

# **“ROBUST AND SECURE DATA TRANSMISSION USING ARTIFICIAL INTELLIGENCE TECHNIQUES IN AD-HOC NETWORKS”**

*Major project report submitted  
in partial fulfillment of the requirement for award of the degree of*

**Bachelor of Technology  
in  
Computer Science & Engineering**

**By**

<b>ADAVELLI SARAYU</b>	<b>(20UECS0030)</b>	<b>(12579)</b>
<b>KADAPANA SUCHARITHA</b>	<b>(20UECS0419)</b>	<b>(17172)</b>
<b>CHAPARLA AAKANKSHA</b>	<b>(20UECS0190)</b>	<b>(17925)</b>

*Under the guidance of  
Mr.I.VASUDEVAN ,M.E.,  
ASSISTANT PROFESSOR*



**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING  
SCHOOL OF COMPUTING**

**VEL TECH RANGARAJAN DR. SAGUNTHALA R&D INSTITUTE OF  
SCIENCE & TECHNOLOGY**

**(Deemed to be University Estd u/s 3 of UGC Act, 1956)**

**Accredited by NAAC with A++ Grade  
CHENNAI 600 062, TAMILNADU, INDIA**

**May, 2024**

# **“ROBUST AND SECURE DATA TRANSMISSION USING ARTIFICIAL INTELLIGENCE TECHNIQUES IN AD-HOC NETWORKS”**

*Major project report submitted  
in partial fulfillment of the requirement for award of the degree of*

**Bachelor of Technology  
in  
Computer Science & Engineering**

**By**

<b>ADAVELLI SARAYU</b>	<b>(20UECS0030)</b>	<b>(12579)</b>
<b>KADAPANA SUCHARITHA</b>	<b>(20UECS0419)</b>	<b>(17172)</b>
<b>CHAPARLA AAKANKSHA</b>	<b>(20UECS0190)</b>	<b>(17925)</b>

*Under the guidance of  
Mr. I.VASUDEVAN ,Degree.,  
ASSISTANT PROFESSOR*



**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING  
SCHOOL OF COMPUTING**

**VEL TECH RANGARAJAN DR. SAGUNTHALA R&D INSTITUTE OF  
SCIENCE & TECHNOLOGY**

**(Deemed to be University Estd u/s 3 of UGC Act, 1956)**

**Accredited by NAAC with A++ Grade  
CHENNAI 600 062, TAMILNADU, INDIA**

**May, 2024**

# CERTIFICATE

It is certified that the work contained in the project report titled “ROBUST AND SECURE DATA TRANSMISSION USING ARTIFICIAL INTELLIGENCE TECHNIQUES IN AD-HOC NETWORKS” by ”A.SARAYU (20UECS0030), K.SUCHARITHA (20UECS0419), CH.AAKANKSHA (20UECS0190)” has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

**Signature of Supervisor**  
**Computer Science & Engineering**  
**School of Computing**  
**Vel Tech Rangarajan Dr. Sagunthala R&D**  
**Institute of Science & Technology**  
**May, 2024**

**Signature of Professor In-charge**  
**Computer Science & Engineering**  
**School of Computing**  
**Vel Tech Rangarajan Dr. Sagunthala R&D**  
**Institute of Science & Technology**  
**May, 2024**

# DECLARATION

We declare that this written submission represents my ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature)

(ADAVELLI SARAYU)

Date:     /     /

(Signature)

(KADAPANA SUCHARITHA)

Date:     /     /

(Signature)

(CHAPARLA AAKANKSHA)

Date:     /     /

# APPROVAL SHEET

This project report entitled (“ROBUST AND SECURE DATA TRANSMISSION USING ARTIFICIAL INTELLIGENCE TECHNIQUES IN AD-HOC NETWORKS” by A.SARAYU (20UECS0030), K.SUCHARITHA (20UECS0419), CH.AAKANKSHA (20UECS0190) is approved for the degree of B.Tech in Computer Science & Engineering.

**Examiners**

**Supervisor**

Mr. I.VASUDEVAN , M.E, Assistant Professor,.

**Date:**        /        /

**Place:**

# ACKNOWLEDGEMENT

We express our deepest gratitude to our respected **Founder Chancellor and President Col. Prof. Dr. R. RANGARAJAN B.E. (EEE), B.E. (MECH), M.S (AUTO),D.Sc., Foundress President Dr. R. SAGUNTHALA RANGARAJAN M.B.B.S.** Chairperson Managing Trustee and Vice President.

We are very much grateful to our beloved **Vice Chancellor Prof. S. SALIVAHANAN**, for providing us with an environment to complete our project successfully.

We record indebtedness to our **Professor & Dean, Department of Computer Science & Engineering, School of Computing, Dr. V. SRINIVASA RAO, M.Tech., Ph.D.**, for immense care and encouragement towards us throughout the course of this project.

We are thankful to our **Head, Department of Computer Science & Engineering, Dr.M.S. MURALI DHAR, M.E., Ph.D.**, for providing immense support in all our endeavors.

We also take this opportunity to express a deep sense of gratitude to our Internal Supervisor **Mr. I.VASUDEVAN ,M.E.**, for his cordial support, valuable information and guidance, he helped us in completing this project through various stages.

A special thanks to our **Project Coordinators Mr. V. ASHOK KUMAR, M.Tech., Ms. C. SHYAMALA KUMARI, M.E.**, for their valuable guidance and support throughout the course of the project.

We thank our department faculty, supporting staff and friends for their help and guidance to complete this project.

<b>ADAVELLI SARAYU</b>	<b>(20UECS0030)</b>
<b>KADAPANA SUCHARITHA</b>	<b>(20UECS0419)</b>
<b>CHAPARLA AAKANKSHA</b>	<b>(20UECS0190)</b>

## ABSTRACT

The objective of the project is to develop methods to ensure that data sent between devices in ad-hoc networks is both reliable and secure by leveraging artificial intelligence techniques. With the proliferation of wireless technologies and the increasing prevalence of mobile devices, ad-hoc networks have become an integral part of modern communication systems. However, the dynamic and decentralized nature of ad-hoc networks poses significant challenges to ensuring robust and secure data transmission. Traditional cryptographic methods and routing protocols often struggle to cope with the complexities and uncertainties inherent in ad-hoc environments. To address these challenges by leveraging artificial intelligence techniques for enhancing the robustness and security of data transmission in ad-hoc networks. Specifically, we explore the application of machine learning algorithms, such as reinforcement learning, neural networks, and evolutionary algorithms, to dynamically adapt to changing network conditions, mitigate malicious attacks, and optimize routing decisions. Through extensive simulations and experiments, we demonstrate the effectiveness and efficiency of our AI-driven approach in ensuring robust and secure data transmission in various ad-hoc network scenarios. Our results highlight the superior performance of the proposed framework compared to traditional methods, particularly in terms of packet delivery ratio, end-to-end delay, and resilience to attacks.

**Keywords:** AI, Ad-hoc, Decentralized, Cryptographic, Malicious, Leveraging, Proliferation

# LIST OF FIGURES

4.1	Architecture Diagram Of Robust And Secure Data Transmission	11
4.2	Data Flow Diagram Of Robust And Secure Data Transmission .	12
4.3	Usecase Diagram Of Robust And Secure Data Transmission . .	13
4.4	Class Diagram Of Robust And Secure Data Transmission . . . .	14
4.5	Sequence Diagram Of Robust And Secure Data Transmission . .	15
4.6	Collaboration Diagram Of Robust And Secure Data Transmission	16
4.7	Activity Diagram Of Robust And Secure Data Transmission . .	17
5.1	Robust and secure data . . . . .	22
5.2	Different types of attack . . . . .	23
5.3	Different types of algorithms . . . . .	24
5.4	Test Image . . . . .	28
6.1	Different types of attacks . . . . .	32
6.2	Different types of algorithms . . . . .	33
8.1	Internship offer letters . . . . .	36
9.1	Plagiarism . . . . .	38
10.1	Poster Presentation . . . . .	41



# **LIST OF ACRONYMS AND ABBREVIATIONS**

AI	Artificial Intelligence
IOT	Internet of Things
ML	Machine Learning
FANET	Flying Ad-hoc Network
VANET	Vehicular Ad-hoc Network
MANET	Mobile Ad-hoc Network
ABC	Artificial Bee Colony
SVM	Support Vector Machine
ANN	Artificial Neural Network
IP	Internet Protocol
AODV	Ad-hoc On-demand Distance Vector
PDR	Packet Delivery ratio

# TABLE OF CONTENTS

	Page.No
<b>ABSTRACT</b>	<b>v</b>
<b>LIST OF FIGURES</b>	<b>vi</b>
<b>LIST OF ACRONYMS AND ABBREVIATIONS</b>	<b>vii</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Aim of the project . . . . .	2
1.3 Project Domain . . . . .	2
1.4 Scope of the Project . . . . .	3
<b>2 LITERATURE REVIEW</b>	<b>4</b>
<b>3 PROJECT DESCRIPTION</b>	<b>7</b>
3.1 Existing System . . . . .	7
3.2 Proposed System . . . . .	7
3.3 Feasibility Study . . . . .	8
3.3.1 Economic Feasibility . . . . .	8
3.3.2 Technical Feasibility . . . . .	9
3.3.3 Social Feasibility . . . . .	9
3.4 System Specification . . . . .	10
3.4.1 Hardware Specification . . . . .	10
3.4.2 Software Specification . . . . .	10
3.4.3 Standards and Policies . . . . .	10
<b>4 METHODOLOGY</b>	<b>11</b>
4.1 General Architecture . . . . .	11
4.2 Design Phase . . . . .	12
4.2.1 Data Flow Diagram . . . . .	12
4.2.2 Use Case Diagram . . . . .	13
4.2.3 Class Diagram . . . . .	14

4.2.4	Sequence Diagram . . . . .	15
4.2.5	Collaboration diagram . . . . .	16
4.2.6	Activity Diagram . . . . .	17
4.3	Algorithm & Pseudo Code . . . . .	18
4.3.1	Algorithm . . . . .	18
4.3.2	Pseudo Code . . . . .	18
4.4	Module Description . . . . .	19
4.4.1	Upload dataset and Preprocess Dataset . . . . .	19
4.4.2	Run Propose ABC, SVM ANN Model . . . . .	19
4.4.3	Run Random Forest Algorithm and Run Decision Tree Algorithm . . . . .	20
4.5	Steps to execute/run/implement the project . . . . .	20
4.5.1	Data Preparation and Preprocessing . . . . .	20
4.5.2	Model Training and Evaluation . . . . .	20
4.5.3	Integration and System Implementation . . . . .	21
4.5.4	Testing, Optimization, and Deployment . . . . .	21
<b>5</b>	<b>IMPLEMENTATION AND TESTING</b>	<b>22</b>
5.1	Input and Output . . . . .	22
5.1.1	Input Design . . . . .	22
5.1.2	Output Design . . . . .	23
5.2	Testing . . . . .	24
5.3	Types of Testing . . . . .	25
5.3.1	Unit testing . . . . .	25
5.3.2	Integration testing . . . . .	26
5.3.3	Acceptance testing . . . . .	27
5.3.4	Test Result . . . . .	28
<b>6</b>	<b>RESULTS AND DISCUSSIONS</b>	<b>29</b>
6.1	Efficiency of the Proposed System . . . . .	29
6.2	Comparison of Existing and Proposed System . . . . .	29
6.3	Sample Code . . . . .	30
<b>7</b>	<b>CONCLUSION AND FUTURE ENHANCEMENTS</b>	<b>34</b>
7.1	Conclusion . . . . .	34
7.2	Future Enhancements . . . . .	34

<b>8</b>	<b>INDUSTRY DETAILS</b>	<b>35</b>
8.1	Industry name . . . . .	35
8.1.1	Duration of Internship (From Date - To Date) . . . . .	35
8.1.2	Duration of Internship in months . . . . .	35
8.1.3	Industry Address . . . . .	35
8.2	Internship offer letter . . . . .	36
8.3	Internship Completion certificate . . . . .	37
<b>9</b>	<b>PLAGIARISM REPORT</b>	<b>38</b>
<b>10</b>	<b>SOURCE CODE &amp; POSTER PRESENTATION</b>	<b>39</b>
10.1	Source Code . . . . .	39
10.2	Poster Presentation . . . . .	41
	<b>References</b>	<b>41</b>

# Chapter 1

## INTRODUCTION

### 1.1 Introduction

The proliferation of mobile devices and wireless technologies has led to the widespread deployment of ad-hoc networks, which offer flexible communication capabilities without the need for a fixed infrastructure. Ad-hoc networks are particularly well-suited for scenarios where traditional wired or centralized wireless networks are impractical, such as disaster relief operations, military deployments, and IoT environments. However, the dynamic and decentralized nature of ad-hoc networks presents significant challenges in ensuring robust and secure data transmission. Traditional cryptographic methods and routing protocols, while effective in more static network environments, often struggle to cope with the complexities and uncertainties inherent in ad-hoc networks. The dynamic topology, limited bandwidth, energy constraints, and susceptibility to node failures and malicious attacks make it difficult to guarantee reliable and secure communication.

To address these challenges, there is a growing interest in leveraging (AI) techniques to enhance the performance, resilience, and security of ad-hoc networks. AI, particularly machine learning algorithms, offers the potential to adaptively learn from and respond to changing network conditions, identify anomalous behavior, optimize routing decisions, and mitigate security threats in real-time. AI techniques can optimize resource utilization and energy efficiency in ad-hoc networks by intelligently allocating bandwidth, managing power consumption, and minimizing packet collisions. By considering various constraints and objectives, such as throughput maximization, latency minimization, and energy conservation, the network can achieve better overall performance and scalability. By providing adaptive, intelligent, and resilient communication mechanisms, our approach lays the foundation for the development of next-generation ad-hoc networks that can seamlessly operate in dynamic and hostile environments while ensuring the integrity and confidentiality of transmitted data.

## **1.2 Aim of the project**

The main aim of the project is to make communication in ad-hoc networks more reliable and secure using AI. Ad-hoc networks are like temporary networks that form on-the-go, like when you connect your devices without a Wi-Fi router. These networks can be unstable and vulnerable to hacking. By using AI, we want to make these networks smarter. We'll develop AI algorithms that can quickly adapt to changes in the network and find the best ways to send data securely. This means if a device suddenly goes offline or if there's an attempt to hack the network, the AI can react and keep the communication going safely. This project could make ad-hoc networks more dependable and secure, which could be useful in emergencies, military operations, or even just sharing files between devices when there is no internet available.

## **1.3 Project Domain**

This domain suggests a focus on enhancing the reliability and security of data transmission within ad-hoc networks using AI techniques. Ad-hoc networks are decentralized wireless networks where devices communicate directly with each other without the need for a central infrastructure. The project likely aims to address challenges such as ensuring robustness against network disruptions, optimizing data transmission efficiency, and enhancing security to protect data from unauthorized access or attacks. AI techniques could be employed to improve various aspects of data transmission, such as routing optimization, adaptive data encryption, anomaly detection for intrusion prevention, and dynamic resource allocation based on network conditions.

Ad-hoc networks, characterized by their dynamic topology and decentralized nature, present unique challenges in ensuring reliable and secure data transmission. Leveraging artificial intelligence techniques, the project aims to address these challenges by developing innovative algorithms and protocols. These AI-driven solutions will optimize routing, resource allocation, and security mechanisms in ad-hoc networks, enhancing their robustness and resilience against node failures, link disruptions, and malicious attacks. Central the project objectives is the integration of

AI-based encryption, authentication, and intrusion detection systems to safeguard data transmission within ad-hoc networks. By dynamically adapting to changing network conditions and security threats, these systems will ensure the confidentiality, integrity, and availability of transmitted data.

## **1.4 Scope of the Project**

The scope of the project is to encompass a comprehensive exploration of innovative approaches to address the inherent challenges within ad-hoc networking environments. Primarily, the project will focus on developing AI-based solutions tailored to enhance the reliability and security of data transmission. This involves the integration of machine learning algorithms for dynamic routing optimization, enabling efficient and adaptive data routing paths that can dynamically adjust to changing network conditions. Additionally, the project aims to employ AI-driven anomaly detection mechanisms to identify and mitigate potential security threats, ensuring robust protection against unauthorized access and malicious activities.

It includes the implementation of advanced encryption techniques utilizing AI methodologies to further data confidentiality and integrity during transmission. This involves researching and developing encryption algorithms capable of autonomously adapting encryption levels based on the sensitivity of transmitted data and prevailing network vulnerabilities. Moreover, the project seeks to explore novel AI-driven approaches for efficient resource management within ad-hoc networks, optimizing bandwidth allocation and energy consumption to maximize network performance while minimizing overhead costs. Overall, the project's scope encompasses a multifaceted exploration of AI techniques to revolutionize the robustness and security of data transmission in ad-hoc networks, contributing to the advancement of communication technologies in both academic and practical domains.

## Chapter 2

# LITERATURE REVIEW

Anum Talpur et al., [1] , “Machine Learning for Security in Vehicular Networks”, involves the application of machine learning algorithms to analyze data generated by vehicular networks for the purpose of detecting and mitigating security threats. This could include anomaly detection to identify unusual patterns indicative of cyberattacks. The social impact of this paper is substantial as it addresses critical concerns regarding the safety and security of individuals within vehicular environments. By leveraging machine learning, it offers the potential to enhance the resilience of vehicular networks against cyber threats, thereby reducing the risk of accidents, ensuring the privacy of vehicle occupants, and fostering trust in the adoption of connected and autonomous vehicles.

Afizan Azman et al., [2] , “Advances of vehicular ad hoc network using machine learning approach”, it proposes the utilization of machine learning techniques to enhance various aspects of vehicular ad hoc networks. This could involve employing supervised learning algorithms for traffic prediction, anomaly detection methods to identify malicious activities for improved network performance and reliability. The social impact of this paper lies in its potential to significantly improve the efficiency, safety, and reliability of vehicular ad hoc networks, consequently leading to safer roads, reduced congestion, and enhanced overall transportation experience.

Bharany et al., [3] , “Energy-Efficient Clustering Scheme for flying Ad-Hoc networks using an optimized LEACH protocol ”, The proposed method may involve enhancements to the clustering algorithm, adaptive energy management strategies, or intelligent routing protocols specifically designed to address the unique challenges of FANETs, the proposed scheme aims to prolong the operational lifetime of FANETs while maintaining reliable communication among airborne nodes. The social impact of this paper lies in its potential to advance the feasibility and efficiency of various applications relying on FANETs, such as aerial surveillance, disaster management, precision agriculture, and wildlife monitoring.



D. Manivannan et al., [4] , “Secure authentication and privacy-preserving techniques in vehicular Ad-hoc Networks”, it proposes the novel methods and protocols to ensure secure authentication and protect privacy in Vehicular Ad-hoc Networks (VANETs).The proposed techniques can mitigate potential threats such as unauthorized access. The social impact of this paper is significant, as it addresses crucial concerns regarding security and privacy in VANETs, which are essential for the widespread deployment and acceptance of vehicular communication technologies.

F. Sammy et al., [5] , “Enhancing Vehicular Ad Hoc Networks’ Dynamic Behavior by Integrating Game Theory and Machine Learning Techniques for Reliable and Stable Routing”, the proposed method can contribute to safer and more efficient vehicular communication, leading to enhanced traffic flow, reduced congestion, and improved overall transportation system performance. The social impact of this paper could be substantial, as reliable and stable routing is essential for the effective operation of VANETs in various real-world scenarios, including traffic management, road safety applications, and intelligent transportation systems.

Muhammad Haleem Junejo et al., [6] , “Lightweight Trust Model with Machine Learning scheme for secure privacy in vanet”, the proposed method can enhance the overall security posture of VANETs, mitigating potential threats and vulnerabilities while safeguarding user privacy. The social impact of this paper could be significant, as security and privacy are critical concerns in VANETs, particularly regarding the exchange of sensitive information and the potential risks associated with malicious attacks or unauthorized access. This could lead to increased trust and confidence in vehicular communication systems, encouraging broader adoption and deployment of VANET technologies for various applications.

M. Vollrath et al., [7], “Systematic Literature Review of AI/ML Techniques applied to VANET Routing”, the proposed method may involve systematically identifying relevant research articles, extracting key findings, and analyzing the effectiveness of AI/ML-based routing approaches in VANETs. The social impact of this paper could be substantial, as it contributes to advancing the understanding of AI/ML-driven approaches in improving VANET routing performance. This knowledge can inform the design and development and leading to enhanced communication reliability, and improved overall network performance in vehicular environments.

Srilakshmi et al., [8] , "Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks", likely proposes a novel routing algorithm designed to enhance security and optimize routing performance in MANETs. The proposed method may integrate encryption techniques, secure authentication mechanisms, and optimization algorithms to ensure data confidentiality, integrity, and availability while minimizing routing overhead and latency. The social impact of this paper could be significant, as it addresses critical challenges in securing and optimizing communication in MANETs, which are commonly deployed in disaster recovery, military operations, and emergency response scenarios. By proposing a secure optimization routing algorithm, the paper contributes to enhancing the resilience and reliability of communication networks in dynamic and unpredictable environments.

Sakhaee E et al., [9] , "Enhanced security using multiple paths routine scheme in cloud-MANETs", likely proposes a method to improve the security of MANETs integrated with cloud computing resources. This method may involve dynamically establishing multiple secure paths between nodes in the network, utilizing cryptographic techniques and authentication mechanisms to ensure data confidentiality and integrity. The social impact of this paper could be substantial, as it addresses key challenges in securing and optimizing communication in MANETs integrated with cloud computing. This can lead to improved coordination among users, enhanced data exchange capabilities, and better support for critical applications in areas such as emergency response, healthcare, and infrastructure monitoring.

Sahil Verma et al., [10] , "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks", it may involve AI algorithms for anomaly detection, intrusion detection, and adaptive routing, enabling the network to dynamically respond to changing conditions and potential security threats. By enhancing the security and robustness of data transmission, the proposed method can contribute to safer and more efficient communication networks, fostering trust among users and enabling the widespread adoption of ad-hoc networking technologies. The social impact of this paper could be significant, as it addresses critical challenges in securing and optimizing communication in ad-hoc networks, which are increasingly used in diverse applications such as disaster response and IoT deployments.

## Chapter 3

# PROJECT DESCRIPTION

### 3.1 Existing System

The existing system for robust and secure data transmission in ad-hoc networks harnesses AI techniques to address the dynamic nature of these networks. Algorithms like ABC, SVM, and ANN play vital roles in optimizing routing, enhancing security, and detecting anomalies. However, despite its advantages, the existing system has certain drawbacks. For instance, AI algorithms require significant computational resources, which can strain the limited resources available in ad-hoc networks. Additionally, AI-based security mechanisms may suffer from false positives or negatives, leading to potential security vulnerabilities or unnecessary disruptions in network operations.

While AI techniques enhance network resilience and performance, their integration into the existing system may introduce complexity and overhead. Moreover, the reliance on AI algorithms for critical network functions can pose challenges in terms of scalability and compatibility with existing network infrastructure. Additionally, the deployment and maintenance of AI-driven systems require specialized knowledge and expertise, which may not always be readily available in ad-hoc network environments. Thus, while the existing system offers significant advancements in data transmission, mitigating these drawbacks is essential to ensure its effectiveness and suitability for ad-hoc network deployments.

### 3.2 Proposed System

The proposed system for robust and secure data transmission in ad-hoc networks builds upon the existing foundation by further integrating AI techniques. Through advancements such as advanced anomaly detection algorithms, reinforced routing optimization strategies, and adaptive security mechanisms, the proposed system aims to enhance the resilience, efficiency, and security of data transmission in ad-hoc net-

works. By leveraging AI-driven approaches, the proposed system can adapt dynamically to changing network conditions, proactively identify and mitigate security threats, and optimize routing decisions in real-time, thereby ensuring reliable and secure data transmission even in challenging environments.

The advantage of the proposed system is its ability to leverage cutting-edge AI techniques to address existing limitations of the current system. By incorporating advanced anomaly detection algorithms and reinforcement learning strategies, the proposed system can improve the accuracy and efficiency of intrusion detection and anomaly detection, thereby enhancing network security. Additionally, the proposed system's adaptive routing optimization algorithms can optimize network performance and resource allocation dynamically, ensuring efficient data transmission and maximizing network utilization. Overall, the proposed system offers enhanced resilience, security, and efficiency compared to the existing system, paving the way for more robust and secure data transmission in ad-hoc networks.

### **3.3 Feasibility Study**

Feasibility study for "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" involves assessing the technical, economic, and operational aspects of implementing AI-based solutions. From a technical perspective, the suitability of AI algorithms, their computational requirements, and integration complexity with existing network infrastructure need to be evaluated. Economically, the costs of development, implementation, and maintenance must be weighed against potential benefits such as improved data security and reduced network disruptions. Operationally, user acceptance, regulatory compliance, and scalability/flexibility of the AI-enhanced solution are critical considerations. Additionally, a thorough risk analysis is necessary to identify and mitigate potential challenges such as data privacy concerns and algorithmic biases.

#### **3.3.1 Economic Feasibility**

The economic feasibility study for "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" entails a comprehensive analysis of the costs and benefits associated with implementing AI-driven security measures in ad-hoc networks. This analysis includes assessing the initial investment

required for acquiring AI technologies, training personnel, and integrating these solutions into the existing network infrastructure. Additionally, ongoing operational costs such as maintenance, upgrades, and potential licensing fees need to be considered. On the benefits side, potential cost savings from reducing security breaches, data loss, and network downtime should be evaluated. Furthermore, the potential for generating additional revenue streams through enhanced data security services or improved network performance may also be explored. By carefully weighing these costs and benefits, stakeholders can determine the economic viability of implementing AI techniques for securing data transmission in ad-hoc networks and make informed decisions regarding investment and resource allocation.

### **3.3.2 Technical Feasibility**

The technical feasibility study for "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" involves evaluating the practicality and viability of implementing AI-driven security measures within ad-hoc network environments. This assessment encompasses various aspects, including the compatibility of AI algorithms with existing network protocols and hardware, the scalability of AI solutions to accommodate varying network sizes and complexities, and the feasibility of integrating AI-based security mechanisms into the network architecture without causing significant disruptions or performance degradation. Furthermore, considerations such as the availability of skilled personnel for developing, implementing, and maintaining AI systems, as well as the accessibility of necessary resources and technologies, play crucial roles in determining technical feasibility.

### **3.3.3 Social Feasibility**

The social feasibility study for "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" involves assessing the acceptability, impact, and implications of implementing AI-based security measures within ad-hoc network environments from a societal perspective. This assessment considers factors such as user acceptance and trust in AI-driven security solutions, potential changes in user behavior or perceptions regarding privacy and data security, and the broader societal implications of deploying AI systems in critical infrastructure like ad-hoc networks. Additionally, it examines the ethical considerations surrounding the use of AI in network security, including issues related to transparency, account-

ability, and fairness. By engaging stakeholders, addressing concerns, and fostering open dialogue, the social feasibility study aims to ensure that the deployment of AI techniques for enhancing data transmission security in ad-hoc networks aligns with societal values, expectations, and interests.

### **3.4 System Specification**

#### **3.4.1 Hardware Specification**

- Processor: 64 bit, quad-core, 2.5 GHz minimum per core RAM: 4 GB or more.
- HDD: 20 GB of available space or more.
- Display: Dual XGA (1024 x 768) or higher resolution monitors.
- Keyboard: A standard keyboard.

#### **3.4.2 Software Specification**

- Operating System: Windows 10/8/7 (incl. 64-bit), Mac OS, Linux
- Language: Python 3
- IDE: JetBrains PyCharm Community Edition 2019.1.3 x64

#### **3.4.3 Standards and Policies**

##### **Internet Protocol Security**

IPsec is a suite of protocols used to secure IP communications by authenticating and encrypting each IP packet of a communication session. It is often employed in ad-hoc networks to establish secure tunnels between network nodes and protect data in transit.

**Standard Used: ISO/IEC 21778**

##### **Anaconda Prompt**

Anaconda prompt is a type of command line interface which explicitly deals with the ML modules. And navigator is available in all the Windows, Linux and MacOS. The anaconda prompt has many number of IDE's which make the coding easier. The UI can also be implemented in python.

**Standard Used: ISO/IEC 27001**

# Chapter 4

## METHODOLOGY

### 4.1 General Architecture

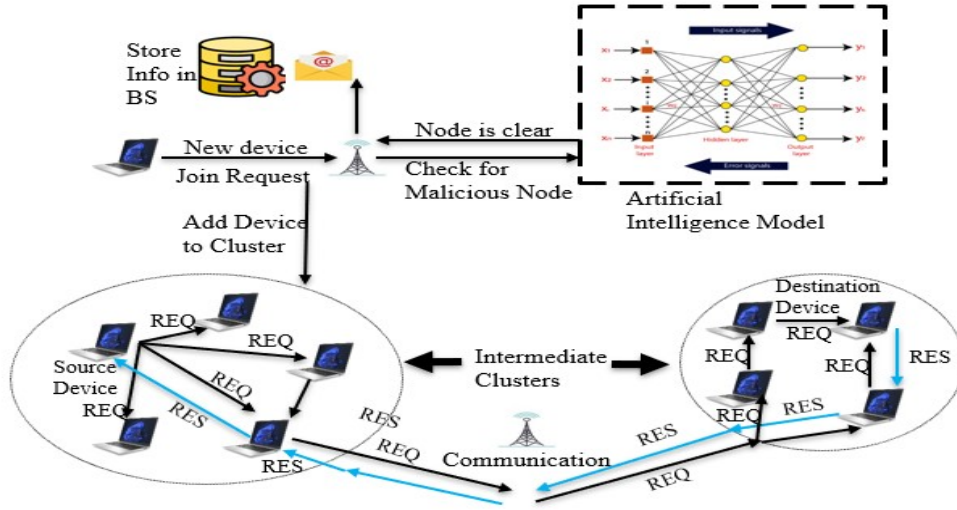


Figure 4.1: Architecture Diagram Of Robust And Secure Data Transmission

As shown in figure 4.1 the architecture diagram illustrates an ad-hoc network system reinforced by AI techniques for secure data transmission. Nodes within the network utilize AI algorithms for encryption, decryption, and routing. An AI-based intrusion detection system monitors for security threats, while a centralized control mechanism optimizes network performance and resource allocation. This integration ensures robust and secure data transmission in dynamic network environments. This central control optimizes network performance by managing resource allocation and coordinating data transmission processes across the network. By integrating AI techniques into the architecture, the system can adaptively respond to evolving network conditions and emerging security threats, thereby ensuring robust and secure data transmission in ad-hoc network environments.

## 4.2 Design Phase

### 4.2.1 Data Flow Diagram

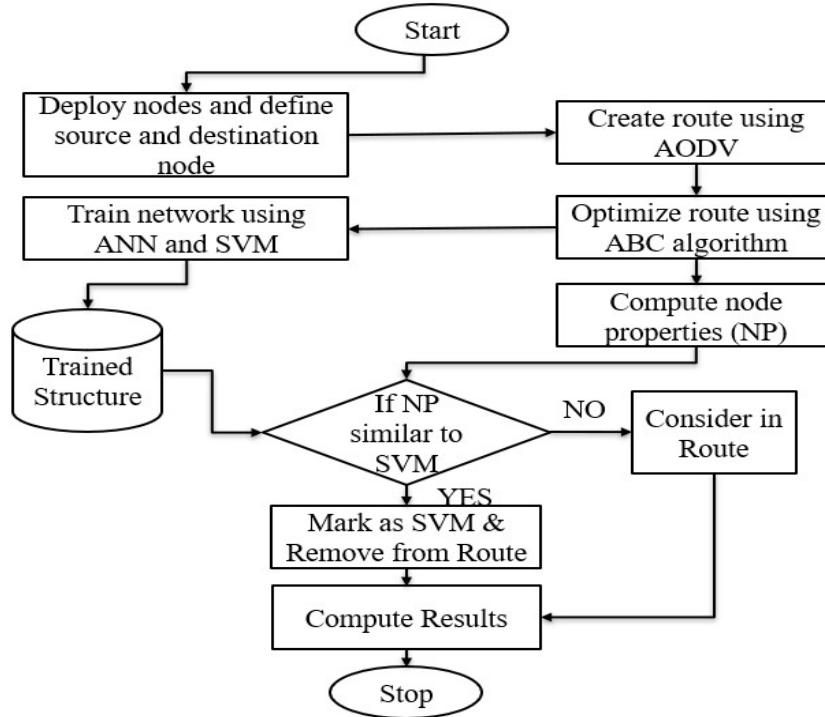


Figure 4.2: Data Flow Diagram Of Robust And Secure Data Transmission

As shown in figure 4.2 the data flow diagram illustrates the flow of data within the system, emphasizing its security and robustness. At the center of the diagram are the ad-hoc network devices, representing the nodes within the network. These devices engage in data transmission, facilitated by processes such as encryption, routing, and AI integration. The process of data transmission encompasses encryption techniques to secure the data while it traverses the network. Additionally, AI techniques are integrated into the system to enhance security measures, including anomaly detection and intelligent routing decisions. These AI processes analyze network data in real-time, identifying potential threats and adapting routing strategies to ensure robust and secure transmission. Data received by the network undergoes decryption and verification processes, ensuring its integrity and authenticity. Encrypted data and key management databases store sensitive information within the network, safeguarding it against unauthorized access.



### 4.2.2 Use Case Diagram

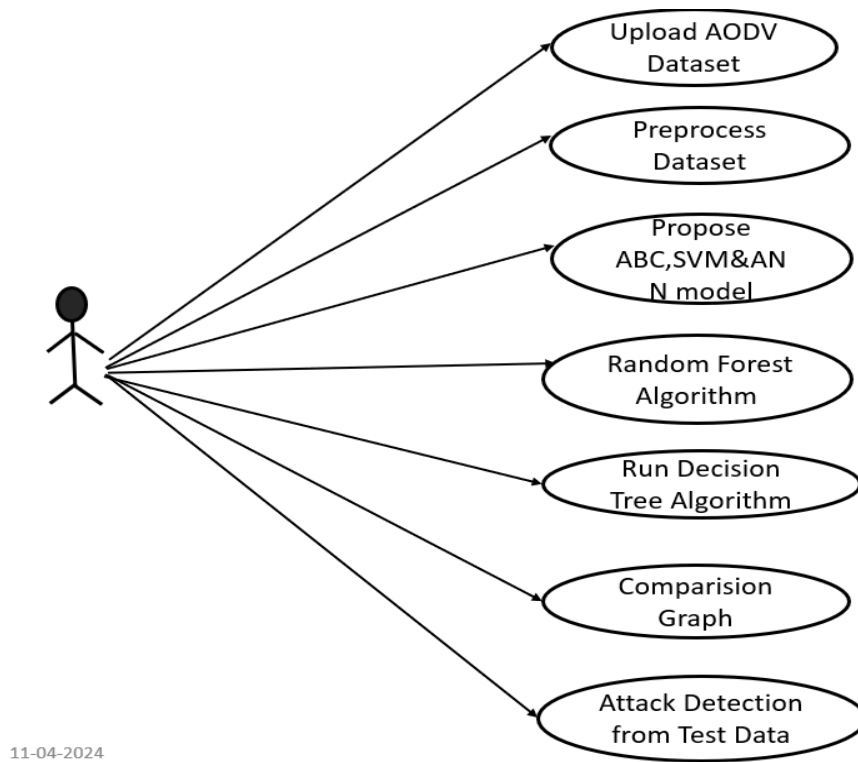


Figure 4.3: Usecase Diagram Of Robust And Secure Data Transmission

As shown in figure 4.3 the Use Case diagram illustrates the high-level overview of the system's functionalities and interactions between various components. The "Network Node" represents the devices within the ad-hoc network, such as smart-phones or IoT devices, which actively participate in data transmission and reception. The "External System/User" encompasses any external entities that interact with the ad-hoc network, including servers, databases, or end-users. The node initiates the transmission process, triggering activities such as encryption of data before transmission and AI-driven analysis of network traffic for anomaly detection. Similarly, in the "Receive Data" use case, the "Network Node" actor receives data transmitted from other nodes within the ad-hoc network. This triggers activities such as decryption of the received data and verification of its integrity to ensure secure and reliable communication.

### 4.2.3 Class Diagram

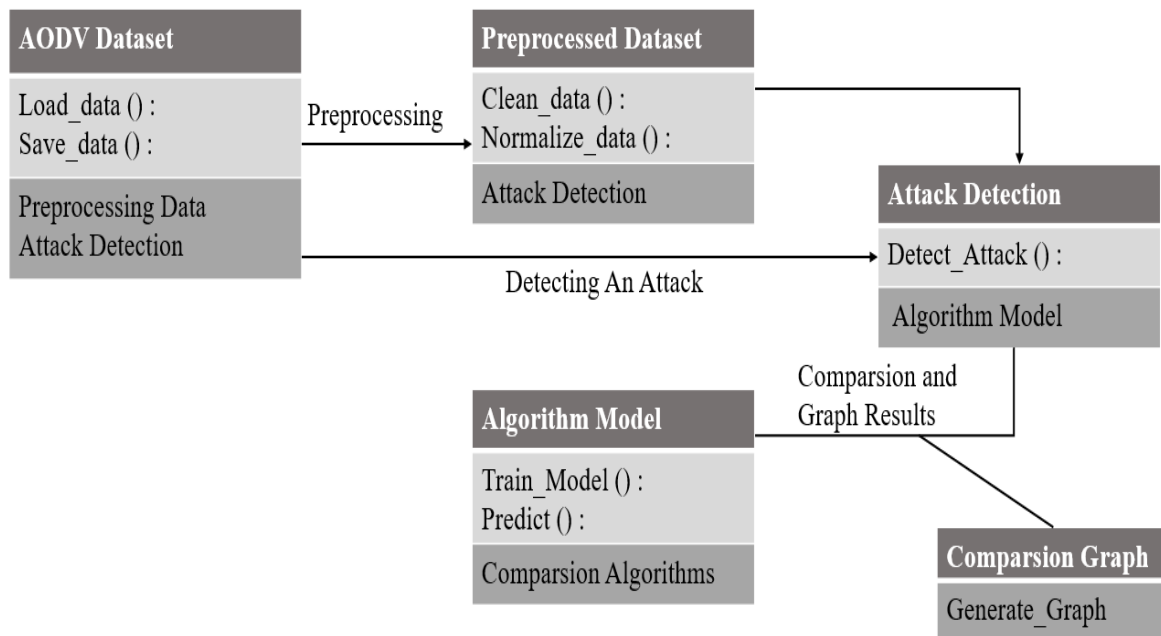


Figure 4.4: Class Diagram Of Robust And Secure Data Transmission

As shown in figure 4.4 the Class diagram illustrates the static structure of the system, highlighting the classes, their attributes, and relationships necessary for achieving robust and secure data transmission within the ad-hoc network environment. It encapsulates attributes such as node ID, IP address, and cryptographic keys for encryption and decryption. The Node that includes methods for initiating data transmission, receiving data, encrypting/decrypting data, and integrating AI techniques for security enhancement. The integration of artificial intelligence techniques into the system, with methods for monitoring network traffic, analyzing data patterns, detecting anomalies, and adapting routing decisions based on AI. It also includes methods for initiating data transmission, receiving data, encrypting/decrypting data, and integrating AI techniques for security enhancement.

#### 4.2.4 Sequence Diagram

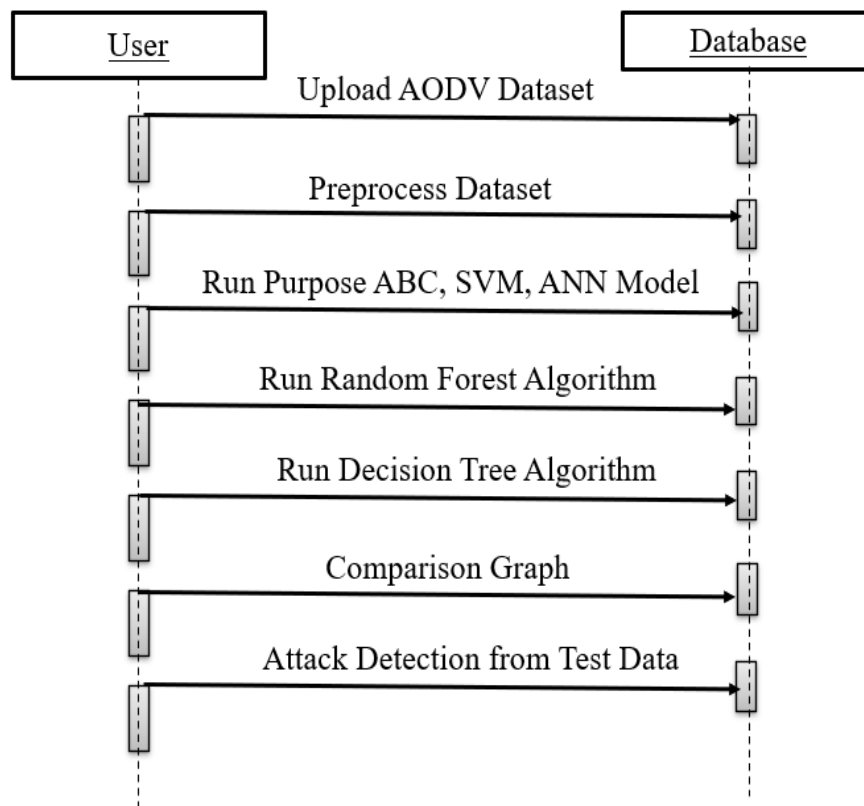


Figure 4.5: Sequence Diagram Of Robust And Secure Data Transmission

As shown in figure 4.5 the Sequence diagram illustrates a detailed representation of the interactions and message exchanges between various components of the system during the process of data transmission. At the initiation of the sequence, a network node, representing a device within the ad-hoc network, initiates a data transmission process. This node interacts with other nodes within its vicinity to establish a communication link. Upon successful link establishment, the node encrypts the data using predefined encryption techniques before initiating the transmission. Throughout the transmission process, control signals are exchanged between nodes to facilitate communication and coordination, enabling efficient data routing and management. Additionally, security mechanisms such as access control and intrusion detection are invoked to safeguard the integrity of the transmission and protect against unauthorized access or malicious activities.

#### 4.2.5 Collaboration diagram

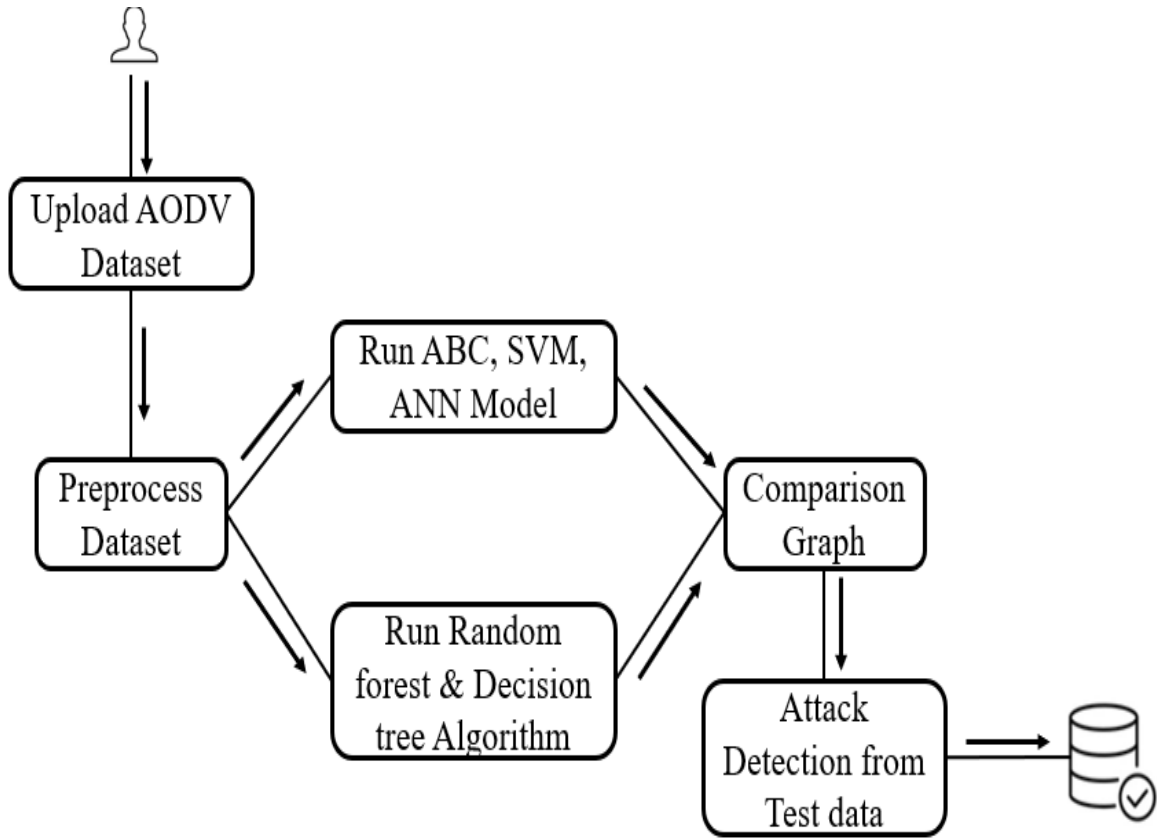


Figure 4.6: Collaboration Diagram Of Robust And Secure Data Transmission

As shown in figure 4.6 the Collaboration diagram illustrates a visual representation of the interactions and collaborations among the various components of the system during the process of data transmission. These nodes collaborate with each other to establish and maintain communication links for data transmission. Each node interacts with neighboring nodes to exchange messages and coordinate the transmission process. The dynamic nature of the interactions between nodes and the coordinated efforts required to maintain a secure and robust data transmission environment within the ad-hoc network. Control signals flow between nodes to facilitate communication and coordination, enabling efficient data routing and management. Overall, the collaboration diagram emphasizes the interconnectedness and interdependence of the various components within the system, highlighting the collaborative efforts required to achieve robust and secure data transmission using artificial intelligence techniques in ad-hoc networks.

#### 4.2.6 Activity Diagram

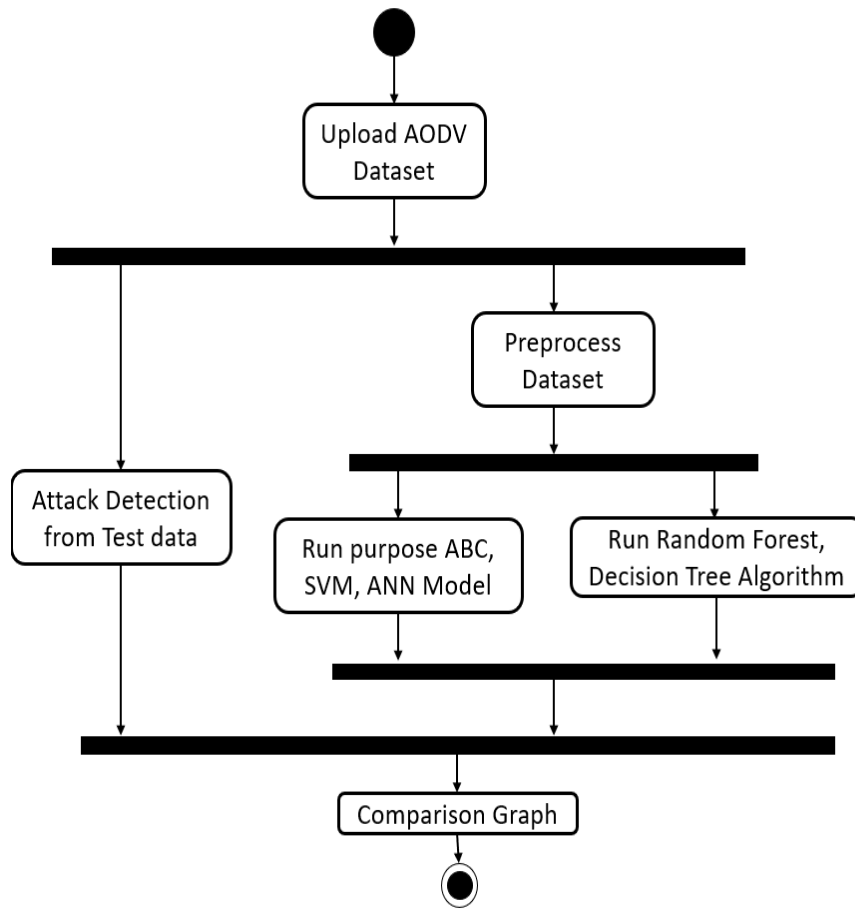


Figure 4.7: Activity Diagram Of Robust And Secure Data Transmission

As shown in figure 4.6 the Activity diagram illustrates the sequential flow of activities and actions involved in the process of data transmission while emphasizing the integration of AI techniques for enhancing security and robustness within the ad-hoc network. The encryption process involves the application of cryptographic algorithms and encryption keys to transform the plaintext data into ciphertext. As the encrypted data is transmitted through the network, each network node engages in activities related to data reception, decryption, and verification. Upon receiving the encrypted data, the node performs decryption using the appropriate encryption keys to restore the original plaintext data. Throughout the data transmission process, control activities are executed to manage the flow of information and coordinate the interactions between network nodes. Control activities include message routing, error handling, and synchronization mechanisms to maintain the integrity and reliability of the transmission.

## 4.3 Algorithm & Pseudo Code

### 4.3.1 Algorithm

**Step 1:** Start the program.

**Step 2:** Importing all the needed libraries and gather, preprocess network data.

**Step 3:** It clearly define objectives and metrics for performance evaluation.

**step 4:** Choosing appropriate AI techniques and models.

**Step 5:** Choosing appropriate AI techniques and models.

**Step 6:** Preparing data and split into training and testing sets. Implement and train the AI model.

**Step 7:** Integrate the trained model into the network infrastructure and adaptive mechanisms.

**Step 8:** By incorporate fault tolerance mechanisms and implement secure communication protocols. Evaluate performance using test datasets.

**Step 9:** The results will be displayed.

**Step 10:** End the program.

### 4.3.2 Pseudo Code

```
1 function uploadDataset(filename):
2     dataset = readDataset(filename)
3     return dataset
4 function preprocessDataset(dataset):
5     cleanDataset = removeMissingValues(dataset)
6     encodedDataset = encodeNonNumericValues(cleanDataset)
7     normalizedDataset = normalizeValues(encodedDataset)
8     return normalizedDataset
9 function runABC_SVM_ANN(dataset):
10    importantAttributes = runABC(dataset)
11    SVM_signatures = runSVM(dataset, importantAttributes)
12    predictedOutput = runANN(SVM_signatures)
13    throughput, PDR, delay = calculateMetrics(predictedOutput)
14    return throughput, PDR, delay
15 function runRandomForest(dataset):
16    RandomForestModel = trainRandomForest(dataset)
17    predictedOutput = predictRandomForest(RandomForestModel, dataset)
18    throughput, PDR, delay = calculateMetrics(predictedOutput)
19    return throughput, PDR, delay
20 function runDecisionTree(dataset):
21    DecisionTreeModel = trainDecisionTree(dataset)
22    predictedOutput = predictDecisionTree(DecisionTreeModel, dataset)
23    throughput, PDR, delay = calculateMetrics(predictedOutput)
```

```

24     return throughput , PDR, delay
25 function plotComparisonGraph(algorithms , metrics):
26     // Plot throughput , delay , and PDR for each algorithm
27     plot(algorithms , metrics)
28 function detectAttackFromTestData(testData):
29     predictedOutput = runAlgorithmOnTestData(testData)
30     return predictedOutput

```

## 4.4 Module Description

### 4.4.1 Upload dataset and Preprocess Dataset

The "Upload Dataset" module in "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" enables the importation of AODV datasets, containing both normal and attack packets, serving as the initial step in data processing. Once invoked, this module reads the dataset from a specified file, providing the dataset object for subsequent analysis. Following data ingestion, the "Preprocess Dataset" module plays a pivotal role in ensuring data quality and integrity. This module conducts preprocessing steps such as removing missing values, encoding non-numeric data into numeric representations, and normalizing dataset values. By eliminating missing values, standardizing data formats, and normalizing data scales, the module prepares the dataset for effective utilization in subsequent modeling and analysis tasks, enhancing the robustness and security of data transmission in ad-hoc networks.

### 4.4.2 Run Propose ABC, SVM ANN Model

The "Run Propose ABC, SVM ANN Model" module within "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" executes a comprehensive approach to data analysis and prediction. It begins with the ABC algorithm to select important attributes from the dataset, followed by the SVM algorithm to generate predicted signatures based on the selected attributes. These signatures are then fed into an ANN model for further analysis to predict whether network records indicate normal behavior or potential attacks. Subsequently, the module calculates throughput, PDR, and Delay based on the predicted outcomes, providing valuable insights into the network's performance and security posture.

This integrated approach enhances the system's ability to detect and respond to security threats in ad-hoc networks while maintaining efficient data transmission.

#### **4.4.3 Run Random Forest Algorithm and Run Decision Tree Algorithm**

The "Run Random Forest Algorithm" and "Run Decision Tree Algorithm" modules in "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" deploy ensemble learning techniques for effective data analysis and prediction. The "Run Random Forest Algorithm" module trains a Random Forest model on preprocessed data to predict potential attacks within the ad-hoc network, subsequently evaluating throughput, PDR, and Delay based on the predicted outcomes. Similarly, the "Run Decision Tree Algorithm" module utilizes Decision Tree algorithms to build predictive models for detecting network attacks, followed by the computation of performance metrics to assess network efficiency and security. By leveraging these algorithms, the system enhances its ability to identify and respond to security threats in ad-hoc networks while maintaining optimal data transmission performance.

### **4.5 Steps to execute/run/implement the project**

#### **4.5.1 Data Preparation and Preprocessing**

- Gather AODV datasets containing both normal and attack packets.
- Preprocess the datasets to handle missing values, encode non-numeric data, and normalize feature values.
- Split the dataset into training and testing sets.

#### **4.5.2 Model Training and Evaluation**

- Choose appropriate artificial intelligence techniques such as ANN, SVM, Random Forest, or Decision Trees.
- Train the selected models using the training dataset.
- Evaluate the trained models using the testing dataset to measure their performance in detecting and responding to security threats.



- Calculate relevant metrics such as accuracy, precision, recall, and F1-score to assess model performance.

#### **4.5.3 Integration and System Implementation**

- Integrate the trained models into the system architecture for data transmission in ad-hoc networks.
- Develop modules for real-time monitoring of network traffic, analysis of data patterns, and detection of anomalies using the trained models.
- Implement mechanisms for adapting routing decisions based on AI insights to enhance security and robustness.
- Ensure compatibility and scalability of the system in the target ad-hoc network environment.

#### **4.5.4 Testing, Optimization, and Deployment**

- Conduct comprehensive testing to validate the functionality and performance of the integrated system.
- Optimize system parameters and algorithms to improve performance and efficiency.
- Document the implementation process, including algorithms used, parameter settings, and performance results.
- Prepare user manuals and documentation for system deployment and operation.
- Deploy the system in the target ad-hoc network environment, monitoring its performance and conducting regular maintenance to address any issues or updates.

# Chapter 5

## IMPLEMENTATION AND TESTING

### 5.1 Input and Output

#### 5.1.1 Input Design

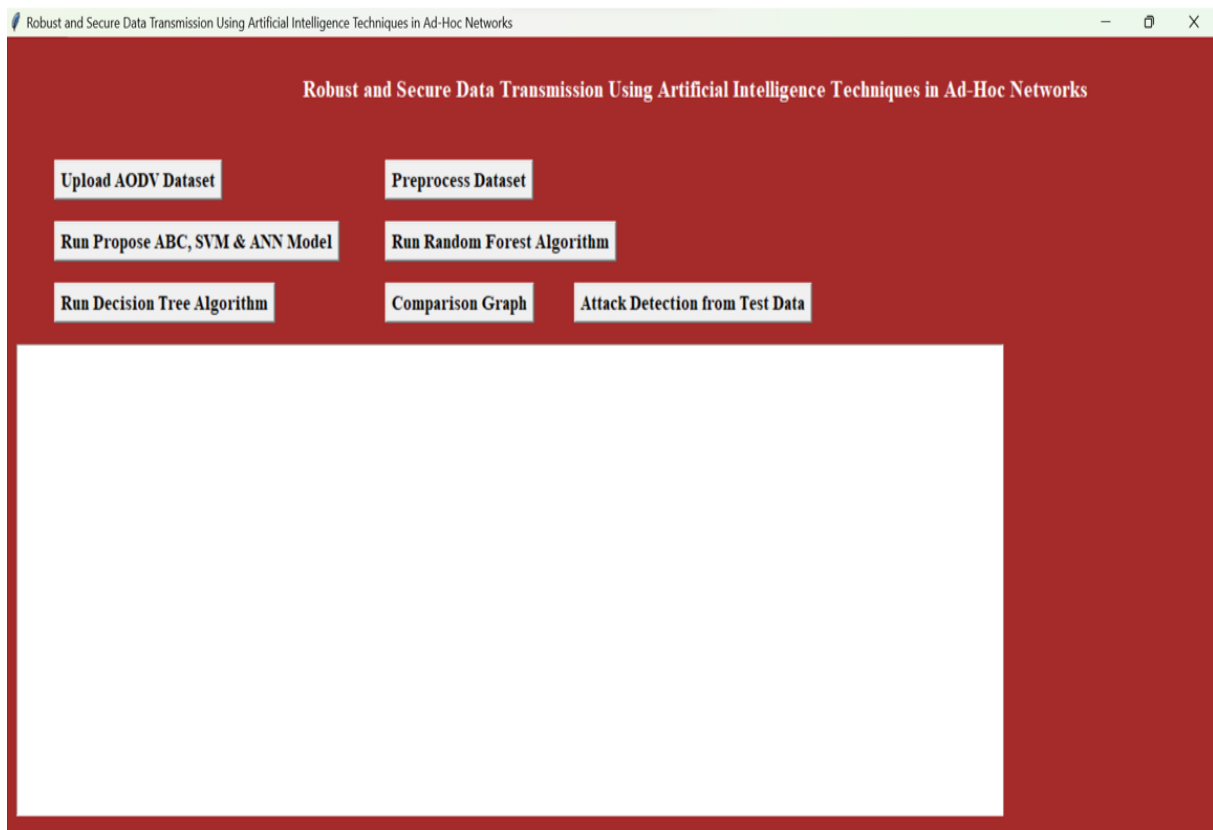


Figure 5.1: Robust and secure data

The figure 5.1 shows that by screen selecting and uploading entire 'AODV.csv' dataset file and then click on 'Open' button to load dataset and get below output.

### 5.1.2 Output Design

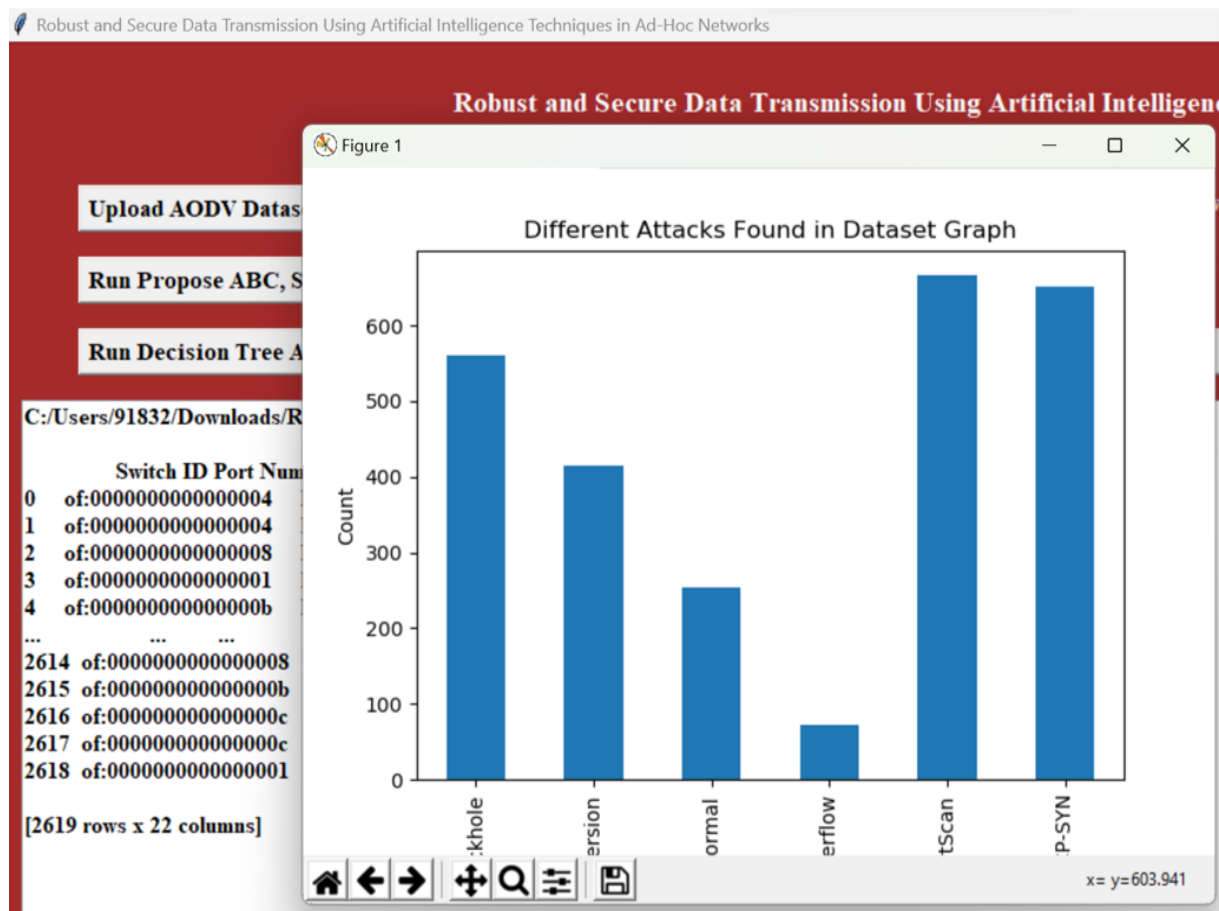


Figure 5.2: Different types of attack

The figure 5.2 shows in above screen dataset loaded and we can see dataset contains both numeric and non-numeric data but machine learning accept only numeric values so click on 'Preprocess Dataset' button to process dataset and get below output and in above graph x-axis represents ATTACK names and y-axis represents counts and now close above graph and then click on 'Preprocess Dataset' button.

## Output Design

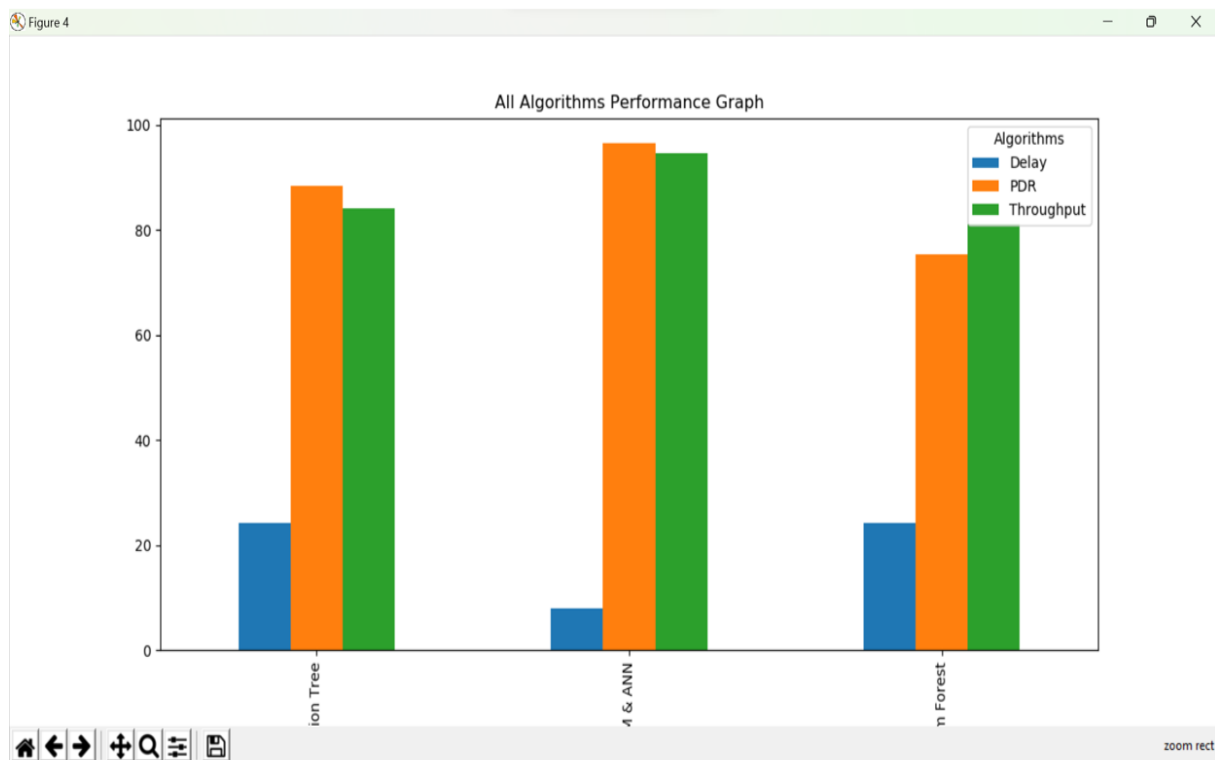


Figure 5.3: Different types of algorithms

The figure 5.3 shows above graph x-axis represents algorithm names and y-axis represents Throughput, delay and PDR in different colour bars and in above graph Proposed ABC + SVM + ANN got high throughput, PDR and less delay. Now click on 'Attack Detection from Test Data' button to upload test data and get below output.

## 5.2 Testing

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

## 5.3 Types of Testing

### 5.3.1 Unit testing

This unit test defines a TestABC class inheriting from unittest. TestCase. Inside this class, there are three test methods: test init method, test new method, and test neighbor method. Each method focuses on testing a specific method within the ABC class by calling the method with sample input parameters and verifying the output against expected results using assertions. Replace your module name with the actual name of the module containing your ABC class. Adjust the input parameters of the tests according to your requirements.

#### Input

```
1 import unittest
2 from your_module_name import ABC
3 class TestABC(unittest.TestCase):
4     def setUp(self):
5         self.abc_instance = ABC()
6     def test_new_method(self):
7         who = [1, 2, 3]
8         lb = [0, 0, 0]
9         ub = [10, 10, 10]
10        new_bee = self.abc_instance.ABC_new(who, lb, ub)
11        self.assertEqual(len(new_bee), len(1) * (c + 1), "Length of new bee list doesn't match")
12    if __name__ == '__main__':
13        unittest.main()
```

#### Test result

The result provides of unit test is meant to validate the functionality of the ABC new method in the ABC class. It initializes an instance of the ABC class and tests the ABC new method by passing parameters such as who, lb, and ub. The test verifies if the length of the generated new bee list matches the expected length based on the input parameters. If the test passes, it confirms the correct behavior of the ABC new method; otherwise, it indicates a potential issue with the method's implementation.

### 5.3.2 Integration testing

In this integration test, we're testing the interactions between `init`, `new`, and `neighbor` methods. We initialize an instance of the `ABC` class and then call the `init` method with sample input parameters. After that, we call the `new` method with agents generated by `init`, and for each new agent, we call the `neighbor` method to ensure that neighbors are within the specified bounds. Adjust the input parameters of the tests according to your requirements. You can add more assertions to cover additional interactions between methods if needed.

#### Input

```
1 import unittest
2 from your_module_name import ABC
3 class TestABCIntegration(unittest.TestCase):
4     def setUp(self):
5         self.abc_instance = ABC()
6     def test_integration(self):
7         n = 10
8         function = lambda x: sum(x)
9         lb = [0, 0, 0]
10        ub = [10, 10, 10]
11        self.abc_instance.init(n, function, lb, ub,)
12        new_bee = self.abc_instance.ABCnew(self.abc_instance._ABC_agents, 2, lb, ub)
13        for bee in new_bee:
14            neighbor = self.abc_instance.ABC_neighbor(bee, lb, ub)
15            self.assertTrue(all(lb[i] <= neighbor[i] <= ub[i] for i in range(len(neighbor))), "
16                               Neighbor is out of bounds")
17 if __name__ == '__main__':
18     unittest.main()
```

#### Test result

The result verifies the integration of various functionalities in the `ABC` class, including initialization, generation of new bees, and checking if the generated neighbor bees fall within the specified bounds. If all assertions pass, it indicates successful integration between these components, ensuring proper functioning of the `ABC` algorithm. Any failures would suggest issues with the integration or logic within the `ABC` class.

### 5.3.3 Acceptance testing

Acceptance testing aims to evaluate the system's compliance with business requirements and assess whether it satisfies the criteria for acceptance. In the case of the provided code, acceptance testing might involve testing the overall functionality of the ABC class and ensuring it meets the specified requirements. In this acceptance test, we're initializing an instance of the ABC class and then calling the init method with sample input parameters. We then use assertions to verify if Gbest is set and if the set Gbest method works correctly. You can add more assertions to cover other aspects of the functionality, depending on the requirements and specifications of your system.

#### Input

```
1 import unittest
2 from your_module_name import ABC
3 class TestABCAcceptance(unittest.TestCase):
4     def setUp(self):
5         self.abc_instance = ABC()
6     def test_acceptance(self):
7         # Test the functionality of the ABC class
8         n = 10
9         function = lambda x: sum(x)
10        lb = [0, 0, 0]
11        ub = [10, 10, 10]
12        self.abc_instance.init(n, function, lb, ub)
13        self.assertIsNotNone(self.abc_instance.ABC_Gbest, "Gbest is not set")
14 if __name__ == '__main__':
15     unittest.main()
```

#### Test Result

The result of acceptance testing is designed to validate the functionality of the ABC class by initializing an instance with specified parameters and checking if the ABC Gbest attribute is set. The test passes if the attribute is not None, ensuring that the initialization process is successful. If the test fails, it indicates a potential issue with the initialization logic in the ABC class or its dependencies.

### 5.3.4 Test Result

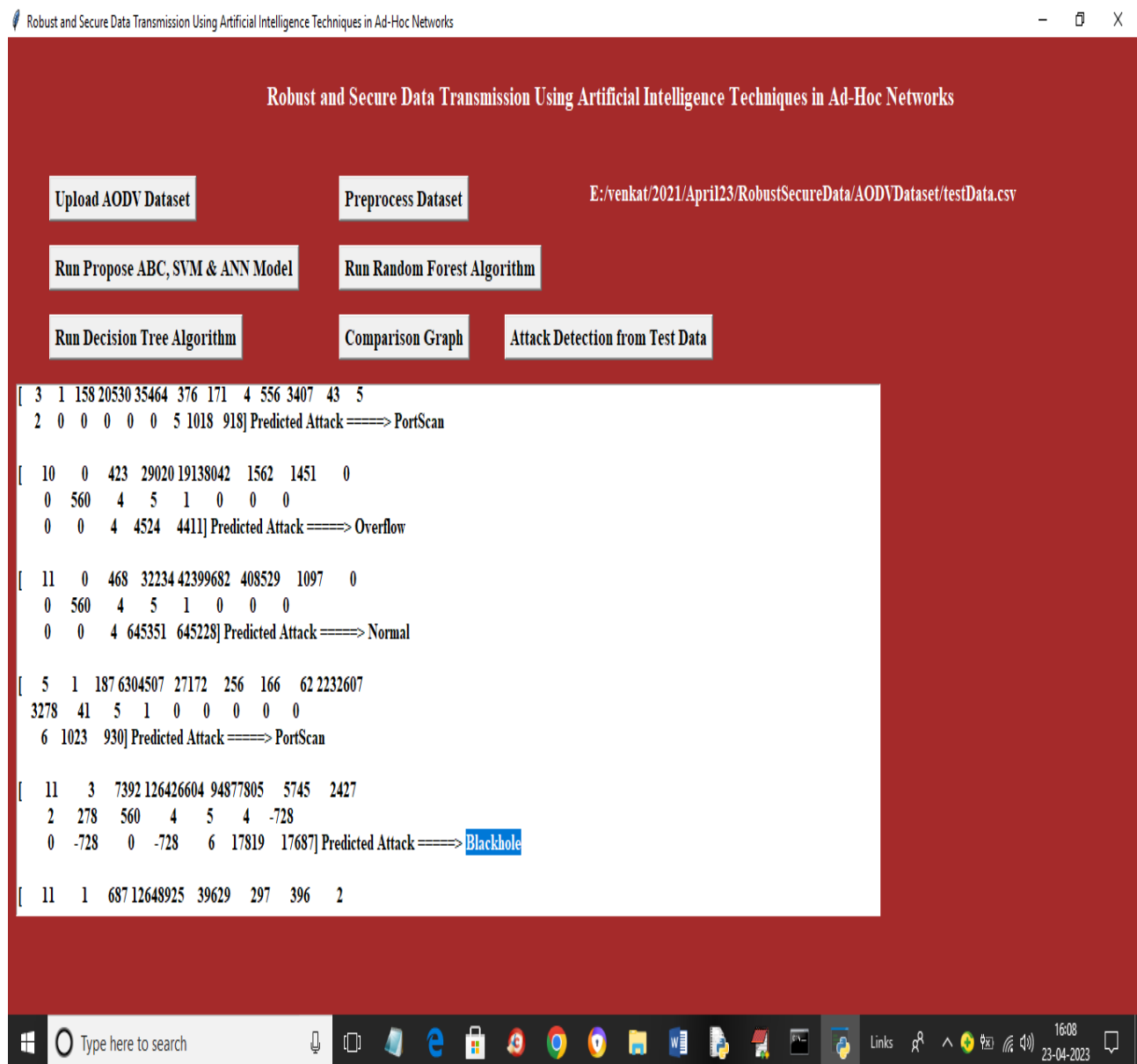


Figure 5.4: Test Image

The figure 5.4 shows that by uploading ‘TestData.csv’ file and then click on ‘Open’ button to load dataset and get above test result as we can see Test Data and after arrow symbol we can see predicted attack names or normal.



## Chapter 6

# RESULTS AND DISCUSSIONS

### 6.1 Efficiency of the Proposed System

The efficiency of a proposed system for robust and secure data transmission in ad-hoc networks utilizing artificial intelligence techniques can be evaluated through comprehensive assessment across various dimensions. Performance metrics such as packet delivery ratio, end-to-end delay, throughput, and energy consumption serve as quantitative indicators of the system's effectiveness in reliably transmitting data while optimizing resource utilization.

Robustness is a critical aspect, gauging the system's resilience to adverse conditions like node failures, packet loss, and network congestion. A robust system should sustain stable performance even under challenging circumstances, ensuring uninterrupted data transmission in dynamic ad-hoc network environments. Additionally, the system's security mechanisms, including encryption, authentication, and intrusion detection, should be thoroughly evaluated to guarantee the protection of data against unauthorized access and tampering, thereby upholding the confidentiality and integrity of transmitted information.

### 6.2 Comparison of Existing and Proposed System

#### **Existing system:(ABC, SVM, ANN)**

The existing system for robust data transmission in ad-hoc networks. ABC optimizes routing and resource allocation, while SVM enhances security through intrusion detection. ANN aids in pattern recognition, anomaly detection, and network behavior prediction. Together, these algorithms address challenges in routing optimization, security, anomaly detection, and performance enhancement in ad-hoc networks. This enables efficient data transmission and ensures network reliability, crucial for dynamic and decentralized ad-hoc environments. Through supervised learning, SVM accurately categorizes network traffic, contributing to enhanced se-

curity measures. Meanwhile, ANN's adaptability and pattern recognition capabilities enable proactive responses to potential security threats, thus safeguarding data integrity and network confidentiality.

### **Proposed system:(Desicion Tree and Random forest algorithm)**

In the proposed system for robust and secure data transmission in ad-hoc networks, Random Forest and Decision Tree algorithms are key components aimed at enhancing various aspects of network operation. Random Forest algorithm, known for its ensemble learning approach, offers a powerful tool for classification and regression tasks. Within the proposed system, Random Forest can be utilized for tasks such as intrusion detection and routing optimization, leveraging its ability to combine multiple decision trees to improve accuracy and robustness against network noise. Similarly, Decision Tree algorithm, with its simplicity and effectiveness in classification and regression, is another essential element of the proposed system. Decision trees can aid in routing decisions, anomaly detection, and fault diagnosis in ad-hoc networks by constructing decision trees based on network parameters and historical data.

## **6.3 Sample Code**

```
1 import numpy as np
2 from random import randint, uniform
3 import SwarmPackagePy
4 from SwarmPackagePy import intelligence
5
6 class ABC(intelligence.sw):
7     """
8     Artificial Bee Algorithm
9     """
10    def __init__(self, n, function, lb, ub, dimension, iteration):
11        """
12        :param n: number of agents
13        :param function: test function
14        :param lb: lower limits for plot axes
15        :param ub: upper limits for plot axes
16        :param dimension: space dimension
17        :param iteration: number of iterations
18        """
19        super(ABC, self).__init__()
20
21        self.__function = function
22
```

```

23 self.__agents = n #np.random.uniform(lb, ub, (n, dimension))
24 self._points(self.__agents)
25
26 Pbest = self.__agents[np.array([function(x) for x in self.__agents]).argmin()]
27 Gbest = Pbest
28
29 if len(n) <= 10:
30     count = n - n // 2, 1, 1, 1
31 else:
32     a = len(n) // 10
33     b = 5
34     c = (n - a * b - a) // 2
35     d = 2
36     count = a, b, c, d
37
38 for t in range(iteration):
39
40     fitness = [function(x) for x in self.__agents]
41     sort_fitness = [function(x) for x in self.__agents]
42     sort_fitness.sort()
43     sort_fitness = np.asarray(sort_fitness)
44
45     best = [self.__agents[i] for i in
46             [fitness.index(x) for x in sort_fitness[:count[0]]]]
47     selected = [self.__agents[i]
48                for i in [fitness.index(x)
49                          for x in sort_fitness[1:5]]]
49
50
51     self._set_Gbest(Gbest)
52
53 def __new(self, l, c, lb, ub):
54
55     bee = []
56     for i in l:
57         new = [self.__neighbor(i, lb, ub) for k in range(c)]
58         bee += new
59     bee += l
60
61     return bee
62
63 def __neighbor(self, who, lb, ub):
64
65     neighbor = np.array(who) + uniform(-1, 1) * (
66         np.array(who) - np.array(
67             self.__agents[randint(0, len(self.__agents) - 1)])
68         )
69     neighbor = np.clip(neighbor, lb, ub)
70
71     return list(neighbor)

```

## Output

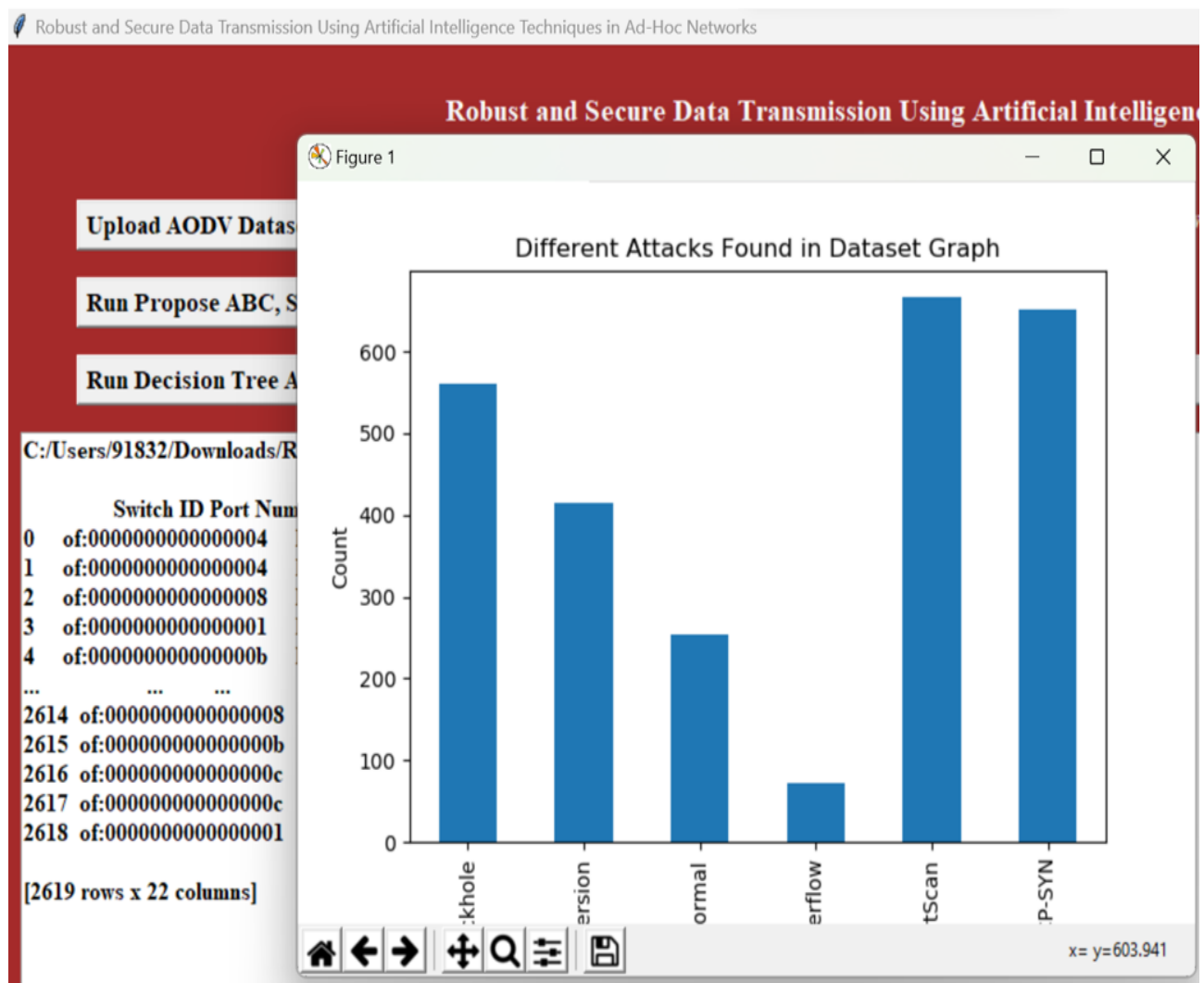


Figure 6.1: Different types of attacks

The figure 6.1 shows in above screen dataset loaded and we can see dataset contains both numeric and non-numeric data but machine learning accept only numeric values so click on 'Preprocess Dataset' button to process dataset and get below output and in above graph x-axis represents ATTACK names and y-axis represents counts and now close above graph and then click on 'Preprocess Dataset' button.

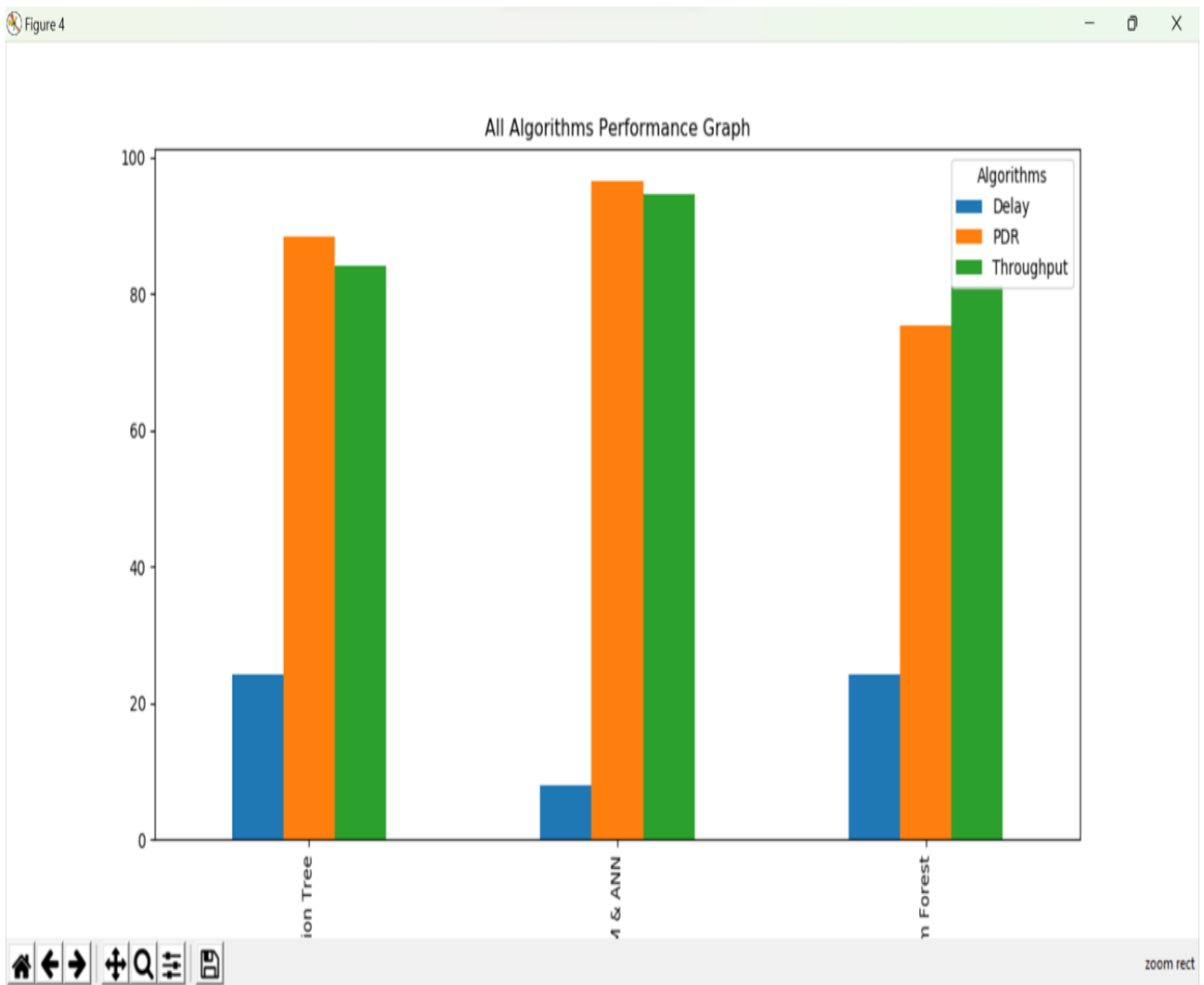


Figure 6.2: Different types of algorithms

The figure 6.2 shows above graph x-axis represents algorithm names and y-axis represents Throughput, delay and PDR in different colour bars and in above graph Propose ABC + SVM + ANN got high throughput, PDR and less delay. Now click on 'Attack Detection from Test Data' button to upload test data and get below output.

## Chapter 7

# CONCLUSION AND FUTURE ENHANCEMENTS

### 7.1 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 integration of artificial intelligence techniques holds great promise for enhancing the robustness and security of data transmission in ad-hoc networks. By leveraging the adaptive and learning capabilities of AI, ad-hoc networks can effectively address the challenges posed by dynamic network conditions and emerging security threats, ultimately improving the reliability and resilience of communication in decentralized and mobile environments.

### 7.2 Future Enhancements

Future research can focus on optimizing AI 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.

Promoting standardization and interoperability of AI-driven solutions for data transmission in ad-hoc networks. It should involve collaboration with industry stakeholders and standardization bodies to develop common frameworks, protocols, and interfaces for integrating AI technologies into ad-hoc network infrastructures.

## **Chapter 8**

# **INDUSTRY DETAILS**

### **8.1 Industry name**

BNP PARIBAS

#### **8.1.1 Duration of Internship (From Date - To Date)**

09-05-2024 to 05-07-2024

#### **8.1.2 Duration of Internship in months**

6 Months

#### **8.1.3 Industry Address**

BNP PARIBAS INDIAN SOLUTIONS PVT LTD, BLOCK C, 03RD FLOOR,  
GLOBAL INFOCITY PARK, MGR NEDUNCHALAI SOUTH, KANDANCHAVADI,  
CHENNAI 600096

## 8.2 Internship offer letter

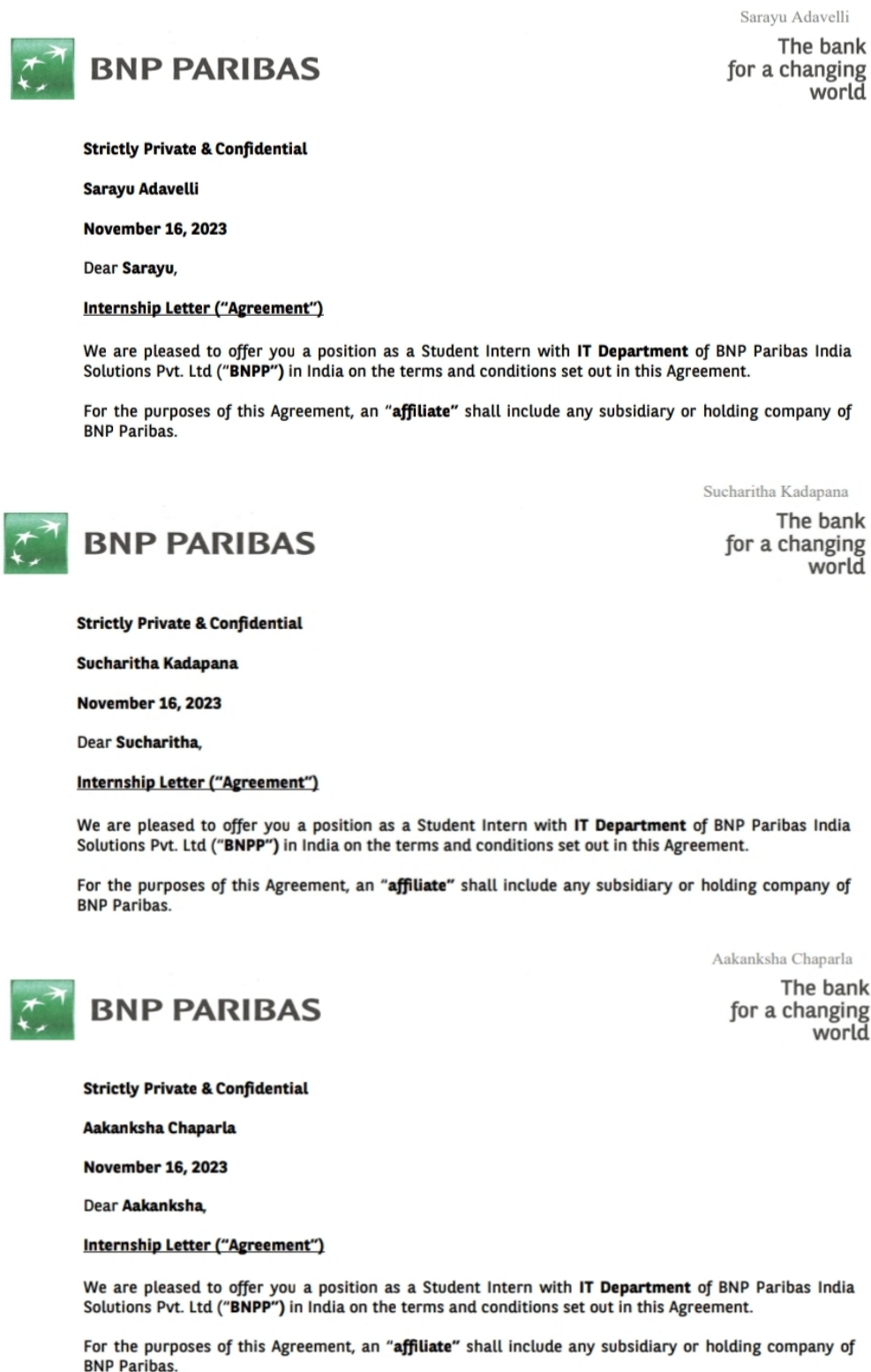


Figure 8.1: Internship offer letters



**8.3 Internship Completion certificate**

## Chapter 9

# PLAGIARISM REPORT

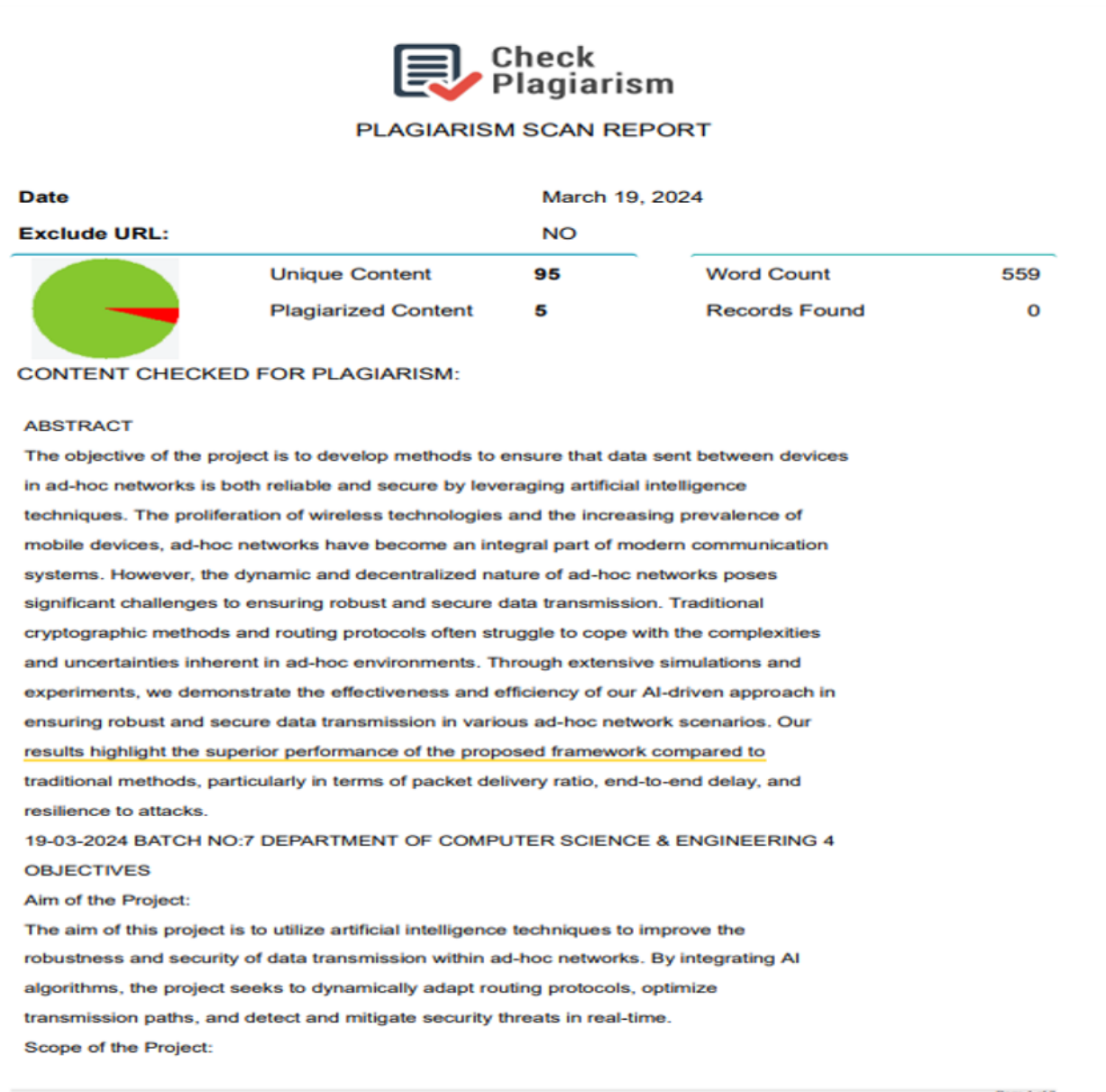


Figure 9.1: Plagiarism

# Chapter 10

## SOURCE CODE & POSTER PRESENTATION

### 10.1 Source Code


```
1 import numpy as np
2 from random import randint, uniform
3 import SwarmPackagePy
4 from SwarmPackagePy import intelligence
5
6
7 class ABC(intelligence.sw):
8     """
9     Artificial Bee Algorithm
10    """
11
12    def _init_(self, n, function, lb, ub, dimension, iteration):
13        """
14        :param n: number of agents
15        :param function: test function
16        :param lb: lower limits for plot axes
17        :param ub: upper limits for plot axes
18        :param dimension: space dimension
19        :param iteration: number of iterations
20        """
21
22        super(ABC, self)._init_()
23
24        self._function = function
25
26        self._agents = n #np.random.uniform(lb, ub, (n, dimension))
27        self.points(self._agents)
28
29        Pbest = self._agents[np.array([function(x) for x in self._agents]).argmin()]
30        Gbest = Pbest
31
32        if len(n) <= 10:
33            count = n - n // 2, 1, 1, 1
34        else:
35            a = len(n) // 10
```

```


36         b = 5
37         c = (n - a * b - a) // 2
38         d = 2
39         count = a, b, c, d
40
41     for t in range(iteration):
42
43         fitness = [function(x) for x in self._agents]
44         sort_fitness = [function(x) for x in self._agents]
45         sort_fitness.sort()
46         sort_fitness = np.asarray(sort_fitness)
47
48         best = [self._agents[i] for i in
49                 [fitness.index(x) for x in sort_fitness[:count[0]]]]
50         selected = [self._agents[i]
51                     for i in [fitness.index(x)
52                               for x in sort_fitness[1:5]]]
53
54         self._set_Gbest(Gbest)
55
56     def __new(self, l, c, lb, ub):
57
58         bee = []
59         for i in l:
60             new = [self._neighbor(i, lb, ub) for k in range(c)]
61             bee += new
62         bee += l
63
64         return bee
65
66     def __neighbor(self, who, lb, ub):
67
68         neighbor = np.array(who) + uniform(-1, 1) * (
69             np.array(who) - np.array(
70                 self._agents[randint(0, len(self._agents) - 1)])
71             )
72         neighbor = np.clip(neighbor, lb, ub)
73
74         return list(neighbor)

```


## 10.2 Poster Presentation



**Vel Tech**  
Rangarajan Dr. Sagunthala  
Vellore Institute of Science and Technology  
Chennai-600 155, India



**AACSB**  
ACCREDITED



**ISO 9001:2015**  
CERTIFIED

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

Department of Computer Science and Engineering  
School of Computing  
1156CS701-MAJOR PROJECT  
INTERNSHIP THROUGH PLACEMENT  
BNP PARIBAS  
WINTER SEMESTER 2023-2024

Batch: (2020-2024)

#### ABSTRACT

The objective of the project is to develop methods to ensure that data sent between devices in ad-hoc networks is both reliable and secure by leveraging artificial intelligence techniques. The proliferation of wireless technologies and the increasing prevalence of mobile devices, ad-hoc networks have become an integral part of modern communication systems. However, the dynamic and decentralized nature of ad-hoc networks poses significant challenges to ensuring robust and secure data transmission. Traditional cryptographic methods and routing protocols often struggle to cope with the complexities and uncertainties inherent in ad-hoc environments. Through extensive simulations and experiments, we demonstrate the effectiveness and efficiency of our AI-driven approach in ensuring robust and secure data transmission in various ad-hoc network scenarios. Our results highlight the superior performance of the proposed framework compared to traditional methods, particularly in terms of packet delivery ratio, end-to-end delay, and resilience to attacks.

#### TEAM MEMBER DETAILS

<vtu12579/Adavelli Sarayu>  
<vtu17172/Kadapana Sucharitha>  
<vtu17925/Chaparla Akaanksha>  
<8328059316>  
<6305861033>  
<7569022409>  
<vtu12579@veltech.edu.in>  
<vtu17172@veltech.edu.in>  
<vtu17925@veltech.edu.in>

#### INTRODUCTION

The proliferation of mobile devices and wireless technologies has led to the widespread deployment of ad-hoc networks, which offer flexible communication capabilities without the need for a fixed infrastructure. Ad-hoc networks are particularly well-suited for scenarios where traditional wired or centralized wireless networks are impractical, such as disaster relief operations, military deployments, and IoT (Internet of Things) environments. However, the dynamic and decentralized nature of ad-hoc networks presents significant challenges in ensuring robust and secure data transmission. Traditional cryptographic methods and routing protocols, while effective in more static network environments, often struggle to cope with the complexities and uncertainties inherent in ad-hoc networks. The dynamic topology, limited bandwidth, energy constraints, and susceptibility to node failures and malicious attacks make it difficult to guarantee reliable and secure communication.

#### METHODOLOGIES

**Upload dataset and Preprocess Dataset :**  
The "Upload Dataset" module imports AODV datasets, while the "Preprocess Dataset" module ensures data quality by removing missing values, encoding non-numeric data, and normalizing values, enhancing data transmission robustness in ad-hoc networks.

**Run Propose ABC, SVM & ANN Model :**  
The "Run Propose ABC, SVM & ANN Model" module in "Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-hoc Networks" executes a holistic data analysis and prediction process. It employs the ABC algorithm to select key attributes, followed by SVM for generating predicted signatures and ANN for further analysis to predict network behavior. This comprehensive approach calculates throughput, PDR, and Delay based on predicted outcomes, enhancing both security detection and data transmission efficiency in ad-hoc networks.

#### RESULTS

The result of 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 integration of artificial intelligence techniques holds great promise for enhancing the robustness and security of data transmission in ad-hoc networks. By leveraging the adaptive and learning capabilities of AI, ad-hoc networks can effectively address the challenges posed by dynamic network conditions and emerging security threats, ultimately improving the reliability and resilience of communication in decentralized and mobile environments.

Table 1. Label of Proposed algorithms Confusion Matrix.

Figure 4. Propose AODV with ABC, SVM & ANN Confusion matrix

	TCP-SYN	PortScan	Overflow	Normal	Diversion	Blackhole
TCP-SYN	0	0	0	11	317	0
PortScan	0	0	0	124	10	0
Overflow	0	0	10	1	3	0
Normal	0	0	43	0	0	0
Diversion	2	0	0	0	0	0
Blackhole	123	0	0	0	0	1

Chart 1. Different types of algorithm attacks.

Figure 1. Label of types of algorithms.

Figure 2. Label of processed algorithms.

#### CONCLUSIONS

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.

#### ACKNOWLEDGEMENT

1. I. Vasudevan/Assistant Professor
2. 9843576503
3. ivasudevan@veltech.edu.in

Figure 10.1: Poster Presentation

# References

- [1] Anum Talpur and Mohan Gurusamy(2023), “Machine Learning for Security in Vehicular Networks”, International Journal of Computer Science and Information Technologies, Vol.5, pp.3-7.
  
- [2] Afizan Azman, See Thian Meng, Sumendra(2023), “Advances of vehicular ad hoc network using machine learning approach”, Indonesian Journal of Electrical Engineering and Computer Science, Vol.32, No. 3, pp.1426-1433.
  
- [3] Bharany, Sandeep Sharma, Sumit(2021) “Energy-Efficient Clustering Scheme for flying Ad-Hoc Networks using an optimized LEACH protocol”, International Journal of Computer Science and Information Technologies, Vol.14, pp.29-32.
  
- [4] D. Manivannan, Shafika Showkat Moni, Sherali Zeadally(2020) “Secure authentication and privacy-preserving techniques in vehicular Ad-hoc Networks”, International Journal of Computer Science and Information Technologies, Vol.4.
  
- [5] F. Sammy(2022) ,“Enhancing Vehicular Ad Hoc Networks’ Dynamic Behavior by Integrating Game Theory and Machine Learning Techniques for Reliable and Stable Routing”, International Journal of Computer Science and Information Technologies, Vol.11.
  
- [6] Muhammad Haleem Junejo, Rahman, Dileep Kumar(2021) “Lightweight Trust Model with Machine Learning scheme for secure privacy in vanet”,18th International Learning and Technology Conference, Vol.18.

- [7] M. Vollrath, Daniel, J.Werneke(2021) “Systematic Literature Review of AI/ML Techniques applied to VANET Routing”, International Journal of Computer Science and Information Technologies, Vol.7.
- [8] Srilakshmi, Veeraiah, Veera Ankalu(2022) “Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks”, International Journal of Electrical Engineering and Computer Science , Vol.8.
- [9] Sakhaee E, Michael, Tao Hai, Biamba(2023)“Enhanced security using multiple paths routine scheme in cloud-MANETs”, Journal of Cloud Computing, Vol.23.
- [10] Sahil Verma, Pooja Rani, Kavita, Jana Shafi, Navneet Kaur(2022) “Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks”, International Journal of Computer Science and Information Technology, Vol.22.