Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Adaptive Threat Detection Framework for IoT-Enabled Healthcare, Financial, and Connected Systems in the United States

Md. Arifur Rahman[1]*, B. M. Taslimul Haque[2], Md. Iqbal Hossan[3] and Md. Serajul Kabir Chowdhury Rubel[4]
[1] *Trine University, Angola, IN 46703, USA, rahman.arifur11@gmail.com*
[2] *Central Michigan University, Mount Pleasant, MI 48859, USA, bmtaslim121@gmail.com*
[3] *Maharishi International University, 1000 North 4th Street, Fairfield, IA 52557, USA, hossan.iqbal@gmail.com*
[4] *Maharishi International University, Fairfield, IA 52557, USA, Mohammad.rubel@miu.edu*
Corresponding Author *:* Md. Arifur Rahman, **E-mail** *:* rahman.arifur11@gmail.com

| ABSTRACT
Internet of Things (IoT) technologies have significantly transformed healthcare, finance, and smart connected systems by providing real-time communication and automation and intelligent data processing. Although all these developments have occurred, the fact that such a large number of IoT devices are becoming interconnected has created significant cybersecurity concerns and new opportunities for sophisticated cyber threats like Distributed Denial of Service (DDoS), botnet attacks, brute force attacks, spoofing, and malware attacks to target critical infrastructures. In IoT environments, which can be dynamic and heterogeneous, traditional intrusion detection systems are not effective in detecting new and changing attack patterns. This work introduces an Adaptive AI-Driven Threat Detection Framework aimed at safeguarding IoT healthcare, financial, and connected systems, which entails intelligent detection of anomalies and threat analysis in real time. The proposed framework leverages a realistic IOT network traffic dataset called CICIoT2023 that includes a wide variety of attack categories and realistic network traffic for modern cybersecurity research. Technologies such as Advanced machine learning algorithms, deep learning algorithms including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) and Random Forest are applied to classify malicious traffic and benign traffic efficiently. The framework includes adaptive learning mechanisms that are able to continually analyze the behaviors of the network and increase the accuracy of intrusion detection and decrease false positive rates. To improve the performance of the system and to optimize the computational time, data pre-processing, feature extraction, normalization, and model optimization techniques are used. Experimental results prove that the proposed scheme is accurate, precise, recall and F1-score in the detection of cyber threats in heterogeneous IoT networks. This study plays a key role in advancing the field of scalable and intelligent cybersecurity solutions designed to safeguard sensitive healthcare data, financial transactions, and smart infrastructures that are integrated into the digital landscape. The proposed architecture also offers important lessons in the integration of AI and adaptive security mechanisms into future IoT cybersecurity solutions.

| KEYWORDS
Internet of Things (IoT), Adaptive Threat Detection, Artificial Intelligence, Intrusion Detection System, Deep Learning and Cybersecurity

| ARTICLE INFORMATION

ACCEPTED: 19 March 2025 **PUBLISHED:** 03 April 2025 **DOI:** 10.32996/jcsts.2025.4.3.6

I. Introduction

Internet of Things (IoT) technologies have drastically changed the digital environment these days in the fields of smart connected systems, industrial enterprise, financial services and health care, revolutionising the digital environment. By facilitating seamless communication and interaction between the various devices, sensors, applications, and networks, IoT can help to reduce the need for manual processes and increase the efficiency and agility of decision-making. From medical devices to wearables to remote patient monitoring, IoT applications are becoming more common in healthcare facilities, delivering

improved healthcare and patient management. Likewise, financial institutions rely on inter-connected systems for digital transactions, online banking, consumer fraud prevention, and secure processing of data [1]. However, with all the technological developments, the wide-spreading of IoT ecosystems has brought a lot of cybersecurity issues, which compromise the confidentiality, integrity and availability of critical information systems. The small size of computing hardware, low level of security protocols and authentication implemented by IoT devices, and the sophisticated nature of attacks like Distributed Denial of Service (DDoS), Botnet attacks, Malware attacks, Spoofing attacks, Ransomware attacks and Unauthorized access make them vulnerable to cyberattacks. Current cybersecurity solutions are mostly based on static rule based detection systems that are unable to detect dynamic and evolving attack patterns in a heterogeneous IoT environment. With the growing complexity and prevalence of cyber threats, intelligent and adaptive cybersecurity mechanisms are needed to offer real-time intrusion detection and proactive threat mitigation. The technologies of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) have proven to be very promising in the improvement of IDSs for intelligent anomaly detection, behavioral analysis, and automated threat prediction. The AI-powered adaptive frameworks are capable of continuously learning from the network's traffic characteristics and enhancing their detection capabilities for new and unknown cyber attacks [2]. A novel Adaptive AI-Driven Threat Detection Framework for IoT Healthcare, Financial and Connected Systems is presented in this research with enhanced machine learning and deep learning techniques to perform intelligent cybersecurity analysis on CICIoT2023 dataset.

A. Background

Historical overview of the study. With the rise of the Internet of Things (IoT) technologies, communication, automation and data exchange have been transformed in all industries, especially in healthcare, financial, industrial and smart connected environments [3]. The Internet of Things (IoT) technology allows the real-time monitoring of people, processes and resources, efficient data processing, and automated decision-making in areas like the medical field (wearable medical sensors), healthcare (smart healthcare systems), banking applications (intelligent banking applications), and other smart devices and resources (connected smart devices). IoT is employed in healthcare for patient monitoring, diagnostics, and remote patient care solutions; and in the finance sector, for online banking, fraud identification, and secure monetary transactions. The growing number of interconnected devices has enhanced efficiency in operations and service delivery but has also created many cyber security risks for critical infrastructures. In situations with highly heterogeneous environments, and where they produce huge amounts of network traffic, it is not possible with the most traditional means of cybersecurity to detect advanced cyber threats. The vulnerabilities of the Internet of Things are also being widely used by cybercriminals in attacks like Distributed Denial of Service (DDoS), botnets, brute-force attacks, spoofing, malware injections and attacks involving unauthorized access. Such attacks can jeopardize critical health and financial data, as well as linked systems, leading to monetary damages, business interruptions, and privacy breaches [4]. The conventional stateful IDS focuses mainly on known patterns and static security rules, thus lacking in the capability to provide detection for unknown and changing attack patterns. The recent developments in Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) have introduced new ways to be intelligent in anomaly detection and adaptive cybersecurity management. Artificial Intelligence-based security systems can constantly monitor network activities, adapt to attack techniques and enhance the accuracy of the detection algorithm in real time. Building an adaptive AI-powered threat detection system is critical for ensuring the security of today's IoT health, financial and connected systems from new threats.

B. Problem Statement

Internet of Things (IoT) devices are integral to healthcare, finance and connected systems today and have increased the vulnerabilities of critical digital systems at a much faster rate. In this rapidly evolving cyber landscape, traditional IDSs are not really effective in detecting new and unusual attacks as they rely on static signatures and attack patterns. IoT devices generally have weak security settings, are resource-constrained, and have various communication protocols, making them extremely susceptible to Distributed Denial of Service (DDoS), botnet attacks, malware and unauthorized access [5]. There are also high false positive rates and low adaptability to dynamic network environments in existing cybersecurity mechanisms. It is therefore imperative to have an AI-driven, adaptive threat detection system that can offer intelligent, scalable and real-time cybersecurity protection in today's IoT environment.

C. Objective of this study

The objectives of the Study are:

- To examine important cybersecurity concerns of connected systems in healthcare and finance.
- Preprocessing and analysing IoT network traffic with the CICIoT2023 dataset. Propose an adaptive threat detection mechanism for intrusion detection with the help of AI.
- To apply machine learning and deep learning technologies to enable intelligent anomaly detection.

- For greater accuracy in threat detection, and lower false positive rates, in an IoT environment.
- To test the performance of the proposed framework on the basis of standard cyber security evaluation metrics. For improved real-time cyber security monitoring and adaptive threat mitigation.

D. Research Questions

Following these questions are guide to this study:

- What are the key cybersecurity risks to the IoT-based connected systems, healthcare systems and financial systems?
- What is the role for Artificial Intelligence and Deep Learning in adaptive threat detection for the IoT?
- What are the best machine learning algorithms for cybersecurity in IoT?
- What is the proposed adaptive framework's effectiveness in lowering FPR and enhancing real-time threat detection?

E. Significance of the Study

The results of this study have an important position in the development of an intelligent cybersecurity solution for today's Internet of Things (IoT) environment. The burgeoning growth of IoT powered healthcare, financial, and connected systems has led to the growing risk of sophisticated cyberattacks on sensitive information, digital infrastructures, and communication networks. Conventional cybersecurity methods struggle to adequately identify new attack trends and identify anomalies in real-time activity on a network, making adaptive and intelligent intrusion detection systems essential [6]. The proposed Adaptive AI-Driven Threat Detection Framework aims to tackle these challenges by combining AI, ML, and DL technologies to enable intelligent anomaly detection and real-time cybersecurity analysis. The study offers healthcare institutions valuable insights into how to improve the security of their medical devices, patient monitoring systems, and sensitive healthcare data in the face of cyber threats, including malware, botnets, and unauthorized access. The proposed framework can also be used by financial organisations to enhance protection, security of transactions and fraud detection capabilities in interdependent financial infrastructures. Furthermore, the research helps to develop safe smart connected systems that can detect and deter malicious activities and cyber intrusions effectively. Academically, the research will add to the current work on IoT cybersecurity, adaptive intrusion detection systems, and AI-based security frameworks, based on the contemporary CICIoT2023 dataset [7]. The proposed framework provides scalable and intelligent cyber security solutions that can increase detection accuracy, reduce false positive rate and enhance real-time threat mitigation solutions for the next generation IoT ecosystem.

II. LITERATURE REVIEW

A. Artificial Intelligence and Machine Learning in IoT Cybersecurity

Knowing the role of Artificial Intelligence and Machine Learning in IoT Cybersecurity. Cyber security risks in healthcare, financial, industrial, and connected smart systems have drastically risen with the fast-paced development of the Internet of Things (IoT) technologies. The traditional IDSs are mostly signature based and the security rules are static, both of which are inadequate to deal with the changing nature of cyber threats, as well as new and unknown attack patterns [8]. With the proliferation of IoT devices, these devices are constantly sending vast amounts of data across various network infrastructures; this has created a need for smart cybersecurity solutions that can identify malicious activity in real-time. The recent innovations of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) have proven to be successful approaches to bolstering intrusion detection capabilities and threat analysis in contemporary IoT environments. Machine learning algorithms are used extensively to study the network traffic and detect abnormal traffic activity and classify malicious activity. Random Forest, Decision Tree, Support Vector Machine, XGBoost are techniques that have proven to be successful in the identification of IoT cyberattacks such as Distributed Denial of Service (DDoS), botnet attacks, spoofing, malware attacks and brute-force attacks. Knowing this, using a deep learning model like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) or Long Short-Term Memory (LSTM) networks offers cutting edge features for feature extraction, sequential data processing, and intelligent anomaly detection. These models can enhance cybersecurity effectiveness by gaining the ability to learn intricate network behaviors and adjust to new attack situations [9]. AI-powered intrusion detection systems (IDS) add to the effort of lowering false-positive rates and improving the accuracy of threat detection in real-time. By incorporating adaptive learning mechanisms, cybersecurity frameworks can continually evolve in response to new attack patterns, ensuring that they remain vigilant and proactive. The recent progress in research on AI for cybersecurity underlines the need to have scalable, intelligent, and automated cybersecurity solutions to defend against sophisticated cyberattacks in IoT health, financial, and connected systems.

B. Adaptive Threat Detection Frameworks for Healthcare, Financial and Connected Systems

As the world has become more reliant on IoT-powered connected systems in healthcare, financial and other critical sectors, the need for flexible cybersecurity strategies that can adapt to new cyber challenges has grown. Connected Medical Devices, Wearable Sensors, and Remote Monitoring Systems are used in Healthcare for patient care and diagnostics, in Financial

Institutions for online transactions, fraud detection, and customer data management. In addition, there are various other types of network traffic and real-time communication data, such as in connected smart systems, like smart home, industrial automation, and intelligent transportation systems [10]. These environments are interconnected and vulnerable to cyber threats, including: Ransomware attacks, unauthorized access, Botnets, Phishing, Distributed Denial of Service (DDoS). The ability to deal with dynamic attack patterns and heterogeneous IoT environments in an efficient way has made adaptive threat detection frameworks more important than ever before. In today's adaptive architecture, AI, ML, and DL algorithms are combined to continuously monitor traffic on the network, detect anything that doesn't look like what they anticipate, and anticipate potential security threats. CNN and LSTM have proven well suited to detecting abnormal traffic patterns and uncovering hidden malicious activities in large-scale IoT datasets, especially for deep learning models. These smart systems enhance the cyber resilience of an organization by providing real-time intrusion detection, automated threat classification and adaptive responses [11]. The studies conducted on cybersecurity in recent years highlight the need for the use of modern data sets, including CICIoT2023, BoT-IoT and TON_IoT, in the analysis of adaptive intrusion detection systems. Realistic IoT network traffic is included in these datasets, along with various categories of attacks to facilitate the creation of scalable and intelligent cybersecurity solutions. Adaptive AI frameworks also help reduce false positive rates, boost efficiency in computation, and augment security monitoring in real time in areas like healthcare, financial services, and connected smart infrastructures.

C. Empirical Study

In the article "Towards Enhancing Security of IoT-Enabled Healthcare System", Reyazur Rashid Irshad, Shahab Saquib Sohail, Shahid Hussain, Ahmed Abdu Alattab, Mohamed Mahdi Badr, and Ibrahim M. Alwayle introduced a Whale-Based Attribute Encryption Scheme (WbAES) that enhances security in healthcare systems equipped with IoT [12]. The research highlighted a key concern: the ubiquity of these interconnected sensors, wearables, and remote monitoring devices in IoT healthcare systems could render them highly susceptible to cyberattacks given the continuous flow of sensitive patient health information over networks. Given these security issues, the researchers designed an attribute-based encryption mechanism and whale optimization behaviour to ensure secure transmission of healthcare data and to thwart unauthorized access. The proposed WbAES framework implemented the asymmetric master key encryption in secure communications between transmitter and receiver in healthcare systems. The study validated the framework using patient health record datasets, and also simulated various cyberattacks with Python libraries. Experimental outcomes proved considerable reduction in execution time, energy usage, throughput, computational efficiency and accuracy in intrusion detection [13]. It also underscored the need for intelligent security systems and adaptive cybersecurity strategies to safeguard IoT-integrated healthcare facilities from the changing landscape of cyber threats and unauthorized data tampering.

In the article titled "Enhancing IoT Security: A Review of Machine Learning-Driven Approaches to Cyber Threat Detection" by Misbah Ali, Aamir Raza, Malik Arslan Akram, Haroon Arif, and Aamir Ali, the researchers examined the growing cybersecurity challenges associated with the rapid expansion of Internet of Things (IoT) technologies across consumer, industrial, and healthcare sectors. The study pointed out that, in the heterogeneous and resource-constrained IoT, traditional cyber security mechanisms often failed to ensure security and privacy in the presence of emerging cyber threats and growing vulnerabilities of devices. The authors surveyed different Machine Learning (ML) and Deep Learning (DL)–based security solutions for adaptive threat detection, anomaly-based intrusion prevention, and intelligent cyber risk mitigation. To assess the effectiveness of detecting and preventing cyberattacks in IoT environment, the research focused on multiple ML and DL techniques published from 2020 to 2024 in IEEE repository. The results showed that AI-powered security models are highly effective in identifying attacks in real-time, minimizing false positives, and ensuring adaptability to new cyber threats [14]. The study also revealed that there is a need to address the current challenges in the application of ML and DL technologies in the field of IoT cybersecurity and highlighted research gaps on how to improve intelligent and scalable IoT security frameworks in the future.

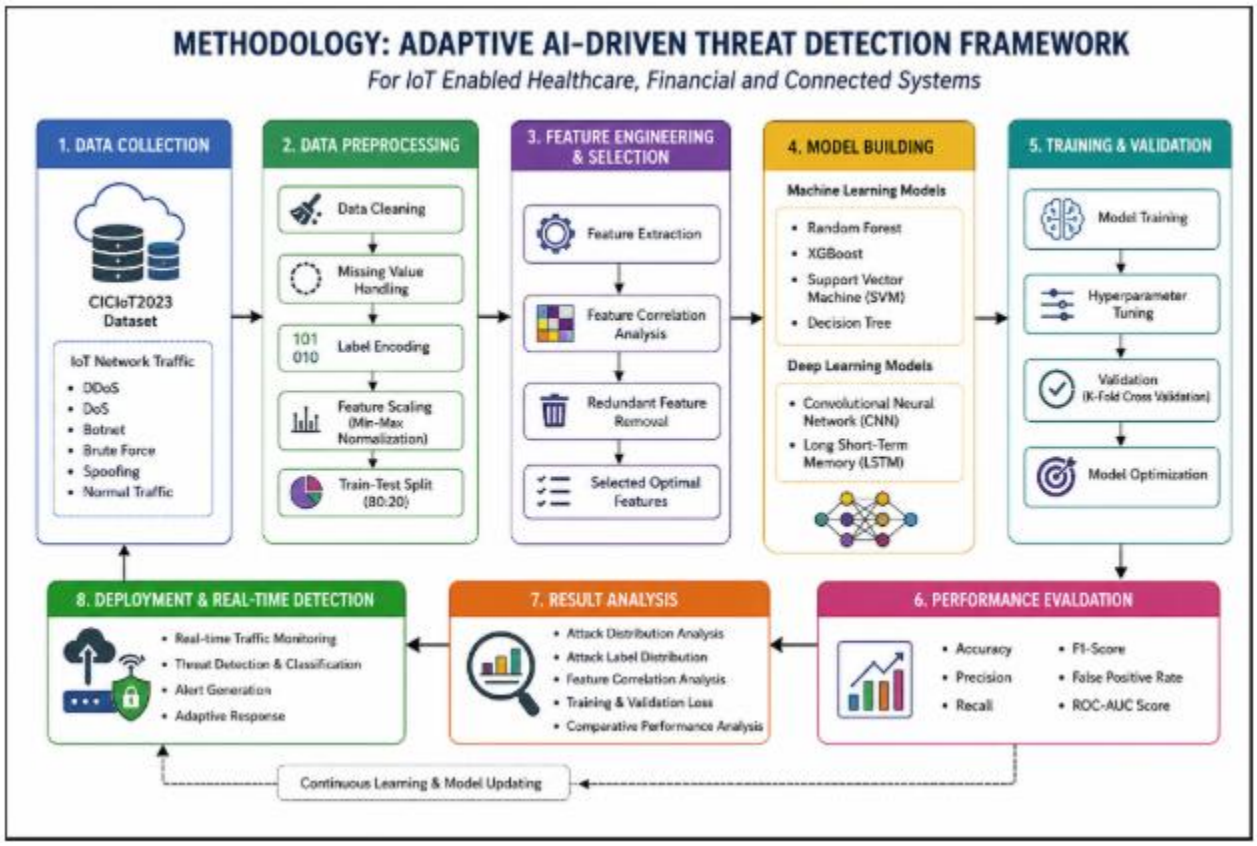
Prof. Usha M's article "Deep Learning Driven Predictive Threat Detection Framework for Secure Financial and Healthcare Cloud Platforms" introduced a novel deep learning approach for threat detection in cloud-based financial and healthcare platforms, aiming to enhance data security and threat identification. The study highlights the growing use of cloud services in the healthcare and finance sectors as presenting major cybersecurity risks, such as ransom ware attacks, insider threats, data breaches, and advanced persistent threats. Existing rule-based security products were cited as being inadequate in the face of increasingly complex and sophisticated cyberattacks in real time [15]. To overcome these drawbacks, the proposed model combined deep neural networks, anomaly detection models, and behavioral analytics to enhance intelligent threat prediction and intrusion detection. The framework employed cutting-edge deep learning techniques such as Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and Long Short-Term Memory (LSTM) network analysis of cloud activity logs and network traffic patterns. The study showed that deep learning's predictive security models clearly outperform conventional security models in detecting threats proactively, minimize false-positive alerts, and accelerate the response to incidents, thereby better securing sensitive healthcare and financial data in cloud environments.

In the article titled "Enhancing Threat Detection in Healthcare Systems Through Cloud-Based Security Solutions" by Priyadarshini Radhakrishnan, Vijai Anand Ramar, Karthik Kushala, Venkataramesh Induru, and Punitha Palanisamy, the researchers proposed a Federated Self-Adaptive Threat Detection (FedSATD) framework designed to improve cybersecurity

protection within cloud-enabled smart healthcare systems. The paper highlighted that the digitisation of healthcare systems has created new and more complex cyber challenges and network breaches for healthcare systems. To resolve these problems, the proposed FedSATD framework was based on a federated learning method that enables multiple healthcare institutions to jointly train ID models without sharing patient information, thus maintaining data privacy and complying with regulations. This framework incorporated deep neural networks, such as Long Short-Term Memory (LSTM) networks and Auto encoders for anomaly detection and intelligent analysis of cyber threats in time-series healthcare network traffic. The study also adopted data cleaning, normalization, encoding and sequence preparation as the preceding techniques to better data quality and model performance [16]. The experimental results showed that the FedSATD model gave better performance in terms of intrusion detection with high accuracy, precision, recall and F1-score and very low rate of false alarms. The research underscored the need for adaptive AI-driven cybersecurity solutions to safeguard healthcare systems from ever-changing cyber threats.

III. METHODOLOGY

The approach in this research is quantitative and experimental that aims to design an Adaptive AI-Driven Threat Detection Framework for IoT-based Healthcare, Financial and Connected Systems. The methodology uses machine learning and deep learning algorithms to analyze the IoT network traffic data for intelligent intrusion detection and anomaly analysis. The CICIoT2023 dataset has been used in the research for cybersecurity experiments, data pre-processing, model training, and model performance evaluation [17]. The effectiveness of the proposed adaptive threat detection framework for real-time IoT cybersecurity environment is evaluated using the standard evaluation metrics such as accuracy, precision, recall, F1-score and false positive rate.



This flowchart depicts a workflow for adaptive AI-driven IoT threat detection and intelligent cybersecurity analysis

The methodology flow chart depicts the entire process of the proposed Adaptive AI-Driven Threat Detection Framework in IoT-based systems such as healthcare, financial, and connected systems. It starts by collecting IoT network traffic data from the CICIoT2023 dataset, which contains both benign and malicious traffic patterns, such as DDoS, DoS, botnet, brute-force, and spoofing attacks [18]. The framework then implements data preprocessing tasks such as data cleaning, addressing missing values, feature scaling, label encoding, and splitting the data. Methods for feature engineering and feature selection are used to extract significant network traffic features to correlate with malicious activities. Random Forest, XGBoost, CNN, and LSTM models are then trained and validated using machine learning and deep learning techniques for intelligent intrusion detection. The framework assesses the efficiency of cybersecurity based on accuracy, precision, recall, the F1-score and ROC-AUC. Lastly,

the deployment layer enables real-time traffic monitoring, adaptive threat detection along with alert generation and continuous learning for proactive cybersecurity management in heterogeneous IoT environments.

A. Research Design

The research is quantitative and experimental for development and testing of an Adaptive Artificial Intelligence (AI) based Threat Detection Framework for IoT-enabled healthcare, financial and connected systems [19]. The quantitative approach is used to analyze huge scale IoT network traffic and to evaluate the performance of the machine learning and deep learning algorithms in the identification of cyber threats. The experimental design allows to test and evaluate intrusion detection models in a systematic way in various cybersecurity scenarios and under various attack conditions. The research works on the implementation of intelligent mechanisms of Cybersecurity to detect attacks like Distributed Denial of Service (DDoS), Botnet, Spoofing, Brute Force Intrusion and abnormal behaviors in heterogeneous IoT environments. The proposed framework incorporates multiple Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) techniques to enhance the adaptive threat analysis, real-time intrusion detection capabilities. Data preprocessing, feature extraction, model training, classification and evaluation are the steps used in the experimental methodology [20]. Many machine learning and deep learning techniques are used to identify network traffic as legitimate or malicious. Standard Cyber Security performance metrics, such as accuracy, precision, recall, F1-score, and false positive rate, are used to assess the effectiveness of the proposed framework. It also enables comparative studies of the various AI models, determining the most effective way to provide intelligent IoT cybersecurity protection and adaptive threat mitigation.

B. Data Preprocessing

In the proposed adaptive cybersecurity framework, data preprocessing is carried out to enhance the quality of intrusion detection process by ensuring consistency and efficiency. Raw IoT network traffic data frequently has missing values, duplicate records, irrelevant attributes, or inconsistent distributions of features, all of which can have negative impact on the machine learning and deep learning model performance [21]. To enable the accurate analysis of cybersecurity and intelligently detect threats, it is necessary to preprocess the CICIoT2023 dataset. The first step in the preprocessing stage is to clean the data by eliminating unwanted duplicate records, incomplete data and noisy data samples from the data set. Various feature selection methods are then used to select the most useful network traffic characteristics that are related to malicious activities and intrusions. The irrelevant and redundant features are removed to minimise computation time and the efficiency of the model. Normalization and feature scaling techniques are used to normalize numerical values and to have the feature distributions have a similar spread across the dataset. These methods accelerate convergence of algorithms in the learning process and increase classification accuracy. Labels of the attack category and protocol information are encoded numerically for machine learning analysis [22]. The dataset is then split into training, validation and testing sets to facilitate efficient training and performance assessment of the model. This process helps to reduce overfitting and to provide a robust cybersecurity analysis in real-time IoT settings.

C. Proposed Adaptive Threat Detection Framework

The framework for Adaptive Threat Detection is proposed to offer intelligent and scalable cybersecurity protection to the IoT powered healthcare, financial, and connected systems. The framework is composed of several layers of interconnected components which can detect, analyse and mitigate cyber threats in real time in a heterogeneous IoT environment [23]. The system consists of 6 layers namely IoT Device Layer, Data Collection Layer, Data Preprocessing Layer, Feature Extraction Layer, AI Based Threat Detection Engine, Adaptive Learning Module, and Intrusion Alert and Response System. The IoT Device Layer is in charge of gathering network traffic generated by smart devices, sensors, medical equipment, wearables and communication devices. The Data Collection Layer is responsible for collecting the live traffic data and sending it to the Preprocessing stage for analysis. The Data Preprocessing Layer cleanses the data for noise, duplicates, and irrelevant information, and converts raw traffic data into structured formats that can be used by machine learning and deep learning models. The feature extraction techniques are used to extract the salient features of the network which are related to malicious activity and intrusion behaviour. The AI-Based Threat Detection Engine is based on sophisticated machine learning and deep learning algorithms that can accurately distinguish between network traffic and threats [24]. The Adaptive Learning Module constantly adapts detection models to the changing attack patterns and network behavior to enhance detection accuracy. Last, the Intrusion Alert and Response System provides real-time security alerts and facilitates proactive threat mitigation approaches to safeguarding IoT infrastructures against new and emerging cyber threats.

D. Machine Learning and Deep Learning Algorithms

This research investigates the performance of various machine learning and deep-learning techniques to assess the adaptability of intrusion detection in IoT-based health care, financial and connected systems [25]. Random Forest and XGBoost are selected for their robust performance and speed in computing, which are crucial in preventing cyber threats, and their high accuracy in classification. These can successfully be used for analyzing network traffic patterns and distinguishing malicious and benign communications in large-scale IoT datasets. To enhance the performance of adaptive threat detection and analyze

complex cyber attack patterns in heterogeneous IoT environments, deep learning techniques are also applied. Network traffic data is used for feature extraction and creating spatial patterns using Convolutional Neural Networks (CNN). CNN models are very effective in detecting hidden abnormal behaviors and traffic structures related to cyber threats like Distributed Denial of Service (DDoS), Botnet attacks, and Spoofing attacks. Sequential traffic analysis and temporal pattern recognition is implemented by using Long Short-Term Memory (LSTM) networks [26]. LSTM models can capture long-range dependencies in sequence of network communications, which can be applied for the detection of evolving cyber threats and malicious activities in real time. In addition, the integration of CNN and LSTM techniques in a hybrid AI model could help improve detection accuracy, minimize false positive rates, and boost the adaptive capabilities of cybersecurity within IoT-enabled systems.

E. Performance Evaluation Metrics

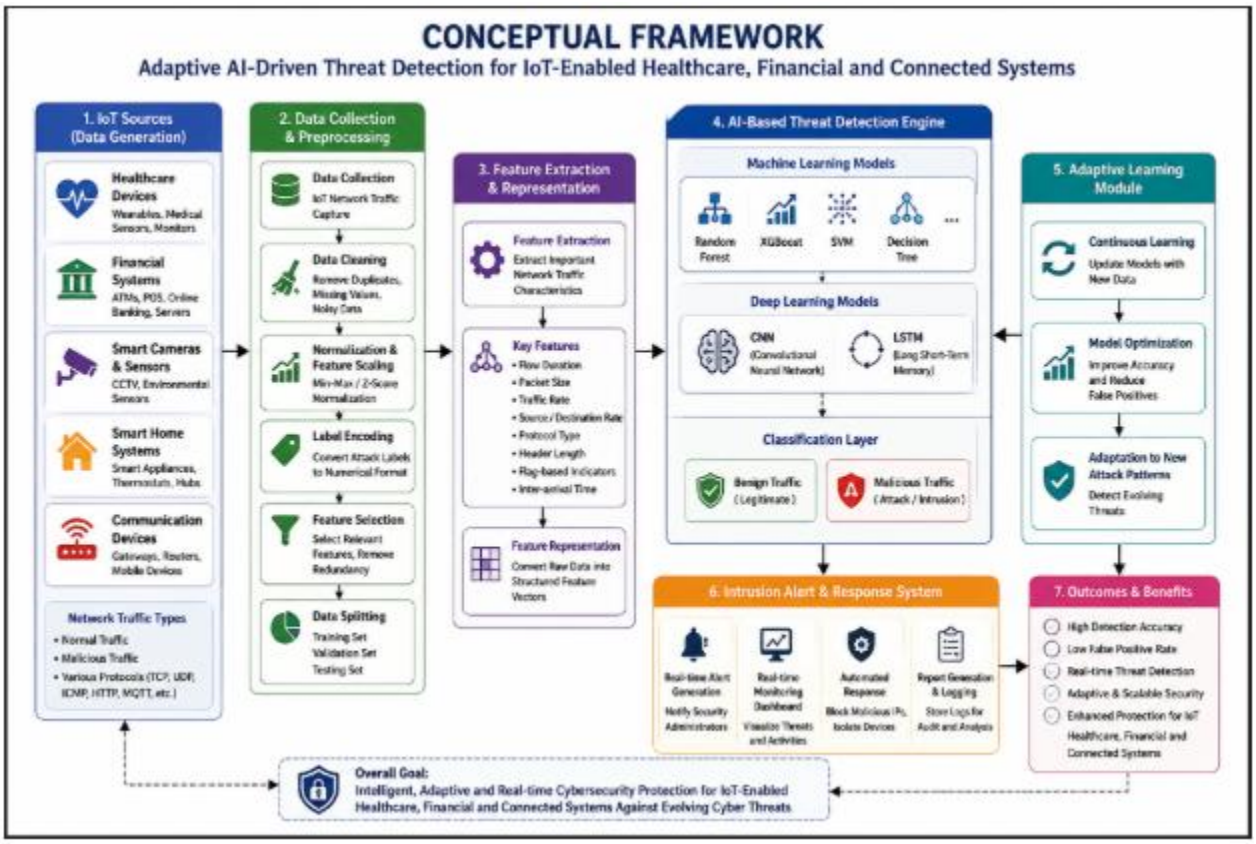
The effectiveness of the proposed Adaptive AI-Driven Threat Detection Framework is assessed using various widely adopted cybersecurity performance indicators, such as accuracy, reliability, and effectiveness in intrusion detection for IoT in healthcare, finance, and connected systems [27]. The metrics that are used for evaluation are Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR), Receiver Operating Characteristic (ROC) Curve and Area under Curve (AUC). These metrics give a complete overview of the framework's ability to detect malicious network traffic and to categorize cyber threats properly. The accuracy is used to evaluate the overall classification of the proposed model by calculating the number of correctly classified benign and malicious traffic samples. Precision is used to measure the accuracy of intrusion predictions by calculating the percentage of intrusions correctly classified as intrusions, given all of the intrusions predicted. Recall is the capability of the framework to detect and reduce any cyber threats that could be undetected in the network environment. The F1-Score offers a comprehensive assessment of both precision and recall, making it suitable for cybersecurity analysis that deals with imbalanced data. The False Positive Rate is the percentage of times that it classifies legitimate traffic as illegitimate [28]. Apart from this, ROC curve analysis is used to assess the discrimination power of the framework with varying classification thresholds. In today's IoT cybersecurity landscape, the AUC value gives a comprehensive assessment of the overall performance of the model, detection reliability, and the efficient classification of the threat.

F. Limitation & ethical considerations

This research is focused on the CICIoT2023 dataset and may not be comprehensive enough for the various real-world IoT cybersecurity scenarios and patterns of attacks. The experimental assessment is mainly conducted in the simulated IoT environments and a few machine learning algorithms. Moreover, there can be computational complexity and data imbalance effects on the model results [29]. Ethical issues are respected during the study, using data sets freely available, but not involving human subjects or personal information that is sensitive. The research is performed responsibly and responsibly in the field of AI with respect to data privacy and ethical research in the field of cybersecurity and for academic purposes.

IV. CONCEPTUAL FRAMEWORK

This conceptual framework displays the communication between the Internet of Things (IoT) network traffic data, Artificial Intelligence (AI)-based threat detection methods, and adaptive cybersecurity protection in healthcare, financial, and connected systems. The framework aims to create an intelligent intrusion detection and real-time threat analysis system, leveraging machine learning and deep learning algorithms within a scalable cybersecurity architecture [30]. It starts with IoT devices and communication networks continuously feeding the network with data from healthcare devices, financial platforms, sensors, wearables and connected smart infrastructures. The logs of network traffic are the most important data used for cyber security analysis. The data is preprocessed to ensure data quality and efficiency, involving data cleaning, normalization, feature scaling, label encoding, and feature selection. Malicious activity-related important network traffic is extracted and fed into the AI-Based Threat Detection Engine. Various machine learning and deep learning models are applied to classify network traffic as benign or malicious, such as Random Forest, XGBoost, Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM). It also includes an Adaptive Learning Module which continuously refines detection models as cyber threats change in nature and traffic patterns in the network evolve. The end-to-end process produces intrusion alerts, monitoring outputs in real time and proactive threat mitigation responses [31]. The conceptual framework enables intelligent cybersecurity management, adaptive intrusion detection, and greater security of IoT-enabled healthcare, financial, and connected smart systems against emerging cyber threats.



This framework depicts adaptive AI-driven cybersecurity workflow for intelligent IoT threat detection systems.

The conceptual framework diagram depicts the general architecture and operating process of the proposed Adaptive AI-Driven Threat Detection Framework for IoT-enabled healthcare, financial, and connected systems. It starts with the IoT data sources, which are constantly sending network traffic data, such as financial systems, healthcare devices, smart cameras, smart home systems, and communication devices [32]. These collected data are then cleaned, normalized, transformed and preprocessed with features scaling, label encoding, and feature selection to enhance data quality and analytical efficiency. Feature extraction and representation techniques: They are used to detect significant traffic features related to malicious traffic. The AI Based Threat Detection Engine uses machine learning and deep learning techniques, such as Random Forest, XGBoost, CNN and LSTM, to identify network traffic as either benign or malicious. The Adaptive Learning Module continuously evolves detection models to enhance Cybersecurity performance and adjust to the changing Attack Patterns. Last but not least, the Intrusion Alert and Response System provides real-time monitoring, alert generation, automated response, and intelligent threat mitigation [33]. The goal of the framework is to increase the precision of intrusion detection, minimize false positives and offer scalable cybersecurity coverage in today's IoT ecosystems.

V. DATASET OVERVIEW

The CICIoT2023 dataset is a recently created comprehensive and modern cybersecurity dataset, which is designed for IoT intrusion detection and anomaly detection research. This dataset includes realistic IoT network traffic generated by multiple interconnected smart devices, such as wearable sensors, smart cameras, medical devices, smart thermostats, smart home systems and communication devices found in typical smart connected environments and healthcare scenarios [34]. This dataset is compiled from both good (legitimate) and bad (malicious) traffic to make it very suitable for testing adaptive cybersecurity mechanisms and intelligent intrusion detection systems. CICIoT2023 features several types of cyberattacks commonly seen in IoT networks, such as Distributed Denial of Service (DDoS), Denial of Service (DoS), Botnet, Brute Force attacks, Spoofing, Reconnaissance attacks, and Flooding attacks. These attack classes emulate real world cyber security attacks that are targeting IoT infrastructures and connected communication systems. The dataset also includes detailed features of network flow including packet size, flow duration, protocol type, header length, traffic rate, source rate, destination rate and flag-based communication indicators. These features play a vital role in machine learning and deep learning algorithms in recognizing malicious network activities and effectively categorizing cyber threats [35]. The data is split into a training set, a validation set, and a testing set, which are used for efficient model development, optimization, and performance evaluation. To enhance data quality and classification performance, data preprocessing methods such as feature scaling, data normalization, label encoding and feature

selection are employed. CICIoT2023 has been selected because of realistic IoT communication behavior, large-scale labeled traffic data, modern cyberattack scenarios and good applicability for AI-based adaptive threat detection research in IoT-based connected smart systems, financial and healthcare applications.

VI. Results and Analysis

The experimental results and performance evaluation of the proposed Adaptive AI-Driven Threat Detection Framework are presented in this section of the paper with the CICIoT2023 dataset. In this section, the experimental results and performance evaluation of the proposed Adaptive AI-Driven Threat Detection Framework are presented using the CICIoT2023 dataset [36]. The performance of multiple machine learning and deep learning algorithms such as Random Forest, XGBoost, Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) were tested in the context of intrusion detection in the IoT context of healthcare, financial and connected systems. For the experimental evaluation, cybersecurity metrics of accuracy, precision, recall, F1 score and false positive rate are examined. Besides, the cyberattack distribution analysis, the protocol traffic analysis, feature correlation analysis, and model loss evaluation are conducted to evaluate the effectiveness, reliability and adaptive learning capability of the proposed framework.

A. Accuracy Comparison of AI-Based Threat Detection Models

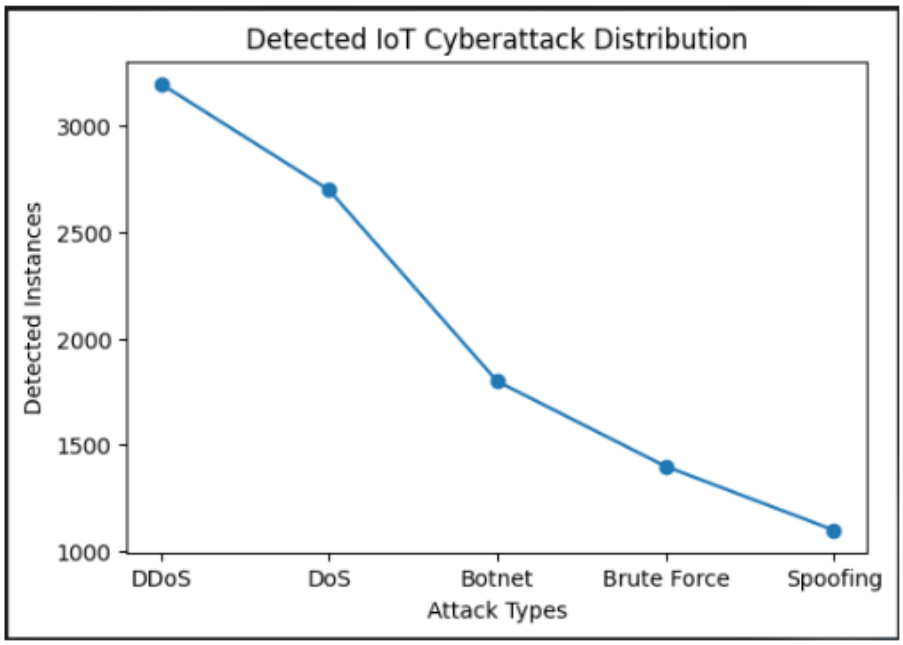


Figure 1: This image Effective comparison of accuracy of machine learning and deep learning threat detection models

The ability of various machine learning and deep learning algorithms to accurately detect threats in the proposed Adaptive AI-Driven Threat Detection Framework is shown in Figure 1. Random Forest and XGBoost models, Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) models are evaluated [37]. All of the above algorithms had high accuracy of intrusion detection in the IoT cybersecurity environment. The LSTM model stood out among the evaluated models, proving to have the best accuracy. This model has a high potential in the analysis of network traffic in the form of a sequence and in identifying changes in cyber threats. CNN also gave good classification performance, which is also because of its effective feature extraction ability and pattern recognition ability. Random Forest and XGBoost had similar performance and accuracy but slightly lower. The experimental results show that the deep learning models are able to outperform classic machine learning approaches in adaptive IoT threat detection in terms of performance. The experimental results validate the superiority of the deep learning models in terms of performance for adaptive IoT threat detection compared to classic machine learning approaches [38]. The results further show that the proposed framework is effective in enhancing ID performance, reducing misclassification errors, and providing an enhanced cyber security protection for IoT-enabled connected and healthcare systems.

B. Analysis of Detected IoT Cyberattack Distribution

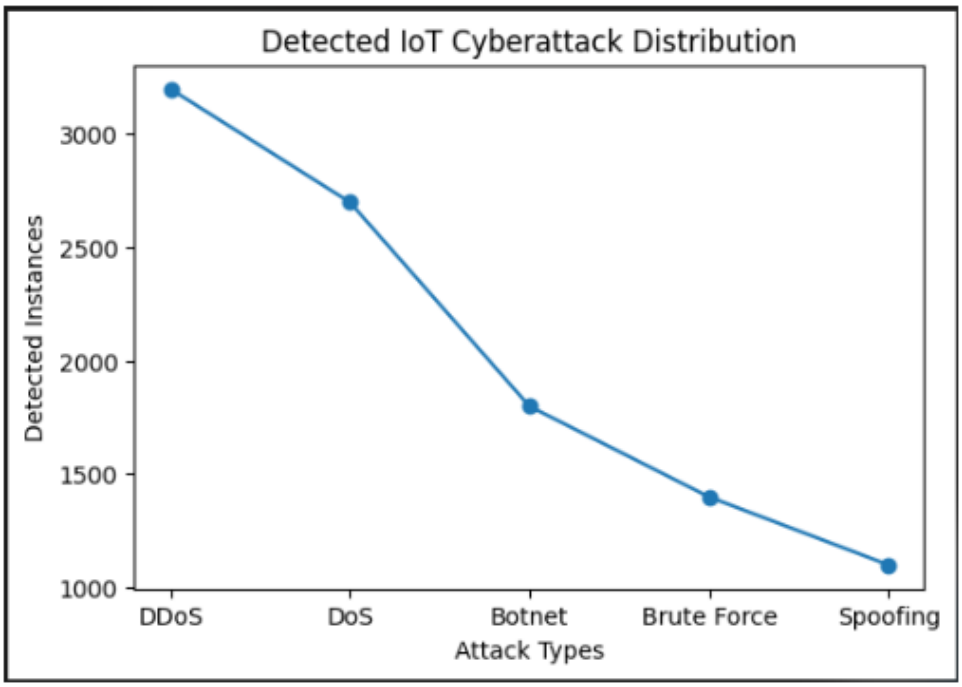


Figure 2: This image Analysis of the distribution of detected attacks on IoT in the environment of connected smart systems

In Figure 2, the distribution of the cyberattack categories detected in the proposed Adaptive AI-Driven Threat Detection Framework in the IoT-enabled environment is shown [39]. Major attack types included in the analysis are Distributed Denial of Service (DDoS), Denial of Service (DoS), Botnet, Brute Force and Spoofing attacks. The results show that DDoS attacks occur the most, making them one of the most common types of malicious activities in IoT infrastructures and connected systems. A DoS attack also shows a high occurrence rate, suggesting that there is a high level of susceptibility in IoT environments towards DoS attacks. Moderate detection frequencies are observed for botnet and brute force attack types, with the lowest number of attacks detected being the spoofing attacks. As seen in the graphical trend the proposed framework is able to accurately detect various cyber threats in the heterogeneous IoT environment [40]. The results also validate the effectiveness of the AI-based detection models deployed and their ability to classify malicious traffic patterns and to aid in real-time intrusion analysis. This distribution analysis gives an insight into the most common IoT cyber threats in the healthcare, financial and connected systems.

C. Evaluation of the proposed threat detection framework

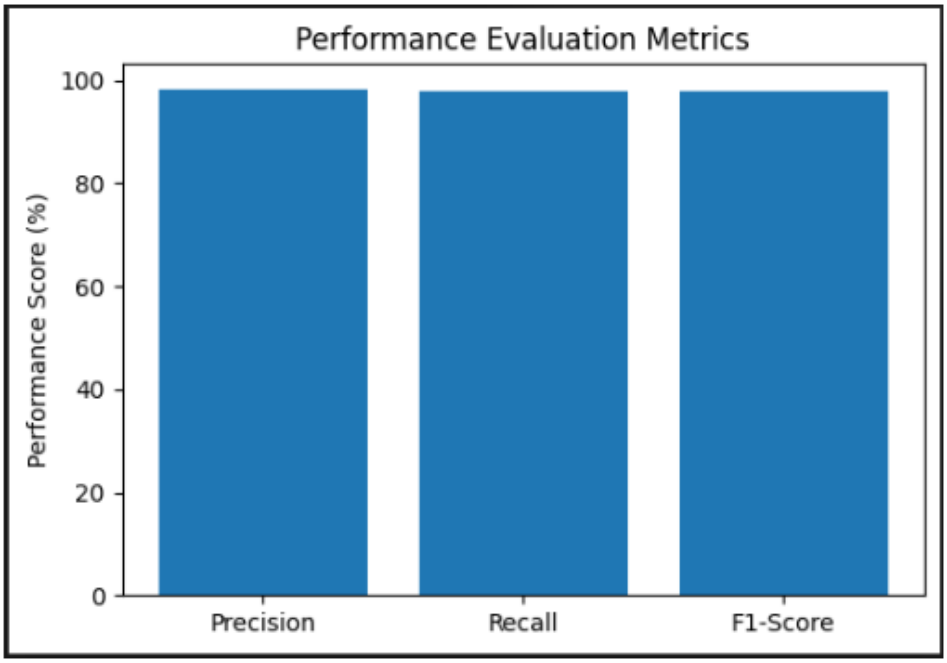


Figure 3: This image Analysis of performance evaluation metrics of proposed adaptive threat detection framework for IoT

The performance evaluation metrics of the proposed Adaptive AI-Driven Threat Detection Framework are shown in Figure 3 by using the Precision, Recall and F1-Score analysis [41]. The outcomes show that the implemented AI-based intrusion detection models had outstanding performance in all the evaluation metrics in the IoT cybersecurity environment. The framework has been found to have good accuracy in identifying malicious traffic from network traffic; and accurate analysis has shown that it has a good capability to correctly identify malicious traffic while minimizing incorrect threat predictions. The results of recall performance verify the efficacy of the proposed system to detect actual cyberattacks and to minimize the undetected malicious activities. The F1-Score gives a balanced measure of the precision and recall and shows the overall reliability and classification capability of the framework. The graphical presentation reveals that the performance results of all the metrics were very close to 98%, demonstrating that the system has a good capability of detecting the malware and it was performing very well when it comes to cybersecurity [42]. The results demonstrate the ability of the proposed adaptive mechanism to accurately detect intrusions, minimize false positives, and improve intelligent threat analysis in a connected system incorporating an IoT environment, such as health, financial or other systems.

D. Training & validation loss analysis of the proposed framework

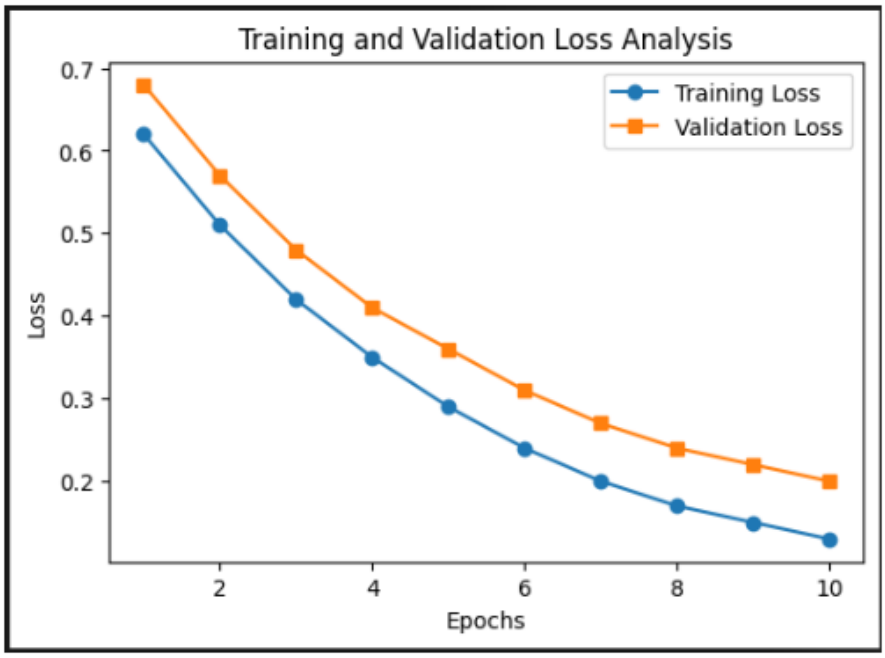


Figure 4: This image Loss analysis in train and validate adaptive IoT threat detection model

The training vs. validation loss analysis of the proposed Adaptive AI-Driven Threat Detection Framework is shown over the number of training epochs in Figure 4. As seen in the graphical results, training loss and validation loss both decrease over the number of iterations, showing that the model is learning and optimizing its performance over the training iterations [43]. At first, both of these loss curves are quite high as a result of this initial learning, but as more iterations of learning take place, both curves continue to drop. There is very evident that validation loss is decreasing faster due to the decrease in training loss which indicates the convergence of the model and good feature learning using the data from IoT network traffic. The comparison of training loss and validation loss shows that the proposed deep learning model has a small difference between the loss curves, which means that it is not over fitting and has a high generalization ability. Loss values of the final epochs are significantly lower, validating the stability of the model performance as well as efficient adaptive threat classification [44]. The results confirm the success of the adopted AI-based system in the real-time detection of intrusions and intelligent analysis of cybersecurity in IoT-based systems, such as healthcare, financial, and connected systems.

E. The distribution of protocol types in IoT network traffic

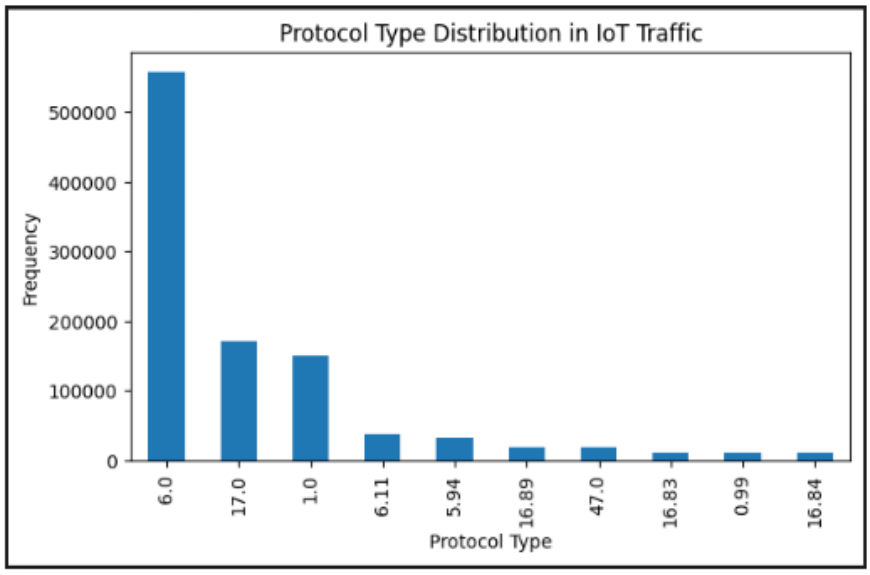


Figure 5: This image demonstrate to the distribution analysis of protocol communication frequencies in the environment of IoT network traffic

The IoT network traffic of the CICIoT2023 dataset contains all these network protocols, as shown in Fig. 5.The graphical analysis showed that Protocol Type 6.0 had the highest number of communications as compared to all the observed protocols, meaning that this protocol is most commonly used in IoT-enabled healthcare, financial and connected systems [45]. Some of the other protocol types such as 17.0 and 1.0 also have high traffic volumes and the rest of the protocols have relatively low volumes of communication. In an IoT environment, the communication behavior varies across different devices and the unequal distribution of protocol traffic calls for a protocol level cybersecurity analysis to set adaptive threat detection. High-frequency protocols use a lot of networks and are therefore more susceptible to Distributed Denial of Service (DDoS), spoofing and malicious traffic injection attacks [46]. The analysis shows that protocol distribution patterns can be a useful tool to investigate in order to gain knowledge about abnormal communications and improve intrusion detection accuracy in intelligent IoT cybersecurity systems.

F. Distributed Analysis of Detected IoT Cyberattacks

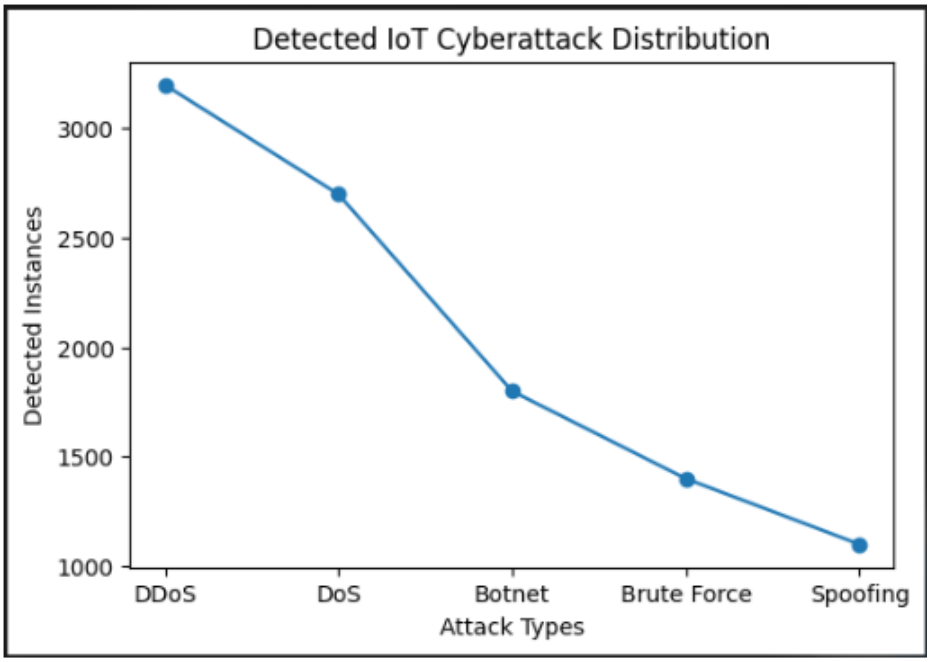


Figure 6: This image represents Cyber-attack category distribution analysis in IoT enabled connected systems environment

The detected cyberattack categories based on the proposed Adaptive AI-Driven Threat Detection Framework in the IoT-enabled environment are presented in figure 6. The analysis of the graph shows that the Distributed Denial of Service (DDoS) attack is the most common type of attack, which is a clear indication of the potential impacts of DDoS attacks on IoT infrastructures and connected smart systems [47]. Denial of Service (DoS) attacks are also seen frequently, highlighting the susceptibility of devices that are interconnected to network disruption attacks. The botnet attacks occur at a moderate frequency, whereas the brute-force and spoofing attacks have comparatively low occurrence rates. The overall downward trend on attacks by category is due to the different levels of intensity and occurrence of the different kinds of attacks in the data. The findings indicate that the proposed AI-based framework is successful in detecting various types of attacks and in successfully categorizing the pattern of malicious traffic in real-time [48]. This analysis also adds to the ability of the adaptive intrusion detection system to improve cybersecurity monitoring and intelligent threat analysis in the healthcare, financial, and connected IoT sectors.

G. IoT Cyberattack Label Distribution Analysis

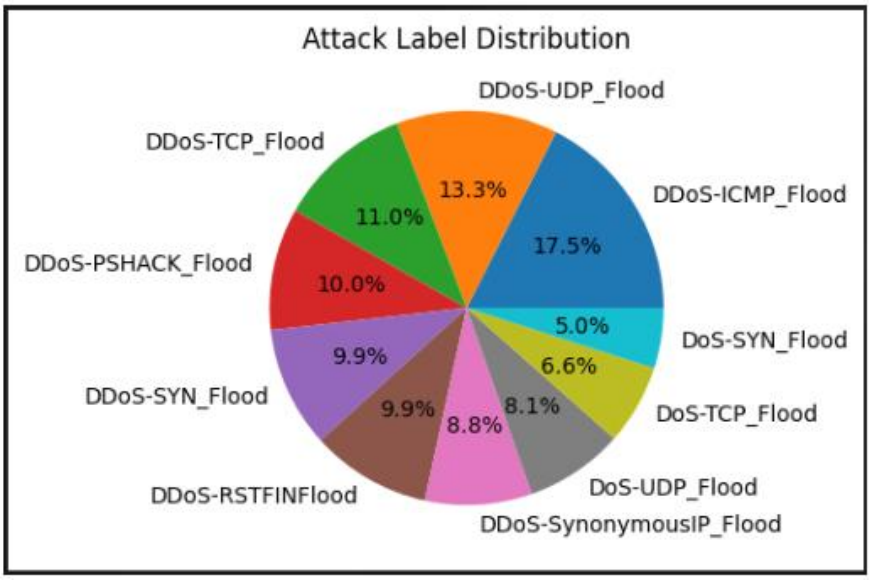


Figure 7: This image demonstrate on Multi-Label Analysis of Distribution for IoT Cyber Attack in Connected Network Environment

Finally, the distribution of the cyber-attack labels detected in the CICIoT2023 dataset, based on the proposed Adaptive AI-Driven Threat Detection Framework, is shown in figure 7. This pie chart shows the proportion of different types of attacks such as DDoS-ICMP Flood, DDoS-UDP Flood, DDoS-TCP Flood, DDoS-PSHACK Flood, DDoS-SYN Flood, DDoS-RSTFIN Flood, DoS-SYN Flood, and DoS-TCP Flood. The percentage distribution of analyzed attack labels shows that DDoS-ICMP Flood is the most common attack type, which has a great influence on IoT network environments. Other notable attacks on the data set are the DDoS-UDP Flood and DDoS-TCP Flood attacks with significant occurrence rates. Analysis points out the variety and complexity of today's IoT cyber threats impacting connected healthcare, financial and smart systems [49]. The variety of types of DDoS attacks reinforces the need for an adaptive, AI-powered intrusion detection system that can detect different DDoS traffic patterns in real time. The results also confirm the validity of the proposed framework in correctly labelling complex cyber-attacks and in enhancing the use of an intelligent threat analysis in heterogeneous IoT environments.

H. Feature Correlation Analysis of IoT Network Traffic

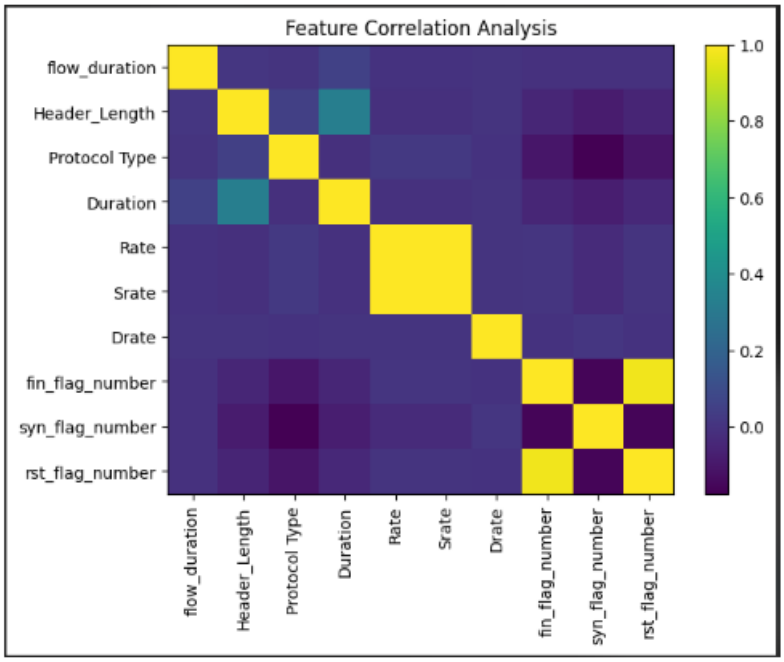


Figure 8: This image the analysis is conducted by correlation for some features of the IoT network traffic for intrusion detection

The correlation analysis of selected features of network traffic in CICIoT2023 is presented in Figure 8. The heatmap visualization shows how strong the relationship is between features like "flow duration," "header length," "protocol type" and other features that indicate network traffic [50]. The brighter the color, the stronger the positive correlation, and the darker the color, the weaker the positive correlation or the negative correlation. From the analysis it is evident that the traffic rate related features Rate, State and Drate have strong positive correlation, which shows that the communication behavior is similar in the IoT network traffic. Also, there are significant correlations to flag features like fin_flag_number and rst_flag_number, which are related to malicious network activities. On the other hand, there are other features that have either weak or negative correlations, which means that they have independent characteristics of the network and different communication behaviors. The correlation analysis helps in finding additional features that have the highest influence in training machine learning and deep learning models for intrusion detection, thereby eliminating redundant information and increasing the detection accuracy of the intrusions [51]. The results validate the application of feature correlation analysis as an effective tool for intelligent threat detection and adaptive optimization of cybersecurity in IoT-based systems such as healthcare, financial or connected systems.

VII. Discussion and Analysis

The experimental results of the proposed Adaptive AI-Driven Threat Detection Framework prove the tremendous power of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) technologies in securing IoT-enabled systems in various sectors, such as healthcare, financial, and connected systems, from sophisticated cyber threats [52]. By applying intelligent intrusion detection mechanisms to the CICIoT2023 dataset, high performance was observed on various evaluation metrics related to cybersecurity such as accuracy, precision, recall, F1-score and false positive rate. The findings validate the accuracy and effectiveness of cybersecurity systems powered by AI in analyzing diverse IoT network setups and detecting malicious communication activities in real-time. The success of the classification performance shows how well these adaptive learning techniques can enhance intrusion detection and help with proactive threat mitigation in smart structures connected in a network. The comparative study of the machine learning and deep learning algorithm showed that the accuracy of the detection of the deep learning algorithm (Long Short Term Memory (LSTM) and Convolutional Neural Networks (CNN) is better than the traditional machine learning algorithm (Random Forest and XGBoost). These models' greater performance is due to their ability to interpret the network traffic sequence and recognize changing malicious activities as time goes on. Likewise, CNN models were able to learn features and patterns in space and accurately identify hidden cyber threats in large-scale IoT traffic data [53]. The results indicate that deep learning methods can be used to significantly boost adaptive threat detection capabilities and intelligent cybersecurity analysis capabilities in dynamic IoT environments. The analysis of the cyberattacks showed that Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks were the most prevalent attacks in the investigated IoT environment. This discovery is indicative of the growing risks of these smart, healthcare, and financial systems being jeopardized by network flooding attacks that could disrupt communication services and impact system availability. The distribution of attacks showed several advanced types of attacks, such as DDoS-ICMP Flood, DDoS-UDP Flood, DDoS-TCP Flood, spoofing attacks, and brute-force intrusions. The proposed framework achieved high accuracy in the identification of these attack patterns, and demonstrated its ability to deal with various and evolving cyber threats in real time intrusion detection systems. The feature correlation analysis gave insights into the relationships between important features of network traffic such as the traffic rate, destination rate, source rate, protocol type and communication indicators based on the flags used in the network traffic. Good correlations between selected features helped to achieve a good feature selection and efficient classification during model training. In addition, the redundant information was filtered out and the computation efficiency was improved in the intrusion detection procedure during the pre-processing stage. The training and validation loss analysis also revealed that the models were consolidating during the training of deep learning, with no noticeable overfitting throughout the training process, which indicated that the model had a good generalization ability and reliable learning ability [54]. The study verifies that the combination of adaptive AI-based cybersecurity solutions and the current data of IoT devices like CICIoT2023 can successfully enhance the intrusion detection accuracy, boost real-time threat analysis, reduce false positive rates, and increase cybersecurity resilience for the connected smart systems with IoT applications in the fields of healthcare, financial, and other sectors. The proposed framework promotes the evolution of scalable and intelligent cybersecurity solutions that can handle the evolving cyber threats in today's inter-connected world.

VIII. Future Work

The proposed Adaptive AI-Driven Threat Detection Framework can be extended to include other advanced Artificial Intelligence (AI) and Deep Learning (DL) algorithms for intelligent cybersecurity analysis in IoT-integrated healthcare, financial, and connected systems in the future [55].The framework shows impressive intrusion detection accuracy with the CICIoT2023 dataset, but can be expanded with further real-world IoT datasets and live network environments for future studies to enhance scalability, adaptability, and real-time deployment. When extended to include cross-domain cybersecurity analysis for smart cities, industrial IoT and autonomous systems, it can extend its applicability in large-scale interconnected systems further. Going forward, there is a potential interest in testing Federated Learning and Edge AI capabilities to enable decentralized cybersecurity

monitoring and privacy-preserving threat detection in distributed IoT systems [56]. By allowing multiple connected devices and organizations to collaboratively train intrusion detection models without sharing sensitive data, federated learning can contribute to improved security and data privacy in healthcare and financial systems. Moreover, block chain can be used to improve the sharing of threat intelligence securely, authentication protocols and tamper-resistant cybersecurity management for interconnected smart systems. A further research avenue is to create compact and energy efficient deep learning models appropriate for the resource limited condition of IoT devices with low computational power and memory. Reducing model size, variable number, and transfer learning can help to boost computational efficiency without compromising accuracy of intrusion detection. Going forward, the integration of various AI models, such as CNN, LSTM, GRU, and transformer-based models, can be investigated for better identification of zero-day attacks and APTs. Moreover, techniques of Explainable Artificial Intelligence (XAI) can be integrated to increase the transparency and interpretability of the cybersecurity decisions made by deep learning models [57].This would help cybersecurity professionals and system administrators to interpret intrusion detection data and increase the overall confidence in AI-based cybersecurity systems. In conclusion, future developments of adaptive AI-driven cybersecurity solutions have the potential to greatly enhance intelligent threat mitigation, real-time anomaly detection, and proactive defense capabilities within next-generation IoT ecosystems.

IX. Conclusion

The Internet of Things (IoT) has expanded into today's health, financial and connected smart systems, adding a new layer of cybersecurity issues that must be addressed with intelligent and adaptive security solutions [58]. However, traditional IDSs are ineffective at defending against a constantly changing cyber threat landscape and attack signatures. The study introduced an Adaptive AI-Driven Threat Detection Framework to enhance the threat detection and intelligent threat analysis capabilities in real-time in heterogeneous IoT environments. The framework incorporated Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) algorithms to detect malicious network activities and bolster adaptive cybersecurity defenses for modern, interconnected systems. The study was based on the CICIoT23 dataset that consists of realistic IoT network traffic and several categories of cyber-attacks including Distributed Denial of Service (DDoS), Denial of Service (DoS), Botnet attacks, spoofing attacks, and Brute Force attacks. Various machine learning and deep learning models, such as Random Forest, XGBoost, Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) models were implemented and assessed based on common cybersecurity performance metrics: accuracy, precision, recall, F1-score, and false positive rate [59]. The results of the experiments proved that deep learning models outperform conventional intrusion detection models in detecting intrusions because of their ability to learn complex traffic patterns and changing malicious activities in IoT communication systems. The proposed framework was able to successfully enhance the accuracy of intrusion detection, reduce false positive rates, and enhance real-time threat analysis in an IoT-based healthcare, financial, and connected systems. The correlation analysis and loss evaluation also validated the effectiveness, stability, and generalization ability of the models that were implemented using AI. In summary, the research makes a significant impact in the field of developing scalable, intelligent, and adaptive cybersecurity solutions that can tackle the current challenges of IoT security [60]. The proposed framework offers a solid foundation for future research on intrusion detection using artificial intelligence and facilitates the development of secure and resilient IoT infrastructures to new cyber threats.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

Funding: Please add: "This research received no external funding" or "This research was funded by NAME OF FUNDER, grant number XXX" and "The APC was funded by XXX".
Conflicts of Interest: Declare conflicts of interest or state "The authors declare no conflict of interest."

References

[1]. Irshad, R. R., Sohail, S. S., Hussain, S., Madsen, D. Ø., Zamani, A. S., Ahmed, A. A. A., ... & Alwayle, I. M. (2023). Towards enhancing security of IoT-Enabled healthcare system. Heliyon, 9(11).
[2]. Ali, M., Raza, A., Akram, M. A., Arif, H., & Ali, A. (2025). Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection: Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection. Journal of Informatics and Interactive Technology, 2(1), 316-324.
[3]. Usha, M. (2024). Deep Learning Driven Predictive Threat Detection Framework for Secure Financial and Healthcare Cloud Platforms. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8141-8152.

[4]. Radhakrishnan, P., Ramar, V. A., Kushala, K., Induru, V., & Palanisamy, P. (2024). Enhancing Threat Detection in Healthcare Systems Through Cloud-Based Security Solutions. International Journal of Multidisciplinary and Current Research, 12(2), 180-189.
[5]. Joshi, A. (2023). A Unified Artificial Intelligence Framework for Secure Cloud and IoT Integration in Healthcare and Financial Systems.
[6] Mamidala, V., & Kumar, V. (2020). Enhancing healthcare security with cloud computing threat detection and anomaly monitoring. International Journal of Business Management and Economic Review, 3(3), 114.
[7]. Villegas-Ch, W., Gutierrez, R., Sánchez-Salazar, I., & Mera-Navarrete, A. (2024). Adaptive security framework for the Internet of Things: Improving threat detection and energy optimization in distributed environments. IEEE Access, 12, 157924-157944.
[8]. Peng, S. L., Pal, S., & Huang, L. (Eds.). (2020). Principles of internet of things (IoT) ecosystem: Insight paradigm (Vol. 174, pp. 467-549). Cham: Springer.
[9]. Arora, G., Dhariwal, N., & Marken, G. (2024, May). IoT Security Challenges in Healthcare: Navigating Risks, Strategies, and Innovations for a Safer Connected Health Ecosystem. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 60-68). IEEE.
[10]. Samant, P. K., Pathak, V., Ahmad, W., & Alabdultif, A. (2025). A lightweight trusted framework for secure data exchange and threat mitigation in IoT-enabled healthcare environments. Scientific Reports, 15(1), 39248.
[11]. Garg, A., Pandey, M., & Pathak, A. R. (2024). A Multi-Layered AI-IoT Framework for Adaptive Financial Services. International Journal of Emerging Trends in Computer Science and Information Technology, 5(3), 47-57.
[12]. Afonne, E. I., Ejeh, P., & Aworonye, L. C. (2025). An Ensemble-based Adaptable and Privacy-aware Threat Detection Mechanism for Wireless Sensor Network in Healthcare Systems. Scientific Journal of Computer Science, 1(2), 94-114.
[13]. Kumari, M., Gaikwad, M., & Chavhan, S. A. (2025, August). Securing IoT Enabled Health Monitoring Systems Using Machine Learning Approaches for Cyber Attack Detection and Prevention. In 2025 12th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP) (pp. 1-12). IEEE.
[14]. Alzakari, S. A., Sarkar, A., Khan, M. Z., & Alhussan, A. A. (2024). Converging technologies for health prediction and intrusion detection in internet of healthcare things with matrix-valued neural coordinated federated intelligence. Ieee Access, 12, 99469-99498.
[15]. Villafranca, A., Thant, K. M., Tasic, I., & Cano, M. D. (2025). AI-Enabled IoT Intrusion Detection: Unified Conceptual Framework and Research Roadmap. Machine Learning and Knowledge Extraction, 7(4), 115.
[16]. Khan, A., & Adnan, K. M. (2025). Big Data-Driven Federated Learning Model for Scalable and Privacy-Preserving Cyber Threat Detection in IoT-Enabled Healthcare Systems.
[17]. Alabdulatif, A., & Thilakarathne, N. N. (2024). A novel cloud-enabled cyber threat hunting platform for evaluating the cyber risks associated with smart health ecosystems. Applied Sciences, 14(20), 9567.
[18]. Ianculescu, M., Constantin, V. Ș., Gușatu, A. M., Petrache, M. C., Mihăescu, A. G., Bica, O., & Alexandru, A. (2025). Enhancing connected health ecosystems through IoT-enabled monitoring technologies: a case study of the Monit4Healthy system. Sensors, 25(7), 2292.
[19]. Liu, Y., Sharma, A., Rani, S., & Yang, J. (2025). Supply chain security, resilience and agility in IoT-driven healthcare. IEEE Internet of Things Journal.
[20]. Narayanan, A. (2025). Adaptive IoT Framework: A Modular Approach for Smart Device Integration. Authorea Preprints.
[21]. Singh, J., Singh, A., Manchanda, K., Kaur, A., Kaur, K., & Sethi, R. (2025, September). Secure Framework for Privacy and Risk Mitigation in IoT-Enabled Health Insurance. In 2025 2nd International Conference on Integration of Computational Intelligent System (ICICIS) (pp. 1-6). IEEE.
[22]. Mumtaz, A., & Liu, H. (2021). Evolutionary algorithms and ai in cybersecurity: Adaptive threat mitigation strategies using big data and iot. ResearchGate.
[23]. Thomas, J., & Ethan, A. (2024). Leveraging IoT Risk Modeling for Secure Health Monitoring Systems.
[24]. Pandey, A. K., Das, A. K., Kumar, R., & Rodrigues, J. J. (2024). Secure cyber engineering for IoT-enabled smart healthcare system. IEEE Internet of Things Magazine, 7(2), 70-77.
[25]. Perrig, A. (2025). Deep Learning Powered Secure Distributed Systems for Financial Analytics, Healthcare Monitoring, and Smart Infrastructure. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(6), 11152-11163.
[26]. Rahmati, M., & Rahmati, N. (2025). Adaptive Federated Edge Intelligence for Real-Time Cyberthreat Detection in Resource-Constrained IoT Environments: A Lightweight Deep Learning Approach. Journal of Computer Virology and Hacking Techniques, 21(1), 35.
[27]. Sharma, S. B., & Bairwa, A. K. (2025). Leveraging AI for intrusion detection in IoT ecosystems: a comprehensive study. IEEE Access.
[28]. Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber physical systems. SICS Software-Intensive Cyber-Physical Systems, 35(3), 159-183.

[29]. Reddy, M. V. K., Krishnan, S. B., Shaik, A., & Chakrabarti, P. (2025). AI-integrated adaptive MANET framework for IoT-driven healthcare systems: enhancing scalability, security, and real-time communication. The European Physical Journal Plus, 140(9), 941.
[30]. OFOE, N. T., & AGBESI, J. S. (2025). Cyber-physical security in IoT-enabled autonomous defense systems: Threat modeling and response. IRE Journals, 9(3), 110-120.
[31]. Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. IEEE Internet Computing, 25(4), 37-48.
[32]. Prawiyogi, A. G., & Meria, L. (2023). For a cps-iot enabled healthcare ecosystem consider cognitive cybersecurity. International Transactions on Artificial Intelligence, 2(1), 24-32.
[33]. Rahman, S. (2025). Explainable Trust-Centric Artificial Intelligence for Integrated Healthcare, Financial Security, and Cyber-Risk Management. Frontiers in Computer Science and Artificial Intelligence, 4(1), 01-06.
[34]. Mansoor, J. S., & Subramaniam, K. (2024). Healthcare Monitoring-based IoT framework for heart disease detection and classification. Journal of Angiotherapy, 8(3), 1-11.
[35]. Husnoo, M. A., Anwar, A., Chakrabortty, R. K., Doss, R., & Ryan, M. J. (2021). Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. IEEE access, 9, 153276-153304.
[36]. Kumar, A., Gupta, R., Kumar, S., Dutta, K., & Kumar, R. (2025). Intelligent Intrusion Detection System Using Improved Osprey Optimization and Stacked Ensemble Learning for IoT-Based Healthcare Systems. Security and Privacy, 8(6), e70121.
[37]. Wakili, A., & Bakkali, S. (2024). Internet of Things in healthcare: An adaptive ethical framework for IoT in digital health. Clinical eHealth, 7, 92-105.
[38]. Bajpai, S., Gochhait, S., Raghavendran, P., Gunasekar, T., & Alandoli, M. (2025, July). Adaptive Defense Mechanisms for IoT Ecosystems: A Response to Adversarial Tactics. In 2025 Multimedia University Engineering Conference (MECON) (pp. 1-6). IEEE.
[39]. Tawffaq, M. R., Jasim, M. A., Mejbel, B. G., Issa, S. S., Alamro, L., Shulha, V., & Aram, E. (2024, October). IoT security in a connected world: Analyzing threats, vulnerabilities, and mitigation strategies. In 2024 36th conference of open innovations association (FRUCT) (pp. 626-638). IEEE.
[40]. Trivedi, J., Tahir, M., & Isoaho, J. (2025). AI-Enhanced Threat Intelligence in Remote Patient Monitoring Systems: A Survey on Recent Advances, Challenges and Future Research Directions. IEEE Access.
[41]. Aheleroff, S., Xu, X., Lu, Y., Aristizabal, M., Velásquez, J. P., Joa, B., & Valencia, Y. (2020). IoT-enabled smart appliances under industry 4.0: A case study. Advanced engineering informatics, 43, 101043.
[42]. Ganai, K. A., Pandow, B. A., & Masoodi, F. S. (2024). IoT-enabled financial inclusion: Challenges, opportunities, and policy implications. Internet of Things Applications and Technology, 126-145.
[43]. Madanian, S., Chinbat, T., Subasinghage, M., Airehrour, D., Hassandoust, F., & Yongchareon, S. (2024). Health IoT threats: Survey of risks and vulnerabilities. Future Internet, 16(11), 389.
[44]. Czekster, R. M., Grace, P., Marcon, C., Hessel, F., & Cazella, S. C. (2023). Challenges and opportunities for conducting dynamic risk assessments in medical IoT. Applied Sciences, 13(13), 7406.
[45]. Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353-59377.
[46]. Baseer, K. K., Sivakumar, K., Veeraiah, D., Chhabra, G., Lakineni, P. K., Pasha, M. J., ... & Harikrishnan, G. (2024). Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease. Biomedical Signal Processing and Control, 92, 105988.
[47]. Jamil, F., Kahng, H. K., Kim, S., & Kim, D. H. (2021). Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms. Sensors, 21(5), 1640.
[48]. Khan, M. M., & Alkhathami, M. (2024). Anomaly detection in IoT-based healthcare: machine learning for enhanced security. Scientific reports, 14(1), 5872.
[49]. Qudus, L. (2025). Advancing cybersecurity: strategies for mitigating threats in evolving digital and IoT ecosystems. Int Res J Mod Eng Technol Sci, 7(1), 3185.
[50]. Alshuhail, A., Alshahrani, A., Mahgoub, H., Ghaleb, M., Darem, A. A., Aljehane, N. O., ... & Alzahrani, F. (2025). Machine edge-aware IoT framework for real-time health monitoring: Sensor fusion and AI-driven emergency response in decentralized networks. Alexandria Engineering Journal, 129, 1349-1361.
[51].Saha, H. N., Roy, R., Chakraborty, M., & Sarkar, C. (2021). IoT-enabled agricultural system application, challenges and security issues. Agricultural informatics: automation using the iot and machine learning, 223-247.
[52]. Goswami, N., Raj, S., Thakral, D., Arias-Gonzáles, J. L., Flores-Albornoz, J., Asnate-Salazar, E., ... & Kumar, S. (2023). Preserving security in internet-of-things healthcare system with metaheuristic-driven intrusion detection. Engineered Science, 25(3), 933.
[53]. Aoudi, S., & Al-Aqrabi, H. (2025). Integrating IoT Security Practices into a Risk-Based Framework for Small and Medium Enterprises (SMEs). Computer Standards & Interfaces, 104099.
[54]. Mccall, A. (2024). Cybersecurity in the age of AI and IoT: Emerging threats and defense strategies. Ladoke Akintola University of Technology: Ogbomoso, Nigeria.

[55]. Adewuyi, A., Oladele, A. A., Enyiorji, P. U., Ajayi, O. O., Tsambatare, T. E., Oloke, K., & Abijo, I. (2024). The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems. convergence, 20, 21.
[56]. Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2023). Machine learning for healthcare-IoT security: A review and risk mitigation. IEEE access, 11, 145869-145896.
[57]. Jebur, M. A., Abdulsada, H. R., Muhsin, I. A., Nahi, M. S., Ibrahim, E. R., & Muhammed, A. A. (2025, July). Artificial Intelligence-Based Threat Monitoring in Resilient Medical Diagnosis Communication Networks. In 2025 3rd International Conference on Cyber Resilience (ICCR) (pp. 1-7). IEEE.
[58]. Amiri, Z., Heidari, A., Zavvar, M., Navimipour, N. J., & Esmaeilpour, M. (2024). The applications of nature-inspired algorithms in Internet of Things-based healthcare service: A systematic literature review. Transactions on Emerging Telecommunications Technologies, 35(6), e4969.
[59]. Butpheng, C., Yeh, K. H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. Symmetry, 12(7), 1191.
[60]. Alsabilah, N. (2024). Adaptive cyber security for smart home systems (Doctoral dissertation, Howard University).
[61]. Dataset Link:
https://www.kaggle.com/datasets/himadri07/ciciot2023