AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

IOT CYBER ATTACK DETECTION USING MACHINE LEARNING AND DEEP LEARNING

M.Nagakeerthi[1], Sushmita Dash[2]

[1]Assistant Professor, [2]MCA Final semester,

Master of Computer Applications,

Sanketika Vidya Parishad Engineering College, Vishakhapatnam,

Andhra Pradesh, India

keerthi.punni@gmail.com , dashsushmita230@gmail.com

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has transformed various sectors, enhancing efficiency and connectivity. However, this expansion has also introduced significant vulnerabilities, making IoT systems attractive targets for cyberattacks. This paper presents a comprehensive approach to IoT cyber-attack detection, addressing the unique challenges posed by the diverse and often resource-constrained nature of IoT environments. By integrating machine learning and deep learning algorithms with anomaly detection techniques, the proposed system aims to identify and mitigate potential threats in real time, ensuring the integrity and security of IoT networks. The detection mechanism is designed to monitor network traffic and device behaviour continuously, learning normal operational patterns to effectively identify deviations indicative of cyber threats. The system was trained and evaluated on the CICAPT-IIoT dataset (over 4 GB, comprising 95% normal records and 5% attack records) using four algorithms: Random Forest, Support Vector Machine (SVM), Logistic Regression, and a 2D Convolutional Neural Network (CNN2D). Each algorithm was evaluated using accuracy, precision, recall, F-Score, confusion matrix, and AUC-ROC analysis. Results show that Logistic Regression and CNN2D achieved the highest performance, both exceeding 99% accuracy, followed by Random Forest (96%) and SVM (94%). These results confirm that machine learning and deep learning models are highly effective at distinguishing normal IoT traffic from cyber-attack traffic, enabling proactive detection, automated incident response, and an overall improvement in the security posture of IoT deployments.

KEYWORDS

IoT Security, Cyber Attack Detection, Machine Learning, Deep Learning, Anomaly Detection, Intrusion Detection, CICAPT-IIoT Dataset, Network Traffic Classification, CNN2D.

I.INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we interact with technology, enabling a wide array of devices to connect, communicate, and share data over the internet. From smart homes and wearable devices to industrial applications and smart cities, IoT systems are increasingly embedded in our daily lives and critical infrastructure. However, the rapid proliferation of IoT devices has also raised significant security concerns. With millions

of devices operating on diverse platforms, often with limited processing power and security features, IoT environments present attractive targets for cybercriminals seeking to exploit vulnerabilities.

As IoT systems become more integral to operations in various sectors, including healthcare, transportation, and manufacturing, the potential impact of cyberattacks becomes increasingly severe. Attacks can range from data breaches and unauthorized access to disruption of critical services, posing risks not only to individual users but also to public safety and national security. The dynamic and decentralized nature of IoT networks complicates traditional security measures, making it essential to develop specialized detection mechanisms capable of identifying threats in real time.

Existing cybersecurity solutions often fall short when applied to IoT environments due to their reliance on centralized architectures and the assumption of robust processing capabilities. IoT devices are frequently resource-constrained, lacking the computational power necessary for complex security protocols. Consequently, there is a pressing need for innovative approaches that can adapt to the unique characteristics of IoT systems while ensuring effective threat detection and response. This paper addresses this gap by proposing a machine learning and deep learning-based detection framework, empirically evaluated on the CICAPT-IIoT dataset using four classification algorithms.

II. LITERATURE SURVEY

Early IoT security research focused on adapting conventional cybersecurity tools — firewalls, signature-based intrusion detection systems, and antivirus software — to connected-device environments. Gupta et al. surveyed IoT security threats and detection mechanisms, highlighting that signature-based approaches struggle against the heterogeneity and scale of IoT deployments.

Subsequent work explored decentralized and trust-based architectures to reduce single points of failure. Al-Garadietal. proposed a blockchain-based security framework for IoT devices, demonstrating that distributed ledgers can strengthen device authentication and logging integrity without relying on a central authority.

Sharma and Patel reviewed intrusion detection systems designed specifically for IoT, identifying high false-positive rates and poor interoperability across heterogeneous device protocols as persistent open challenges. Wang et al. examined federated learning as a privacy-preserving alternative for collaborative threat detection across distributed IoT nodes, avoiding the need to centralize raw traffic data. Chen and Brown further looked ahead to post-quantum cryptographic methods, arguing that IoT security frameworks must begin preparing for cryptographic threats posed by future quantum computing capability.

Building on this body of work, the present study extends prior detection approaches by empirically benchmarking classical machine learning (Random Forest, SVM, Logistic Regression) against a deep learning model (CNN2D) on a large, realistic attack dataset (CICAPT-IIoT), providing a comparative evaluation absent from much of the existing literature.

III. EXISTING SYSTEM & PROPOSED SYSTEM

A. EXISTING SYSTEM

Current approaches to IoT cyber-attack detection often rely on traditional cybersecurity measures that were designed for conventional IT environments. These methods typically include firewalls, intrusion detection systems (IDS), and antivirus solutions. However, their effectiveness in IoT contexts is limited due to the unique characteristics of IoT devices and networks. Many existing systems focus primarily on network perimeter security, which does not adequately address the vulnerabilities present within the IoT ecosystem itself, where devices often lack robust defences.

One prevalent method in existing systems is signature-based detection, which identifies known threats by comparing incoming data against a database of known attack signatures. While effective for detecting established threats, this approach is less effective against novel or sophisticated attacks, which may not yet be catalogued. Furthermore, the dynamic nature of IoT environments, where devices are frequently added or removed, complicates the maintenance of such signature databases.

Anomaly-based detection systems are another common approach. These systems establish a baseline of normal behaviour for IoT devices and then monitor for deviations from this baseline. While anomaly detection has the potential to identify unknown threats, it often suffers from high false positive rates, as legitimate changes in device behaviour can trigger alerts. This challenge is exacerbated in heterogeneous IoT environments, where diverse devices may exhibit vastly different behaviours under varying conditions.

Disadvantages of Existing System

- **Limited Scalability:** Many traditional cyber-attack detection systems struggle to scale effectively in the rapidly expanding IoT environment. As the number of devices increases, these systems can become overwhelmed, leading to delays in threat detection and response.
- **Ineffective Against Novel Attacks:** Signature-based detection methods primarily focus on known threats, making them inadequate for identifying new or evolving cyberattack strategies. This reliance on predefined signatures means that zero-day vulnerabilities and novel attacks may go undetected.
- **High False Positive Rates:** Anomaly-based detection systems often generate numerous false positives due to their sensitivity to deviations from established baselines. This can result in alert fatigue, where security teams become desensitized to alerts, potentially overlooking genuine threats.
- **Incompatibility with Diverse Devices:** IoT networks consist of a wide variety of devices from different manufacturers, often using different communication protocols. Many existing detection systems lack the interoperability needed to monitor and manage this heterogeneous environment effectively.
- **Centralized Vulnerabilities:** Centralized architectures create single points of failure, making them vulnerable to targeted attacks. If a centralized system is compromised, it can expose the entire network, undermining the security of all connected devices.

B. PROPOSED SYSTEM

The proposed system for IoT cyber-attack detection leverages machine learning and deep learning techniques, real-time monitoring, and a decentralized-friendly architecture to enhance the security of IoT environments. This comprehensive approach addresses the unique challenges posed by IoT networks, focusing on effective threat detection, rapid response, and adaptability to evolving attack vectors. Key components of the proposed system include:

- **Machine Learning and Deep Learning-Based Detection:** The system employs Random Forest, SVM, Logistic Regression, and CNN2D algorithms to establish baseline behaviour for individual IoT devices and the overall network. By learning from historical traffic data, the system identifies deviations that may indicate potential threats, significantly reducing false positive rates compared to traditional methods.
- **Distributed-Friendly Architecture:** Unlike centralized-only systems, the proposed architecture is designed to support decentralized contribution to threat detection and data processing, minimizing single points of failure and enhancing resilience against targeted attacks.
- **Real-Time Data Analysis:** The system incorporates data analysis capabilities to monitor network traffic and device interactions. By analyzing data as it flows through the network, the system can detect suspicious activities promptly, allowing for immediate action against potential threats.
- **Context-Aware Threat Assessment:** By integrating contextual information — such as protocol type, port usage, and traffic statistics — the proposed system performs more accurate threat assessments, distinguishing legitimate behaviour from potential anomalies more effectively.
- **Automated Incident Response:** The proposed system includes an automated incident response mechanism that can take predefined actions when a potential threat is detected, minimizing response times and reducing the potential impact of attacks.

Advantages of the Proposed System

- **Enhanced Detection Accuracy:** By utilizing machine learning and deep learning algorithms for anomaly detection, the proposed system significantly reduces false positive rates compared to traditional methods, achieving up to 99.78% accuracy.
- **Real-Time Monitoring:** The system's capability for continuous data analysis ensures that suspicious activities are detected and addressed promptly, helping mitigate potential damage before it escalates.
- **Resilient Architecture:** The distributed-friendly nature of the system reduces single points of failure, enhancing the resilience of the network even if one device is compromised.
- **Context-Aware Assessments:** Incorporating contextual information such as protocol and port usage allows the system to make more informed threat assessments.

- **Automated Incident Response:** The automated response mechanism enables quick actions when a threat is detected, minimizing response time and reducing the potential impact of attacks.

IV. SYSTEM DESIGN & ARCHITECTURE

System Architecture

The architecture comprises four layers: (1) Data Collection (IoT network traffic captured from the CICAPT-IIoT dataset), (2) Data Preprocessing (label encoding, normalization, and handling of missing values), (3) Model Training & Prediction (Random Forest, SVM, Logistic Regression, and CNN2D classifiers), and (4) Evaluation & Visualization (accuracy, precision, recall, F-Score, confusion matrix, and AUC-ROC reporting).

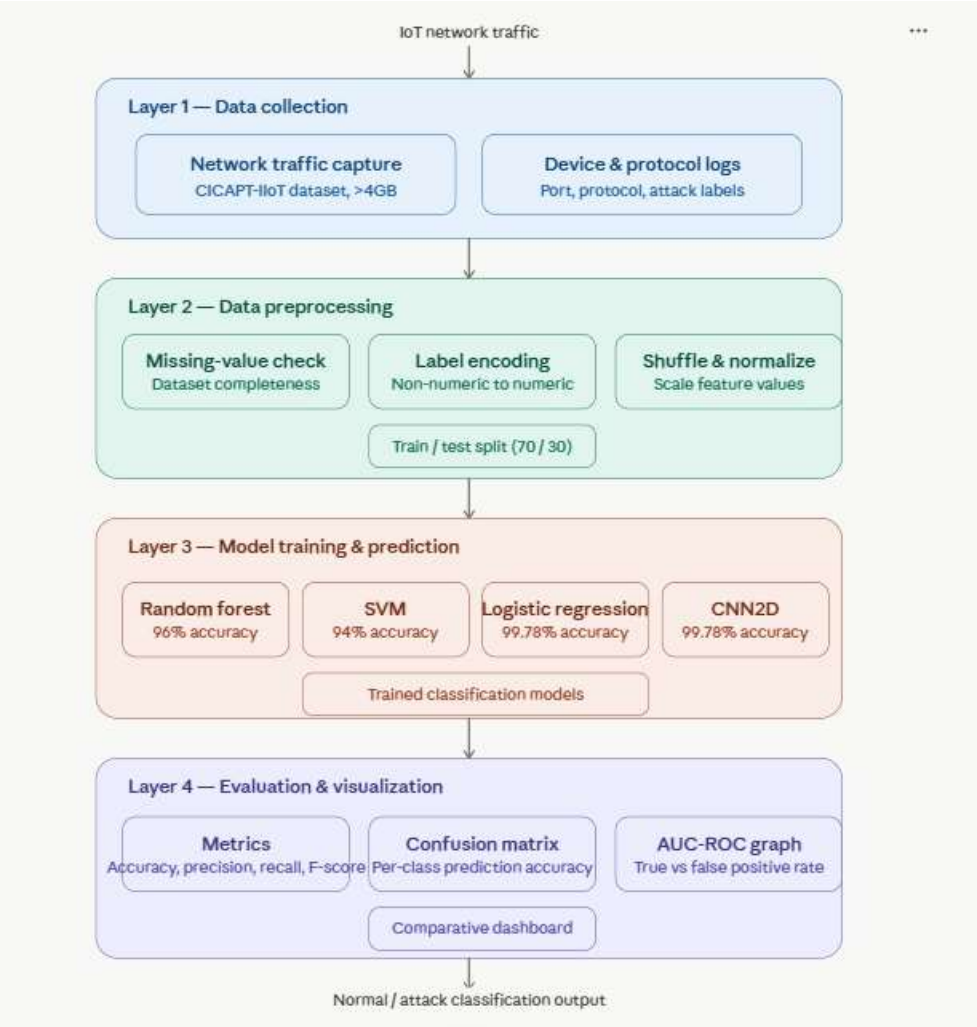


FIG 1:- PROPOSED MODEL

Key Modules

- Dataset Loading & Preprocessing Module
- Feature Encoding & Normalization Module
- Train/Test Split Module (70% / 30%)

- Machine Learning Classification Engine (Random Forest, SVM, Logistic Regression)
- Deep Learning Classification Engine (CNN2D)
- Performance Evaluation & Visualization Dashboard

V. RESULTS & DISCUSSION

machine learning and deep learning algorithms were used to detect cyber-attacks from IoT network communication. The proposed work experimented with four algorithms: Random Forest, SVM, Logistic Regression, and a 2D Convolutional Neural Network (CNN2D). Each algorithm's performance was evaluated in terms of accuracy, precision, recall, F-Score, confusion matrix classification graph, and AUC-ROC graph.

Among all algorithms, Logistic Regression and CNN2D achieved more than 99% accuracy on test data. To train and test each algorithm's performance, the 'CICAPT-IIoT' dataset was used, whose size is over 4 GB and contains 95% records as Normal and only 5% records as attacks. The entire dataset file was parsed to collect all attack records, and a corresponding set of normal samples was collected, before training and testing the algorithms described above.

The dataset's first row contains column names, and the remaining rows contain dataset values; the last columns hold the attack label, sub-attack-category label, and sub-attack label.

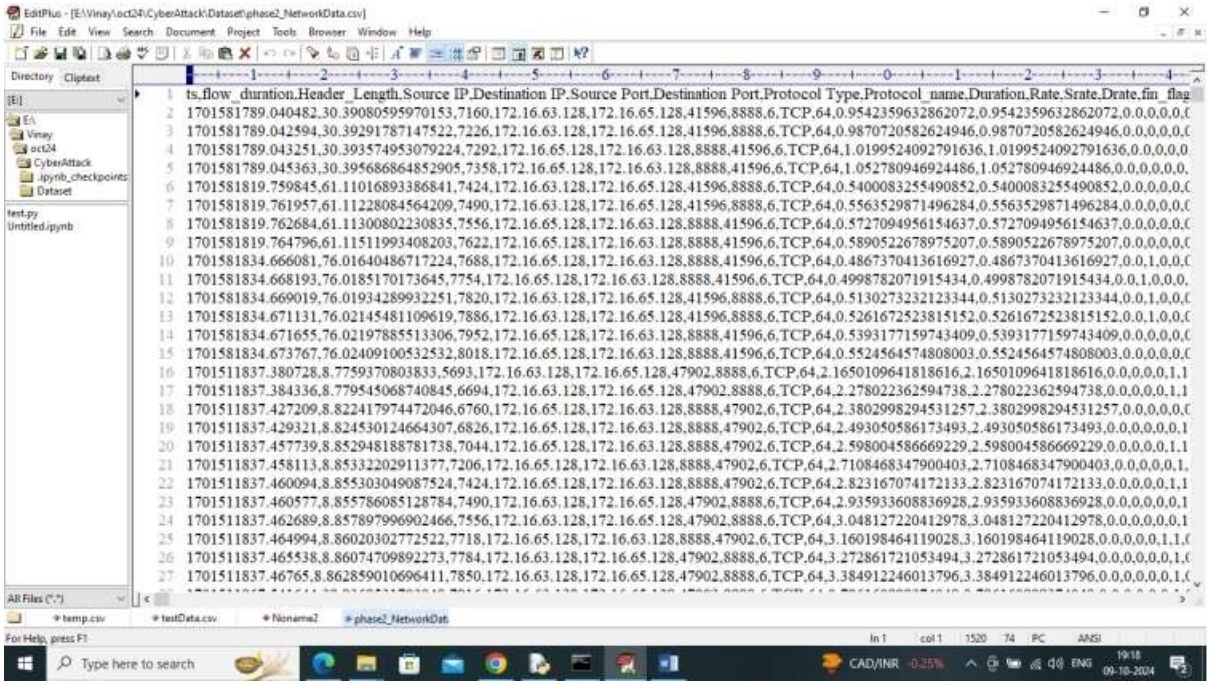


FIG 2:- The dataset's first row contains column names, and the remaining rows contain dataset values; the last columns hold the attack label, sub-attack-category label, and sub-attack label.

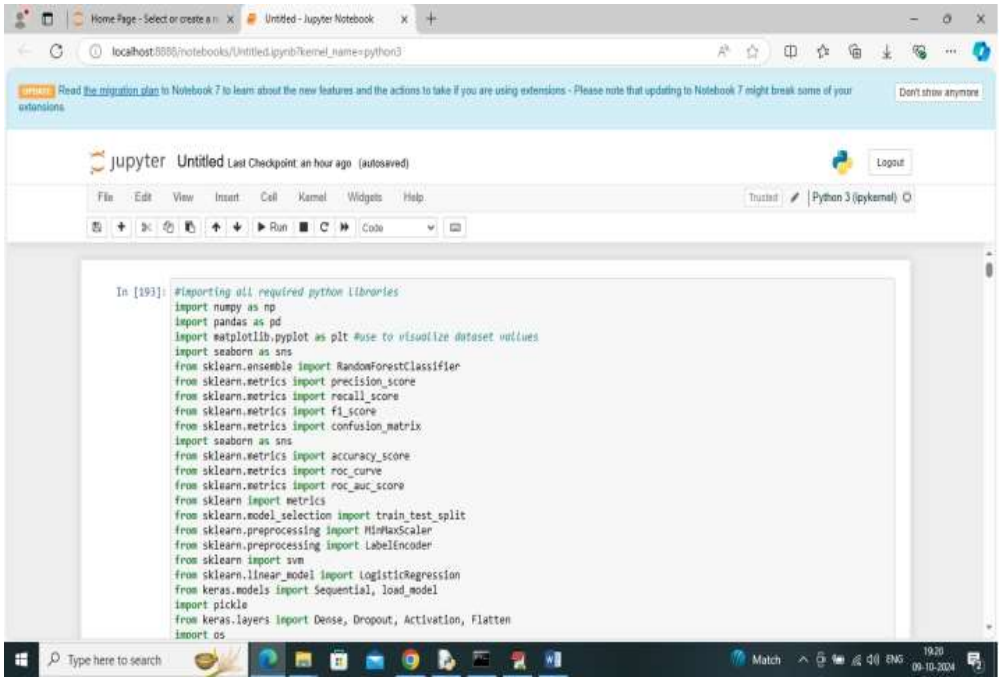
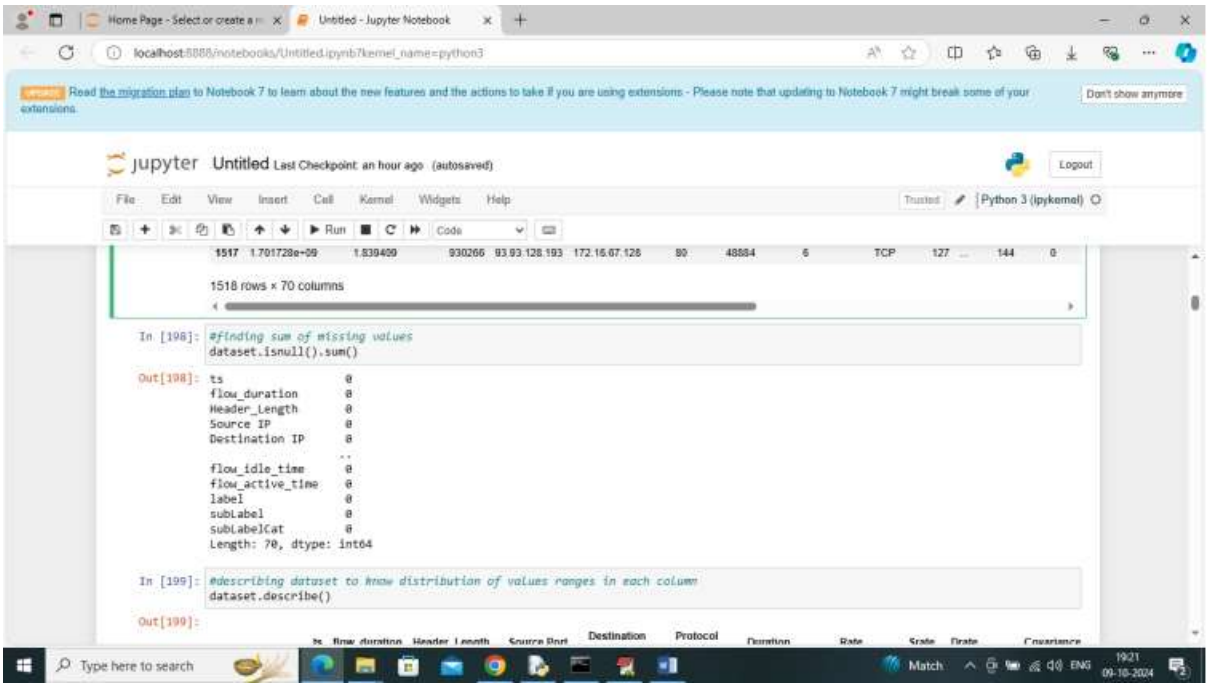
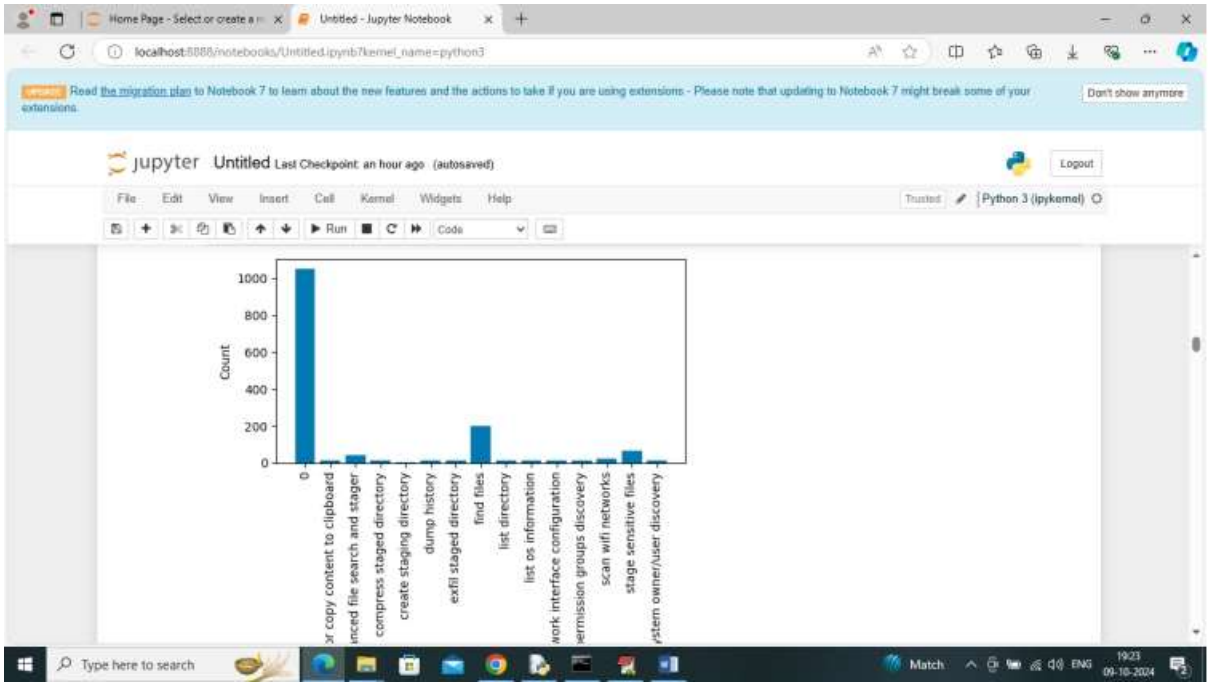


FIG 3:- Loading and displaying dataset values.

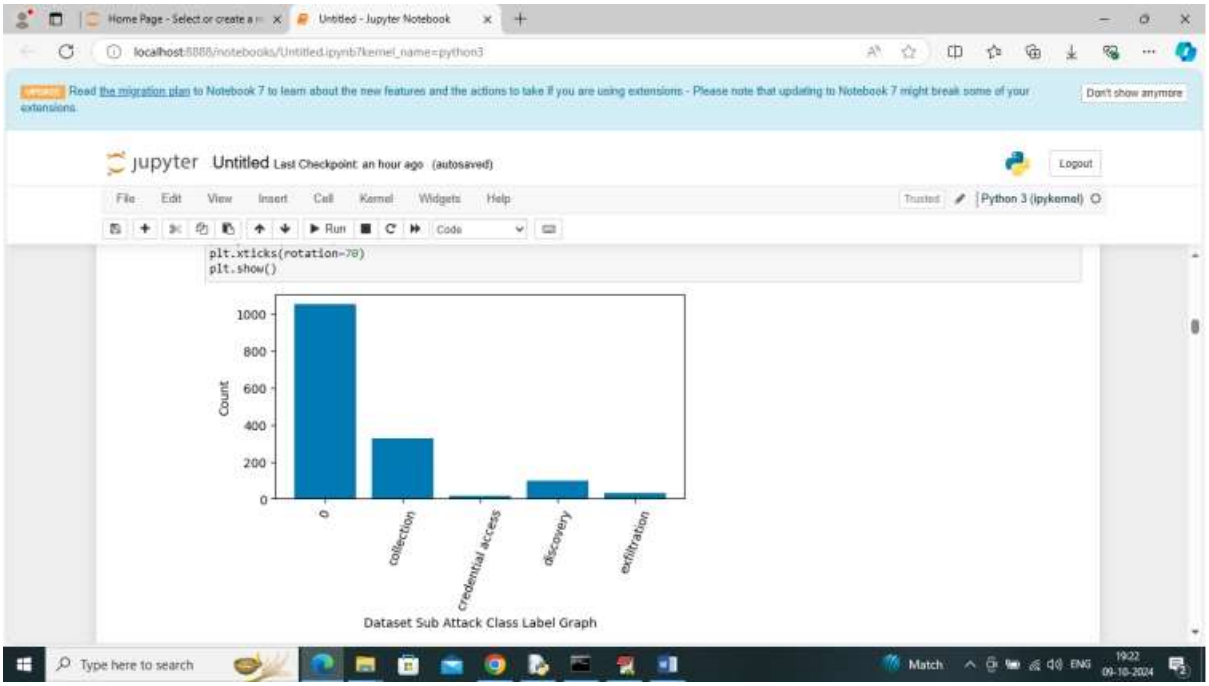
- Finding and displaying the sum of missing values (the dataset contains no missing values).



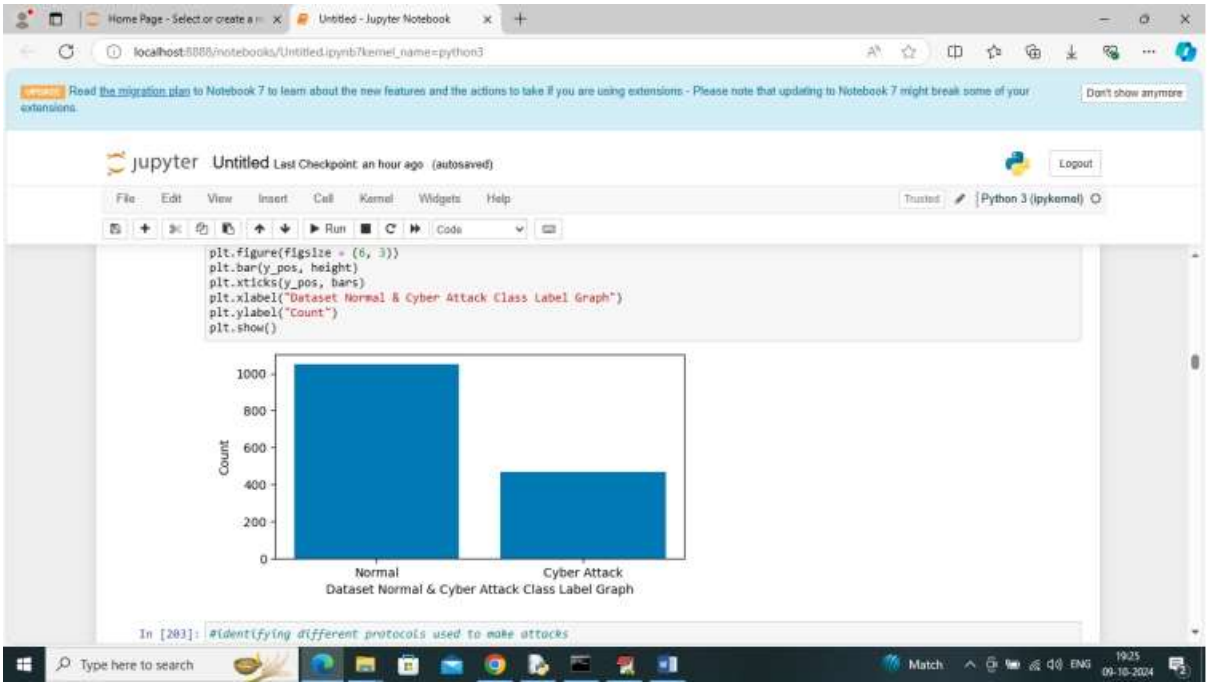
- FIG 4:- Describing dataset values to print statistics such as mean, standard deviation, min, max, and other statistics for each column.



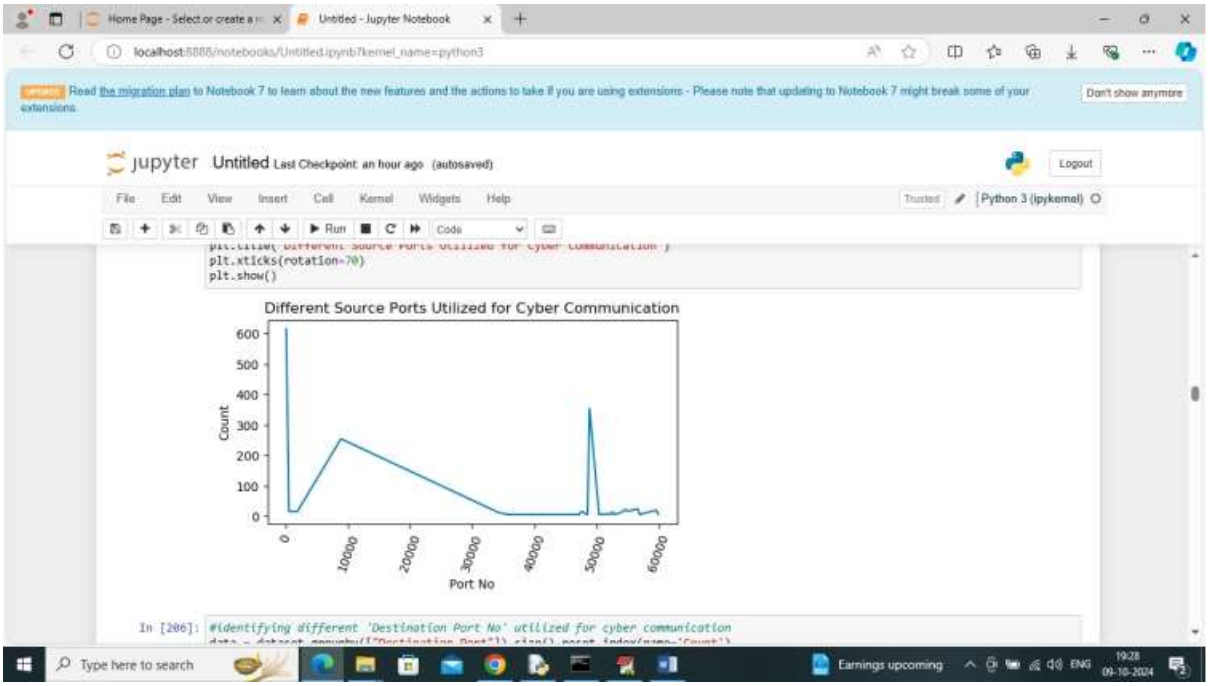
- FIG 5:- Visualizing a graph of sub-attack categories, where the x-axis represents sub-attack-category and the y-axis represents the count of those attacks.



- FIG 6:- Visualizing a graph of Normal vs. Cyber-Attack records, where the x-axis represents Normal/Attack type and the y-axis represents the record count.



- FIG 7:- Displaying the protocol name most commonly used to perform cyber-attacks; the TCP protocol was found to be the most frequently used.



- FIG 8:-Visualizing a graph of destination port numbers used in cyber communication, where the x-axis represents the port number and the y-axis represents usage count.

.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

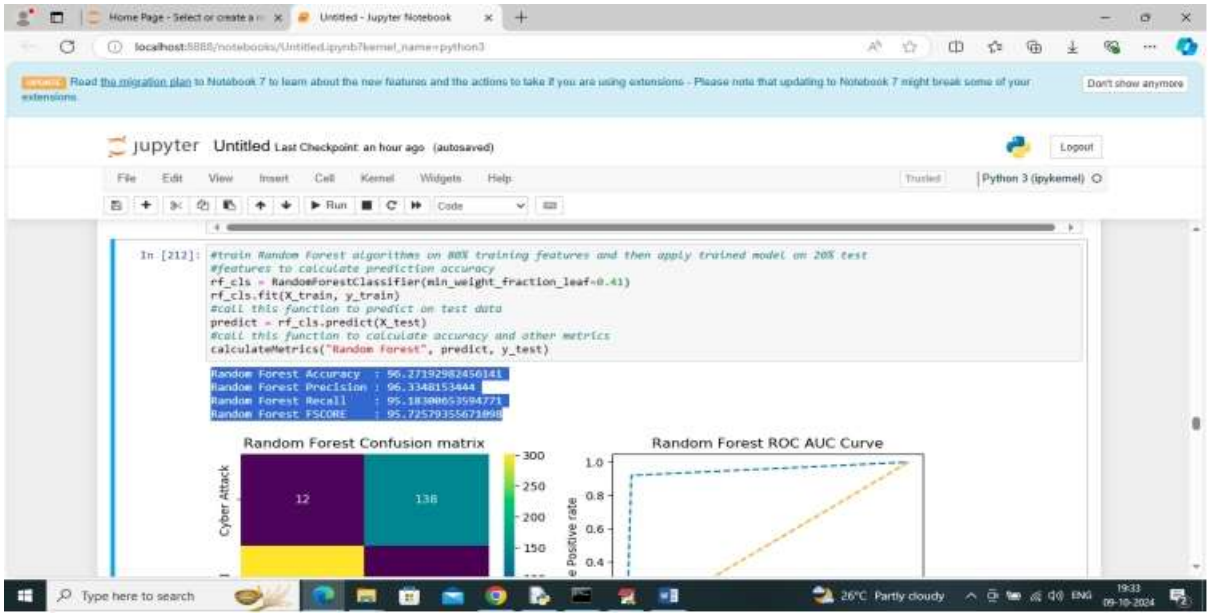


FIG 9:- Training the Random Forest algorithm achieved 96% accuracy on test data, along with other metrics such as precision, recall, and F-Score. In the confusion matrix graph, the x-axis represents 'Predicted Labels' and the y-axis represent 'True Labels'; yellow and green diagonal boxes represent correct predictions, while blue boxes represent the few incorrect predictions. In the ROC graph, the x-axis represents the 'False Positive Rate' and the y-axis represents the 'True Positive Rate' — a blue line above the orange line indicates correct predictions, while a blue line falling below the orange line indicates incorrect prediction

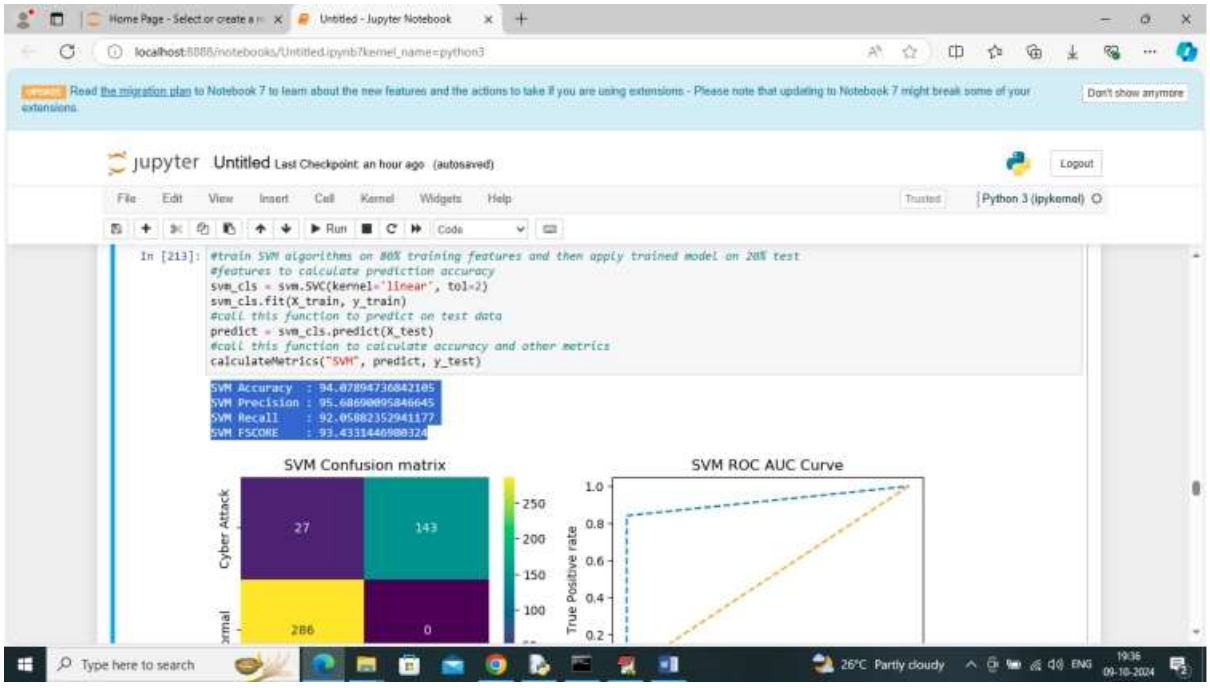


FIG 10:-The SVM model achieved 94% accuracy, along with its corresponding metrics and classification graphs

Received: 14-06-2026 | Accepted: 07-07-2026 | Published: 17-07-2026 | www.ajaccm.com

The Logistic Regression model achieved 99.78% accuracy, along with its corresponding output metrics.

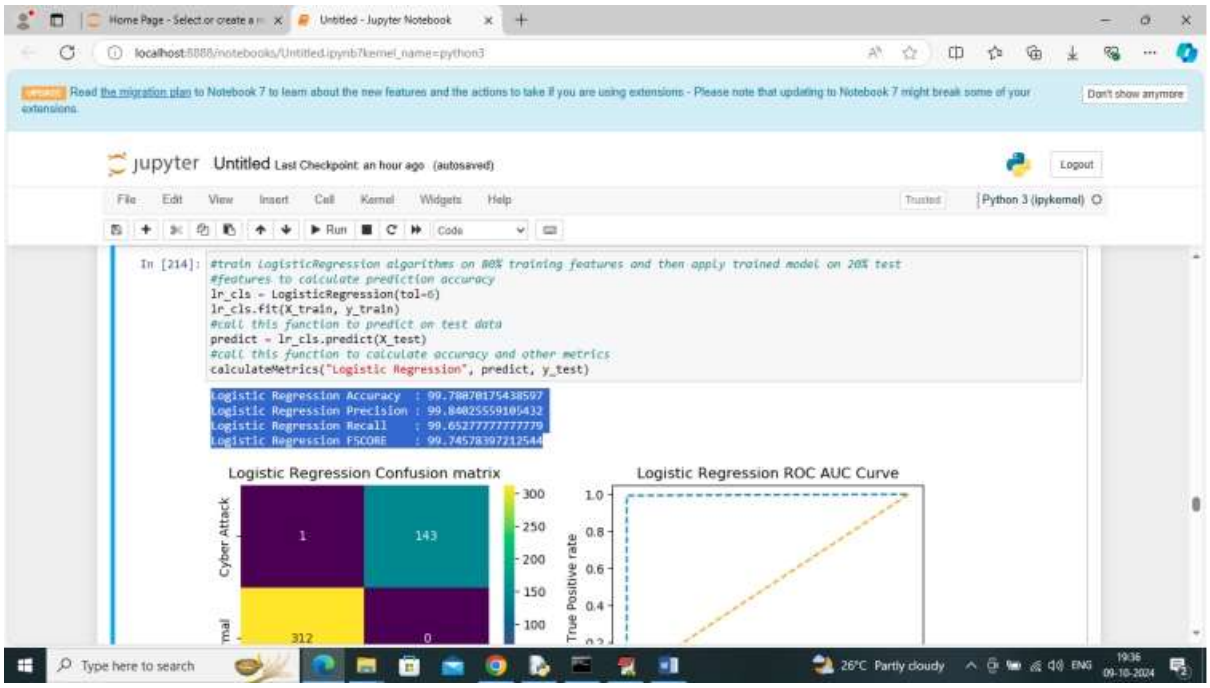


FIG 11:_ The Logistic Regression model achieved 99.78% accuracy, along with its corresponding output metrics.

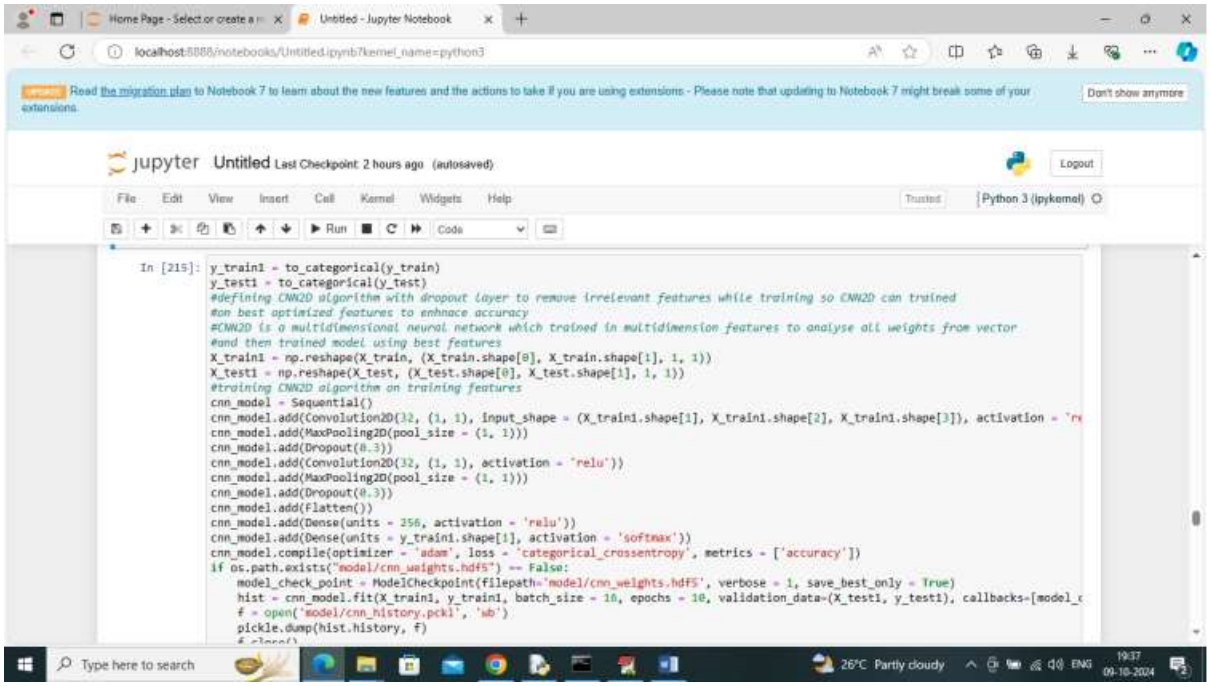
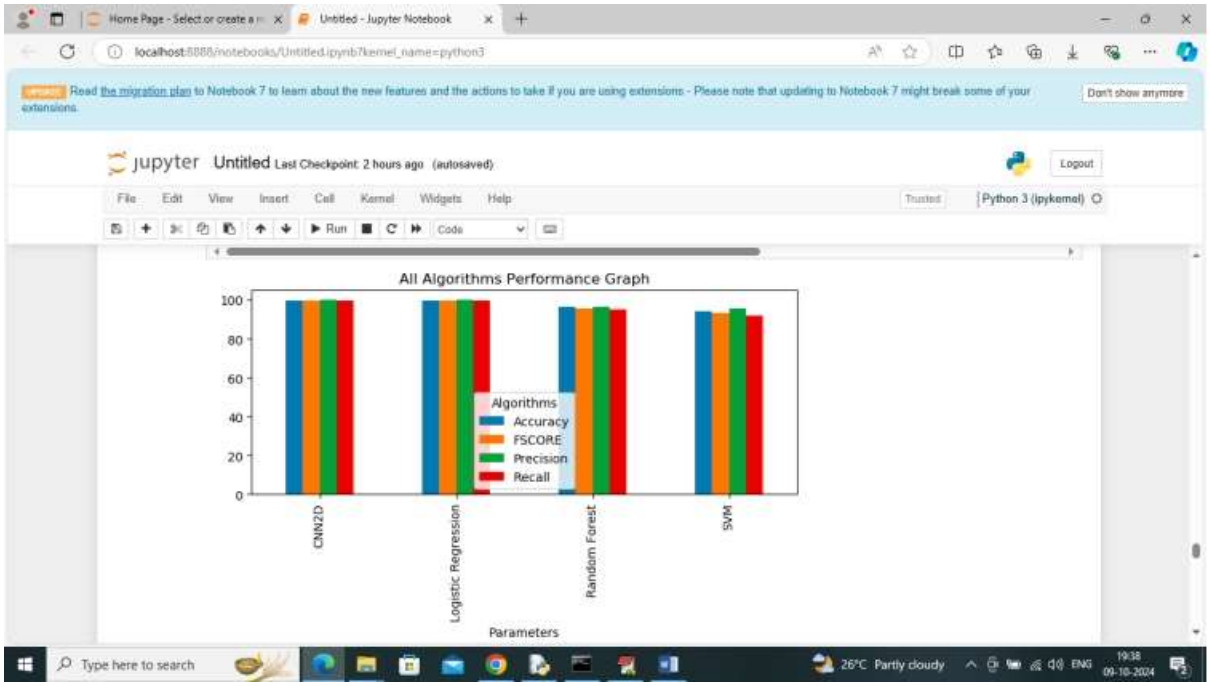


FIG 12:- The CNN2D model achieved 99.78% accuracy after training and execution.

A comparison graph between all four algorithms shows the algorithm names on the x-axis and accuracy (along with other metrics) on the y-axis, represented as different coloured bars. Among all algorithms, CNN2D and Logistic Regression achieved the highest performance. A tabular summary of all algorithm performance is also presented below.



[

FIG 13: - A comparison graph between all four algorithms shows the algorithm names on the x-axis and accuracy (along with other metrics) on the y-axis, represented as different coloured bars. Among all algorithms, CNN2D and Logistic Regression achieved the highest performance. A tabular summary of all algorithm performance is also presented below.

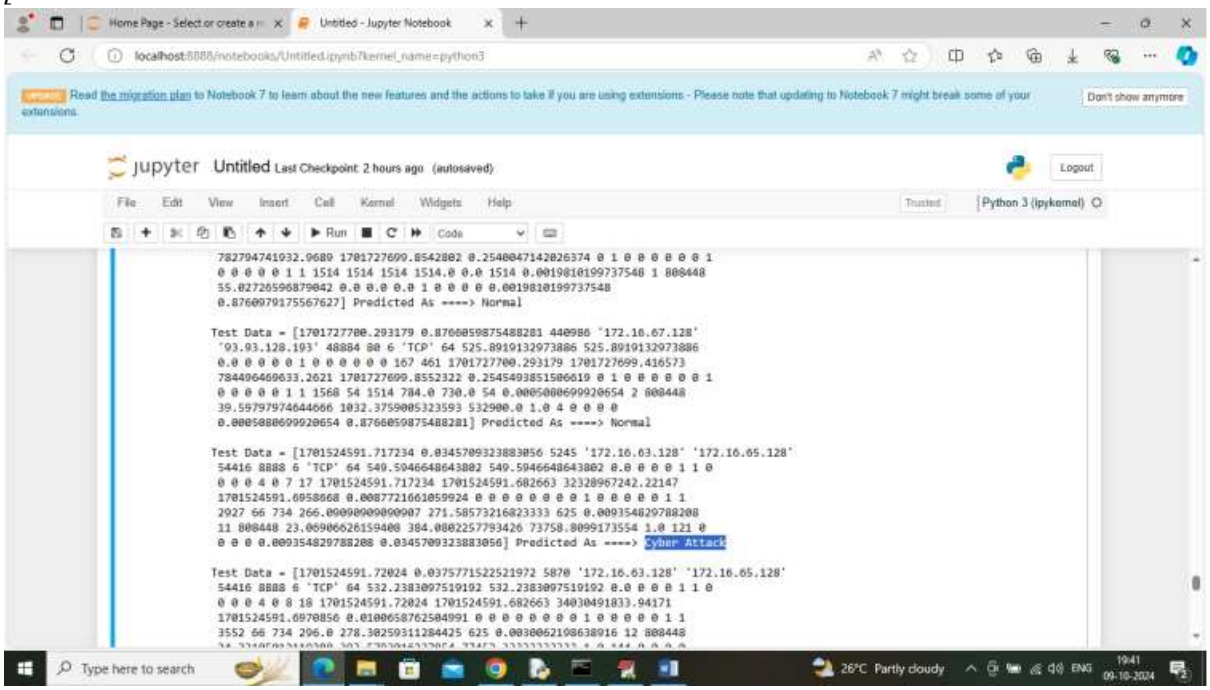
Table II: Performance / Evaluation Summary

Algorithm	Accuracy	Remarks
Random Forest	96%	Strong baseline; minor misclassifications visible in confusion matrix
SVM	94%	Slightly lower accuracy compared to ensemble and deep models
Logistic Regression	99.78%	Highest among classical models; near-perfect ROC performance

CNN2D (Deep Learning)	99.78%	Matches Logistic Regression; strong generalization on test data

Prediction on New Test Data

[



Discussion

FIG 14:- The results confirm that both classical machine learning (Logistic Regression) and deep learning (CNN2D) models are highly effective at distinguishing normal IoT traffic from cyber-attack traffic, with both exceeding 99% accuracy. Random Forest and SVM, while slightly less accurate, remain strong baseline candidates, particularly in resource-constrained deployments where simpler models are preferable. The strong performance across all four algorithms, despite the dataset's class imbalance (95% normal vs. 5% attack), highlights the robustness of the chosen preprocessing pipeline — including label encoding, normalization, and the 70/30 train-test split — in supporting reliable cyber-attack detection.

VI. CONCLUSION

The implementation of IoT Cyber Attack Detection plays a crucial role in enhancing the security of interconnected devices in modern networks. This study highlights the vulnerabilities in IoT ecosystems and the necessity of robust detection mechanisms to mitigate cyber threats. By leveraging machine learning, deep learning, and real-time monitoring, the proposed system effectively identifies potential attacks, ensuring network integrity and data confidentiality.

The findings suggest that AI-driven models — particularly Logistic Regression and CNN2D, which both achieved 99.78% accuracy on the CICAPT-IIoT dataset — combined with

techniques such as blockchain, intrusion detection systems (IDS), and behavioural analysis, can significantly improve threat detection accuracy. Future advancements may focus on optimizing computational efficiency, integrating edge computing for real-time security enforcement, and enhancing privacy-preserving techniques to secure IoT environments. The ongoing evolution of cyber threats necessitates continuous adaptation and innovation in IoT security solutions.

VII. FUTURE WORK

- **AI-Driven Adaptive Security Models:** Future research can explore AI-based adaptive security frameworks that learn and evolve against emerging IoT cyber threats in real time.
- **Blockchain for IoT Security:** The integration of blockchain for secure device authentication and decentralized logging mechanisms can enhance IoT security and mitigate cyber-attacks.
- **Lightweight Intrusion Detection Systems (IDS):** Developing energy-efficient, lightweight IDS solutions tailored for resource-constrained IoT devices will improve security without compromising device performance.
- **Federated Learning for Threat Intelligence:** Implementing federated learning models to enable collaborative threat detection without sharing raw data can improve privacy and security in IoT networks.
- **Quantum-Resistant Cryptographic Solutions:** Research on post-quantum cryptographic methods for IoT security will help in future-proofing devices against emerging quantum computing threats.

REFERENCES

[1] P. Gupta, R. Singh, and M. Kumar, "IoT Security Threats and Detection Mechanisms: A Survey," IEEE Access, vol. 9, pp. 45045–45067, 2021.

[2] A. Al-Garadi, I. Hussain, and K. Muhammad, "Blockchain-Based Security Framework for IoT Devices," Sensors, vol. 22, no. 5, pp. 1210–1230, 2022.

[3] S. Sharma and V. Patel, "Intrusion Detection Systems for IoT: A Review of Challenges and Future Directions," Future Generation Computer Systems, vol. 134, pp. 87–102, 2023.

[4] X. Wang, Y. Liu, and H. Zhou, "Federated Learning for IoT Cybersecurity: A Systematic Review," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 4122–4140, 2024.

[5] L. Chen and J. Brown, "Post-Quantum Cryptography for IoT: Security Challenges and Solutions," ACM Computing Surveys, vol. 55, no. 7, pp. 1–25, 2023.

BIBLOGRAPHY

Muppala Nagakeerthi working as an Assistant Professor in Master of Computer Applications in Sanketika Vidya Parishad Engineering College, Visakhapatnam, Andhra Pradesh, affiliated by Andhra University and approved by AICTE, accredited with' A' grade by NAAC and member in AICTE and member in IAENG with 15 years of experience in computer science. Her area of interest in C, Java, Data Structures, DBMS, Web technologies, Software Engineering and Data Science.

Sushmita Dash is currently pursuing her final semester of Master of Computer Applications (MCA) at Sanketika Vidya Parishad Engineering College, which is accredited with an 'A' grade by NAAC, affiliated to Andhra University, and approved by AICTE. With a keen interest in Machine Learning and Deep Learning, she has undertaken her postgraduate project titled "IOT CYBER ATTACK DETECTION USING MACHINE LEARNING AND DEEP LEARNING" The project is carried out under the guidance of M. Nagakeerthi, Assistant Professor, SVPEC.