International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

"An AI-Driven Framework for Ransomware Detection and Defense in Smart Healthcare IoT Systems"

Mr.ShaikhFareed
P.G. Student, Department of ComputerScience&Engineering
Anjuman College of Engineering & Technology, Nagpur,
Maharashtra, India
Email:shaikhfareed21@gmail.com

Dr Manish Asudani
Professor,DepartmentofComputer Science & Engineering
AnjumanCollegeofEngineering& Technology, Nagpur, Maharashtra, India
:

Abstract—The growth of Internet of MedicalThings (IoMT) has made real-time patient monitoring and clinical decision-making much easier, but at the same time, security threats havealso surged sharply owing to the constraints of the resources used, different communications protocols, and the increasing numberofcyber-attacks.Tosolve the identified issue, in this work, we present asmart and explainable Software-as-a-Service (SaaS) solution Ransomware detection system (IDS) specifically designed for IoMT applications that are constrained in terms of resources. For feature selection in the proposed framework, the PSO method has been adopted, while ML and DL methods were used to distinguish between benign and malicious traffic. Doctors could rely on explanations in case of suspicious decisions thanksto SHAP being used as the explanation approach. Our IDS has been evaluated using IoMT synthetic data and WUSTL-EHMS-2020 dataset, where we achieved outstanding performance in terms of accuracy proving our model's ability to work inreal-time and scale up via cloud computing.

Keywords — *IoMT Security, RansomwareDetection System (IDS), Explainable AI, Particle Swarm Optimization, SHAP Analysis, Machine Learning, Deep Learning, SaaS Architecture*

I. INTRODUCTION

Internet of Medical Things (IoMT) is a disruptive technology, a new era in the healthcare industry. IoMT connects medical devices, sensors, andcloud computing to provide a smart healthcare environment. The integration facilitates greater patient monitoring, improved diagnoses and clinical decisions that result in better quality of healthcare services. While the advantages of IoMT-enabled devices are significant, the widespread adoption of IoMT in critical sectors, including hospitals, emergency facilities,wearable devices for monitoring patients' health status, and smart home health monitoring, provides a broader scope for attacks that are capable of exploiting cyber vulnerabilities. Most IoMT devices are constrained in terms of limited processing power, reduced storage capability, decreased battery life, and the use of energy-saving signaling protocols. This limits the possibility of employing existing security measures in the IoMT and increases susceptibility to intrusion and tampering, as wellas data exfiltration and unauthorized access. Cyberattack on IoMT-based systems can lead to risks for patient privacy as well as patient safety and operational reliability of healthcare organizations. Considering this context, the need for sophisticated Ransomware Detection Systems becomesparamount.Todealwithcurrentissues,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

theproposedprojectaimstobean all-encompassingandfullyunderstandable SaaS-based IDS system explicitly built for IoMT environments with constrained resources. Accuracy in detecting intrusions and minimum computation cost can both be guaranteed through the use of cutting-edge Machine Learning and Deep Learning models with PSO for optimal selection of features. With the inclusion of SHAP explainability on top of that, medical users can have access to the advantages of clarity and trust, as they will be able to understand not only the prediction outputs but also the reasons behind intrusion alerts.

II. LITERATURESURVEY

The rapid expansion of the Internet of Medical Things (IoMT) sector has posed some issues in terms of cybersecurity, which are not easy to solve. Medical-IoT devices typically possess constrained computing capacity, exhibit heterogeneity of the IoT devices, handle highly sensitive information concerning patients, and operate in critical settings. Hence, the need for developing Ransomware Detection IDS that fit into the IoMT environment becomes highly relevant.

1. Surveys and foundational work

There are several surveys and review papers discussing the current situation regarding the securityofIoMTandIDSsystems. Hernández-Jaimes et al. are among those who categorize IDS techniques, architectures, and challenges for IoMT based on their features. [1] Nagh ib et al. conduct a comprehensive literature review on IDS in IoMT, which considers AI models, data sets, detection approaches, and evaluation criteria. [2] Si-Ahmed et al. conduct a survey on RansomwareDetectionforIoMTusing machinelearningapproachesandanalyze three-layered architectures, types of threats, and machine learning data sets. [3] All these papers share one thing in common: while machine learning/deep learning approaches are applied broadly, issues of resource efficiency, interpretabilityofthemodel,dataset

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

generalizability, and implementation remain unresolved.

2. Featureselectionandoptimization

Due to the restrictions in the nature of someIoMT devices, it is usually advised to reduce the feature dimensionality and the computational complexity. The PSO-DNN approach proposedby Chaganti et al. can successfully identify the IoMT intrusion activities with an accuracy of around 96%. [4] On the other hand, Basha et al. have used filter/hybrid approaches to develop feature selection algorithms for the IoMT/IDS domain on high-dimensional data sets. [5] In addition, Rehman et al. have compared different filter-based feature selection approaches (such as Info Gain, MI, etc.), suggesting that it could be adequate to employ fewer features for obtaining acceptable results. [6] These pieces of evidence provide solid proof regarding the importance of feature selection and optimization in the application of IDS in IoMT with resource constraints.

3. ML / DL-based IDS in IoMT

There has beenanincreasinginterestintheuseof classical Machine Learning algorithms (e.g., Random Forest, XGBoost), Deep Learning algorithms (e.g., CNN,LSTMandauto-encoders) to detect ransomware in IoMT networks. For instance, Alalhareth et al. emphasize the importance of meta-learning for the creation of ensemble learning models for IoMT IDS. [7] Manoharan &Thathanpresenta"GroupTeaching Optimized Probabilistic Deep Auto-Encoder" for IoMT IDS, which provides excellent precision and recall performance levels. [8] Ramya et al. develop an "Advanced Ransomware Detection Technique (AIDT)" which uses the PSO algorithm for feature selectionandPNNclassifier for IoMT network detection. [9] The emerging trend is that of greater complexity inlearnersand architectures, but challenges due to implementation remain a major constraint.

4. Explainable AI(XAI)andinterpretabilityin IDS

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

The importance of transparency in IDS models becomes critical in the healthcare industry because it is the automated alerts that clinicians and administrativestaffwilldependonintheend. Memon et al. proposed a methodology for explainable Ransomware Detection systems inthe Internet of Medical Things (IoMT) based on the application of Particle Swarm Optimization (PSO) for feature selection andtheLIMEmethod for explanations. [10] Wu et al. use SHAP/ ALE/ PDP methods for explaining the decisions of cross-layer IoMT IDS. [11] Hosain et al. developed a SHAP + LIME-based XGBoost IDS with an accuracy level above 99%. [12] The literature shows thatXAIisgraduallybecominga component of IoMT IDS, but it is not fully integrated yet.

5. Dataset benchmarking, evaluation metrics & gaps

Benchmark data and test methods arefundamental to achieving consistency. Several studies emphasize that a majority of the studies rely on a small number of data sets, such as WUSTL-EHMS-2020, mainly focused on the efficiency of the systems in terms of accuracy/precision, without considering latency, memory, power consumption, and other deployment-based measurements. [2] Doménech et al. examine the assessment of Ransomware detection in Internet of Things (IoT)/Internet of Medical Things (IoMT) settings and suggest realistic benchmark testing procedures. [13] The literature continues to stress the importance of cross-data set evaluations, real-time assessments, and interpretation of false positives.

6. Currenttrendsandemerging methods

More recent work pushes the envelope further. TheworkbySunetal.proposesthePSO-AdaBoost Ransomware Detection algorithm for IoT/IoMT, and this started the debate about the relevance of swarm-based algorithms for feature selection/IDS design. [14] In the case of Hafidetal.,theytacklethe“security-costtrade-off” challenge faced by IoMT machine learning/intrusiondetectionsystemsusingSHAP

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

to evaluate features within the XGBoost fusion model. [15]

III. METHODOLOGY

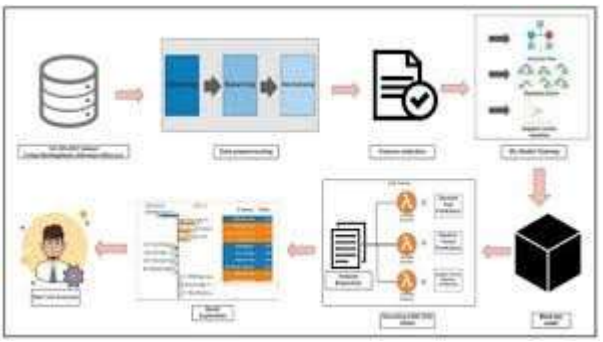


Fig .1. Block Diagram

Figure 1 shows the flow of the ransomware detection system IDS that can be implemented in the IoMT or Internet of Medical Things scenario. The whole process begins from receiving the raw data and concludes with providing insight data to the medical professionals.First,theheterogeneous data collection from IoMT devices serves as the initial input data that will be stored in the centralized storage. Next, the received raw data goes through a systematic pre-processing stage where any noise or outliers are removed from the data, missing values are handled, and normalization takes place. Following this stage, feature selection takes place whereby relevant attributes for the model are selected via optimization and statistics methods.These optimized features are provided to the training module for the machine learning algorithms, such as Random Forest, XGBoost, or even deep learning models, that learn how to differentiate between good and bad behaviors. Once the training phase is completed, the developed model is encapsulated into a modular black-box service that can be implemented inthecloudenvironment for the purpose of implementing Ransomware Detection. The stream of IoMT datathatcomesto the system is continuously processed by backend services with the help of lightweight serverless functions.

Themethodologyadoptedforconductingthe

research is quite systematic, thus enabling the researchers to designanefficient,explainable,and resource-aware Ransomware Detection IDS forthe IoMT systems. The first step in the process is collecting the raw data from the networks and sensors of the IoMT system. However, such datais not free from inconsistencies, noise, andmissing values; hence, a need for employing a robust pre-processing phase for preparing the collected data. The cleaning, transformation, normalization, attribute encoding, and class balancing are some of the approaches used for processing the collected data into high-qualitydata for analysis. Once the data is processed, the next phase is performing feature selection basedon Particle Swarm Optimization (PSO) or any other optimization technique for identifying the most important features related to ransomware detection. Reducing the number of features is beneficial in reducing computation time and improving the performance of the model besides making its deployment feasible on limitedresource IoMT devices.

Depending on the selected attributes, different Machine Learning andDeepLearningmodelswill be trained, includingRandomForest,XGBoost,as well as classifiers based on neural networks.These algorithms will be adjusted, verified and assessedthroughaccuracy,precision,recall, F1-score, and ROC-AUC values in order toselect the one which can be considered as the most suitable for implementation. Besides the improvements in the reliability and explainability which are crucial when dealing with healthcare cases, the best algorithm will also be enhanced through Explainable AI (XAI) methods, specifically SHAP (SHapley Additive exPlanations) whichwilladdbothglobalandlocal interpretability due to the presentation of the influence exerted on the algorithm's results by individual features. Once the model is ready for use, it will be encapsulated into a unit that will allow its scalability and modular implementation through a SaaS-based cloud computing infrastructure.

Inthereal-timeprocessing,theback-end

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

processes process the inputtedIoMTdatastreams, and the data goes into the trained machine/deep learning model for classification. The outcomes such as classified outputs, risk scoring, SHAP explainability, and alerts are then transmitted to the user dashboard which is interactive for visualizing threats and understanding model predictions. The synergy of data preprocessing, PSO for feature selection, ML/DL classification, SHAP explainability, and the SaaS model make sure that the whole process remains light-weight, transparent, scalable,andhighlysuitableforIoMT applications.

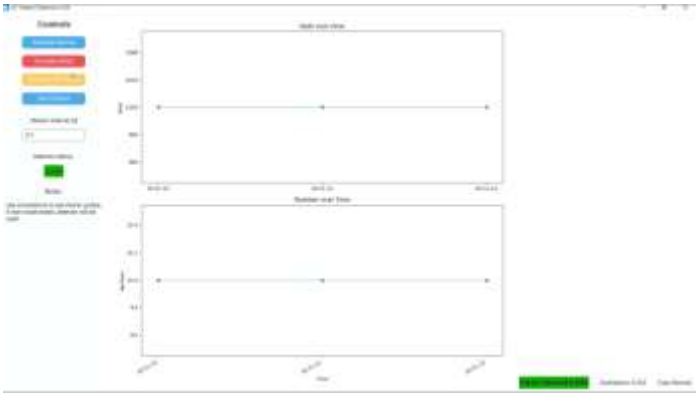
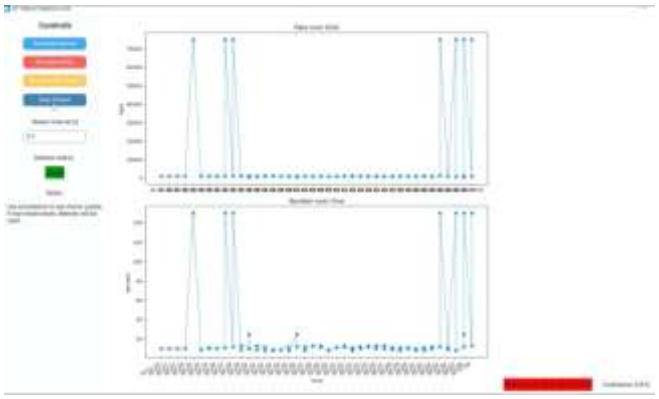


Fig2:WebPageOverview:RequestaFree Quote Section

Fig. 2presentsthegraphicaluserinterface(GUI)of the IoT attack detection system in real-time, allowing the users to test different scenarios for traffic—normal traffic, DDoS attacks, and ARP Spoofing—and seehowtheRansomwareDetection system will behaveineachcase.Theleftsidepanel contains the Control Panel from where users can start different simulations, change the streaming time, start live data streaming and show the detector's status, indicating that the model is successfully loaded and analysis of packetsstarted. Two panels are used for the real-time graph plotson the right side of the screen—one showing the amount of traffic by time and another representing the amount of packets/events detected during this time. The graphs keep changing as the simulations progress. This visualization makes it easier forusers to observe any anomalies orpatternsandfind out about possible attacks. Finally, statuses are providedbelowinthesystemstatespanel

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

containing information about live detector's inference such as normal traffic or malice; prediction confidence scores and possible type of the attack when it occurs.Hence, a useful graphical user interface can be utilized to show the behavior of IDS and observe the alteration in traffic and determine if the system was able to distinguish normal IoT activities from those that were malicious.



The visual representation outputted from the GUI clearly illustrates the responses that occur withinthe network while simulating IoT attack scenario. Packet Rate and Packet Count demonstrate significant and fast variations in their values over time, which are typical features of networkresponse in caseofDDoSorARPspoofingattacks. According to the "Rateovertime"graph,thetraffic comes in sudden bursts and contains a lot ofpackets that continue toincreaseinvolumeupuntil they exceed the normal level. Similarly, "Number over time" graph demonstratesnumerousandsharp increments of packets' amount, occurring in brief periods of time.Theseevidentabnormalitiescanbe attributed to the activities of attackers seeking to disrupt the network through submission of excessiveamountofrequests.Fromtheinformation shown in the leftcontrolpanel,itisevidentthatthe model works fine while IDS monitors all the mentioned above changes in real time. Accordingto the current system status indicated in thebottom-right side, the IDS successfully detects a real-time network attack ("ATTACK DETECTED") with a confidence score of 0.810.

Sr. No.	Component	Description / Specification
1	IoMT/IoTData Source	Networktrafficpackets,devicelogs, biometricsensorreadings;supports normal, DDoS, ARP spoof simulations.
2	Data Preprocessing Module	Performs cleaning, normalization, encoding, feature scaling, noise removal;preparesstructureddataset for ML processing.
3	Feature SelectionEngine (PSO)	Uses Particle Swarm Optimization to select optimal features, reduces dimensionality,improvesefficiencyand detection accuracy.
4	ML/DLModel (Detector)	RandomForest/XGBoost/Neural Network model trained to classify Normal,DDoS,ARPSpoofattacks; deployed as a lightweight inference module.
5	Real-Time Inference Engine	Backendengine(serverlessorlocal script) that processes live packet streams,extractsfeatures,andruns predictions in real time.
6	GUIControl Panel	Allowstriggeringsimulations(Normal, DDoS, ARP spoof), adjusting stream interval, monitoring detector status, and visualizing outputs.
7	Visualization Graphs	Real-timeplottingofPacketRateand Packet Number over time, helping usersidentifyabnormalitiesorspikes during attacks.
8	Status&Output Window	Displays classification results, confidence score, and traffic type (Normal / Attack); updates dynamicallywitheachinferencecycle.

TABLENO.1COMPONENTSANDTHEIRSPECIFICATIONS

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Comprehensive Study

The comprehensive research paper offers adetailed analysis of an intelligent, interpretable, and computationally efficient IDS tailored specifically for the IoT medical environment, characterized by strict security requirements, high dependability,andcriticalreal-time decision-making processes. Firstly, the paper highlights the main vulnerabilities of the IoMT network due to its diversity of devices, restricted computingresources,continuousstreamsofdata,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

and confidentiality of patient-specific information. Then, it evaluates the current IDS approaches in terms of scalability, interpretability, and computational complexity. The paper introduces Particle Swarm Optimization as a solution to overcome these limitations, making the proposed IDS able to conduct feature selection, implement dimensionality reduction, require less processing power, and still ensure a high level of detection accuracy. Extensive classification of Machine Learning and Deep Learning models is conducted throughout the training andtestingstagesbasedon the preprocessed IoMT dataset in order to determine the normal behavior of IoMTcompared to DDoS and ARP-spoofing attacks. Another crucial point about the presented research work is the use of SHAP-based Explainable AI, which provideshighertransparencyinthedecision-makingprocessandrevealsthosefeatures that had the greatest impact on the intrusion detection, as well as increasing the trust of clinicians.Moreover, the paper implements the system with an interactive graphical user interface in real time, where the user can analyze the packets' rates, attack patterns, outputclassification results, and level of confidence in these predictions. Moreover, the users can simulate attacks, and in real time, they will be able to observe how the system deals with such threats. Theimplementedmodelismodularandcloud-based, and it has the potential of being expanded at any point, hence ensuring real-time analysis of clinic networks as well as medical infrastructures connected to the cloud. This paper presents a framework combining advanced training, interpretability, real-time analysis, and deployment challenges.

Advantages

LightweightandResource-Efficient

The system employs the advanced techniques of feature selection, including PSO, which reduces the computational overhead involved in this process and makes it possible to use the IDS even on less resource-rich IoMT devices, such as medical sensors.

High Detection Accuracy

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

The inclusion of ML/DL algorithms such as the Random Forest model, the XG Boost model, or Neural Networks will make sure that the IDS is able to differentiate between benignandmalicious traffic with high accuracy.

Real-TimeMonitoringandAlerting

Together with the real-time inference engine, the graphical user interface (GUI) enables monitoring of the network's operations, thus making it possibletoidentifyattackslikedistributed denial-of-service (DDoS) or ARP spoofing immediately.

Limitation

Dependence on Dataset Quality

Data quality and diversity have a huge impact on the performance of the system. In case these datasets lack different variations of actual IoMT traffic, then there would be difficulties in predicting attacks that may occur.

Limited Edge-Device Compatibility

Optimization of featuresiseasyforML/DLmodel butthenagain,itbecomesdifficulttousesuch models for implementation on IoMT devices that have less power consumption,forexample, sensors embedded in the human body.

ModelInterpretability Complexity

While the SHAP framework has the ability to interpret the results, the calculation of SHAP values in large deep models is time-intensive, and it may result in reduced capability to explain the output in real-time under dynamic conditions.

Scalability Challenges Under Heavy Load

Real-time processing of heavy traffic of medical networks may lead to either latency or delay in detection, especially in the case of large-scale DDoS attacks or insufficient cloud computing resources.

IV. RESULTSANDDISCUSSION

TheeffectivenessoftheRansomwareDetection IDSproposedforIoMTnetworkswasexamined

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

via several experiments conducted under varying network conditions, such as Normal, DDoS, and ARP spoofing attacks. The system's performance was measured based on accuracy, speed, visualization output, and user interface response. Using preprocessing techniques and feature selection with PSO, the optimal feature subset helped to minimize the dimensions of the dataset, thereby improving the efficiency of the system without sacrificing accuracy. It was found that the trained machine learning model served as an effective classifier in distinguishing between normal and ransomware attack activities. The curves generated during Normal traffic simulation were stable and had no significant fluctuations,and thus it proved that the system does not give false alarm during normal network operation. In contrast to this, the graph generated during DDoS attacks demonstrated a sudden increase in packet rates and counts that were immediately capturedby the detection status section of the interface asan attack. Similarly, the traffic behavior generated due to ARP spoofing was easily detected by the IDS.

The GUI served as an efficient tool for visualization and confirmation as it presented in real time the varying rates of packets,detectedthe abnormalities in the traffic and the classification results. The “Detector Status” confirmed throughout the process that the model was active and in use, while the system output provided reliable output regarding the type of attack, the level of confidence and classification times. From the above observations, it can be stated that the system was capable of performing efficient predictions with steady performances.

Fig2:Real-TimeIoTAttackMonitoring Initialization Output

Asitcanbeseen from the console output provided in

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Fig 2, the current step describes thepreparationstage when the machine prepares itself for the ongoing observation ofthenetworktrafficanddetectionofthe abnormalities that happen with its help through applying the trained modelofRansomwareDetection System (IDS). During the initial phaseofthesession, the machine prepares several essential parameters including monitoring time of 300 seconds, check interval of 1 second, threshold of 0.8, and 3sequential alertsbasedonahighlyconfidentmodelof abnormality. This approach guarantees the efficiency of Ransomware Detection because all the false positives that may emerge due to temporary fluctuations in traffic patterns will be filtered out. In the next step, there happens the actual monitoring when every second the model checks incoming data and estimates whether the prediction probability exceeds the confidence threshold setearlier.Itshould be noted that despite all predictions provided by the model regarding the presence of anomalies with the probability over 0.8 for three successive times, there will be no alarms as suchrobustnessoftheprocedure is vital for the proper work of IDS.

Fig3:WebPageOverview:AI Landmark Pincode Page

Fig 3 The console output displayed here is from a demonstration of the IoT Attack Detection System that illustrates the functioning of the model when exposed to various simulation ofnetworktraffic.The first example of traffic is thatofnormaltrafficwhich is identified as such (normal traffic), and with a confidence of 0.767. It should be noted herethatthis value shows that the model can accurately identify normal traffic as it would not classify the normal behavior as malicious activity. Next, a DDoS attack trafficwassenttothesystem,anditaccurately

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

identifies it as being malicious and tags it as "attack detected" traffic with a confidence of 0.810. This demonstrates that the model can detect anomalies or attacks that involve high volumes of network traffic or flooding of the systems. Finally, the case of an ARP spoofing attack is used to demonstrate that the model accurately detects such attacks with a confidence level of 0.770. The message "Demo completed!" indicates successful completion of all testcases,whiletheusagetipsareguidelinesto real-world usage of the model.

V. Challenges and Solutions

Sr. No.	Challenges	Proposed Solutions
1	High data dimensionality affecting model performance and processing speed	Use **PSO-based feature selection** to reduce dimensionality and retain only the most relevant features
2	Real-time Ransomware Detection in resource-constrained IoMT devices	Deploy lightweight, optimized ML/DL models and use cloud/SaaS serverless architecture for scalable processing
3	Difficulty in detecting multiple attack types (Normal, DDoS, ARP Spoof)	Train multi-class modelson diverse datasets and simulate attack traffic for improved classification
4	Lack of transparency and trust in ML-based decisions	Integrate **SHAP Explainable AI** to provide feature-level reasoningforeach prediction

VI. CONCLUSION

The proposed Ransomware Detection System for Internet of Medical Things (IoMT) can be viewed asaneffective, highlyaccurate,yet lightand easily

understandable way of ensuring safety in today's networks of healthcare. Apart from the synergic effectofParticleSwarmOptimization(PSO)-optimized feature selection along with advanced Machine Learning and Deep Learning models and the use of SHAP explainable AI techniques, the detector stands out due to its high accuracy, which does not decrease its lightweight nature. The creation of the simulation traffic, including normal traffic, DDoS attacks, and ARP spoofing, was critical for testing the system in order to prove that it is able to identify abnormal patterns with high certainty and low false alert rates.

VII. FUTURE SCOPE:

This idea for IoMT ransomware detection system is a great starting point, however, it can evolve further and get better. The future work might involve expanding the range of the attacks to include not only ransomware but also zero-day attacks and attacks specifically targetingparticular medical devices. Thus, the robustness of the system against constantly changing cyber attacks will be increased. It will be possible to generalize betterandbecomemorepracticalifalargerdataset of real traffic from hospital networks and IoMT devices is used. Moreover, using deep reinforcement learning or federated learning will allow the IDS to discover new attack patterns independently.

VIII. REFERENCES

[1] M.L.Hernández-Jaimes,"Artificialintelligence for IoMT security: A review of Ransomware Detection schemes for IoMT," *Computers & Security*, 2023.

[2] A. Naghib, F. S. Gharehchopogh, and A. Zamanifar, "A comprehensive and systematic literature reviewonRansomwareDetectionsystems in the Internet of Medical Things," *Artificial Intelligence Review*, vol. 58, 2025.

[3] A.Si-Ahmed,M.A. Al-Garadi, and N. Boustia,

"Survey of Machine Learning Based Ransomware Detection Methods for Internet of Medical Things (IoMT)," 2022.

[4] R.Chaganti,A.Mourade,V.Ravi,N.Vemprala, A. Dua, and B. Bhushan, "A Particle Swarm Optimization and Deep Learning Approach for Ransomware Detection System in Internet of Medical Things," *Sustainability*, vol. 14, no. 19, 2022.

[5] S. J. Basha, "AQU-IMF-RFE: An Extended Feature Selection Method for Ransomware Detection Systems," *Journal of Ambient Intelligence and Humanized Computing*, 2025.

[6] M. U. Rehman, "Comprehensive Feature Selection for Machine Learning-BasedRansomware Detection in Healthcare IoMT Networks," *Proceedings*, 2025.

[7] M. Alalhareth, "Enhancing the Internet of Medical Things (IoMT) Security with Ensemble Learning Techniques in Ransomware Detection Systems," 2024.

[8] A. Manoharan and M. Thathan, "Enhanced IoMT Security Framework Using Group Teaching Optimized Probabilistic Deep Auto-Encoder for RansomwareDetection,"*ScientificReports*,vol.14, Article 30360, 2024.

[9] M. Ramya, P. Sudhakaran, and Y. Sivagnanam, "Advanced Ransomware Detection Technique (AIDT) forSecureCommunicationAmongDevices in Internet of Medical Things (IoMT)," *EURASIP Journal on Wireless Communications and Networking*, Article 34, 2025.

[10] S. A. Memon, U. K. Wiil, and M. Shaikh, "Explainable Ransomware Detection for Internetof Medical Things," *SCITEPRESS Proceedings*, 2023.

[11] Y. Wuetal.,"AnExplainable-AIApproachfor InterpretableCross-LayerRansomwareDetectionin IoMT," *Electronics*, vol. 14, 2025.

[12] Y. Hosain et al., "XAI-XGBoost: An Innovative Explainable Ransomware Detection FrameworkforIoMTSystems,"*ScientificReports*,

2025.

[13] J. Doménech, “Evaluating and Enhancing Ransomware Detection Systems in IoT and IoMT Environments,” 2025.

[14] Z. Sun et al., “Optimized MachineLearning-Enabled Ransomware Detection Using PSO-AdaBoost for IoT/IoMT Networks,” 2024.

[15] A. Hafid et al., “Optimizing Ransomware DetectioninIoMTNetworksThroughSHAP-Driven XGBoost Late Fusion Models,” *Mathematics*, vol. 13, no. 10, 1574, 2025