Analyzing Cyber Attack Detection in IoT Healthcare Environments Using Artificial Intelligence

Rawan Marzooq Alharbi, Muhammad Asif Khan
Department of Information Systems-College of Computer Science and Engineering, Taibah University, Madina, Saudi Arabia

***Abstract*—The rapid growth of the Internet of Things (IoT) has significantly increased its integration into daily life. In recent years, the integration of IoT technologies in healthcare has significantly enhanced patient care and operational efficiency. One of the most promising areas for using IoT devices in healthcare or interconnecting medical devices is known as the Internet of Medical Things (IoMT). IoMT supports various healthcare services, e.g., remote patient monitoring. However, there are serious cyber-security concerns, as various attacks have targeted these IoMT devices in recent years. This research presents an analytical approach to understanding how Artificial Intelligence (AI) can improve the detection of cyber-attacks within IoT healthcare environments. The main goal of this research is to provide an AI-based model to detect cyber-attacks in IoMT in the healthcare environment. Many researchers have worked on developing a framework in this field to address critical cybersecurity threats. However, these efforts often fall short of covering other important aspects such as data privacy and interoperability. In this study, a model and framework are proposed to monitor IoT networks, and detect potential security breaches in real-time to help in mitigating risks while maintaining healthcare services. The key findings contribute to strengthening cybersecurity protocols in healthcare IoT environments in order to ensure the protection of sensitive information against emerging cybersecurity vulnerabilities.**

***Keywords*—IoT healthcare security; cyber-attack detection; healthcare security; AI in healthcare; smart medical systems**

I. Introduction

The Internet of Things (IoT) is a network of our daily life physical objects (things) that surround us and are connected together to send or receive data over internet without human intervention to ease human life. These things range from a wrist watch to home appliances and these are embedded with sensors which are smarter and more interactive with both us and the surrounding. The IoT promises to revolutionize our industries and economies by connecting billions of devices across the world. The IoT offers unparalleled opportunities to organizations for automation and novelty. As the technologies become established and matured, the IoT will be an integral part of industrial digital transformation. In future we will see spread of IoT from a smart highway to smart airports, smart home to smart cities, smart building to smart hospitals etc. There are various objects or things which have sensors such as car, door, lights, air conditioner etc. in different sectors can be connected through internet [1].

A survey conducted by Statista Inc [2] depicts there were 7.74 billion devices connected around the world in 2019 which could exceed 25 billion by 2030.

The exponential use of IoT devices in our daily lives has revolutionized various sectors including the healthcare sector. Thus, IoT is enabling the seamless connection of devices and systems to improve patient monitoring, diagnosis, and treatment [3]. Smart medical devices, and wearables have become integral components of modern healthcare, providing clinicians with real-time data and enhancing patient outcomes. Using IoT devices in healthcare or interconnecting medical devices is known as the Internet of Medical Things (IoMT) [4]. IoMT now supports various healthcare services, e.g., remote patient monitoring. However, this increased connectivity has also led to heightened vulnerabilities, making healthcare environments attractive targets for cyber-attacks [5].

The threats of a cyber-attack to target IoT healthcare systems mainly include data breaches, ransomware attacks, and denial-of-service (DoS) attacks [6]. The consequences of these attacks on IoT healthcare systems can be severe, ranging from compromised patient data to disruptions in critical healthcare services [7]. Since healthcare organizations strive to protect sensitive information and maintain operational integrity, traditional cybersecurity measures often fall short due to the complexity and scale of IoT networks. In this context, Artificial Intelligence (AI) emerges as a powerful tool for enhancing cybersecurity in IoMT environments. By leveraging advanced algorithms and machine learning techniques, AI can analyze vast amounts of data, identify patterns, and detect anomalies that may indicate potential threats.

With incessant growth in use and adoption of the IoT devices many IoT devices are found to have inherent security issues. The manufacturers of the devices focus on device functions and cost rather than the security features which in turn create security concerns and vulnerabilities in the devices. Wide spread of IoT devices and the information these devices need to provide features may be compromised, therefore, in this context cyber security has been extreme critical. A lot of research has tried to mimic a variety of hypothetical threats to enhance IoT security. Since more novel, and serious threats are being developed, requiring further work in this field especially in the healthcare sector. Moreover, the IoT devices only have limited amount of memory, computational capacity, and power. In such a situation, any communication issue caused by a cyber-attack might have hazardous consequences on a patient's health, and may even result in death.

Due to the rapid growth of infrastructure of IoT devices in recent years, IoT-based healthcare systems have become vital for detecting cyberattacks. Any attack may have a significant impact on the life of the patient. Therefore, the use of Artificial Intelligence (AI) is one of the finest solutions available to

improve the efficiency of detecting cyber-attacks in IoT healthcare environments. The aim of this research is to analyze the effectiveness of AI in detecting cyber-attacks within IoT healthcare environments, exploring both the current landscape and the future potential of AI-driven security solutions. In order to accomplish it, we have formulated the following research questions and we strive to address them in this research study:

RQ1: How integration of AI and Internet of Things (IoT) technologies can enhance cyberattacks detection and prevention capabilities in healthcare systems?

RQ2: What strategies can be employed to optimize AI cybersecurity model for scalable, cost effective and security compliant healthcare systems?

RQ3: How can AI improve the accuracy of cyberattack detection in IoT healthcare environment?

In order to find the answers of the research questions following hypotheses have been formed:

H_0 - AI Models improve the accuracy of cyberattack detection

H_1 - AI Model has the potential to enhance the detection of cyberattacks on IoT network in healthcare systems

The research study aims to develop an effective AI model to protect IoT healthcare systems by detecting cyberattacks in IoT healthcare networks and to provide an AI-based model that enhances the findings of existing research on an IoT healthcare security dataset. The proposed model aims to provide more accurate results from attack types compared to the relevant research of IoT healthcare datasets. The proposed model will get an optimum performance time compared to current strategies in relevant research of IoT healthcare datasets.

This research contributes to the body of knowledge by providing an efficient AI-based cybersecurity model for protecting IoT healthcare environment and for improving the accuracy and precision of cyber-attacks classification. Moreover, the model will show a potential to improve the sustainability of IoT systems by reducing the wastage of resources in identifying the cyber-attacks on time.

II. Literature Review

Due to the rapid advancement of technology, various communication and information technology-based solutions are being used in healthcare environments to facilitate both healthcare professionals and patients. These technologies mainly include the Internet of Things (IoT), artificial intelligence (AI), virtual reality (VR) and multi-agent systems. With the help of IoT technology, various gadgets having sensors and actuators are integrated to remotely monitor patients and provide different medical services like diagnosis, consultation, treatment, and information through on-ground healthcare staff [8]. Authors in study [9] proposed an IoT-based system to monitor the heartbeat and body temperature of a patient over a remote location through sensors and Bluemix technology. Similarly, authors in study [10] worked on a patient's activity recognition by analyzing the speech and movement patterns of a patient at home. They used a camera, breath sensor, and ECG for patient health monitoring. Likewise, researchers in study [11] developed a smartphone application to provide early medical assistance to elderly people at home.

With the progress of AI technology, healthcare data is now being analyzed and predicted through AI-based expert systems which help healthcare experts to make fast and efficient decisions for remote patients' healthcare. The AI models efficiently process the real-time sensor data and provide helpful information to healthcare professionals for better treatment decisions [12]. Similarly, VR technology is also used in telemedicine to improve the interaction between local healthcare staff and remote expert physicians for real-time patient healthcare including surgeries. Many recent research experiments have revealed that augmented reality (a type of VR) can improve the live motion-based interaction of remote healthcare experts for better diagnosis and treatment [13, 14].

Despite a lot of technological progress in healthcare environments, cybersecurity is a serious concern in IoT-based healthcare environments. Over the past few years, many researchers have worked on improving the security of IoMT-based healthcare systems. Authors in study [15] worked on detecting cyberattacks in IoT healthcare environments. The authors proposed an anomaly detection approach along with machine learning to detect cyberattacks in remote patient monitoring environments. The authors used the CICIoT dataset which contains 33 types of IoT attacks divided into seven main categories. The authors first pre-processed the CICIoT dataset for a balanced sample representation of each class. They further applied features- eliminating methods and features dimensionality reduction methods. Afterwards, they trained various machine learning models including Random Forest (RF), Logistic Regression (LR), Artificial Neural Network (ANN), and Adaptive Boosting (AB). Their proposed model achieved the highest accuracy based on Random Forest (RF), reaching up to 99.55%in binary and multiclass classification.

Similarly, researchers in [16] worked on detecting anomalies in IoT smart hospital environments. The authors proposed a low-latency anomaly detection system (ADS) and implemented it in the Contiki Cooja simulator. The authors achieved on average 80% accuracy in detecting three types of anomalies attacks including Rank and flooding attacks.

A study in [17] proposed an access control system for the privacy preservation of healthcare data in IoT healthcare architecture. The authors proposed a deep learning approach to secure IoT healthcare systems from unauthorized access by users and attackers. They also proposed a secure access control module by focusing on user attributes to protect IoT healthcare systems from cyberattacks caused due to unauthorized access. Their proposed model is based on a convolutional neural network (CNN) and it achieved 98% accuracy and 95% precision and F1-score.

In a study researchers [18] worked on improving the privacy and interoperability issues in IoT healthcare systems. The authors applied various data pre-processing techniques and trained a deep learning model that consists of a convolutional neural network (CNN) and Long Short-Term Memory (LSTM). Their proposed model achieved more than 80% accuracy, precision and recall on various datasets including PhysioNet, MIMIC, and eICU datasets.

In another study [19] proposed the cognitive machine learning based Cyber-Physical healthcare attack detection model to transmit healthcare data mules firmly. The collected data stored over the cloud platform where machine learning algos analyze the cyberattack patterns and predict their behavior accordingly. The proposed Cyber Machine Learning Anomaly Detection Framework (CML-ADF), can detect the cyberattacks over the edge nodes at the physical layer. The experimental results depict, CML-ADF framework achieving an accuracy of 98.2 % with an efficiency ratio of 97.8 % respectively. Moreover, it also outburst the delay and communication cost parameter over existing models with the ratio of 21.3 % and 18.9 % respectively.

The researchers in [20] demonstrate the Intrusion Detection System (IDS) under the umbrella of Internet of Medical Things (IoMT) based on Deep Recurrent Neural Network (DRNN) and supervised Machine Learning (SML) classifiers to forecast the unknown cyberattacks. In order to optimize features, the authors used the bio-inspired particle swarm approach which determines the outstanding results since its inception in the real-world optimization challenges. Under rigorous test beds and experimentation, the proposed SML model outperformed the existing approaches while attaining the accuracy of 99.76 %.

In a study, researchers [21] worked on the AI assisted IoT-CPS framework to diagnose patient diseases such as Diabetes, Heart anomalies and Gait disorders. Each disease has its own set of detection parameters with respect to patient gender, age and complexity. The author used the openly available dataset, acquired from Kaggle repository for the execution of proposed AI-enabled IoT-CPS methodology. The experimental tests showed that the proposed framework outperformed the existing studies with an accuracy of 86.4 % indeed.

A research study [22] proposed the framework to generate IoT based normal and malicious data in order to develop the IoT assisted context aware security solutions for malicious traffic detection in various use cases. The author named the proposed open-source IoT data generator as IoT-Flock. It not only generates the traffic but also converts the captured data into a particular dataset for further analysis and recommendation. While using the proposed framework, the author generates the IoT-healthcare dataset which comprises both normal and IoT attack affected data which is ultimately being detected with the help of multiple ML based classifieds to protect the healthcare system from cyberattacks. The proposed context aware IoT based data generator is very effective to analyze the sensory IoT healthcare use cases in terms of cyber security.

The authors in [23] developed the cyber-attack inclusion with anomaly detection methodology accompanying recursive feature elimination (RFE) and multi-layer perceptron (MLP) approach. Both of these approaches are very effective to identify optimal feature selection and performance evaluators. The proposed model was tested on various IoMT cyber security datasets with an average accuracy of 98.08 % respectively.

In a study [24] proposed the AI assisted Artificial Fish Swarm-driven Weight normalized Adaboost (AF-WAdaBoost) model for the optimization of accuracy and sustainability parameters to identify cyberattacks in IoT healthcare systems. The proposed AF-WAdaBoost mechanism fiercely adjusts the ML classifiers to enhance accuracy and persistence against evolving threats. The experimental study shows the proposed model outperformed traditional IoT- healthcare cyberattack detection approaches with an accuracy of 98.69 %, F-measure and Precision with 94.86 % and 95.72 % respectively.

Researchers in study [25] worked on the novel cyberattack healthcare anomaly detection technique based on Cyber Physical System (CPS) to enhance network security. A quantum cloud Federated learning mechanism has been implemented on the CPS in order to build an IoT healthcare network. Existing approaches lack to achieve reasonable values for Round Trip Time (RTT) using Transmission control Protocol (TCP) packets and are ineffective on the large number of packets. Our proposed model attained network efficiency of 92 %, security analysis with 89 %, training and validation loss of 79 % and 49 % respectively.

A research study [26] suggested the novel approach for assessing the cybersecurity of e-healthcare applications i.e., assistance of quantum machine learning. In this approach the author proposed the deep variational adversarial network encoder with fuzzy Gaussian quantile neutral network to identify and classify the useful characteristics of user activity data patterns to identify the vicious user to enhance the overall network security. The implementation of the proposed approach shows vigorous results in terms of learning rate, prescient misfortune, transmission influence, jitter, throughput and dynamic serverless response time. Moreover, the proposed system attained the random accuracy of 98%, F-1 score of 75 %, Mean Average Precision of 65 % and the kappa Coefficient of 69% which outperformed the existing server based E-healthcare security approaches.

In a study [27] illustrated the comparison between various AI-driven threat detection approaches to enhance security and to mitigate cyber threats in the IoT Healthcare environment. In the world of AI-driven cyber security solutions, the most prominent are transformer based models, federated learning and blockchain integration to step into the real-time threat detection systems. The most prominent approach to mitigate cyberattack in the Enhanced AI-based Network intrusion Detection using Generative Adversarial Networks (GANs) which attained the accuracy of 98.2 % which exceeded the preceding resilient intrusion detection system and multi-domain trojan detection framework which were at 97.8 % and 97.1 % respectively.

The authors in [28] illustrated how future healthcare hubs and proactive smart devices implement their own cybersecurity models to ensure full proof AI assisted healthcare communication channels. The proposed AI based healthcare communication cyber security model set the digital healthcare communication IEEE standards interviewing the cybersecurity policies. Moreover, the Joint Optimized Infrastructure for Network Empowered Research (JOINER) came into existence to ensure secure future communication in the healthcare sector. Now each AI-driven emerging cybersecurity policy relies on JOINER architecture. The proposed approach outperformed the existing communication trends, in terms of data rate, mobility, latency, connectivity gap, and reliability.

A study [29] introduced the framework of trustworthiness and decision-making support mechanism within the internet of

medical things (IoMT) use cases. Keeping in view the shortcomings of risk management and management approaches to accessed the IoMT context aware scenarios in the existing models, lack proper automation and inability to mitigate the various security risks in the healthcare system, the proposed (MLRA-Sec) framework integrate the Hybrid Risk Assessment (RA) model with ML-based anomaly detection technique to ensure and evaluate cumulative IoMT risk. Experimental study shows effective outcome as compared to the state of the art intrusions detection IoT-ML based models.

A research study conducted by study [30] focused on addressing the problem of cyber risk assessment in IoT healthcare environments. The authors proposed a lightweight, efficient and dynamic approach for risk assessment of security events in IoT healthcare infrastructure. The authors generated synthetic data and then executed multiple simulation scenarios on it while mapping the attack surface and applying threat models. The proposed approach not only highlight the security risks but also provides some helpful information to mitigate the cyber threats.

Authors in study [31] highlighted the challenges in the healthcare security system with the advancement of energy constraint communication devices. Considering the severity of the issue, the author developed the monitoring frequency-based detection and dynamic threshold mitigation method using Temporal Convolutional Networks (TCNs) in the 5G healthcare IoT (H-IoT) environment. The proposed approach calculates the H-IoT node's incoming and outgoing data mules counts for five seconds with respect to overall data traffic. This dynamic approach provides adaptive security by taking the mean value of detected malicious data across all nodes to evaluate the threshold cap to enhance the classification accuracy and restricts the true DDos attacks. The experimental test beds conducted under two communication protocols i.e., Message Queuing Telemetry Transport (MQTT) and User Datagram Protocol (UDP) in a realistic 5G based healthcare environment. The proposed model attained the average accuracy of 99 % on MQTT datasets and 99.99 % on UDP dataset with 80 % mitigation.

A research work carried out by study [32] showed the impact and comparison of AI-driven existing IoMT security models. With recent advancement in IoMT, in spite of its effectiveness, it also becomes the easy corner for hackers to breach the patient's sensitive information and use it for their own evil desires. To resiliate these attacks, novel taxonomy of AI based intrusions detection IoMT schemes have been highlighted in this article. Moreover, tasks and processes are carried out over Cloud-Fog-Edge architectures to reduce the overall latency and efficient use of computational resources in real-time to enhance the efficiency of the system, also being a part of its comparison approaches.

Authors in study [33] focused on the vulnerabilities to cyberattacks in the IoT healthcare system. Along with the rapid use of heterogeneous smart devices becomes a more severe concern as the time proceeds. In this paper, author proposed the deep neural network assisted cyberattack detection model to accompanying the unknown cyberattacks in IoT healthcare environment. An AI based proposed anomaly cyber threats have been tested on latest ECU-IoHT dataset and attained the accuracy of 99.85% under the average area receiver characteristic cure is at 0.99 with the false positive is 0.01 that highlights the effectiveness of the proposed cyberattack detection system as compared to the state of the art approach.

Researchers in study [34] worked on preventing cyber threats in IoT healthcare environments. The authors proposed a framework to detect different types of cyberattacks in IoT healthcare networks. The authors used four different types of dataset related to cybersecurity attacks for having maximum cyberattacks coverage and getting a more generalized AI model. The authors applied different data pre-processing techniques like data cleaning, data imputation, and dimensionality reduction. Afterwards, they trained the pre-processed data over an attention-based bi-LSTM deep convolved network to detect the cyber-attacks in IoT healthcare environments. Overall, the authors achieved around 99% accuracy on all datasets.

A research study [35] proposed a hybrid approach to detect cyber-attacks in internet of medical things (IoMT) environment. In order to efficiently detect the cyber-attacks, the authors integrated three AI models which include K-nearest neighbors (KNN), long-short term memory (LSTM), and principal component analysis (PCA). Both the LSTM and PCA models were used for data pre-processing. Afterwards, they trained and tested KNN model for detect cyber-attacks in IoMT environment. The authors tested the proposed hybrid framework over four datasets which include TON-IoT, ECU-IoHT, ICU, and WUSTL-EHMS dataset. Overall, the proposed approach resulted 99% accuracy for detecting cyber-attacks in IoMT environment.

Similarly, researchers in study [36] worked on efficiently detecting the intelligent detection of intrusions in IoMT environment. The authors integrated two deep learning models which include convolutional neural network (CNN) and LSTM for efficient detection of intrusions. The CNN was mainly used for features extraction whereas the LSTM was used sequential network traffic flows prediction. The authors referred the proposed intrusion detection system (IDS) as hybrid deep learning-based IDS solution for IoMT (HIDS-IoMT). The proposed approach was also tested in a fog computing environment where the proposed HIDS-IoMT model was deployed on a Raspberry Pi device which not only demonstrated an accurate detection of intrusions but also reduced the detection latency as the IDS was deployed on an edge device.

Likewise, authors in study [37] designed a framework for intrusion detection in IoMT environments. The authors proposed a stacking ensemble approach by stacking machine learning and deep learning models into two groups to effectively secure the IoMT network. The authors used ECU-IoHT dataset. They first pre-processed the dataset by applying data cleaning, data normalization, data balancing and features selection techniques. The proposed framework combined both machine learning and deep learning classifiers to detect various cyber-attacks in IoMT environment. Moreover, in order to deploy the proposed AI-based IDS in real-time [38], the authors implemented Kappa architecture which helped to update data streams with low latency. The proposed approach resulted 99.1%accuracy for binary class classification and 99.3%accuracy for multi-class classification to detect four types

of cyber-attacks including spoofing, denial of service, scanning, and Smurf attack.

Authors in study [39] proposed a hybrid deep learning framework to enhance the security and quality of service (QoS) in IoT healthcare systems. The authors introduced a novel software-defined network (SDN) based architecture and integrated it with a security module that is responsible to detect cyberattacks in healthcare network. The secure module was mainly developed by training and testing a Bidirectional LSTM model over CICDDoS2019 dataset. In order to improve the QoS by reducing transmission, the authors used CNN model in SDN controller to find the best fog node integrated with SDN which further improved the overall network life. The proposed hybrid deep learning framework resulted 99.59% accuracy, 99.53% F1-score, and 3 ms delay in order to detect cyber-attacks in IoT healthcare environments.

The literature reviewed above provided us information of some datasets used to detect, train and test AI model in healthcare environment. Table I shows short description of these datasets:

TABLE I. DATASETS USED TO DETECT, TRAIN AND TEST AI MODEL IN HEALTHCARE ENVIRONMENT

Dataset	Reference	Description
CICIoT	Khan & Alkhathami, 2024	This dataset consists of real-time normal and cyberattacks traffic. It is widely used to train and test AI models to efficiently detect cyberattacks. It includes real-time network traffic of 105 real IoT devices. It contains mainly 156 features and covers 33 types of cyber-attacks data
Aegean AWID	Pimple & Sharma, 2025	This dataset contains the network attacks traffic of Wi-Fi attacks. It has 156 features
IoT-ICU	Hussain et al., 2021	This dataset mainly focused on ICU environment where different sensors and actuators are connected over a Wi-Fi. It contains different types of cyberattacks and normal traffic
NSLKDD	Saheed & Arowolo, 2021	It is an updated version of KDD intrusion detection dataset. It has some class imbalance issues
ECU-IoHT	Kilincer et al., 2023	This dataset was mainly developed to analyze the vulnerabilities in IoT healthcare environment
CICIDS2017, UNSW-NB15	Alsulami, 2024	These are basically general cyberattack dataset. But these are also used in healthcare environment
IoT-23, LINET 2020, NetML	Prabakar et al., 2024	This dataset mainly contains IoT malware related data to detect and figure out the potential attacks in healthcare environments
Bot-IoT	Ksibi et al., 2025	This dataset mainly contains botnet attack traffic

III. RESEARCH METHODOLOGY

In order to conduct research for finding out solution of the research questions stated earlier, we adopted design science research methodology which consists of five major stages. The Fig. 1 shows the five stages including data collection, data preprocessing, feature selection, AI models training and performance comparison.

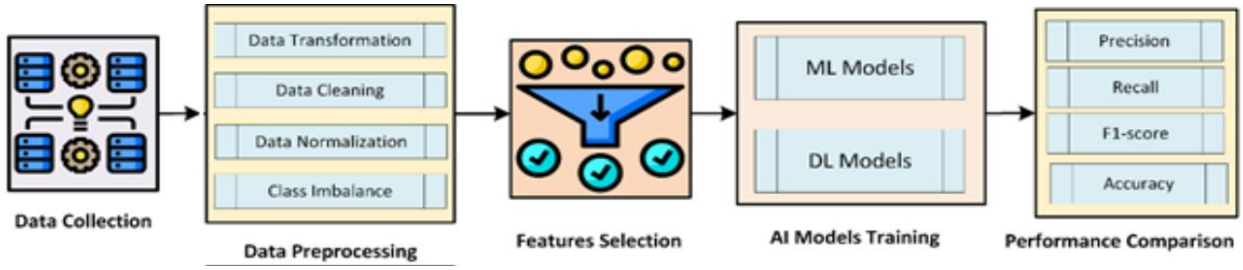

Fig. 1. The proposed methodology for cyber-attacks detection using AI in IoT healthcare environments.

A. Data Collection

The data collection is a primary step of our proposed methodology. To go through further steps to recognize cyber-attack detection using AI in IoT healthcare environments, we first need to collect a dataset. A few researchers have worked on detecting cyber-attacks in IoT healthcare environments. Therefore, we reviewed existing datasets and then selected the dataset with a vast variety of cyber-attacks. The IoT healthcare security dataset named as CIC IoMT dataset (Dadkhah et al., 2024) contains eighteen (18) types of cyber-attacks traffic including spoofing, scanning, TCP, UDP, and MQTT attacks. These eighteen (18) types of cyber-attacks are categorized into five classes which include spoofing, reconnaissance (RECON), MQTT, denial of service (DoS) and distributed DoS (DDoS) attacks. The complete mapping of eighteen (18) types of cyber-attacks along with their classified category are shown in Table II.

TABLE II. CYBERATTACKS WITH CLASSIFIED CATEGORIES

Category	Cyber-attacks
SPOOFIN	ARP Spoofing
RECON	Ping Sweep, Recon VulScan, OS Scan, Port Scan
MQTT	Malformed Data, DoS Connect Flood, DDoS Publish Flood, DOS Publish Flood, DDoS Connect Flood
DOS	DOS TCP, DOS ICMP, DOS SYN, DOS UDP
DDOS	DDoS SYN, DDOS TCP, DDOS ICMP, DDOS UDP

The CIC IoMT healthcare security dataset (Dadkhah et al., 2024) is mainly saved in packet capture (.pcap) file format collected via WireShark tool. A few .pcap files are also converted into the .csv file format. The CIC IoMT dataset (Dadkhah et al., 2024) contains network traffic of 40 IoMT devices including 25 real devices and 15 simulated devices. The dataset contains three types of communication protocols used by

healthcare devices which include Wi-Fi, Bluetooth, and MQTT devices. The MQTT-based healthcare devices are simulated devices whereas the Bluetooth and Wi-Fi-based healthcare devices are real devices integrated into a real-time network. The CIC IoMT dataset (Dadkhah et al., 2024) has 45 features in each .csv file without labels. These features are enlisted and briefly described in Table III. In summary, the CIC IoMT dataset (Dadkhah et al., 2024) is big dataset contains multiple .pcap and .csv files and each .csv file contains samples in range 5000 to 80,000 samples. There is a minor issue of class imbalance if look at it from the perspective of binary or multi-class classification.

TABLE III. LIST OF FEATURES WITH BRIEF DESCRIPTION IN CIC IOMT DATASET (DADKHAH ET AL., 2024)

Feature	Description
Header Length	Mean of the header lengths of the transport layer
Time-To-Live	Time-to-live
Rate	Speed of packet transmission within a window in packets/sec
fin flag number	Proportion of packets with FIN flags in the window
syn flag number	Proportion of packets with SYN flags in the window
rst flag number	Proportion of packets with RST flags in the window
psh flag number	Proportion of packets with PSH flags in the window
ack flag number	Proportion of packets with ACK flags in the window
ece flag number	Proportion of packets with ECE flags in the window
cwr flag number	Proportion of packets with CWR flags in the window
syn count	Count of Syn flag occurrences in packets
ack count	Count of Ack flag occurrences in packets
fin count	Count of Fin flag occurrences in packets
rst count	Count of Rst flag occurrences in packets
IGMP	Average number of IGMP packets in the window
HTTPS	Average number of HTTPS packets in the window
HTTP	Average number of HTTP packets in the window
Telnet	Average number of Telnet packets in the window
DNS	Average number of DNS packets in the window
SMTP	Average number of SMTP packets in the window
SSH	Average number of SSH packets in the window
IRC	Average number of IRC packets in the window
TCP	Average number of TCP packets in the window
UDP	Average number of UDP packets in the window
DHCP	Average number of DHCP packets in the window
ARP	Average number of ARP packets in the window
ICMP	Average number of ICMP packets in the window
IPv	Average number of IPv packets in the window
LLC	Average number of LLC packets in the window
Tot Sum	Total packet length within the aggregated packets (window)
Min	Shortest packet length within the aggregated packets (window)
Max	Longest packet length within the aggregated packets (window)
AVG	Mean packet length within the aggregated packets (window)
Std	Standard deviation of the packet length within the aggregated packets (window)
Tot Size	(Avg.) Length of the packet
IAT	Interval mean between the current and previous packet in the window
Number	Total number of packets in the window
Variance	Variance of the packet lengths in the window
Protocol Type	Mode of protocols in the window

B. Data Preprocessing

Once we are done with data collection, the next step is to pre-process the dataset in order to pass a refined dataset to AI models for better training. As shown in Fig. 2, the first step in data pre-processing is data transformation, i.e., to transform the categorical values to numeric integer values because the AI models only work on number values. So, to perform data transformation, we used the one-hot encoding technique After the data transformation, we performed data cleaning to remove missing values, null values or infinite values from the dataset. Once the dataset is cleaned, we then need to normalize the dataset to scale the feature values in a comparable range. For this purpose, we used Min-Max normalization which scales the feature values in the range [0, 1].

We noticed that there was a class imbalance issue in the dataset. To fix the class imbalance issue, we used the down-sampling technique as there were some attacks where samples were less than 5000. So, when we combined the data-frames of such attack samples based on same class, we came to know that minimum 18000 samples were present in a class. Therefore, to fix the class imbalance issue, we dropped down the samples from other attack classes by randomly selecting 18000 samples from each class via down-sampling technique. Eventually, after the down-sampling, we had 18000 samples from each of five attack classes as mentioned in Table II which in total leads to 18,000 x 5 = 90,000 attack samples. Similarly, we randomly selected 18000 samples from benign, i.e., normal class samples as well. So in total, we had 90,000 (attack samples of five classes) + 18000 (benign samples of 1 class) = 108,000 samples for training and testing AI models.

C. Features Selection

Although the dataset is pre-processed, we further need to perform features selection to provide the most useful features to machine learning models for better performance. For this purpose, we applied four commonly used features selection techniques, i.e., Anova, Chi2, mutual information, and extra tree features selection method to select only useful features from the dataset. Using these four features selection techniques, we tried different numbers of features i.e., 20, 30 features out of total 45 features and check on which feature set the machine learning models yield better performance by comparing the results with the performance achieved while training AI models on all features. Therefore, we considered three scenarios.

- Training and testing AI models on all features.
- Training and testing AI models on 20 features selected via features selection methods.

- Training and testing AI models on 30 features selected via features selection method.

D. Models Training

Before starting training to AI models, we first need to divide the dataset into a training set and a testing set. To split the dataset, we use the 80:20 ratio, i.e., 80% dataset were split randomly into training-set and 20% data were used for testing-set. As shown in Fig. 2, we trained both machine learning models and deep learning models for cyber-attacks detection in IoT healthcare environments. Therefore, we trained five commonly used machine learning models, i.e., decision tree (DT), random forest (RF), Naïve Bayes (NB), k-nearest neighbors (KNN), and logistic regression (LR). Similarly, we trained two commonly used deep learning models, i.e., multi-layer perceptron (MLP), and convolutional neural network combined with long-short term memory (CNN+LSTM) model, for cyber-attacks detection in IoT healthcare environments.

E. Performance Comparison

We compared the performance of all trained models to decide the best-performing model. We used four commonly used performance metrics including accuracy, precision, recall and F1-score. These evaluation metrics are defined in the next results and discussion section.

IV. Results

In order to conduct experiment, we acquired publicly available dataset and proceeded with further stages. For the data preprocessing, data transformation and training and testing of the AI models for cyber-attacks detection in IoT healthcare environments, we used Python programming language and some standard AI models and libraries, such as numpy, pandas, scikit-learn, and tensorflow.

To begin with experimentation, we considered three scenarios in which seven AI models are trained for cyber-attacks detection in IoT healthcare environments. These seven commonly used AI models include decision tree (DT), random forest (RF), Naïve Bayes (NB), k-nearest neighbors (KNN), logistic regression (LR), multi-layer perceptron (MLP), and convolutional neural network combined with long-short term memory (CNN_LSTM) model. All these models were trained with their default parameters set in Python's scikit-learn library except MLP and CNN_LSTM. For MLP and CNN_LSTM, we used tensorflow library. We further used Adam optimizer, set learning rate = 0.001, defined four hidden layers. After training these models, we then need to evaluate their performance on test data for cyber-attacks detection. For this purpose, we used four commonly used performance evaluation parameters, i.e., precision, recall, F1-score, and accuracy. These performance matrices are defined as follows:

1) Precision (PR): It tells us about the capacity of a system to accurately recognize an attack upon the happening of an actual cyber-attack. It presents a correlation between accurately anticipated attacks and actual outcomes. Mathematically, precision is expressed as:

$$PR = \frac{True\ Positives}{\text{True Positives } + \text{ False Positives}} \times 100$$

2) Recall (RE): It tells us about the correctly identified cyber-attack events upon its existence in the network. Mathematically, recall is written as:

$$RE = \frac{True\ Positives}{\text{True Positives } + \text{ False Negatives}} \times 100$$

3) Accuracy (AC): It tells us about how many attack events are categorized as attacks and how many regular network packets are categorized as normal traffic. It also indicates the proportion of accurate predictions relative to the total number of samples. Mathematically, it is expressed as:

$$AC = \frac{\text{True Positives } + \text{ True Negatives}}{\text{Total Samples}} \times 100$$

*4) F1- score:*It is defined as a harmonized average of recall and precision. It tells us about the percentage of correctly predicted testing samples as cyber-attacks. Mathematically, it is expressed as:

$$F1\ score = 2 \times \frac{PR\ x\ RE}{PR + RE}$$

In order to evaluate the best performance among the AI models, we have three scenarios as we mentioned earlier and will find out the best-performing model to recognize cyber-attacks in each scenario.

B. Scenario 1 - Training and Testing AI Models on All Dataset Features

We applied the data preprocessing techniques stated earlier and after cleaning and normalization of the data, we selected all features to test and compare performance of the seven AI models. Table IV shows overall performance of seven AI models for cyberattacks detection in IoT healthcare networks over the test data.

TABLE IV. Performance of All Seven AI Models when All Features Selected

Classifier	Accuracy	Precision	Recall	F1 score
DT	0.97	0.9	0.97	0.97
RF	0.98	0.98	0.98	0.98
NB	0.45	0.41	0.46	0.35
KNN	0.94	0.94	0.94	0.94
LR	0.36	0.40	0.36	0.32
MLP	0.52	0.56	0.52	0.49
CNN_LSTM	0.84	0.85	0.84	0.84

It can be observed that RF classifier efficiently identified critical cyberattacks whereas the LR classifier poorly performed. Overall, the RF classifier resulted 98% accuracy, 98% precision, 98% recall and 98% f1 score for cyberattacks detection IoT healthcare environments. Fig. 2 shows the performance of all the seven models when all features were selected.

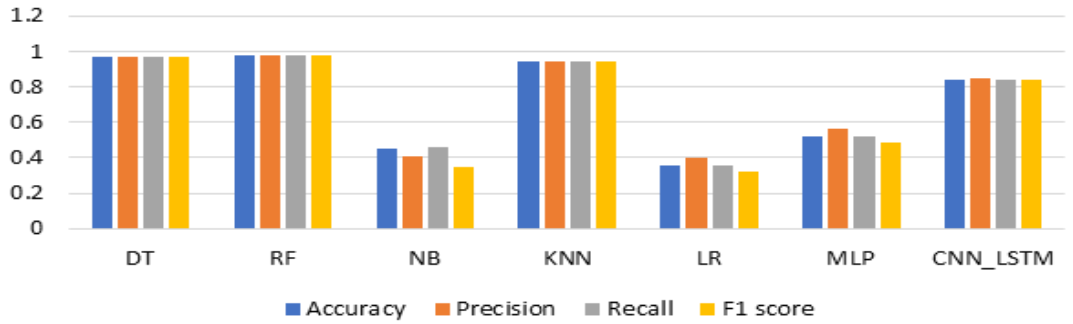

Fig. 2. Test results of all seven AI models when all features selected.

C. *Scenario 2 - Training and Testing AI Models on Top 20 Features*

After the data preprocessing, we selected top 20 features to test and compare the performance of AI models on all features vs. a subset of features according to proposed methodology for cyberattacks detection in IoT healthcare environments. We applied four features selection techniques including Anova, Chi^2, Mutual information and Extra tree using scikit-learn library in Python programming language. Table V shows the accuracy and recall scores of seven AI models for cyberattacks detection in IoT healthcare networks over the test data.

It can be observed that for Accuracy, the RF classifier efficiently identified critical cyberattacks whereas the LR classifier poorly identified cyber-attacks. Overall, the RF classifier resulted 98% accuracy for Anova, 97% accuracy for Chi2, 97% accuracy for Mutual information and 97% accuracy for Extra Tree features selection technique for cyberattacks detection IoT healthcare environments. Similarly, for Recall, the RF classifier efficiently identified critical cyberattacks whereas the LR classifier poorly performed. Overall, the RF classifier resulted 89% recall for Anova, 98% recall for Chi^2, 98% recall for Mutual information and 98% accuracy for Extra Tree features selection technique for cyberattacks detection IoT healthcare environments. Fig. 3 shows accuracy and recall of the seven AI models on top 20 selected features.

We obtained data of Precision and F1 scores for all AI models when 20 features were selected. Table VI shows the data.

TABLE V. ACCURACY AND RECALL SCORES OF SEVEN AI MODELS WHEN 20 FEATURES SELECTED

Classifier	Accuracy				Recall			
	Anova	Chi2	Mutual_Info	Extra_Tree	Anova	Chi2	Mutual_Info	Extra_Tree
DT	0.86	0.97	0.96	0.96	0.87	0.97	0.97	0.97
RF	0.98	0.97	0.97	0.97	0.89	0.98	0.98	0.98
NB	0.37	0.45	0.45	0.45	0.38	0.46	0.46	0.45
KNN	0.78	0.94	0.94	0.94	0.78	0.94	0.94	0.95
LR	0.40	0.35	0.35	0.29	0.41	0.35	0.35	0.29
MLP	0.70	0.46	0.48	0.42	0.71	0.47	0.49	0.43
CNN_LSTM	0.84	0.83	0.84	0.84	0.84	0.85	0.84	0.84

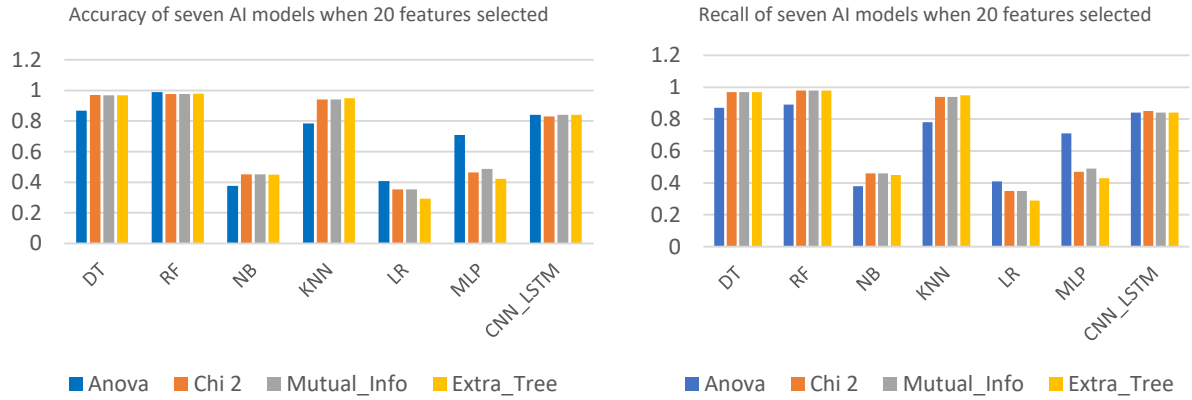

Fig. 3. Test results of Accuracy and Recall of seven AI models when 20 features selected.

TABLE VI. PRECISION AND F1 SCORES OF SEVEN AI MODELS WHEN 20 FEATURES SELECTED

Classifier	Precision				F1 score			
	Anova	Chi2	Mutual_Info	Extra_Tree	Anova	Chi2	Mutual_Info	Extra_Tree
DT	0.47	0.97	0.97	0.97	0.87	0.97	0.97	0.97
RF	0.89	0.98	0.98	0.98	0.89	0.98	0.98	0.98
NB	0.38	0.41	0.41	0.42	0.33	0.36	0.36	0.36
KNN	0.79	0.94	0.94	0.95	0.78	0.94	0.94	0.95
LR	0.26	0.39	0.39	0.29	0.30	0.29	0.29	0.25
MLP	0.77	0.64	0.53	0.44	0.70	0.43	0.46	0.37
CNN_LSTM	0.84	0.85	0.84	0.84	0.84	0.85	0.84	0.84

It can be observed that the RF classifier efficiently identified critical cyber-attacks whereas the LR classifier poorly identified cyber-attacks. Overall, the RF classifier resulted 89% precision for Anova, 98% precision for Chi^2, 98% precision for Mutual information and 98% precision for Extra Tree features selection technique for cyber-attacks detection IoT healthcare environments. Similarly, F1 scores show that RF classifier efficiently identified critical cyber-attacks whereas the LR classifier poorly identified cyber-attacks. Overall, the RF classifier resulted 89% f1-score for Anova, 98% f1-score for Chi^2, 98% f1-score for Mutual information and 98% f1-score for Extra Tree features selection technique for cyber-attacks detection IoT healthcare environments. Fig. 4 shows Precision and F1 scores of the seven AI models on top 20 selected features.

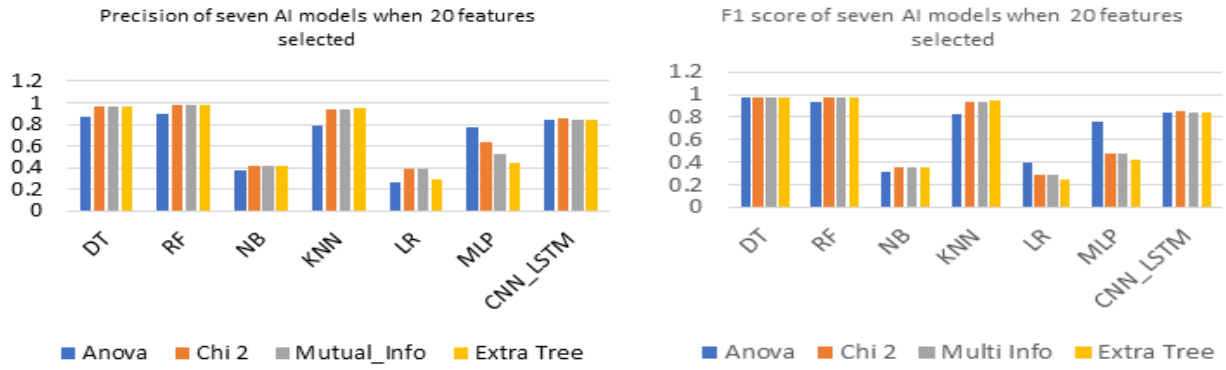

Fig. 4. Test results of Precision and F1 scores of seven AI models when 20 features selected.

D. Scenario 3 - Training and Testing AI Models on Top 30 Features

In this scenario, we selected top 30 features to test and compare the performance of AI models on all features vs. a subset of features according to the proposed methodology for cyber-attacks detection in IoT healthcare environments. Table VII shows the accuracy and recall scores of seven AI models for cyberattacks detection in IoT healthcare networks over the test data.

It can be observed that RF classifier efficiently identified critical cyberattacks whereas the LR classifier poorly identified the cyberattacks. Overall RF resulted 93% accuracy and recall for Anova, 98% accuracy and recall for Chi^2, 98% accuracy and recall for Mutual_Info and 98% accuracy and recall for Extra_Tree features selection techniques for cyberattacks detection in IoT healthcare environments. Fig. 5 shows the Accuracy and Recall scores metrics of seven AI models for 30 features selected.

TABLE VII. ACCURACY AND RECALL SCORES OF SEVEN AI MODELS WHEN 30 FEATURES SELECTED

Classifier	Accuracy				Recall			
	Anova	Chi2	Mutual_Info	Extra_Tree	Anova	Chi2	Mutual_Info	Extra_Tree
DT	0.91	0.97	0.97	0.97	0.91	0.97	0.97	0.97
RF	0.93	0.98	0.98	0.98	0.93	0.98	0.98	0.98
NB	0.38	0.45	0.45	0.45	0.38	0.46	0.46	0.45
KNN	0.82	0.94	0.94	0.95	0.82	0.94	0.94	0.95
LR	0.44	0.35	0.35	0.30	0.44	0.35	0.35	0.29
MLP	0.74	0.5	0.5	0.46	0.74	0.5	0.5	0.46
CNN_LSTM	0.84	0.85	0.84	0.84	0.84	0.85	0.84	0.84

Fig. 5. Test results of Accuracy and Recall scores of seven AI models for 30 features selected.

We obtained the data of Precision and F1 scores of seven AI models for cyberattacks detection in IoT healthcare networks over the test data. Table VIII shows the data.

The RF classifier efficiently identified critical cyberattacks whereas LR poorly performed in identifying the cyberattacks. Overall RF resulted 93% precision and F1 for Anova, 98% precision and F1 for Chi^2, 98% precision and F1 for Mutual_Info and 98% precision and F1 for Extra_Tree features selection techniques for cyberattacks detection in IoT healthcare environments. Fig. 6 shows the Precision and F1 scores metrics of seven AI models for 30 features selected.

TABLE VIII. ACCURACY AND F1 SCORES OF SEVEN AI MODELS WHEN 30 FEATURES SELECTED

Classifier	Precision				F1 scores			
	Anova	Chi2	Mutual_Info	Extra_Tree	Anova	Chi2	Mutual_Info	Extra_Tree
DT	0.91	0.97	0.97	0.97	0.91	0.97	0.97	0.97
RF	0.93	0.98	0.98	0.98	0.93	0.98	0.98	0.98
NB	0.37	-0.41	0.41	0.42	0.31	0.36	0.36	0.36
KNN	0.82	0.94	0.94	0.95	0.82	0.94	0.94	0.95
LR	0.45	0.39	0.39	0.29	0.39	0.29	0.29	0.25
MLP	0.86	0.58	0.58	0.67	0.76	0.47	0.47	0.42
CNN_LSTM	0.84	0.85	0.84	0.84	0.84	0.85	0.84	0.84

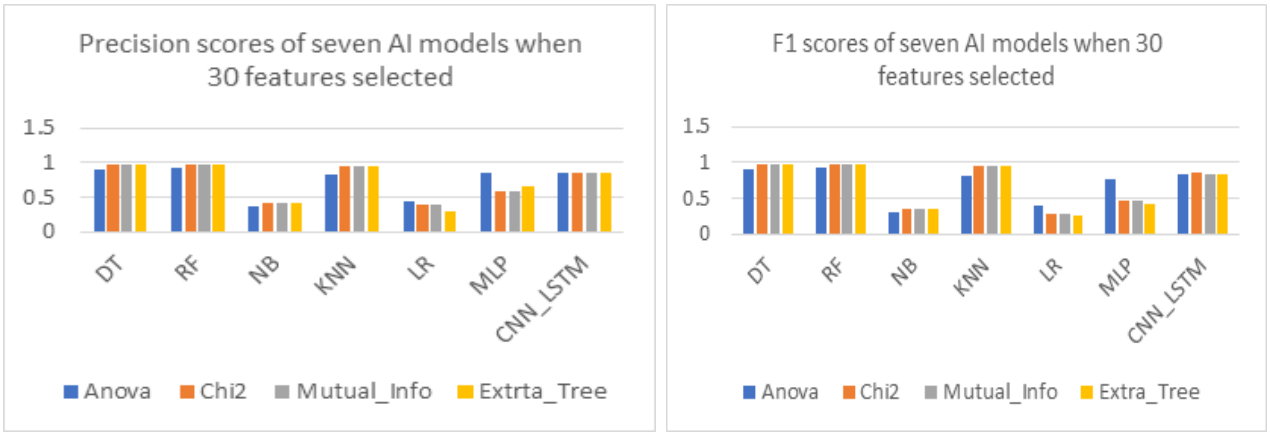

Fig. 6. Test results of Precision and F1 scores of seven AI models for 30 features selected.

V. DISCUSSION

The overall results in all three scenarios revealed that the RF classifier outperformed all other AI models for cyber-attacks detection in IoT healthcare environments. The RF classifier resulted the highest scores in terms accuracy, precision, recall, and F1-score for all three scenarios and across all four features selection techniques. In contrary, the LR classifier resulted the lowest scores in terms accuracy, precision, recall, and F1-score for all three scenarios and across all four features selection techniques. The experimental results support that both our hypothesis H0 and H1 are true since it is proved that the AI models improve the accuracy of cyber-attacks detection in IoT healthcare environments which eventually leads to prove that AI models has potential to enhance the detection of cyber-attacks in IoT healthcare environments.

VI. CONCLUSION AND FUTURE WORK

With the rapid application of IoT devices in healthcare environments, the cyber-attacks are surging in IoT healthcare environment due to limited security features such as limited

memory and processing power integrated in IoT devices. The healthcare environment is highly sensitive and any malfunction of IoT healthcare devices due to cyber-attacks can lead to severe implications even death. Therefore, it is highly essential to secure IoT healthcare devices from cyber-attacks. Hence, in this research, we proposed a methodology for cyber-attacks detection in IoT healthcare environments using AI. The proposed methodology consists of five major stages including data collection, data pre-processing, features selection, AI models training and performance comparison. We acquired a publicly available CIC IoMT dataset for training & testing of the AI models for cyber-attacks detection in IoT healthcare environments using Python language and some standard AI models and libraries. We used four commonly used features selection methods and trained and tested five commonly used machine learning models and two deep learning models. Furthermore, we considered three scenarios in which all seven AI models are trained for cyber-attacks detection in IoT healthcare environments. The experimental results revealed that the Random Forest (RF) classifier outperformed all other AI models for detecting 18 types of cyber-attacks—mapped into five attack classes—and normal traffic in IoT healthcare environments having 98% accuracy, 98% precision, 98% recall and 98% F1-score. Likewise, the best results were achieved on selecting 20 features out of 45 features using mutual information features selection method.

In future, we aim to increase the attack coverage to enable AI model to detect more types of cyber-attack. Furthermore, we aim to deploy the proposed solution in real-time environment in order to test its performance in real-time use case.

REFERENCES

[1] J. Deogirikar and A. Vidhate, “Security attacks in iot: A survey,” International Conference on I-SMAC (I-SMAC), pp. 32–37, 2017. https://doi.org/10.1109/I-SMAC.2017.8058363

[2] Statista Inc., "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by communications technology," Transforma Insights, December 2020 [https://www.statista.com/statistics/1194688/iot-connected-devicescommunications-technology]. [Online]. [Accessed 14-05- 2025].

[3] R. Uddin, & I. Koo, “Real-Time Remote Patient Monitoring: A Review of Biosensors Integrated with Multi-Hop IoT Systems via Cloud Connectivity”, Applied Sciences, vol. 14, 1876, 2024. https://doi.org/10.3390/app14051876

[4] M. Papaioannou, M. Karageorgou, G. Mantas,V. Sucasas, I. Essop, J. Rodriguez, & D. Lymberopoulos, “A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)”, Transactions on Emerging Telecommunications Technologies, vol. 33, e4049, 2022, https://doi.org/10.1002/ett.4049

[5] F. Hussain, S. Abbas, G.,Shah, A., Pires, I. Fayyaz, F. Shahzad, F., M. Garcia, & E. Zdravevski, “A framework for malicious traffic detection in IoT healthcare environment”, Sensors, vol. 21, 3025, 2021. https://doi.org/10.3390/s21093025

[6] S. Bhosale, M. Nenova, & G. Iliev, G., “A study of cyber attacks: In the healthcare sector”, In 2021 Sixth Junior Conference on Lighting (Lighting), pp. 1–6. https://ieeexplore.ieee.org/abstract/document/9598947

[7] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, & S. Yongchareon, “Health IoT Threats: Survey of Risks and Vulnerabilities” Future Internet, vol. 16, 389, 2024a. https://doi.org/10.3390/fi16110389

[8] K. Sutradhar, R. Venkatesh, & P. Venkatesh, “Smart healthcare services employing quantum internet of things on metaverse”, In Healthcare Service in the Metaverse, pp. 170-189, 2024, CRC

[9] A. Kaur, & A. Jasuja, “Health monitoring based on IoT using Raspberry PI”, In 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 1335–1340, 2017. https://doi.org/10.1109/CCAA.2017.8230004

[10] M. Pham, Y. Mengistu, H. Do, & W. Sheng, “Delivering home healthcare through a cloud-based smart home environment (CoSHE)” Future Generation Computer Systems, vol. 81, pp. 129–140, 2018. https://doi.org/10.1016/j.future.2017.10.040

[11] D. Choi, H. Choi, & D. Shon, “Future changes to smart home based on AAL healthcare service”, Journal of Asian Architecture and Building Engineering, vol. 18, pp. 190–199, 2019 https://doi.org/10.1080/13467581.2019.1617718

[12] M. Chen, D. Cui, H. Haick, & N. Tang, “Artificial Intelligence-Based Medical Sensors for Healthcare System”, Advanced Sensor Research, vol. 3, 2300009, 2024, https://doi.org/10.1002/adsr.202300009

[13] K. Ahmed, M. Ismail, Z. Shehata, I. Djirar, S. Talbot, N. Ahmadzadeh, S. Shekoohi, S. Cornett, E. Fox, & A. Kaye, “Telemedicine, E-health, and multi-agent systems for chronic pain management”, Clinics and Practice, vo. 13, pp. 470–482, 2023. https://doi.org/10.3390/clinpract13020042

[14] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, & S. Yongchareon, “Health IoT Threats: Survey of Risks and Vulnerabilities”, Future Internet, vol. 16, 389, 2024b. https://doi.org/10.3390/fi16110389

[15] M. Khan, & M. Alkhathami, “Anomaly detection in IoT-based healthcare: Machine learning for enhanced security”, Scientific Reports, vol. 14, 5872, 2024. https://doi.org/10.1038/s41598-024-56126-x

[16] A. Said, A.Yahyaoui, & T. Abdellatif, “Efficient anomaly detection for smart hospital IoT systems”, Sensors, vol. 21, 1026, 2021. https://doi.org/10.3390/s21041026

[17] K. Thilagam, A. Beno, A. Lakshmi, C. Wilfred, S. George, M. Karthikeyan, V. Peroumal, C. Ramesh, & P. Karunakaran, “Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System”, Journal of Nanomaterials, vol. 2022, 2638613,2022. https://doi.org/10.1155/2022/2638613

[18] N. Alharbe, & M. Almalki, “IoT-enabled healthcare transformation leveraging deep learning for advanced patient monitoring and diagnosis”, Multimedia Tools and Applications, 2024. https://doi.org/10.1007/s11042-024-19919-w

[19] J. Pimple, & A. Sharma, “Enhancing Cyber-Physical System Security in Healthcare Through Ensemble Learning, Blockchain and Multi-Attribute Feature Selection”, In P. Dubey, M. Madankar, P. Dubey, & B. T. Hung (Eds.), The Impact of Algorithmic Technologies on Healthcare, 1st ed., pp. 349–373), 2025, Wiley. https://doi.org/10.1002/9781394305490.ch16

[20] Y. Saheed, & M. Arowolo, “Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms”, IEEE Access, vol. 9, pp. 161546–161554, 2021. https://doi.org/10.1109/ACCESS.2021.3128837

[21] L. Ramasamy, F. Khan, M. Shah, B. Prasad, B, C. Iwendi, & C. Biamba, “Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring”, Sensors, vol. 22, 1076, 2022. https://doi.org/10.3390/s22031076

[22] I. Kilincer, F. Ertam, A. Sengur, R. Tan, & U. Acharya, “Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization”, Biocybernetics and Biomedical Engineering, vol. 43, pp. 30–41, 2023. https://doi.org/10.1016/j.bbe.2022.11.005

[23] M. Alsulami, “An AI-Driven Model to EnhanceSustainability for the Detection of Cyber Threats in IoT Environments”, Sensors, vol. 24, 7179, 2024. https://doi.org/10.3390/s24227179

[24] D. Prabakar,S. Qamar, & R. Manikandan, “Artificial intelligence–based security attack detection for healthcare cyber-physical system: Lightweight deep stochastic learning”, Securing Next-Generation Connected Healthcare Systems, pp. 51–70, 2024, Elsevier. https://doi.org/10.1016/B978-0-443-13951-2.00009-X

[25] Z. Liu, X. Jia, & B. Li, “RETRACTED ARTICLE: E-healthcare application cyber security analysis using quantum machine learning in

malicious user detection", Optical and Quantum Electronics, vol. 56, 476, 2024. https://doi.org/10.1007/s11082-023-05854-x

[26] D. Kavitha, & S. Thejas, "AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation", IEEE Access, vol. 12, pp. 173127 – 173136, 2024. http://doi.org/10.1109/ACCESS.2024.3493957

[27] A. Algarni, & V. Thayananthan, "Digital Health: The Cybersecurity for AI-based healthcare communication", vol. 13, pp.5858-5870, IEEE Access, 2025. https://doi.org/10.1109/ACCESS.2025.3526666

[28] S. Ksibi, F. Jaidi, & A. Bouhoula, "MLRA-Sec: An adaptive and intelligent cyber-security-assessment model for internet of medical things (IoMT)", International Journal of Information Security, vol. 24, pp. 1–20, 2025. https://doi.org/10.1007/s10207-024-00923-y

[29] R. Czekster, T. Webber, L. Furstenau, & C. Marcon, "Dynamic risk assessment approach for analysing cyber security events in medical IoT networks", Internet of Things, vol. 29, 101437, 2025. https://doi.org/10.1016/j.iot.2024.101437

[30] M. Akhi, C. Eising, & L. Dhirani, "TCN-Based DDoS Detection and Mitigation in 5G Healthcare-IoT: A Frequency Monitoring and Dynamic Threshold Approach", vol.13, pp. 12709 – 12733, 2025, IEEE Access. https://doi.org/10.1109/ACCESS.2025.3531659

[31] M. Hernandez-Jaimes, A. Martinez-Cruz, K. Ramírez-Gutiérrez, & C. Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures", Internet of Things, vol. 23, 100887, 2023. https://doi.org/10.1016/j.iot.2023.100887

[32] K. Vijayakumar, K. Pradeep,A. Balasundaram, & M. Prusty, "Enhanced cyber attack detection process for internet of health things (IoHT) devices using deep neural network", Processes, vol. 11, 1072., 2023. https://doi.org/10.3390/pr11041072

[33] J. Maruthupandi, S. Sivakumar, B. Dhevi, S. Prasanna, R. Priya, & S. Selvarajan, "An intelligent attention based deep convoluted learning (IADCL) model for smart healthcare security". Scientific Reports, vol. 15, 136, 2025. https://doi.org/10.1038/s41598-024-84691-8

[34] A. Nasayreh, H. Khalid, H. Alkhateeb, J. Al-Manaseer, A. Ismail, & H. Gharaibeh, "Automated detection of cyber attacks in healthcare systems: A novel scheme with advanced feature extraction and classification", Computers & Security, 150, 104288, 2025. https://doi.org/10.1016/j.cose.2024.104288

[35] A. Berguiga, A. Harchay, & A. Massaoudi, "HIDS-IoMT: A deep Learning-Based intelligent intrusion detection system for the internet of medical thing", IEEE Access, vol. 13, pp. 32863 – 32882, 2025. https://doi.org/10.1109/ACCESS.2025.3543127

[36] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, & M. Ilyas, "Stacking Ensemble Deep Learning for Real-Time Intrusion Detection in IoMT Environments", Sensors, vol. 25, 624, 2025. ; https://doi.org/10.3390/s25030624

[37] M. Babar, M.Tariq, Z. Ullah, F. Arif, Z. Khan, & B. Qureshi, "An Efficient and Hybrid Deep Learning-Driven Model to Enhance Security and Performance of Healthcare Internet of Things", IEEE Access, vol. 13, pp. 22931 – 22945, 2025. https://doi.org/10.1109/ACCESS.2025.3536638

[38] Khan. M, Almulhim. A, Alkati, S, "Towards the evaluation of cybersecurity threats and challenges in higher education institutions in Saudi Arabia", Edelweiss Applied Scienc and Technology, vol. 9, pp. 657-669, 2025. https://doi.org/10.55214/25768484.v9i2.4564

[39] S. Dadkhah, E. Neto, R. Ferreira, R. Molokwu, S. Sadeghi, & A. Ghorbani, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT", Internet of Things, 28, 101351, 2024. https://doi.org/10.1016/j.iot.2024.101351