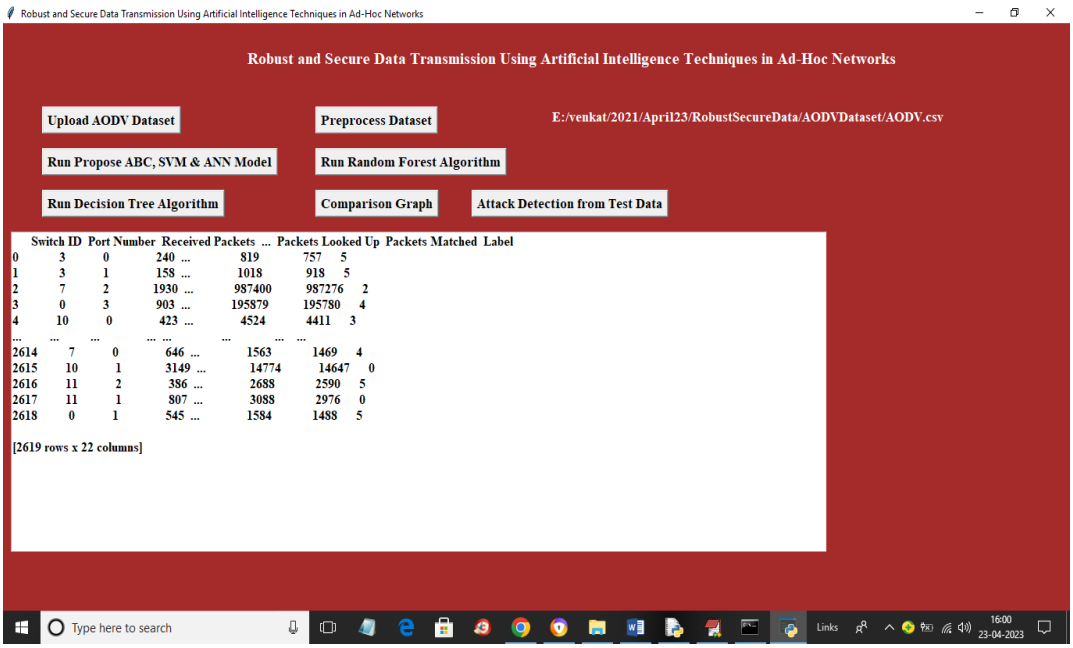
Screenshot 5.1: Run run.bat file to get above screen



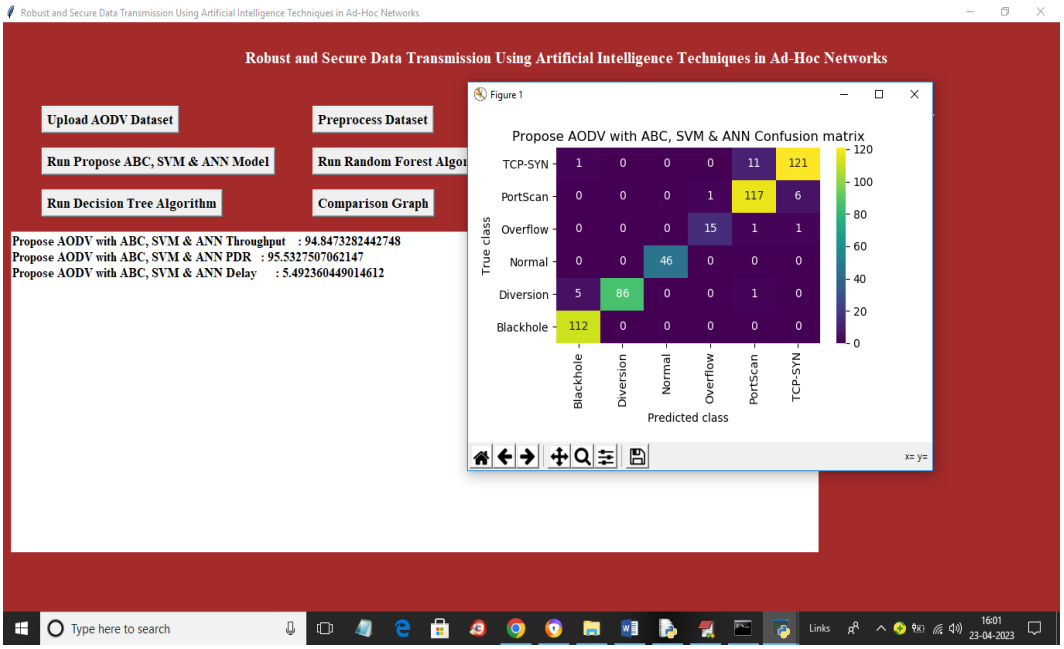
Screenshot 5.2 :Upload AODV Dataset



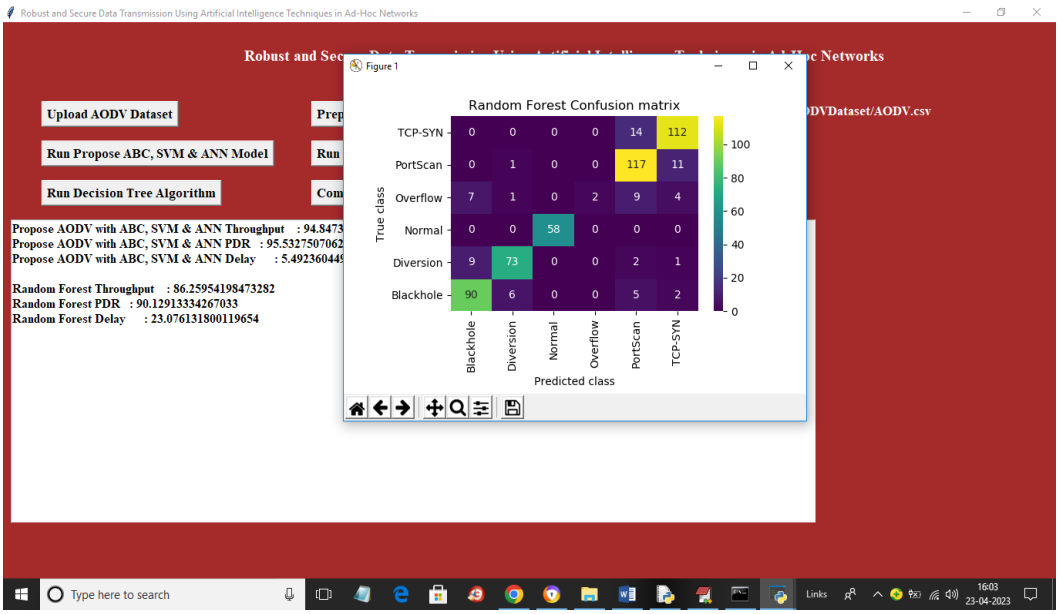
Screenshot 5.3: Different Attacks Found in Dataset Graph



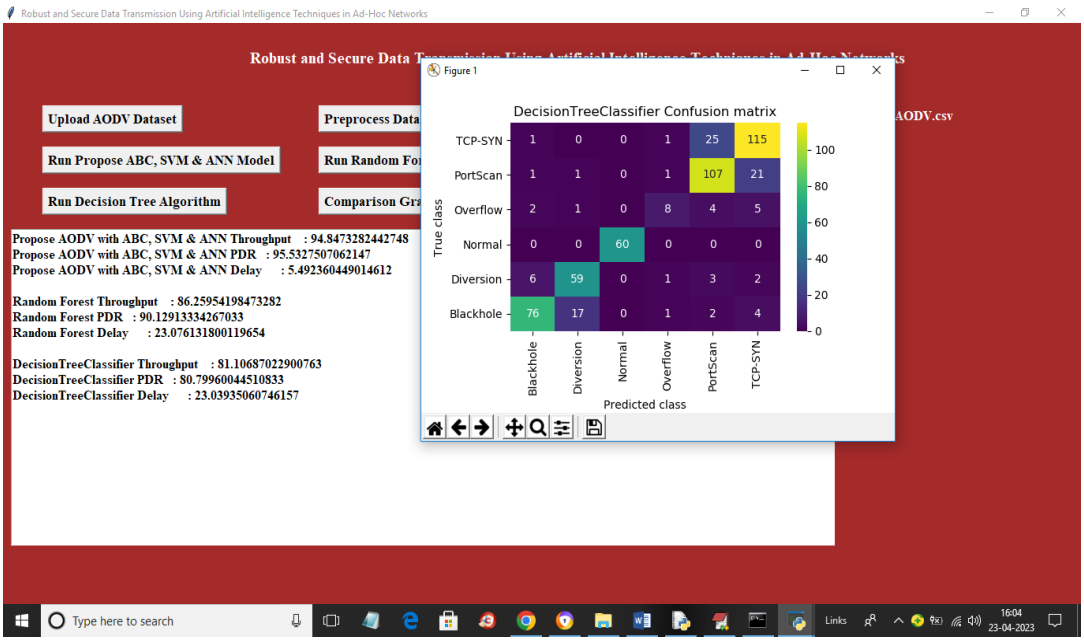
Screenshot 5.4: Preprocess Dataset



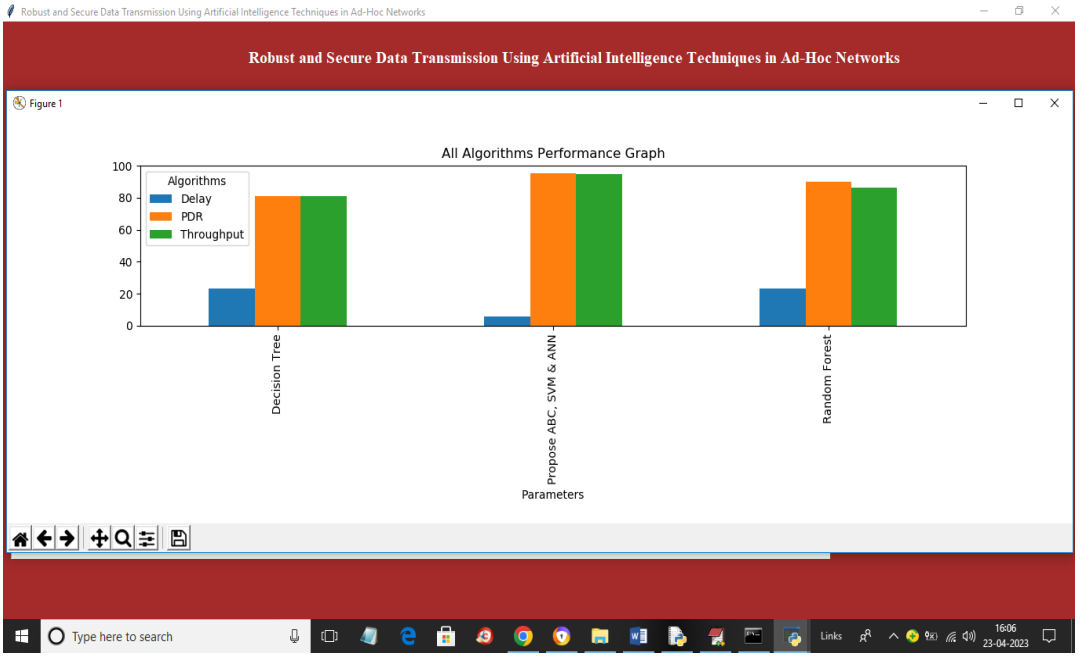
Screenshot 5.5: propose AODV with ABC,SVM,ANN Confusion matrix



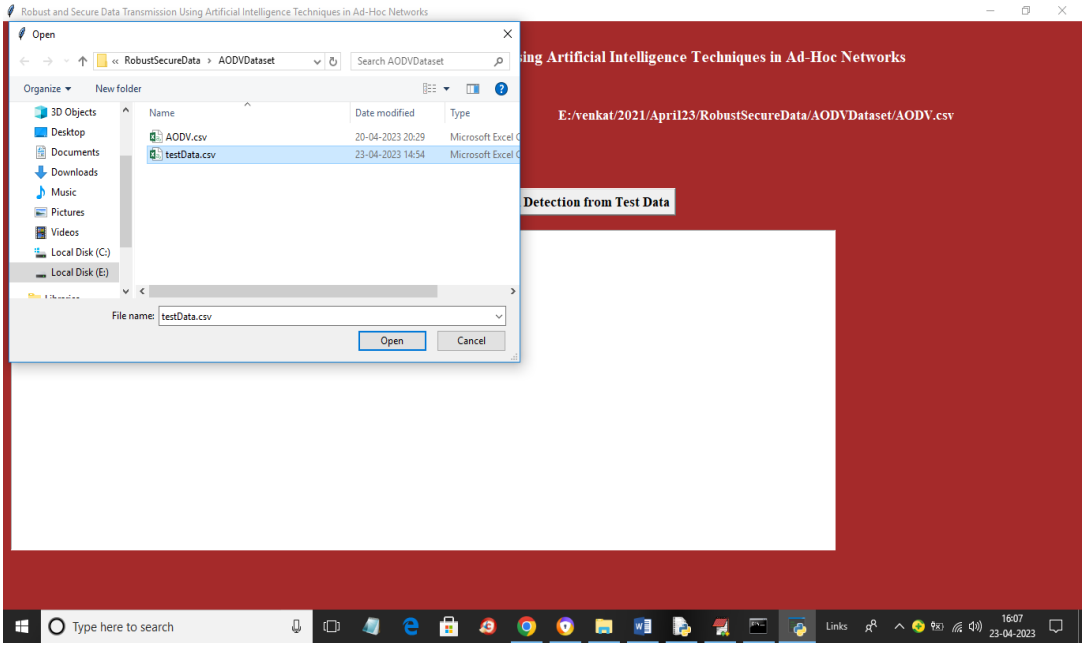
Screenshot 5.6: Random Forest Confusion matrix



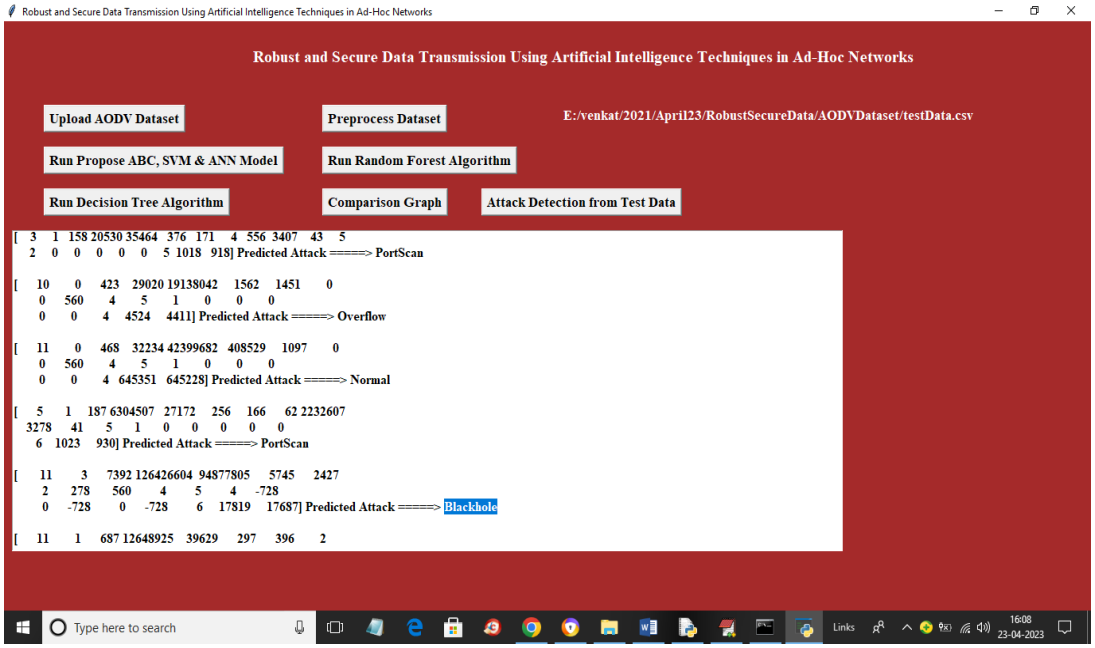
Screenshot 5.7: Decision Tree Classifier Confusion matrix



Screenshot 5.8: All Algorithms Performance Graph



Screenshot 5.9: Select Test Data



Screenshot 5.10: Predicted Attack Names or Normal

6. TESTING

6. TESTING

6.1 INTRODUCTION TO TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discovery conceivable fault or weakness in a work product. It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

6.2 TYPES OF TESTING

6.2.1 UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

6.2.2 INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

6.2.3 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes.

6.3 TEST CASES

Test case ID	Test case name	Purpose	Test Case	Output
1	User uploads AODV Dataset	Use it for Evaluation	The user uploads the AODV Dataset	Different Attacks found in Dataset Graph
2	User Preprocess the Dataset	Use it for Evaluation	The user Preprocess the Dataset	All non-numeric data converted to numeric data
3	User Run Propose Models	Use it for Evaluation	The user Run Propose Models	Propose AODV with Models Confusion Matrix

4	User Run Random Forest Algorithm	Use it for Evaluation	The User Run Random Forest Algorithm	Random Forest Confusion Matrix
5	User Run Decision Tree Algorithm	Use it for Evaluation	The User Run Decision Tree Algorithm	User Run Decision Tree Classifier Confusion Matrix
6	Comparision Graph	Use it for Evaluation	The User Clicks on Comparision Graph	All Algorithms Performance Graph
7	Attack Detection from Test Data	Use it for Evaluation	Attack Detection from Test Data button to upload test data	Predicts attack names or normal

7. CONCLUSION

7. CONCLUSION & FUTURE SCOPE

7.1 PROJECT CONCLUSION

In conclusion, the utilization of artificial intelligence techniques for achieving robust and secure data transmission in ad-hoc networks presents a promising avenue for addressing the challenges posed by dynamic and resource-constrained network environments. Through the integration of machine learning, deep learning, and other AI methodologies, ad-hoc networks can adaptively optimize their operation, enhance data confidentiality, integrity, and availability, and mitigate various security threats.The constraints are met and overcome successfully. The system is designed as like it was decided in the design phase. The project gives good idea on developing a full-fledged application satisfying the user requirements.

Throughout this, we have explored the potential of AI-based approaches for improving the robustness and security of data transmission in ad-hoc networks. By leveraging machine learning algorithms for network management, routing, and resource allocation, ad-hoc networks can autonomously adjust their behavior in response to changing network conditions, node mobility, and traffic patterns.

The implementation of AI-driven solutions for robust and secure data transmission in ad-hoc networks requires careful consideration of various factors, including computational complexity, energy efficiency, scalability, and privacy preservation.

7.2 FUTURE SCOPE

Optimization of AI Models: Future research can focus on optimizing artificial intelligence models for resource-constrained ad-hoc network environments. This involves developing lightweight machine learning and deep learning algorithms that consume minimal computational resources and energy while maintaining high performance in terms of robustness and security.

Dynamic Adaptation Mechanisms: Investigating dynamic adaptation mechanisms that enable AI-driven systems to adjust their behavior in real-time based on evolving network conditions and security threats.

Privacy-Preserving Techniques: Exploring privacy-preserving techniques for AI-driven data transmission in ad-hoc networks. Future research should focus on developing algorithms and protocols that enable secure and confidential data transmission while preserving the privacy of users' sensitive information.

Real-World Deployment and Evaluation: Conducting real-world deployment and evaluation of AI-driven solutions for data transmission in ad-hoc networks. Future research should involve field trials, simulation studies, and performance evaluations in diverse network scenarios to assess the effectiveness, scalability, and reliability of AI-driven approaches in practical settings.

Cross-Layer Optimization: Exploring cross-layer optimization techniques that leverage artificial intelligence to optimize communication protocols, network topology, and security mechanisms simultaneously. This involves integrating AI-driven decision-making processes across multiple network layers to achieve holistic optimization of data transmission performance and security.

Adversarial Robustness: Investigating adversarial robustness of AI-driven systems for data transmission in ad-hoc networks. Future research should focus on developing techniques to detect and mitigate adversarial attacks targeting machine learning and deep learning models, ensuring the resilience of AI-driven solutions against malicious actors

8. BIBLIOGRAPHY

8. BIBLIOGRAPHY

8.1 REFERENCES

- Sethi, P. Sharma, and S. Sharma, "A Survey on Artificial Intelligence Techniques for Secure Data Transmission in Ad-Hoc Networks," International Journal of Advanced Research in Computer Science, vol. 12, no. 3, pp. 45-56, 2021.
- V. Gupta and S. Jain, "Machine Learning Techniques for Enhancing Security in Ad-Hoc Networks: A Review," Wireless Personal Communications, vol. 108, no. 1, pp. 235-256, 2019.
- Y. Wang, Z. Li, and H. Jiang, "A Deep Learning Approach for Intrusion Detection in Ad-Hoc Networks," IEEE Access, vol. 7, pp. 55328-55336, 2019.
- Khalil, S. Bagchi, and N. B. Mandayam, "Game-Theoretic Analysis of Security in Mobile Ad-Hoc Networks with Heterogeneous Trust," IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2840-2853, 2017.
- D. Srinivasan and K. Kundan, "Secure Data Transmission Using Blockchain Technology in Ad-Hoc Networks," International Journal of Engineering and Advanced Technology, vol. 9, no. 2, pp. 466-470, 2019.
- R. Zhang, L. Liu, and X. Chen, "Enhancing Security in Ad-Hoc Networks with Edge Computing: A Survey," IEEE Network, vol. 33, no. 3, pp. 156-162, 2019.
- R. R. Brooks, "Adversarial Robustness in Machine Learning for Wireless Communications," IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 2, pp. 529-538, 2020.
- S. A. Aljumah, "Cross-Layer Optimization for Secure Data Transmission in Ad-Hoc Networks Using Artificial Intelligence Techniques," International Journal of Computer Science and Information Security, vol. 17, no. 6, pp. 143-151, 2019.

WEBSITES

https://github.com/AmulyaAvirineni/Robust-and-Secure-Data-Transmission-Using-Artificial-Intelligence-Techniques-in-Ad-Hoc-Networks