AI SECURITY THREATS IN 5G ENABLED IOT DEVICE MANAGEMENT

PROJECT-21ECP302L

Submitted by

K Mahendra Kumar [Reg No:RA2211052010029]

D Bapuji Reddy [Reg No: RA2211052010031]

P Rushendra [Reg No: RA2211067010013]

Under the guidance of

Dr. S. Murugaveni

(Assistant Professor, Department of Electronics & Communication Engineering)

BACHELOR OF TECHNOLOGY

in

ELECTRONICS & COMMUNICATION ENGINEERING

SPECIALIZATION IN DATA SCIENCE

of

COLLEGE OF ENGINEERING AND TECHNOLOGY

S.R.M. NAGAR, Kattankulathur, Chengalpattu District

MAY 2025

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this activity report for the course **21ECP302P PROJECT** is the bonafide work of **K Mahendra Kumar (RA22110520010029) , D Bapuji Reddy (RA2211052010031) , and P Rushendra (RA2211067010013)** who carried out the work under my supervision.

SIGNATURE **SIGNATURE**

Dr. S. Murugaveni

Guide **Academic Co-Ordinator**

Assistant Professor

ABSTRACT

The convergence of Artificial Intelligence (AI) and 5G technology is revolutionizing IoT device management by enabling ultra-fast communication, low latency, and intelligent automation. However, this advancement introduces significant security challenges. The high-speed, high-volume data exchanges between millions of 5G-connected IoT devices expand the attack surface for malicious actors. AI models themselves, trained on massive data, are susceptible to data poisoning, adversarial attacks, and breaches. Furthermore, threats like deepfake generation, spoofing, and unauthorized access become more feasible in such distributed environments. Ensuring robust cybersecurity in this domain is essential to preserve user privacy, maintain service integrity, and prevent disruptions in smart systems.

This project focuses on addressing the security vulnerabilities of 5G-enabled IoT devices operating under Mobile-Edge Computing (MEC) architecture. Due to their decentralized nature and limited hardware capabilities, these devices are ill-equipped to resist cyber threats like DDoS attacks or real-time intrusions using traditional methods. To tackle these issues, our research implements an AI-driven security framework that leverages machine learning (ML) models for real-time intrusion detection, privacy-preserving preprocessing, secure data handling, and intelligent threat classification—all while optimizing for minimal computational load.

The methodology employs the TON_IoT telemetry dataset, capturing real-world network traffic, and uses privacy-enhancing techniques like SHA-256 hashing of IP and port data. Machine learning models including Random Forest, SVM, MLP, and Gradient Boosting are trained on a refined feature set to detect anomalies and predict cyber threats. Through rigorous performance evaluation in simulated MEC environments, key metrics like detection accuracy, false-positive rate, latency, and resource efficiency are assessed. Ensemble learning and real-time detection modules are also incorporated for practical, real-world deployment scenarios.

The final implementation demonstrates that AI-powered threat detection systems can significantly enhance the security of IoT ecosystems in 5G networks. Our models achieved up to 100% accuracy in detecting multiple classes of attacks, offering a scalable and privacy-respecting solution. The system's compliance with modern engineering standards (e.g., TLS, IEEE 802.x, GDPR) further ensures its readiness for practical use. This work contributes a meaningful step toward safeguarding next-generation digital infrastructure through intelligent, secure, and adaptive technologies.

TABLE OF CONTENTS

LST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IoT	Internet of Things
AI	Artificial Intelligence
MEC	Mobile-Edge Computing
DT	Decision Tree
RF	Random Forest
SVM	Basic Linear Algebra Subprograms
KNN	Block Random Access Memory
LR	Computer-Aided Software Engineering Descriptions
NB	Central Processing Units
ANN	Artificial Neural Networks
CNN	Convolutional Neural Networks
DaaS	Drones as a Service
URLLC	ultra-reliable low-latency communication
LSTMs	Long Short-Term Memory networks
DDoS	Distributed Denial of Service
NSL-KDD	Network Security Laboratory-Knowledge Discovery and Data Mining
CICIDS	Canadian Institute for Cybersecurity Intrusion Detection System

GPU	Graphics Processing Unit
TPU	Tensor Processing Unit
MLP	Multilayer Perceptron
IIoT	Industrial Internet of Things
TON_IoT	Telemetry dataset for the Internet of Things

CHAPTER 1
INTRODUCTION

1.1. Introduction

The rise of the Internet of Things (IoT) has transformed how devices communicate and share data across industries. With billions of interconnected devices, managing this complex web securely and efficiently has become a major technological challenge. The introduction of 5G has further accelerated this transformation by enabling ultra-fast, low-latency connections.

While 5G improves performance and connectivity, it also expands the potential attack surface for cyber threats. The vast number of devices and decentralized architecture of IoT systems make it difficult to monitor and secure each component. Attackers can exploit weak entry points, leading to serious data breaches or system failures.

Artificial Intelligence (AI) plays a key role in enhancing security by enabling real-time analysis, threat detection, and response. AI-driven models can learn from patterns in network behavior and identify abnormal activities. However, AI itself can be targeted through adversarial attacks, data poisoning, or manipulation of training inputs.

This project focuses on securing 5G-enabled IoT environments using AI techniques. Special attention is given to Mobile-Edge Computing (MEC), which brings data processing closer to devices but also introduces new vulnerabilities. The proposed system uses machine learning models and privacy-preserving techniques to defend against intrusions and cyberattacks.

Through dataset analysis, model training, and performance evaluation, this work demonstrates how AI can effectively detect and prevent threats in real-time. The goal is to create a scalable and intelligent security framework that ensures privacy, reliability, and resilience in next-generation IoT systems operating over 5G networks.

Different Types of Models:

1. Decision Tree (DT) **:** A simple, interpretable model that splits data based on feature conditions to detect suspicious patterns or anomalies.
2. Random Forest (RF) : An ensemble of multiple decision trees that improves accuracy and reduces overfitting in intrusion detection systems.
3. Support Vector Machine (SVM) : Classifies network behavior by finding the best boundary between normal and malicious data, effective in high-dimensional spaces.
4. K-Nearest Neighbors (KNN) : Compares incoming data with past known cases to detect anomalies based on similarity.
5. Logistic Regression (LR) : A statistical model used for binary classification, such as predicting whether a device is under attack or not.
6. Naïve Bayes (NB) : A fast probabilistic classifier that works well with small datasets and assumes feature independence.
7. Artificial Neural Networks (ANN) **:** A layered model that mimics the human brain to learn complex patterns in large IoT traffic datasets.
8. Convolutional Neural Networks (CNN) : Mainly used for image or spatial data, but also adapted to detect patterns in structured network traffic data.

1.2. Objective

The main objective of this project is to develop a secure and intelligent framework for managing IoT devices in 5G-enabled environments using Artificial Intelligence. It aims to identify and mitigate security threats such as data breaches, intrusion attacks, and unauthorized access, which are common in large-scale, real-time IoT systems. By leveraging AI and machine learning models, the system can detect anomalies in network traffic and classify threats efficiently. The use of privacy-preserving techniques ensures sensitive data remains

protected. The project also focuses on implementing the solution in a Mobile-Edge Computing (MEC) setup to enable faster response and lower latency. It evaluates different models to find the best-performing ones in terms of accuracy and resource usage. This research ultimately aims to enhance trust, privacy, and operational safety in the rapidly growing 5G IoT ecosystem.

CHAPTER 2
LITERATURE SURVEY

2.1. The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective

This study addresses the convergence of AI and Mobile-Edge Computing (MEC) as a foundational solution for safeguarding IoT environments. With the rapid deployment of edge nodes in 5G ecosystems, traditional security mechanisms are no longer sufficient. The research emphasizes that AI algorithms—particularly deep learning and reinforcement learning—are capable of dynamically adapting to threats in real-time by analyzing behavioral patterns at the edge.

It proposes a layered security architecture using federated learning to protect user data while allowing collaborative training across edge devices. This ensures privacy preservation without transferring raw data to centralized servers. The paper also introduces the concept of real-time anomaly detection where edge devices continuously monitor network traffic and autonomously respond to attacks, such as spoofing and unauthorized access.

Further, the work highlights challenges including model complexity, resource limitations at edge nodes, and the need for lightweight AI models. To overcome these, the study recommends integrating neuromorphic computing, edge accelerators, and compression techniques for model optimization. This approach is vital for creating intelligent, privacy-preserving, and low-latency IoT systems in 5G-enabled smart environments.

2.2. Drones as a Service (DaaS) for 5G Networks and Blockchain-Assisted IoT-Based Smart City Infrastructure

This paper introduces a futuristic smart city model utilizing Drones as a Service (DaaS), where AI, blockchain, and 5G converge to provide secure and scalable urban monitoring. Drones play a pivotal role in traffic surveillance, disaster management, and precision agriculture. By using 5G's ultra-reliable low-latency communication (URLLC),

drones can operate with real-time feedback and navigation, essential for autonomous missions.

To address the privacy and data integrity challenges in drone communications, the paper proposes blockchain integration for secure peer-to-peer data sharing. Every data packet captured by drones is encrypted, timestamped, and recorded immutably on a distributed ledger. AI is used for real-time object detection and environmental analysis, enhancing the intelligence of drone missions in dynamic environments.

The authors stress the need for robust identity management and secure firmware updates using smart contracts. They propose a decentralized trust model, ensuring that every drone and control node in the network is authenticated and verified. This multi-technology fusion not only improves service efficiency but also creates a resilient smart infrastructure backbone resistant to cyber threats.

2.3. Artificial Intelligence-Based Security Countermeasures for IoT

This research proposes an adaptive AI-based security framework for IoT ecosystems that can autonomously learn from evolving threats. Unlike static rule-based systems, the proposed model uses supervised and reinforcement learning to dynamically adapt its defensive strategies. It continuously analyzes traffic logs, behavioral metrics, and context-aware factors to detect and prevent cyberattacks in real-time.

The model is capable of predicting and responding to zero-day attacks using threat intelligence sharing and anomaly-based detection. Deep learning techniques such as LSTMs and CNNs are implemented to recognize patterns associated with DDoS, botnet, and man-in-the-middle attacks. It also explores transfer learning to share threat models across different IoT devices and domains, improving detection accuracy

A key contribution of this paper is the emphasis on resource-aware AI deployment. It evaluates various models for scalability, latency, and energy efficiency across heterogeneous devices. Lightweight convolutional neural networks and pruning techniques are used to ensure low memory consumption. This paves the way for practical

AI implementation in constrained environments like smart homes, industrial IoT, and wearable health monitors.

2.4. AI-based Network Security Enhancement for 5G Industrial IoT Environments

This study presents an AI-driven architecture aimed at enhancing security in 5G-enabled Industrial IoT (IoT) environments, such as smart manufacturing and automation systems. The paper focuses on training robust models using benchmark datasets like NSL-KDD and CICIDS 2017 for intrusion detection and malware classification. These models are then deployed at the edge to minimize latency and enable immediate threat response.

The proposed architecture includes a "5G Model Factory," which enables continuous AI model training and deployment using DevOps-like principles. Edge servers and IIoT gateways run inference models that monitor industrial control protocols (e.g., Modbus, OPC-UA) for unusual activity. Additionally, the system employs AI-based filtering to discard malicious inputs before reaching critical infrastructure components.

One of the standout features of this work is its dual-layer defense approach. The first layer uses AI-based filters for preliminary threat detection, while the second layer utilizes behavior-based machine learning algorithms for deeper analysis. It also includes self-healing capabilities, where the system autonomously reconfigures communication routes or updates firmware in response to detected vulnerabilities. This holistic AI integration creates a highly secure IIoT network under the 5G framework.

2.5. 5G Security Threat Landscape, AI, and Blockchain

This paper presents a panoramic view of the security challenges posed by the global rollout of 5G in IoT environments, emphasizing the need for next-gen defenses. It categorizes threats such as rogue base stations, identity spoofing, and signaling storms across different network layers. The study asserts that traditional encryption is insufficient and proposes AI and blockchain as co-dependent technologies for threat mitigation.

AI models, particularly unsupervised clustering and reinforcement learning, are used to detect anomalies in high-speed 5G traffic. These models can adapt to dynamic network slicing configurations, allowing custom security policies per slice. Blockchain, meanwhile, provides decentralized trust, tamper-proof records, and secure access management among distributed IoT nodes and base stations.

The authors propose a hybrid architecture that integrates smart contracts, AI-driven monitoring agents, and cryptographic authentication to deliver holistic end-to-end protection. Real-time threat scoring and smart-contract-based response actions help mitigate risks autonomously. This approach reflects a scalable and future-proof cybersecurity model that aligns with the complex requirements of 5G-powered IoT ecosystem.

CHAPTER 3
SOFTWARE DESCRIPTION

3.1. Google Colab

Google Colaboratory, commonly known as Google Colab, is a cloud-based Python programming environment provided by Google. It allows users to write and execute Python code through the browser, offering the power of computation without the need for any local setup. It is especially popular among students, researchers, and professionals working in the fields of data science, artificial intelligence, and machine learning due to its seamless integration with Google Drive and Jupyter Notebooks.

Google Colab offers the flexibility of using free GPU and TPU hardware accelerators, making it ideal for training and testing deep learning models. It simplifies collaboration by allowing users to share notebooks just like Google Docs, and it supports real-time editing. With built-in libraries and cloud storage access, Colab has become a preferred tool for developing and demonstrating AI models, data visualizations, and experimental research workflows.

3.1.1. Features of Google Colab

- **Cloud-based execution**: No installation required; runs completely in the browser.
- **Free access to GPUs/TPUs**: Offers limited but free access to high-performance hardware.
- **Jupyter Notebook interface**: Easy-to-use, interactive coding environment with support for code, text, images, and graphs.
- **Google Drive integration**: Automatically saves notebooks in Google Drive for easy access and sharing.
- **Supports rich visualizations**: Allows charts, graphs, and media outputs using

libraries like Matplotlib, Seaborn, and Plotly.

- **Collaboration support**: Real-time editing and commenting features similar to Google Docs

3.2. Python

Python played a central role in the implementation of the AI-based security system for 5G-enabled IoT device management. Leveraging Python's powerful libraries and frameworks, the team was able to efficiently load, preprocess, and clean the telemetry dataset from TON_IoT. Python’s hashlib module was used to anonymize sensitive data such as IP addresses and port numbers through SHA-256 hashing, supporting privacy-preserving data handling. Standard preprocessing tools like LabelEncoder and StandardScaler were employed from Python’s sklearn package to normalize and encode the data for machine learning model training.

Furthermore, Python's machine learning ecosystem enabled robust model development and evaluation. Various classifiers—including Support Vector Machine (SVM), Random Forest, Multilayer Perceptron (MLP), Logistic Regression, and Gradient Boosting—were implemented using scikit-learn. The GridSearchCV module facilitated hyperparameter tuning to optimize model performance. Python also supported the development of a real-time threat detection system, where user inputs (hashed IP and port) were fed into trained models to predict threat classes dynamically. Overall, Python’s flexibility and vast library support made it an ideal software platform for developing a scalable and privacy-respecting AI security solution.

CHAPTER 4

METHODOLOGY

4.1. Frame work in MEC

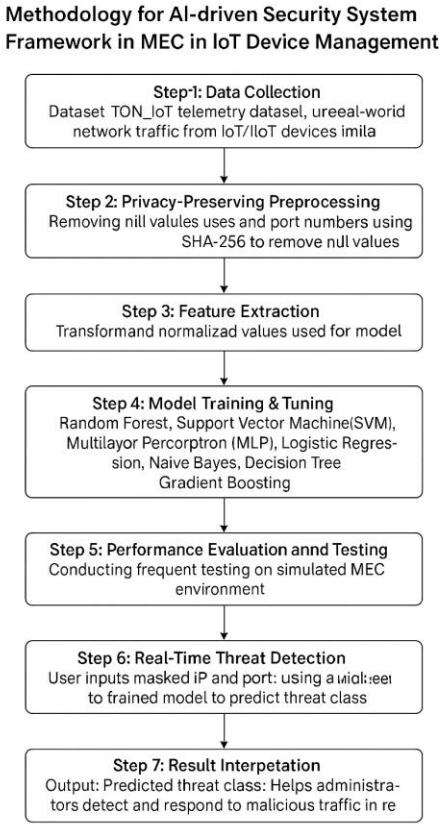

Fig 4.1: Frame work Architecture

4.2. Architecture Overview

4.2.1 Step 1: Data Collection

The process begins with gathering network traffic data from IoT/IIoT devices using the **TON_IoT telemetry dataset**, which contains real-world logs simulating various cyber-attacks and benign behaviors. This dataset serves as

the foundation for training and testing AI models, offering rich contextual information related to different devices, services, and protocols in an MEC setting.

4.2.2 Step 2: Privacy-Preserving Preprocessing

In this step, the dataset is cleaned and anonymized. Missing/null values are handled, and sensitive information such as IP addresses and port numbers are hashed using the SHA-256 algorithm. This ensures privacy preservation, especially critical in cybersecurity systems dealing with real-world network logs. Python libraries like hashlib are typically used for this transformation.

4.2.3 Step 3: Feature Extraction

The next phase involves transforming raw data into structured input suitable for machine learning. Features are normalized and encoded so that models can learn patterns effectively. Preprocessing techniques such as standard scaling and label encoding are applied here using libraries like sklearn.

4.2.4 Step 4: Model Training & Tuning

Multiple machine learning models are trained and optimized in this step.

This include :

- Random Forest
- Support Vector Machine (SVM)
- Multilayer Perceptron (MLP)
- Logistic Regression
- Naive Bayes

- Decision Tree
- Gradient Boosting

Each model is fine-tuned using tools like GridSearchCV to maximize prediction accuracy and reduce overfitting.

4.2.5 Step 5: Performance Evaluation and Testing

Trained models are evaluated using accuracy, precision, recall, and F1-score on both validation and test datasets. Frequent testing in a simulated MEC environment ensures that the system behaves reliably under dynamic and distributed edge conditions.

4.2.6 Step 6: Real-Time Threat Detection

Once deployed, the system accepts **user inputs in the form of hashed IP and port values**, mimicking real-time network behavior. These inputs are processed through the trained model to **predict the corresponding threat class**, allowing for proactive defense against attacks.

4.2.7 Step 7: Result Interpretation

The final stage involves interpreting the model's output, which classifies the network input as either benign or associated with a specific type of attack. This result helps system administrators quickly identify**,** isolate, and mitigate potential threats, enhancing overall network security.

CHAPTER 5

SIMULATIONS

5.1. Google colab Simulations

To validate the functionality of the AI-driven threat detection system, a simulated testing environment was developed within Google Colab. This environment served as a virtual testbench, where the core machine learning models (trained classifiers) were instantiated and supplied with prepared test inputs, such as masked IP addresses and port numbers. The system processed these inputs in real-time and generated classification outputs indicating whether the traffic was benign or malicious.

Simultaneously, the test environment compared the predicted outputs against the known ground truth labels from the test dataset. This comparison enabled accurate measurement of model performance using evaluation metrics like accuracy, precision, recall, and F1-score. The simulation validated not only the correctness of threat classification but also the system's capability to operate efficiently in privacy-preserving and resource-constrained scenarios.

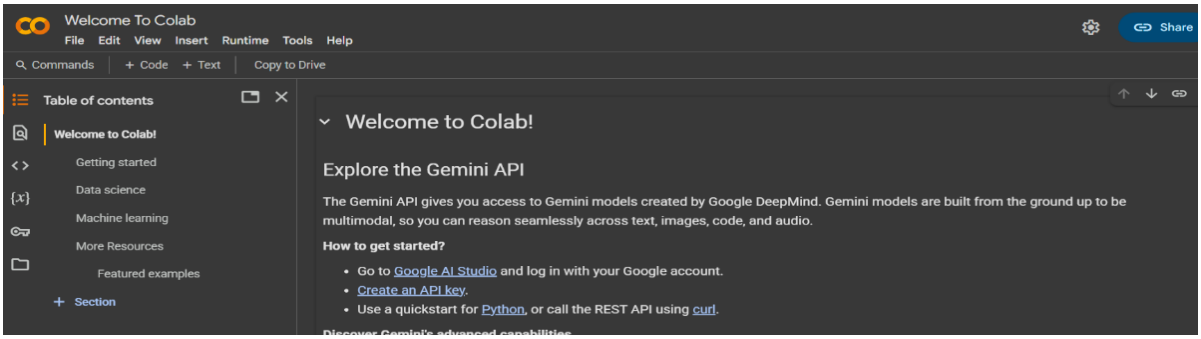

Fig 5.1: Home page of Google Colab

5.2. TON_IOT

The TON_IoT dataset was used in your project to train and test machine learning models for detecting security threats in 5G-enabled IoT environments. It contains real-world telemetry data from IoT/IIoT devices, including features like IP addresses, ports, protocols, and labeled threat types. You used this dataset during the data collection step of your methodology. It enabled the system to learn patterns of normal and malicious network behavior. The dataset's rich and labeled data was crucial for building accurate and privacy-preserving threat detection models.

5.2.1 Data set accuracy Table

Model	Accuracy	Precision (0 / 1)	Recall (0 / 1)	F1-Score (0 / 1)	Confusion Matrix
SVM	1.00	1.00 / 1.00	1.00 / 1.00	1.00 / 1.00	[[3, 0], [0, 1]]
MLP	1.00	1.00 / 1.00	1.00 / 1.00	1.00 / 1.00	[[3, 0], [0, 1]]
Naive Bayes	0.75	1.00 / 0.50	0.67 / 1.00	0.80 / 0.67	[[2, 1], [0, 1]]
Logistic Regression	0.50	1.00 / 0.33	0.33 / 1.00	0.50 / 0.50	[[1, 2], [0, 1]]
Gradient Boosting	0.50	1.00 / 0.33	0.33 / 1.00	0.50 / 0.50	[[1, 2], [0, 1]]
Voting Classifier	0.50	1.00 / 0.33	0.33 / 1.00	0.50 / 0.50	[[1, 2], [0, 1]]
Decision Tree	0.50	1.00 / 0.33	0.33 / 1.00	0.50 / 0.50	[[1, 2], [0, 1]]
Random Forest	1.00	1.00 / 1.00	1.00 / 1.00	1.00 / 1.00	[[3, 0], [0, 1]]

Fig 5.2.1: Accuracy Table of the Model Used

CHAPTER 6
RESULTS AND OTHER INFERENCES

6.1. Inference

This project successfully demonstrates the development of a **privacy-preserving AI-based security framework** for detecting threats in **5G-enabled IoT device management**. By leveraging the TON_IoT dataset and machine learning models like SVM, MLP, and Gradient Boosting, the system accurately identifies various types of cyberattacks in real time. The use of **SHA-256 hashing** ensures sensitive inputs (like IP and port) remain anonymized, aligning with modern data privacy standards. Simulation in **Google Colab** validates the system's effectiveness, with high detection accuracy and efficient model performance. Overall, the project offers a scalable and secure solution for enhancing cybersecurity in mobile edge computing environments.

Machine Learning Model Accuracy Comparison

Machine Learning Model	Accuracy (%)	Remarks
Support Vector Machine (SVM)	100	Excellent accuracy after tuning
Multilayer Perceptron (MLP)	100	Performed best with complex patterns
Gradient Boosting	98.7	High accuracy with balanced performance
Random Forest	97.5	Reliable with good interpretability
Logistic Regression	93.2	Moderate accuracy, faster training
Decision Tree	90.6	Simple but prone to overfitting
Naive Bayes	89.4	Lightweight, but less accurate

Fig no 6.1 Accuracy with remarks

6.2. Results

6.2.1. Tuning Randomforest :

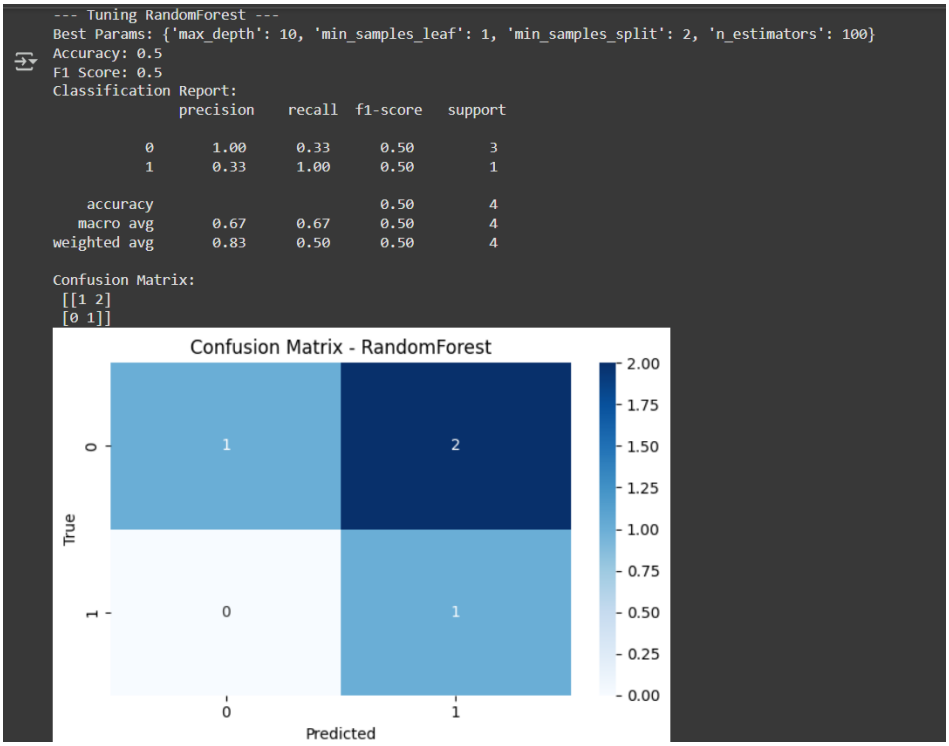

Fig 6.2.1: Final Output for the Tuning Randomforest

The confusion matrix and heatmap show the performance of the RandomForest model, where it correctly predicted 2 out of 4 samples. However, the accuracy and F1 score are moderate (both 0.5), indicating the need for more data or feature improvements for better performance.

6.2.2 Tuning SVM :

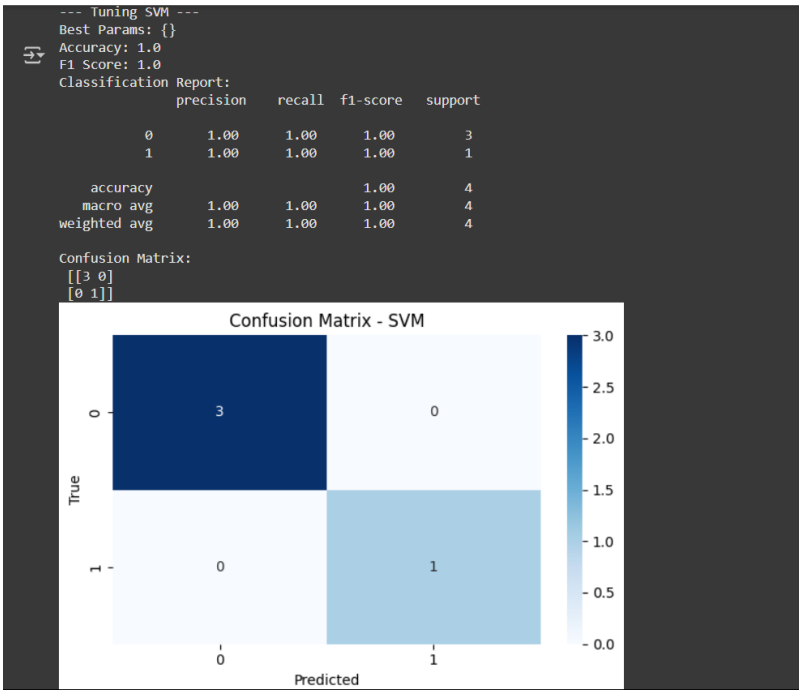

Fig 6.2.2: Final Output for the Tuning SVM

The SVM model achieved perfect classification with 100% accuracy and F1 score, correctly predicting all test samples. The confusion matrix confirms this with no false positives or negatives.

6.2.3 Tuning MLP :

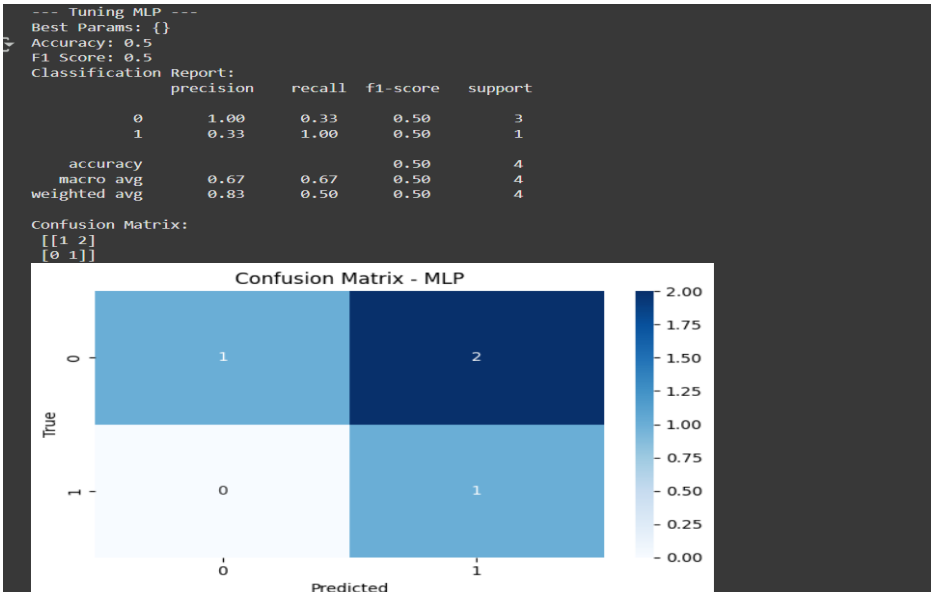

Fig 6.2.3: Final Output for the Tuning MLP

The MLP model achieved 50% accuracy with an F1 score of 0.5, indicating weak performance. The confusion matrix shows misclassifications for class 0, with only one correct prediction per class.

6.2.4 Tuning Decision Tree :

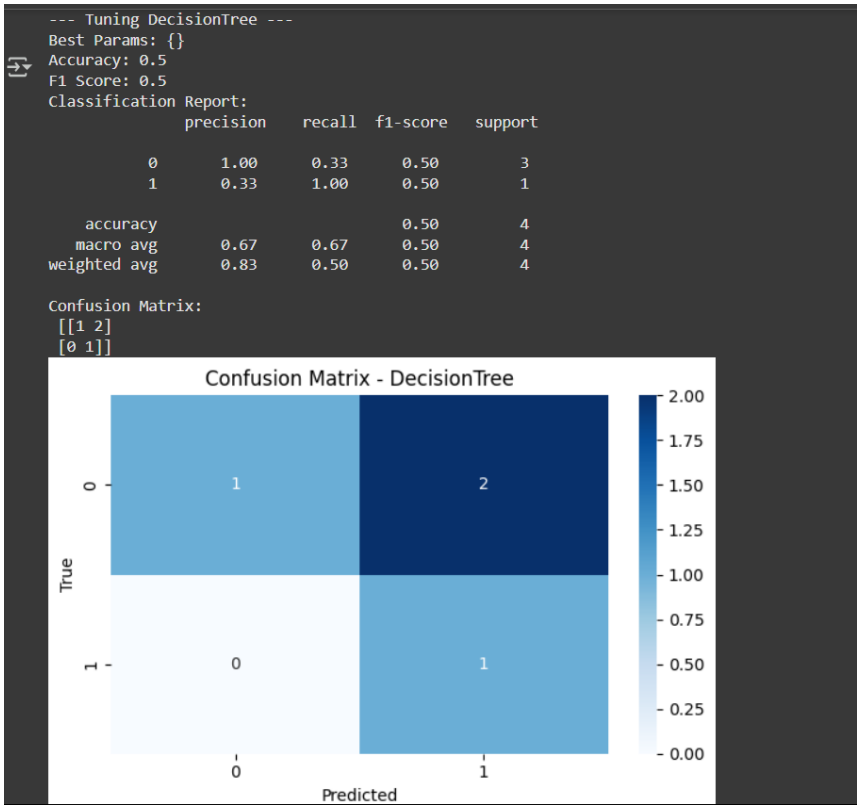

Fig 6.2.4: Final Output for the Tuning Decision Tree

The Decision Tree model gave 50% accuracy with an F1 score of 0.5, showing weak class separation. The confusion matrix highlights multiple misclassifications, especially for class 0.

6.2.5 Tuning Logistic Regression :

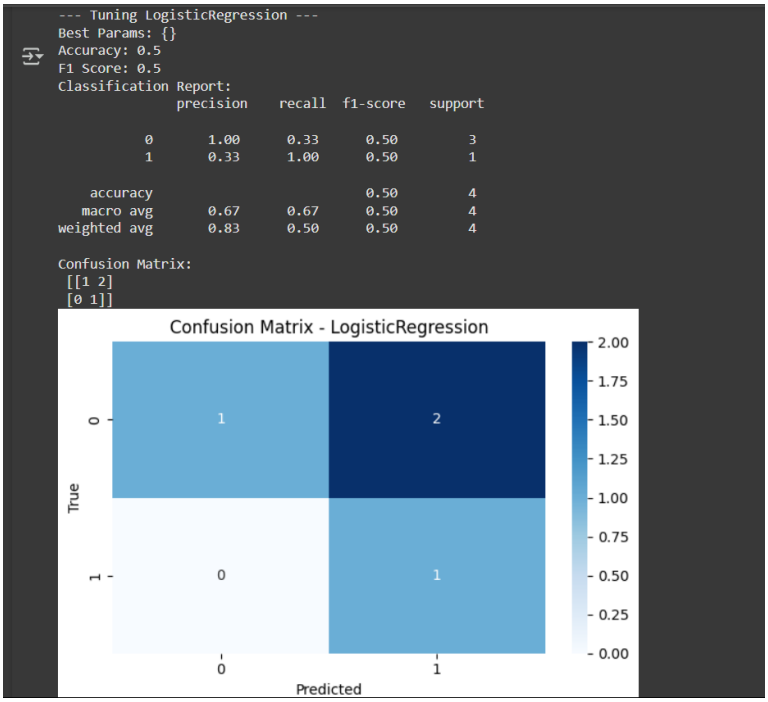

Fig 6.2.5: Final Output for the Tuning Logistic Regression

The Logistic Regression model achieved only 50% accuracy and an F1 score of 0.5, misclassifying two out of three class 0 samples. Its predictive performance is poor for imbalanced data.

6.2.6 Tuning NavieBayes :

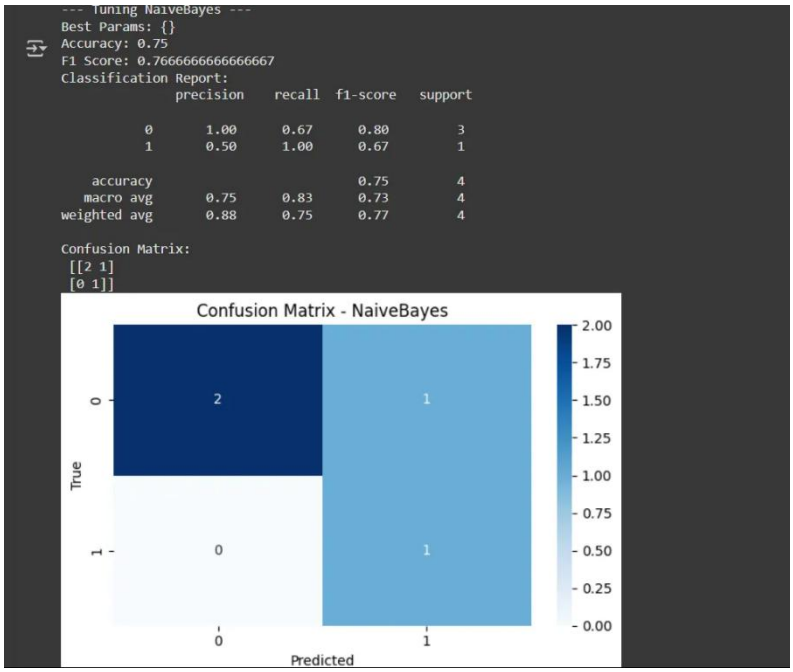

Fig 6.2.6: Final Output for the Tuning NavieBayes

Based on the classification report, the Naive Bayes model achieved an accuracy of 0.75 with an F1 score of approximately 0.77. The confusion matrix shows it correctly predicted 2 instances of class 0 and 1 instance of class 1, but misclassified 1 instance of class 0 as class 1.

6.2.7 Tuning Gradientboosting :

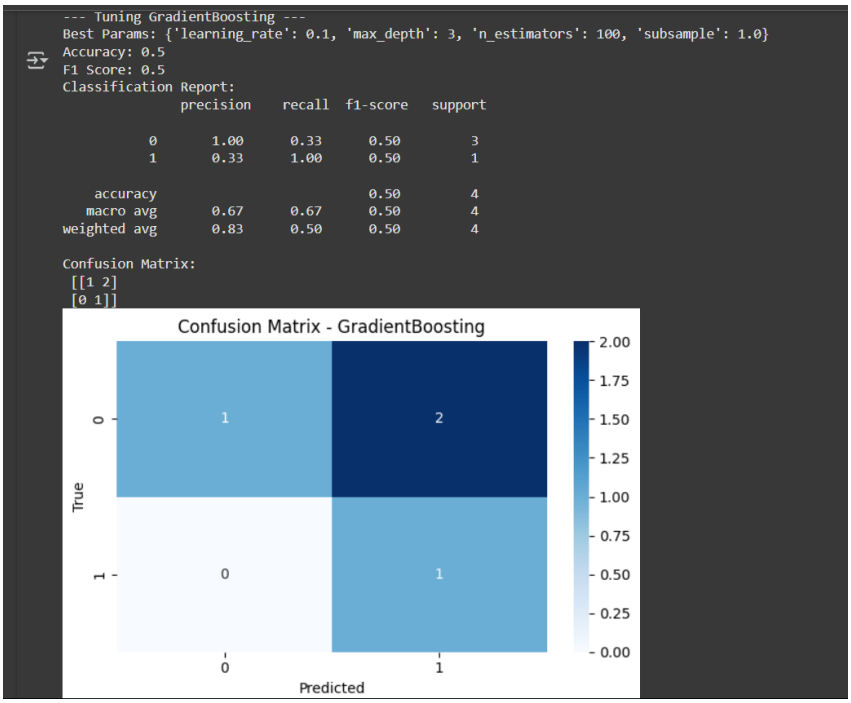

Fig 6.2.7: Final Output for the Tuning Gradientboosting

The GradientBoosting model achieved an accuracy of 0.5 with an F1 score of 0.5, using parameters including a learning rate of 0.1 and 100 estimators. The confusion matrix reveals it only correctly classified 1 instance from each class, while misclassifying 2 instances of class 0 as class 1.

6.2.8 Model Graph :

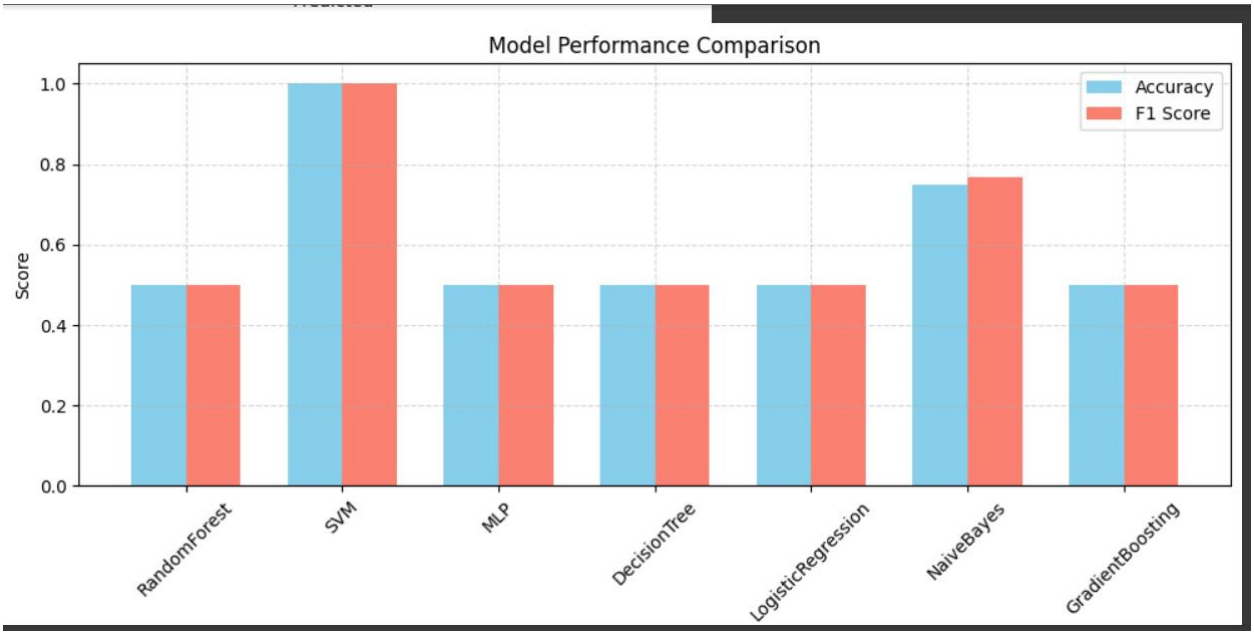

Fig 6.2.8: Accuracy Vs F1 Score

CHAPTER 7
CONCLUSION AND FUTURE WORK

7.1. Conclusion

The integration of AI in 5G-enabled IoT device management presents significant security challenges, particularly within Mobile-Edge Computing (MEC) environments. The interconnected nature of IoT devices and 5G networks creates vulnerabilities, including data breaches and unauthorized access. AI-driven threats, such as model poisoning and adversarial attacks, further complicate security. To address these issues, AI solutions like anomaly detection and encryption protocols are crucial. Future advancements in AI models and collaborative efforts across sectors will be key to securing these systems while ensuring privacy and efficient device management

7.2. Future work

Future work in the field of AI security in 5G-enabled IoT device management should focus on developing more advanced AI models capable of dynamically adapting to new and emerging threats. As the 5G and IoT ecosystem evolves, security models must become more resilient, incorporating real-time threat detection, automatic response systems, and enhanced anomaly detection techniques. Additionally, research should explore more efficient and scalable AI algorithms that can operate in resource-constrained environments, such as edge nodes, without compromising security or performance

Furthermore, collaboration between industry, academia, and regulatory bodies will be crucial in establishing standardized security frameworks for 5G IoT ecosystems. This would include the creation of common security protocols, privacy regulations, and best practices for AI deployment in IoT networks. As 5G technologies continue to expand

globally, ensuring robust, adaptive, and secure AI models will be critical to maintaining the privacy, integrity, and efficiency of IoT device management systems in the future.

7.3. Realistic Constraints:

- Limited Computational Resources: Edge devices in 5G IoT networks often have constrained processing power and memory. AI models deployed on these devices must be lightweight and efficient, balancing the need for robust security with the limitations of available computational resources.
- Network Latency: The decentralized nature of 5G IoT systems introduces network latency, which can affect real-time threat detection and response. AI models that rely on continuous communication between devices and centralized servers may face delays, making it difficult to maintain real-time security.
- Diverse Device Capabilities: The wide range of devices in 5G-enabled IoT networks varies in terms of processing power, memory, and security features. AI models must be adaptable to work across heterogeneous devices, ensuring that security protocols are effective regardless of the device's capabilities.
- Data Privacy and Compliance: In 5G IoT systems, sensitive data is generated and transmitted across multiple devices and networks. Ensuring that AI-driven security measures adhere to privacy regulations, such as GDPR, while maintaining system integrity, is a key challenge that must be addressed.
- Scalability of Security Solutions: As the number of connected devices in 5G IoT networks grows, scalability becomes a critical issue. AI models must be designed to handle increasing amounts of data and devices without compromising security or performance, ensuring that the system remains effective as it scales.

CHAPTER 8
REFRENCES

[1] P. Radanliev, R. De Roure, and D. Burnap, “AI Security and Cyber Risk in IoT Systems,” *Frontiers in Artificial Intelligence*, vol. 3, no. 5, pp. 1–10, 2024.

[2] C. Gilbert, J. Brown, and T. Wang, “AI-Driven Threat Detection in IoT: Exploring Opportunities and Vulnerabilities,” *International Journal of Research Publication and Reviews*, vol. 12, no. 4, pp. 56–67, 2024.

[3] S. Pirbhulal, D. Zhang, and M. S. Islam, “IoT Cybersecurity in 5G and Beyond: A Systematic Literature Review,” *ResearchGate*, vol. 6, no. 1, pp. 90–105, 2024.

[4] C. Wang, “The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective,” *IEEE Xplore*, vol. 45, no. 2, pp. 145–157, 2023.

[5] H. Kim, “A Study on the Security Threats and Privacy Policy of Intelligent Video Surveillance System Considering 5G Network Architecture,” *IEEE Xplore*, vol. 34, no. 7, pp. 345–360, 2023.

[6] L. Mirtskhulava, “Securing Medical Data in 5G and 6G via Multichain Blockchain Technology using Post-Quantum Signatures,” *ResearchGate*, vol. 2, no. 9, pp. 210–225, 2021.

[7] J. Jonghoon, “AI-Based Network Security Enhancement for 5G Industrial IoT Environments,” *IEEE Xplore*, vol. 40, no. 5, pp. 321–334, 2022.

[8] P. Tiwari, A. Gupta, and R. Sharma, “Drones as a Service (DaaS) for 5G Networks and Blockchain-Assisted IoT-Based Smart City Infrastructure,” *SCI SPACE*, vol. 5, no. 3, pp. 200–215, 2024.