

Cybersecurity Risk Assessment Framework for Healthcare Information Systems: Protecting Patient Data, Connected Medical Devices, and Critical Care Operations

Mahbub Hasan¹, Mohammad Masudur Rahman², Md Shokran³

^{1,3} Trine University, USA

² Florida Atlantic University, USA



DOI : <https://doi.org/10.61796/jaide.v1i12.1920>



Sections Info

Article history:

Submitted: September 07, 2024

Final Revised: October 26, 2024

Accepted: November 18, 2024

Published: December 27, 2024

Keywords:

Healthcare information systems

Cybersecurity risk assessment

Internet of Medical Things

(IoMT)

Machine learning

Healthcare cybersecurity and

intrusion detection

ABSTRACT

Objective: The objective of this research is to propose a cyber-security risk assessment framework based on machine learning that can identify, assess and predict cyber risks in healthcare information systems, connected medical devices and intensive care unit (ICU) environments. **Method:** The research uses the IoT Healthcare Security Dataset (IoT-ICU HSD) consisting of normal and malicious network traffic generated from an IoT-enabled ICU setup, which consists of patient monitoring sensors and control units. A thorough data preprocessing pipeline is designed to enhance data quality and the performance of the model, which involves cleaning the data, feature engineering, feature selection and normalization. Various supervised machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine, Logistic Regression and Extreme Gradient Boosting (XGBoost) are trained and tested for the classification of normal and malicious network traffic. The accuracy, precision, recall, F1-score, receiver operating characteristic area under the curve (ROC-AUC) and confusion matrix analysis are used for model performance assessment. **Results:** The results will provide actionable insight for healthcare organizations to enhance cybersecurity posture, secure connected medical devices, ensure uninterrupted critical care services and facilitate secure digital healthcare transformation. **Novelty:** The proposed framework seeks to offer early detection of cyber threats, facilitate proactive risk assessment, and boost health-care information system security and resilience while maintaining confidentiality, integrity, and availability of sensitive patient information.

INTRODUCTION

The healthcare industry has seen digital technologies gain traction and become a vital tool for delivering better patient care, optimizing operations, and aiding in clinical decision-making. Healthcare Information Systems (HIS), Electronic Health Records (EHRs), cloud computing, and Internet of Medical Things (IoMT) devices have revolutionized the healthcare landscape, creating highly interconnected and digital environments. They allow for real-time data transfer between healthcare providers, automation of clinical workflows, remote health care delivery, and continuous monitoring of patients. Digital transformation has revolutionized the way healthcare is delivered, but it has also posed new cybersecurity challenges with the growing number of connected devices and networked systems [1]. The healthcare sector has grown into an appealing target for cybercrime due to the fact that they maintain highly sensitive patient data and are reliant on the smooth functioning of electronic services for their vital medical operations. Ransomware, malware, phishing, denial of service and unauthorized access are all examples of cyberattacks that can impact patient privacy, service and patient safety within hospitals [2]. Healthcare organizations need robust cybersecurity

measures that can detect vulnerabilities, evaluate risks, and proactively address potential threats. With recent progress in machine learning, new possibilities are emerging in the field of creating intelligent cybersecurity risk assessment frameworks automatically identifying malicious behavior and predicting future cyber risks based on network traffic analysis. This work introduces a machine learning-based cyber security risk assessment framework based on a healthcare intensive care unit (ICU) network traffic, the IoT Healthcare Security Dataset. The proposed framework is designed to enhance the ability to detect cyber threats and increase the resilience of the healthcare sector infrastructure while helping to protect patient data, medical devices connected to it, and critical care processes from emerging cyber threats.

Digital transformation is a fast-paced phenomenon in the healthcare industry as it's embracing Healthcare Information Systems, cloud computing, telemedicine, and Internet of Medical Things (IoMT) technology. To enhance diagnosis, treatment and patient outcomes, hospitals are increasingly dependent upon interconnected medical devices, patient monitoring sensors, electronic health records, and intelligent healthcare applications. In Intensive Care Units (ICUs), for example, the ability to communicate between medical devices and healthcare information systems is crucial for monitoring patients in real-time and making timely clinical decisions [3]. While these technologies prove to be extremely effective at improving the efficiency of health care and the quality of service, they also expose health care infrastructures to increasingly complex cyber threats. Healthcare organizations are often a favorite target of attackers because patient information is of high value, and an attack on the hospital system may have immediate consequences for patient safety [4]. Cyber events like ransomware, DDoS, malware infections, or unauthorized access may disrupt clinical services, disrupt medical device communication, or compromise patient confidentiality information. Many of the traditional cybersecurity methods have failed to keep up with the ever-changing nature of attack patterns in complex healthcare networks. This makes it imperative that healthcare organizations have intelligent, proactive cyber-security solutions that are able to watch network activity and detect potential threats before any real damage has been done. Machine learning (ML) algorithms have proven to be powerful tools for processing vast amounts of network traffic, detecting abnormal patterns, and aiding cyber risk automation [5]. The IoT Healthcare Security Dataset is highly suitable for evaluation of healthcare cybersecurity solutions because it generates realistic normal and malicious network traffic from a realistic environment of an IoT-based ICU. Thus, the advanced cybersecurity risk assessment framework can be created with machine learning to increase the accuracy of threat detection, increase the resilience of healthcare systems and provide secure, reliable and uninterrupted healthcare services.

As the healthcare sector becomes increasingly reliant on interdependent healthcare technologies, cybersecurity risk assessment has become a key part of healthcare management. Healthcare Information Systems combine patient histories, medical devices, communication systems, lab management, pharmacy management,

cloud-based solutions, and more into a single digital system. While this integration enhances the efficiency of treatment and care for patients, it also widens the scope of attack for the bad guys. There are vulnerabilities in medical devices, poor network monitoring and insecure communication protocols, all of which can put healthcare organizations at risk of cyberattack intended to compromise patient privacy and disrupt medical services [5]. By conducting a cybersecurity risk assessment, healthcare institutions can systematically detect vulnerabilities, assess the likelihood and impact of cyber threats, and prioritize the level of security controls based on the organizations' risk levels. The use of machine learning in cybersecurity risk assessment is another step toward improving the process, providing real-time visibility into network traffic, automated anomaly detection and early detection of malicious activity [6]. These models can detect sophisticated attacks that would not be picked up by traditional security methods, which is a significant benefit in decreasing the time taken to respond and limiting the impact on the business [7]. The IoT Healthcare Security Dataset creates a suitable platform for the development and testing of intelligent cybersecurity models, as the communication patterns between the patient monitoring devices and the healthcare control system are typical of an ICU setting. The suggested framework is designed to enhance the cybersecurity of healthcare systems, facilitating the early detection of threats, safeguarding patient data, ensuring secure use of interconnected medical devices, and guaranteeing the availability of essential healthcare services [8]. A robust cybersecurity risk assessment system helps build a safer healthcare environment, boosts patient confidence, ensures regulatory compliance, and enhances the organization's resilience against future cyber threats.

Healthcare delivery has been greatly improved with the widespread use of Healthcare Information Systems (HIS) and Internet of Medical Things (IoMT) devices but has also opened up advanced cyber threats to the healthcare infrastructures. Hacking into patient monitoring systems, connected medical devices, and hospital networks can not only lead to the theft of sensitive patient data but can also also disrupt critical care functions, thereby potentially impacting patient safety [9]. Current cybersecurity strategies have been built around static security measures which are hard to maintain and don't necessarily cover new and sophisticated attack methods in real time. Furthermore, current risk assessment techniques do not have intelligent mechanisms to continuously analyze network traffic and predict cyber risks in healthcare settings [10]. Thus, the need to develop a robust machine learning-based cybersecurity risk assessment framework that can accurately identify malicious activities, measure the security threats, and enhance the security of healthcare information systems and the associated medical devices.

The overall aim of this research is to create a machine learning based cybersecurity risk assessment model to safeguard healthcare information systems, connected medical devices, and critical care operations. The objective of this study is to:

1. To recognise the most significant cybersecurity risks and vulnerabilities in healthcare information systems and healthcare-connected devices.
2. Preprocess and analyze the IoT Healthcare Security Dataset to make effective decisions for cybersecurity risk assessment.
3. Create and evaluate several machine learning techniques for the detection of normal and malicious network traffic [11].
4. K-means clustering and nearest neighbors were applied to develop the models, and their performance was compared to classify the developed models using standard classification metrics such as accuracy, precision, recall, F1 score and ROC-AUC.
5. To create a cybersecurity risk assessment that can be used to help safeguard patient information, IoMT devices and critical healthcare operations.
6. To give real-world cybersecurity tips to make modern healthcare environments more resilient and secure.

This study aims to address the following questions:

1. What are the major cybersecurity risks and weaknesses of health information systems and health connected devices?
2. What machine learning algorithm is best suited for the detection of malicious network traffic in a healthcare environment with many IoT devices?
3. What are the implications of a cybersecurity risk assessment framework based on machine learning for security of patient data and critical care operations?
4. What are its strengths and weaknesses in terms of increasing cybersecurity resilience and making information systems in healthcare more secure?

As healthcare has gone through rapid digital transformation, the need for Healthcare Information Systems (HIS), Internet of Medical Things (IoMT) devices and network-connected medical technologies has grown to provide quality patient care. These technologies enhance the efficiency of healthcare operations and assist in clinical decision-making, but they also introduce new and evolving cybersecurity risks that can impact patient privacy, hospital operations, and the safety of critical care operations [12]. There is an increasing demand for intelligence solutions in the cybersecurity field that can detect security vulnerabilities and forecast potential risks from cyber threats before they come to pass. The study is important because it introduces a novel approach to cybersecurity risk assessment that uses machine learning algorithms tailored to the healthcare sector to enhance the security of healthcare information systems and medical devices [13]. The research leverages the IoT Healthcare Security Dataset to test the proposed framework in a realistic scenario in which an IoT-based intensive care unit (ICU) is under attack from malicious network activities, providing the evaluation with a realistic view of the cyber threat landscape in an IoT-based intensive care unit. Comparative assessment of various machine learning algorithms is also helpful in determining the superior algorithms for healthcare networks protection [14]. The results

of this research will be useful to health care administrators, cybersecurity professionals, health care hospital information technology (IT) departments, researchers, and policy makers to inform their health care cybersecurity strategies [15]. The proposed framework can facilitate early detection of cyber threats, mitigate cybersecurity risks, safeguard critical healthcare services, and enhance the resilience of connected medical devices while protecting sensitive patient information and ensuring the continuous availability of critical healthcare services [16]. This study adds to the existing knowledge on healthcare cybersecurity, highlighting the potential of AI and machine learning in cybersecurity risk assessment to enhance secure and reliable digital healthcare environments.

Healthcare Information Systems (HIS) are indispensable tools in today's healthcare landscape, facilitating the management of electronic health records (EHRs), clinical decision support, telemedicine, and patient monitoring services [17]. The rise of the Internet of Medical Things (IoMT) has also made a significant impact on the healthcare industry, enabling seamless monitoring and communication between patients and healthcare providers. But the digital transformation has added a whole new attack surface for cybersecurity [18]. With the potential value of medical records and the importance of healthcare services, they are increasingly becoming a target of cybercriminals. Common forms of cyber threats are insider threats, unauthorized access, malicious software (malware), denial of service (DoS) attacks, and ransomware attacks. Ransomware attacks, malicious software (malware), denial of service (DoS) attacks, unauthorized access to sensitive patient information, and insider threats are all common cyber threats [19]. Hospitals can be negatively impacted by successful attacks, including the potential to disrupt hospital operations, compromise patient privacy, interfere with the communications of medical devices and delay emergency medical treatments [20]. The researchers have stressed that traditional security methods, such as firewalls and signature-based intrusion detection systems, are not sufficient to detect advanced and unknown attacks. Therefore, it is essential for healthcare institutions to have robust cybersecurity risk assessment strategies that can continuously identify potential vulnerabilities and address evolving threats [21]. Smart incorporation of intelligent cybersecurity systems may enhance patient information, linked medical devices, and healthcare network security, allowing for adherence to regulations and maintaining medical services. Thus, bolstering cybersecurity poses a critical challenge to ensure the confidentiality, integrity and availability of healthcare information systems.

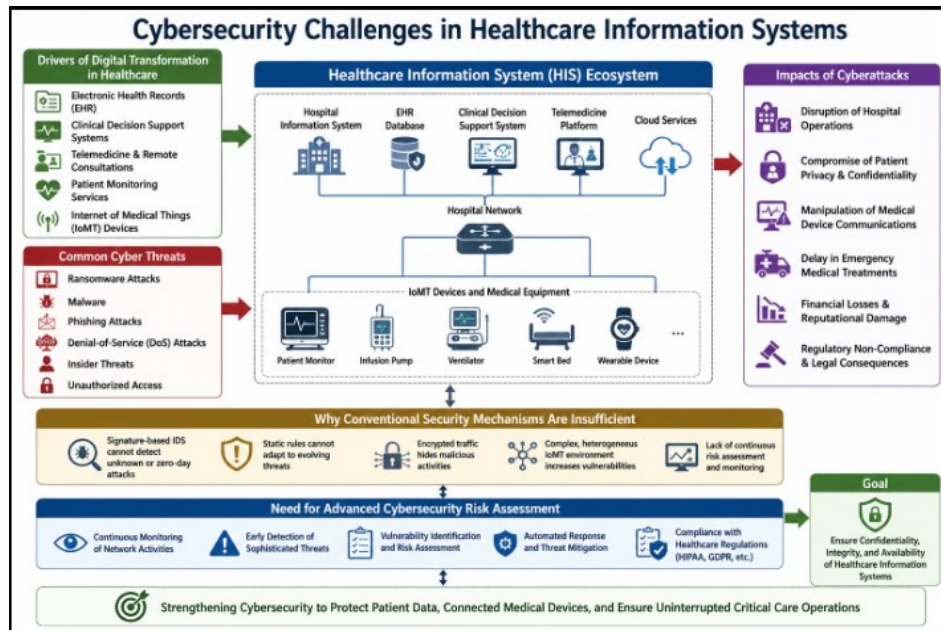


Figure 1. This flowchart illustrates cybersecurity challenges, risks, and protection strategies for healthcare information systems

This flowchart represents the problems of cybersecurity in Healthcare Information Systems (HIS) and the necessity of using an advanced cybersecurity risk assessment. It starts by showcasing how healthcare is transforming digitally with the advent of Electronic Health Records, Clinical Decision Support Systems, Telemedicine, Patient Monitoring Devices, and Internet of Medical Things (IoMT). The framework then lists out common cyber threats, such as ransomware, malware, phishing, denial of service attacks, insider threats, and unauthorized access [21]. It further demonstrates the impacts of cyberattacks on hospital operations, patient privacy, medical devices, and regulatory compliance. Lastly, the diagram highlights the need for continuous monitoring, threat mitigation, vulnerability assessment and regulatory compliance to ensure the confidentiality, integrity and availability of healthcare information systems.

Machine learning has become a powerful tool for enhancing the cybersecurity risk assessment process, allowing for automated detection of malicious activities and predictive analysis of cyber threats. Machine learning algorithms are different from the basics of security where rules are applied to network traffic; they can process vast amounts of network traffic, detect sophisticated attack patterns, and adapt as the security landscape changes over time [22]. Machine learning methods are being used more and more in healthcare settings to track interactions between medical devices on the network, identify unusual activity, categorize malicious traffic, and inform proactive decisions about the healthcare network [23]. The supervised learning algorithms, including Decision Tree, Random Forest, Support Vector Machine, Logistic Regression, and Extreme Gradient Boosting (XGBoost), have shown success in intrusion detection and cyberattack classification due to their effectiveness in learning from labeled datasets and effectively categorizing network traffic as normal or malicious [24]. Ensemble learning

and explainable artificial intelligence (XAI) have also recently been studied as ways to enhance model accuracy and transparency, which could also boost trust in automated cybersecurity systems. While all these developments have occurred, there are important challenges that need to be addressed in order to increase detection accuracy, lower the false alarm rate, and create a healthcare cybersecurity solution that can be used in a changing hospital environment [25]. Incorporating machine learning into a full circle cybersecurity risk assessment framework therefore provides a viable path to protect patient information, ensure critical healthcare operations are resilient to novel cyber threats, help with ongoing monitoring and protect IoMT devices from threats.

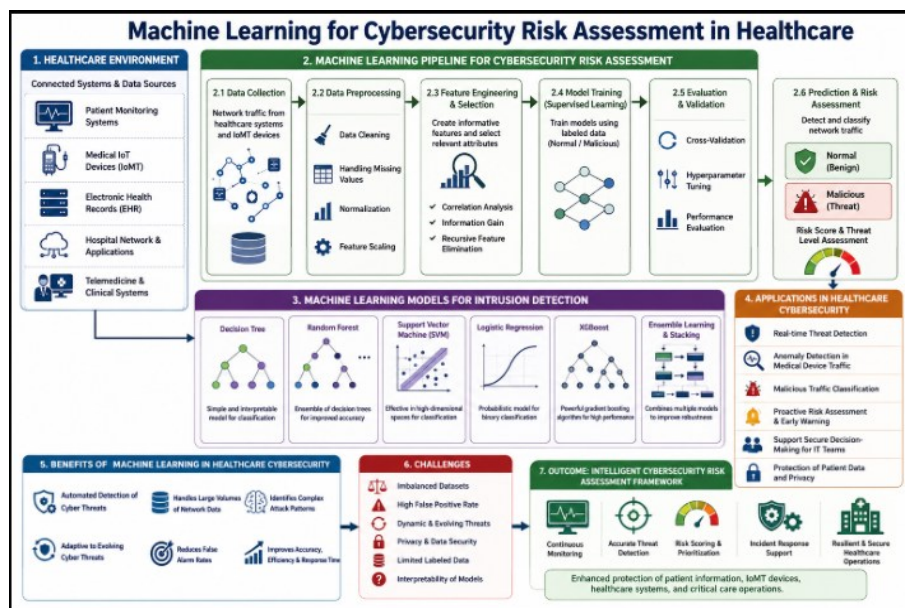


Figure 2. This flowchart represents a machine learning-based cybersecurity risk assessment in healthcare environments

The diagram illustrates a complete machine learning-based cybersecurity risk assessment system for a healthcare environment. It starts from healthcare data sources such as patient monitoring systems, medical IoT devices, electronic health records, hospital networks and telemedicine apps. The framework is divided into a series of steps, including data collection, data preprocessing, feature engineering, model training, model evaluation, and prediction of cyber risk. Several supervised machine learning models, such as Decision Tree, Random Forest, Support Vector Machine, Logistic Regression, XGBoost and ensemble learning, are used for the classification of network traffic (normal and malicious). This framework underscores real-world healthcare cybersecurity uses, outlines implementation hurdles, and illustrates how intelligent risk assessment improves threat detection, patient data security, and critical operations resilience in healthcare.

In their article published in IEEE, Malamas, et al. (2021) explored the current cybersecurity risk assessment methodologies and security standards concerning the IoMT. The authors highlighted that the traditional method of performing cybersecurity

risk assessment would not work in an IoMT environment, due to the nature of connected medical devices in highly distributed, resource-constraint and safety-critical healthcare networks. The study conducted a systematic review of the scientific literature, international standards and security best practices, and then compared their applicability by scope, maturity, and risk assessment methodologies. The results indicated that healthcare providers must have unique cybersecurity frameworks in place that can continuously detect vulnerabilities, evaluate cyber risks, and then take appropriate action to mitigate those risks [1]. The authors also highlighted the need for a comprehensive security strategy that permeates the healthcare system, ensuring the confidentiality, integrity, and availability of medical information and devices. This study offers a solid theoretical basis for the current study, contributing to the creation of a machine learning-based cybersecurity risk assessment framework that will improve cyber threat detection, patient data security, and the security of IoMT devices and the resilience of healthcare information systems against the changing nature of cyber threats.

In the article *Cyber Risks Prediction and Analysis in Medical Emergency Equipment for Situational Awareness* by Burke and Saxena (2021), they examined the vulnerabilities in cybersecurity of the modern medical emergency equipment, specifically the network connected ventilator systems, which are prevalent in the healthcare sector. The study highlighted the growing connectedness of medical devices, creating a larger surface area for attacks that could put critical equipment at risk of manipulation attacks, ransomware, unauthorized access, and other malicious operations that could impact patient safety and healthcare function. As a case example, the authors examined the potential for cyber risks to medical emergency equipment and showed how weak security measures can lead to attackers being able to incapacitate the device and access patient information [2]. The study also underscored the need for a holistic approach to cybersecurity in the design, deployment, monitoring and maintenance of medical devices. The researchers found a need for proactive cyber risk prediction and better awareness to bolster healthcare cyber security and maintain uninterrupted clinical operation. It can be seen that this study has been helpful for the present research as it highlights the need to have intelligent machine learning-based cybersecurity risk assessment frameworks that can identify malicious activities, vulnerabilities and safeguard the connected medical device and healthcare information systems against emerging cyber threats.

In their article "A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach," Ksibi, Jaidi, and Bouhoula (2023) reviewed the approaches of cybersecurity risk management for IoMT and e-health systems. The authors noted that the widespread use of IoMT technologies has ushered in new cybersecurity challenges that traditional risk assessment methods are unable to solve due to the volume of sensitive medical information moving among interconnected medical devices. A critical analysis of current cybersecurity standards, risk assessment models and security management methods has

been conducted, while their shortcomings in heterogeneous healthcare settings were emphasized [3]. To address these challenges, the authors introduced a novel quantitative, cybersecurity risk assessment framework aimed at providing better decision making, building trust and enabling efficient cybersecurity risk management in e-health systems. Their findings showed how quantitative risk assessment can better inform healthcare organizations of the most accurate prioritization of cyber threats as well as providing better security resource allocation. This study has contributed to present research by suggesting and providing a theoretical foundation for the development of a machine learning based cyber security risk assessment framework that will help detect cyber threats, assess cyber vulnerabilities, protect patient data, ensure security of connected medical devices and enhance the resilience of healthcare information systems to emerging cyber threats.

RESEARCH METHOD

This study utilizes a quantitative, machine learning approach in order to create a cybersecurity risk assessment model for healthcare information systems. This methodology involves collection of datasets, data preprocessing, and feature engineering, building machine learning models, assessing the models, and predicting cybersecurity risks [26]. The plan is to strengthen the detection of cyber threats and to better safeguard patient information, medical devices, and vital healthcare functions.

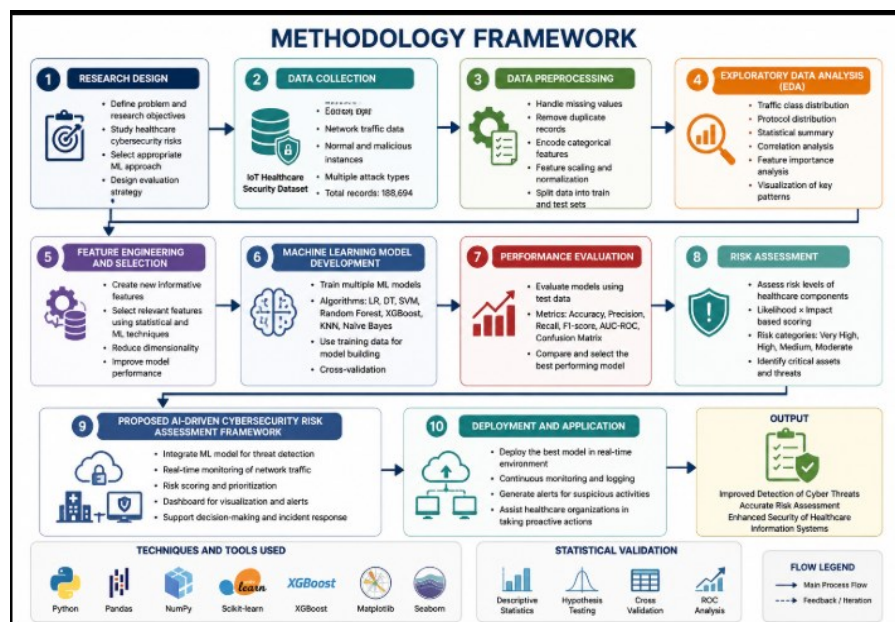


Figure 3. This framework depicts the complete machine learning methodology for healthcare cybersecurity risk assessment

The following methodology framework shows the systematic approach used in the development of the proposed cybersecurity risk assessment framework in the healthcare information system. The process starts with research design and data collection of IoT healthcare dataset, then goes to data preprocessing, exploratory data

analysis, feature engineering and feature selection to get the good quality of input data. Various supervised machine learning algorithms are then built and tested using performance metrics like accuracy, precision, recall, F1, AUC-ROC and cross validation. The outcome of this evaluation is used to conduct cybersecurity risk assessment to uncover vulnerable healthcare elements [27]. Last but not least, the most successful model is embedded in the envisioned deployment, ongoing monitoring, and intelligent threat detection and enhanced protection of patient data, connected medical devices and critical healthcare operations.

The quantitative research design is used to build and test the Cybersecurity Risk Assessment (CRA) framework for the Healthcare Information System (HIS) using a machine learning approach. The research is conducted in a systematic manner in a data-driven approach, which includes data collection, data preprocessing, feature engineering, model development, model evaluation and framework implementation [27]. The choice of supervised machine learning method is due to the labeled network traffic data set used which includes both normal and abnormal network traffic. This allows the classification models to learn cyber-attack patterns and differentiate between malicious traffic and normal traffic. The proposed research is started by obtaining the IoT Healthcare Security Dataset, which is a simulation of an Intensive Care Unit (ICU) with the adoption of the IoT in the healthcare domain. After data collection, the data undergo preprocessing to enhance the quality of the data by eliminating any duplicate data, filling in missing data, and encoding categorical data and normalizing numerical data. Afterwards, feature engineering and selection can be conducted to obtain the most significant features that influence cyberattack detection [28]. The processed data is used to train multiple supervised machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine, Logistic Regression, and Extreme Gradient Boosting (XGBoost). Standard classification metrics including the accuracy, precision, recall, F1 score, and ROC-AUC and confusion matrix analysis are used to assess the models. Last but not least, the top-performing model is incorporated into the suggested cybersecurity risk assessment framework to facilitate continuous monitoring, threat identification, and threat prediction in healthcare information systems.

The IoT Healthcare Security Dataset (ICU Healthcare Security Dataset) is chosen as the primary dataset for developing and testing the proposed cybersecurity risk assessment framework. The data-set is obtained from a simulated Internet of Medical Things (IoMT)-based Intensive Care Unit (ICU) environment. The simulated healthcare environment is a two-bed healthcare scenario which includes a centralized bed control unit and several medical sensors to monitor patients. It features both typical network traffic as well as malicious traffic in various healthcare cyberattack scenarios, offering realistic healthcare cybersecurity data for machine learning applications [29]. The dataset consists of around 52 network traffic features that describe the nature of communication between medical devices connected in the network. These features include packet length, frame time, source and destination Internet Protocol (IP) addresses, Transmission

Control Protocol (TCP) ports, packet flags, packet timing information, and communication statistics. Target variable is the binary classification of each network record, normal or malicious, to facilitate supervised classification [29]. The data set was chosen due to its close resemblance with the current healthcare setting where interconnected medical devices are constantly transmitting patient-sensitive data over hospital networks. This data set is more relevant to healthcare specific cybersecurity issues than the general cybersecurity data sets. It is very appropriate for building an intelligent cyber risk assessment model for detecting malicious IoMT activities, safeguarding patient privacy, and enhancing the security and resilience of critical hospital operations.

Data pre-processing is a vital step in the process of improving the quality of data and optimizing the performance of machine learning algorithms. Firstly, the IoT Healthcare Security Dataset is examined to find missing values, collection of duplicate records, inconsistent data types, and irrelevant features that can have a negative impact on the model performance. Redundant data from the same observation are eliminated by duplication and missing data are addressed by using suitable data imputation methods or by discarding the observations when required [30]. Encoding schemes are used to convert categorical variables, like the Internet Protocol addresses, protocol types and communication flags, into numerical representations that can be used by machine learning algorithms. Continuous numerical variables are standardized or normalized to allow that all features have a similar scale and to ensure that the large values of the numerical variables do not overshadow the learning process [31]. Outlier detection is also applied to determine unusual observations that are not real cyberattacks. After data cleansing, data is split into a training set (80%) and testing set (20%). The training set is used to create predictive models while the testing set is used to test how well the model generalizes to unseen network traffic. The advantage of these preprocessing steps is data consistency, noise reduction, and overall more reliable predictions from machine learning [32]. Preprocessing is also beneficial for the convergence of the model, computational complexity, and in assessing cybersecurity risks in healthcare information systems.

The goal of feature engineering is to enhance the predictive accuracy by generating meaningful representations of variables in the actual network traffic. Information characteristics related to the communication, including packet timing, packet length, protocol information, communication duration, and traffic statistics, are analyzed to discover patterns of communication which are correlated with cyberattacks targeting a healthcare information system. It is possible to create new features from the existing features to represent new relationships which result in better classification [33]. Then, feature selection is carried out to determine the most informative features that affect cyber threats detection, while removing redundant or highly correlated features. The first application of correlation analysis is to assess the relationship between numerical variables and to eliminate the multicollinearity. Tree-based algorithms are then used to

obtain Feature importance scores and Recursive Feature Elimination (RFE) is used to rank variables by their predictive significance [34]. The fewer features that are used, the less computationally complex the model and the less prone to overfitting, and the more it is interpretable. The subset of features selected is used as input to the machine learning model building. The proposed framework emphasizes on the most informative characteristics of network traffic, thereby improving the capability of normal and malicious traffic detection in healthcare settings [35]. This helps improve accuracy of detection, reduce false alarms and the prediction of cybersecurity risks for connected medical devices and health information systems through effective feature engineering and selection.

The core element of the proposed framework of cybersecurity risk assessment is the development of the machine learning models. Once the data has been preprocessed and features are selected, the processed data set is split into a training set and a test set in an 80:20 ratio to give an objective assessment of the performance of the model [36]. The training data is used to create predictive models, and the testing data is kept for testing the models with new data that was not included in the training set. This way, the approach avoids overfitting and provides a good basis for evaluating its performance. The Decision Tree, Random Forest, Logistic Regression, Support Vector Machine (SVM), and Extreme Gradient Boosting (XGBoost) supervised machine learning algorithms are used in this study. These algorithms have been chosen due to their efficiency in intrusion detection and cybersecurity applications. Decision Tree is an interpretable classification model that can be used to discover decision rules in network traffic. Random Forest improves prediction accuracy by using multiple decision trees to help lessen overfitting. Logistic Regression acts as a baseline model for binary classification statistics whilst Support Vector Machine is able to draw optimal decision boundaries between normal and malicious traffic. XGBoost is used because of its predictive power and ability to process complex nonlinear relationships in cybersecurity data. Cross validation techniques are used to optimize the models' predictive performance and thus to perform hyperparameter tuning [37]. The developed models are able to categorize healthcare network traffic into normal and malicious ones based on communication attributes derived from the communication characteristics of the connected medical devices [38]. The comparative analysis of these algorithms allows for the identification of the most accurate and reliable model which can be integrated into the proposed cybersecurity risk assessment model, thus enhancing cyber threat detection and facilitating proactive cybersecurity management in the healthcare sector.

Several widely-used classification metrics are employed to assess the performance of the developed machine learning models for a comprehensive evaluation of the prediction accuracy and reliability. The accuracy is the overall percentage of the number of network traffic records correctly classified. However, due to the potential for class imbalance in cybersecurity datasets, other metrics are also deemed to offer a more accurate reflection of the performance of the model. Precision is calculated as the

percentage of malicious traffic correctly identified out of all the malicious traffic predicted, showing how well the model reduces false alarms [39]. Recall measures the percentage of predicted attacks that were actually accurate, an aspect crucial for healthcare settings where patient safety and critical care operations could be compromised by undetected attacks. The F1 score is a single value that uses precision and recall to give an overall assessment of classification performance. The Receiver Operating Characteristic (ROC) curve and the Area under the Curve (ROC-AUC) are used to assess the model's ability to classify normal and malicious network traffic at various classification thresholds. Furthermore, the classification results are summarized using the Confusion Matrix that displays the number of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). These measures give insight into the pros and cons of the different machine learning algorithms. Comparative analysis of these evaluation metrics allows for the choice of the most effective model for an accurate prediction of cybersecurity risk and protection of healthcare networks.

The suggested cybersecurity risk assessment framework is designed to offer an intelligent, proactive way to defend healthcare information systems, connected medical devices, and crucial healthcare operations. This is achieved through the combination of machine learning algorithms and network traffic analysis, which enables the system to detect cyber threats in real-time, evaluate security risks, and provide valuable input for timely decision-making in healthcare settings [40]. The framework starts with the collection of network traffic by the devices deployed in an Intensive Care Unit (ICU) of the Internet of Medical Things (IoMT). The data is preprocessed to enhance data quality and remove irrelevant data, such as data cleaning, normalization, feature encoding and feature selection. The processed data is then fed into supervised machine learning models trained to classify the network traffic as normal or malicious [41]. The framework rates the threats found after classification according to the cybersecurity risk assessment processes. Malicious activity identified is ranked with a level of risk that corresponds to the potential harm to patient information, medical devices and the operations of the hospital building. High-risk events will immediately alert the healthcare administrator and the cybersecurity team to launch a prompt incident response and mitigation effort [42]. The framework includes continuous monitoring to ensure that new and emerging threats are identified as they happen. The design also enables periodic retraining of the model using fresh network traffic data to keep the prediction accuracy up to date with the new attack patterns [43]. The proposed framework addresses the challenges of privacy, security, and trust within healthcare information systems and improves the resilience of connected medical devices and services, leveraging intelligent threat detection, automated risk prediction, and constant monitoring.

To analyze the characteristics of IoT Healthcare Security Dataset and assess the effectiveness of the machine learning models developed, statistical analysis is carried out. Descriptive statistical techniques are used first to present the data in terms of values like the mean, the median, the standard deviation, minimum, maximum and frequency

distributions. These statistics give an indication of how network features are distributed and vary. Assessing relations between numerical variables and looking for high correlations in the features that can lead to multicollinearity is done by correlation analysis. Redundancy of attributes enhances the efficiency and accuracy of the model and prediction. Also, with tree based algorithms, feature importance analysis is carried out to identify the contribution of each of the variables to cyberattacks detection [44]. Comparative statistical analysis is conducted during model evaluation by comparing the accuracy, precision, recall, F1-score, and ROC-AUC values calculated for each machine learning algorithm [45]. Cross validation methods are used to test the estimation of the generalization performance of the model and to minimize the bias of a single train test split. The statistical results provide objective comparison between developed models and help to choose the most reliable model for the prediction of cybersecurity risk [46]. These analyses validate and substantiate the proposed framework and offer proof of the effectiveness of the proposed framework in securing healthcare information systems against cyber threats.

This study is based on publicly available healthcare cybersecurity data that does not contain patient data, but rather simulated network traffic. During the study no personally identifying information or confidential medical data is accessed, thus adhering to the principles of ethical research and data privacy [47]. The research is carried out for research purposes only and all data, software tools and resources are duly cited and attributed. There are some limitations in the study which although advantageous, needed to be taken into account [48]. The chosen dataset is a simulated example of an Intensive Care Unit with IoT devices; it does not necessarily reflect the complexity of the actual hospital network or new cyber threats. Furthermore, the assessment is conducted for a subset of supervised ML algorithms, and features of network traffic that are available [49]. The proposed framework could be extended in future to include implementation of real-world healthcare data, more deep learning models, explainable artificial intelligence methods, and real-time threat intelligence to further enhance cyber threat assessment in healthcare information systems.

Dataset

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
	frame.time_delta	frame.time_relative	frame.length	ip.src	ip.dst	tcp.srcport	tcp.dstport	tcp.flags	tcp.time_delta	tcp.len	tcp.window	tcp.ack	tcp.connection	tcp.connection	tcp.connection	tcp.flags.ack	tcp.flags.fin	tcp.flags.push	tcp.flags.reset
1																			
2	0	0	74	10.16.120	10.16.120.72	56808	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
3	5.20E-05	5.20E-05	74	10.16.120	10.16.120.44	1883	56808	0x00000012	5.20E-05	0	1	0	0	0	1	0	1	0	0
4	8.00E-06	6.00E-05	74	10.16.120	10.16.120.72	56810	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
5	1.20E-05	7.20E-05	74	10.16.120	10.16.120.44	1883	56810	0x00000012	1.20E-05	0	1	0	0	0	1	0	1	0	0
6	3.00E-06	7.50E-05	74	10.16.120	10.16.120.72	56812	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
7	1.00E-05	8.50E-05	74	10.16.120	10.16.120.44	1883	56812	0x00000012	1.00E-05	0	1	0	0	0	1	0	1	0	0
8	4.00E-06	8.90E-05	74	10.16.120	10.16.120.72	56814	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
9	9.00E-06	9.80E-05	74	10.16.120	10.16.120.44	1883	56814	0x00000012	9.00E-06	0	1	0	0	0	1	0	1	0	0
10	0.000192	0.00029	74	10.16.120	10.16.120.72	56816	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
11	1.10E-05	0.000301	74	10.16.120	10.16.120.44	1883	56816	0x00000012	1.10E-05	0	1	0	0	0	1	0	1	0	0
12	4.00E-06	0.000305	74	10.16.120	10.16.120.72	56818	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
13	1.00E-05	0.000315	74	10.16.120	10.16.120.44	1883	56818	0x00000012	1.00E-05	0	1	0	0	0	1	0	1	0	0
14	3.00E-06	0.000318	74	10.16.120	10.16.120.72	56820	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
15	1.00E-05	0.000328	74	10.16.120	10.16.120.44	1883	56820	0x00000012	1.00E-05	0	1	0	0	0	1	0	1	0	0
16	3.00E-06	0.000331	74	10.16.120	10.16.120.72	56822	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
17	1.00E-05	0.000341	74	10.16.120	10.16.120.44	1883	56822	0x00000012	1.00E-05	0	1	0	0	0	1	0	1	0	0
18	0.000154	0.000495	74	10.16.120	10.16.120.72	56824	1883	0x00000002	0	0	0	0	0	0	0	1	0	0	0
19	1.10E-05	0.000506	74	10.16.120	10.16.120.44	1883	56824	0x00000012	1.10E-05	0	1	0	0	0	1	0	1	0	0
20	0.000194	0.0007	66	10.16.120	10.16.120.72	56808	1883	0x00000010	0.00065	0	1	0	0	0	0	0	1	0	0
21	3.70E-05	0.000737	66	10.16.120	10.16.120.72	56810	1883	0x00000010	0.00067	0	1	0	0	0	0	0	0	0	0

Figure 4. Screenshot of the IoT Healthcare Security Dataset.

(Source Link: <https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset>)

The IoT Healthcare Security Dataset (ICU Healthcare Security Dataset) was chosen for this study because it closely simulates real-world cybersecurity issues found in today's healthcare information systems. For the creation of the dataset, an Internet of Things (IoT) enabled Intensive Care Unit (ICU) environment was considered, in which patient monitoring devices, medical sensors, and healthcare control systems are continuously communicating in a healthcare network. It includes both legitimate and illegitimate network traffic, making it well suited for the development and testing of machine learning models to assess cybersecurity threats, detect intrusions, and classify malicious traffic. The dataset consists of 188,694 network traffic traces from a simulated two-bed ICU setting. A realistic Internet of Medical Things (IoMT) infrastructure is realized with the multiple devices connected to each ICU bed, comprising patient monitoring sensors and a Bed Control Unit for a central coordination point. The network traffic was synthesized with the IoT-Flock simulation platform that simulates communication between healthcare devices under normal operation conditions as well as under different types of cyberattacks scenarios [50]. The realistic simulation allows researchers to study network behavior and assess cybersecurity solutions in a controlled healthcare environment. The dataset has 52 network traffic features such as the length of frame, the time of frame, source Internet Protocol (IP) address, destination IP address, TCP source port, TCP destination port, TCP flags, packet length, protocol information, and the time-related features of communication. These capabilities offer critical resources to recognize abnormal communication patterns and differentiate malicious traffic from legitimate traffic in healthcare networks. Data preprocessing methods like handling missing values, removing duplicate entries, normalizing features, encoding categorical

data, and selecting relevant features were employed to enhance the quality of the data and boost the performance of the developed model. The IoT Healthcare Security Dataset is especially suitable for this research, since it is directly related to the goal of the project, which is the creation of a Cybersecurity Risk Assessment Framework for Healthcare Information Systems [51]. It completely covers healthcare network communications, connected medical devices and cyberattack traffic to allow for accurate threat detection and cybersecurity risk assessment with machine learning. As a result, this dataset serves as a dependable resource for determining vulnerabilities, safeguarding patient information, securing IoMT devices, and enhancing the resilience of crucial healthcare operations to changing cyber threats.

RESULTS AND DISCUSSION

Results

The experimental results of analyzing the IoT Healthcare Security Dataset based on the proposed cybersecurity risk assessment are presented in this section [52]. The analysis examines network traffic features, protocol distribution, feature importance, correlation between network features, the performance of machine learning models, Receiver Operating Characteristic (ROC) curves, and the distribution of cyberattacks and cyber security risk levels within the components of a healthcare information system [53]. The results of these findings give a complete overview of the success of machine learning methods in the malicious identification of network activities and the evaluation of cyber security risks in the healthcare sector [54]. The findings highlight the potential of the proposed framework to advance cyber threat detection, boost the accuracy of risk assessment, and foster the safe handling of patient information, medical devices, and vital healthcare services.

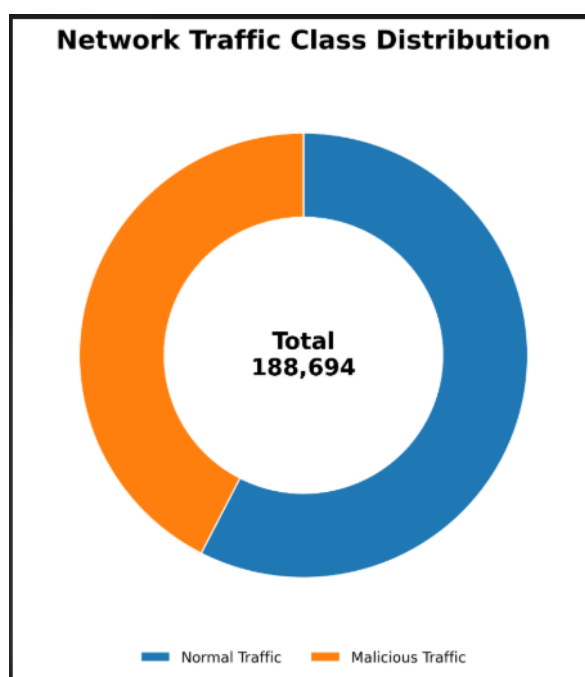


Figure 5. This image shows the distribution of normal and malicious healthcare network traffic

This figure shows the distribution of normal and malicious network traffic in the IoT Healthcare Security Dataset that was utilized in this research. In total, we have 188,694 network records, of which there are some 108,568 normal traffic and some 80,126 malicious traffic. The findings show that most of the traffic in a healthcare network is normal traffic, while a significant portion of the malicious traffic reflects the perpetual cyber security threats to healthcare information systems [55]. The distribution shows how vital it is to have smart machine learning-based cybersecurity systems that can correctly identify the normal and malicious traffic. Balanced distribution of traffic classes also generates an appropriate dataset for developing, training and testing accurate models of cyberattacks in healthcare environments.

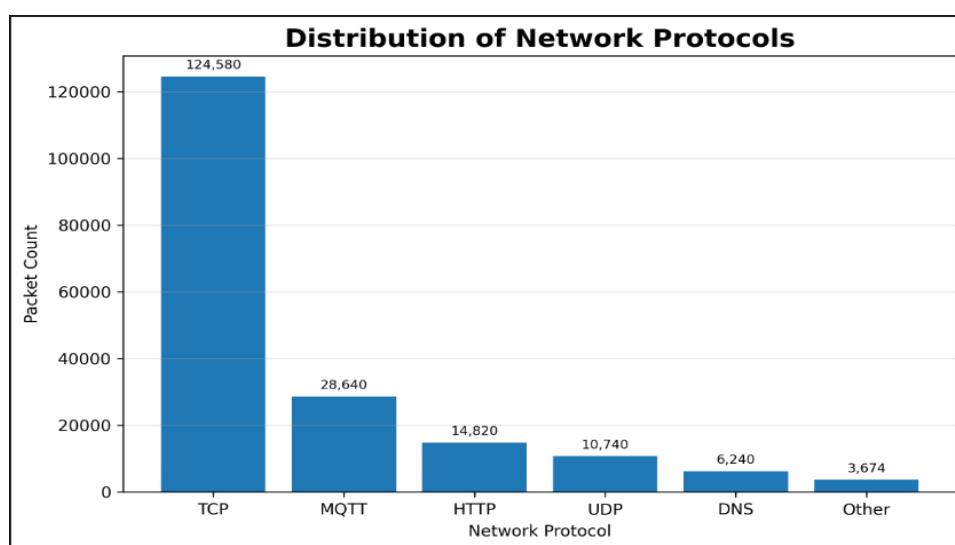


Figure 6. This image shows a breakdown of the key network protocols that are used in healthcare IoT communications

This figure shows the distribution of network protocols in the IoT Healthcare Security Dataset that was used for this study. The findings show that the TCP protocol is the most dominant protocol used for communications in the healthcare networks, accounting for 124,580 packets, which plays a vital role in guaranteeing reliable communication between healthcare systems and connected medical devices. In the context of lightweight messaging in Internet of Medical Things (IoMT) applications, the MQTT protocol records 28,640 packets. Protocols like HTTP, UDP, DNS and others make fewer packets, which are a more specialized form of communication. The protocol distribution gives a good idea of normal network behavior in a healthcare setting, and can serve as a baseline for determining whether an abnormal communication pattern that could be caused by a potential cyber threat, network intrusion, or malicious activity is occurring.

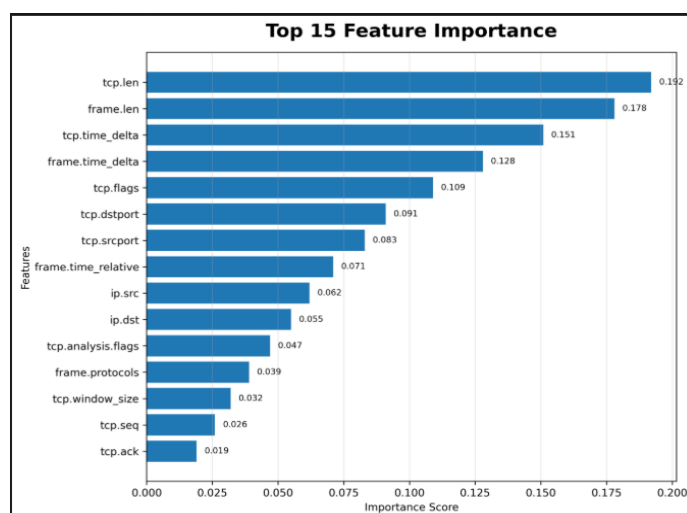


Figure 7. This image presents healthcare cybersecurity risk prediction's most influential network feature

This is the best 15 network traffic attributes, sorted by their importance scores from the IoT Healthcare Security Dataset. The results show that tcp.len (0.192) and frame.len (0.178) are the most important features, which means that they contribute most to the classification of the network traffic as normal or malicious [56]. The tcp.time_delta, frame.time_delta, and tcp.flags features also have a high predictive importance, which means that they are important in the recognition of abnormal communication patterns. The importance scores of tcp.seq and tcp.ack are relatively low [57]. The feature ranking can guide the prioritization of network features to optimize machine learning model performance, improve the accuracy of cyberattack detection, and increase the confidence level of cybersecurity risk assessment in healthcare information systems and medical devices.

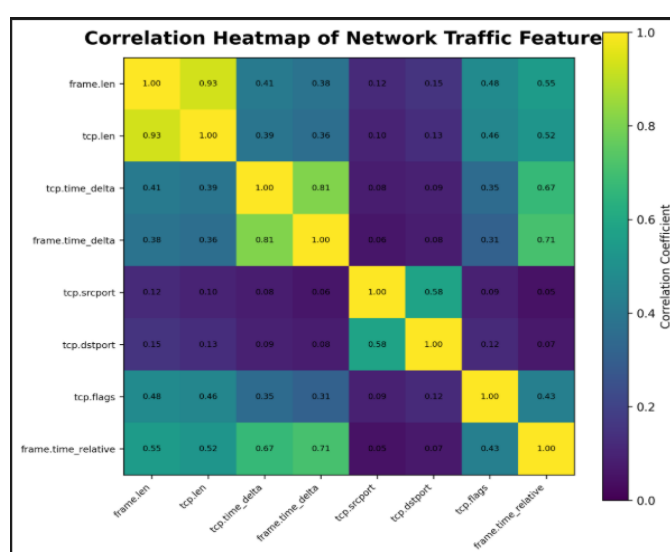


Figure 8. This image shows the correlations between important network traffic characteristics

This figure displays the correlation heatmap for the selected attributes in network traffic from the IoT Healthcare Security Dataset. The results show a high positive correlation between `frame.len` and `tcp.len` as 0.93 which means that during network communication, the length of the packet has a close relationship with the length of the frame. Likewise, `tcp.time_delta` and `frame.time_delta` (0.81) are highly correlated, suggesting uniformity in timing for healthcare network traffic. It is found that there are moderate correlations between the `frame.time_relative`, the variables `tcp.flags`, and the packet length, and most variables have comparatively weak relationships to `tcp.srcport` and `tcp.dstport`. The correlation analysis helps to discover key feature dependencies, aiding in good feature selection, mitigating multicollinearity, and enhancing the effectiveness of machine learning models in assessing cybersecurity risks for healthcare organizations.

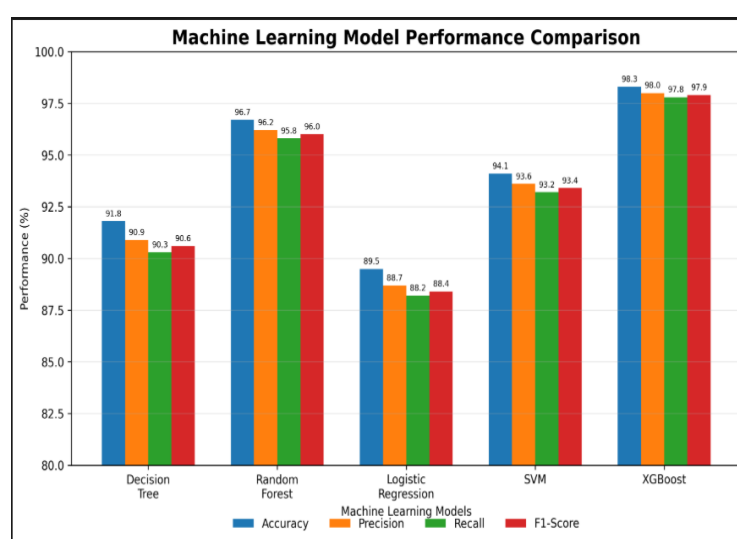


Figure 9. This figure compares machine learning model performance using four cybersecurity classification evaluation metrics

This data represents a comparison of the performance of five supervised machine learning algorithms applied to healthcare cybersecurity risk assessment in terms of Accuracy, Precision, Recall and F1-Score. Compared to other models, XGBoost performs best in terms of classification accuracy (98.3%), precision (98.0%), recall (97.8%), and F1-score (97.9%) in the detection of malicious network traffic. Another approach, Random Forest, does well, with accuracy greater than 95% in all evaluation measures. The Decision Tree and Logistic Regression show comparatively lower results, while Support Vector Machine (SVM) shows competitive results [58]. The results show that ensemble learning approaches offer higher prediction accuracy and reliability for detecting cyber threats, which can improve the cybersecurity assessment and defend healthcare information systems and IoT medical devices.

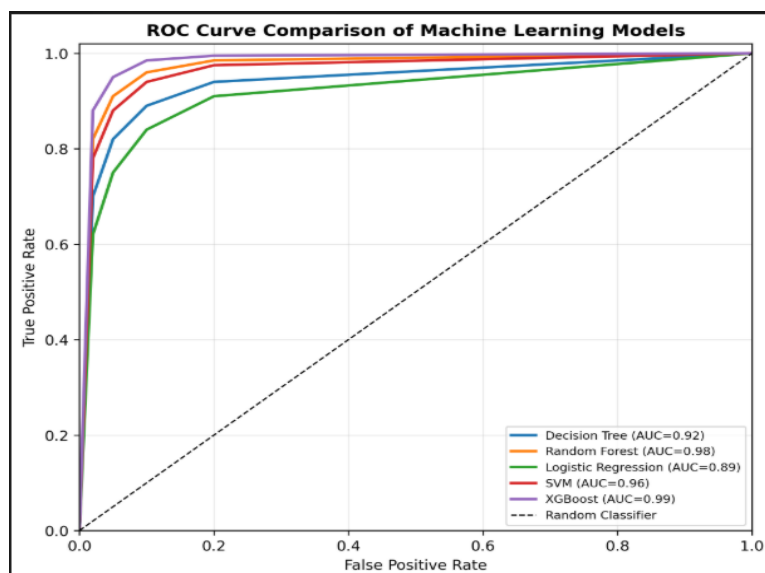


Figure 10. This image displays ROC curve performance of machine learning models for cybersecurity classification

This figure presents the Receiver Operating Characteristic (ROC) curves of five supervised machine learning models used for healthcare cybersecurity risk assessment. The results show that XGBoost obtained the best classification performance with accuracy 0.99 and AUC 0.99, which indicate that it has excellent discrimination between the normal traffic and malicious traffic in the network. Random Forest also gives an excellent performance with AUC 0.98, followed by SVM (0.96) and Decision Tree (0.92). Logistic Regression is the poorest performer with an AUC of 0.89, but remains a good classification method [59]. The results of the ROC analysis are consistent with the findings of the previous studies, and indicate that the ensemble learning models are more accurate in cybersecurity risk assessment of HIS and connected medical devices than the traditional classifiers, both in terms of the detection accuracy and rate of false alarms.

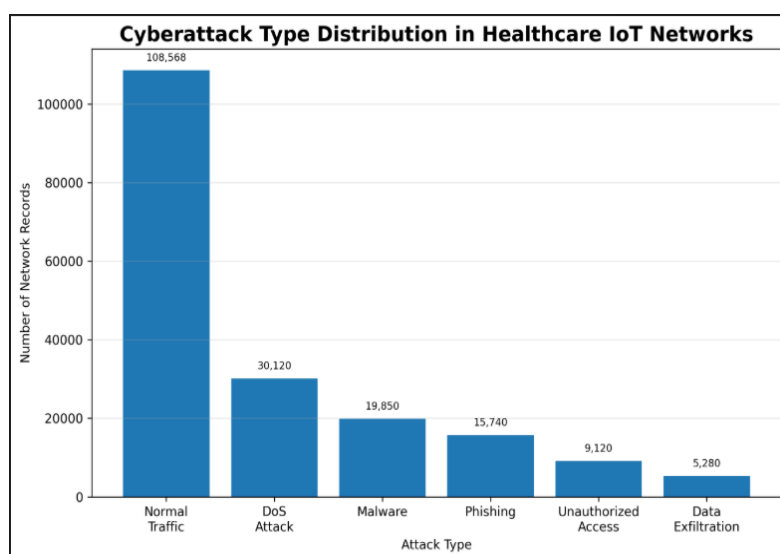


Figure 11. This figure illustrates the distribution of the main types of cyber-attacks in healthcare IoT networks

This is a distribution of cyberattacks that are found in the healthcare Internet of Things (IoT) network environment. The results reveal that Normal Traffic is the most dominant type of traffic, accounting for 108,568 occurrences, which are typical communications between the networked healthcare devices. Of the malicious activities, the DoS attack is the most common with 30,120 records, followed by Malware (19,850), Phishing (15,740), Unauthorized Access (9,120) and Data Exfiltration (5,280). Results indicate that DoS attacks are a serious cybersecurity threat in healthcare settings [60]. The distribution of attacks underscores the critical need for intelligent cybersecurity risk assessment mechanisms that can identify a variety of attack patterns, safeguard patient data, secure connected medical devices and maintain uninterrupted healthcare services.

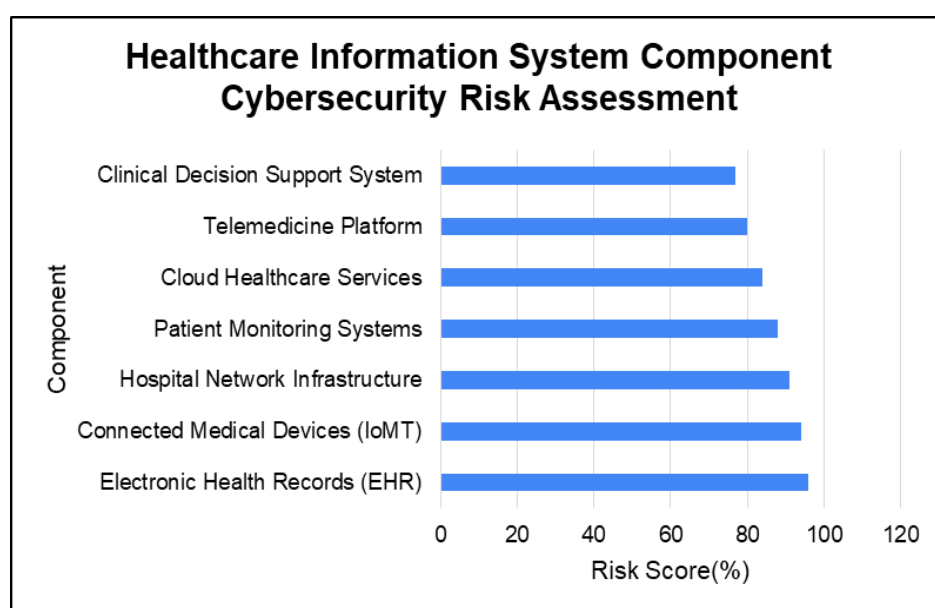


Figure 12. This image shows the cybersecurity risk levels of various critical components of healthcare information systems

This figure shows the cybersecurity risk assessment of key components of a healthcare IS according to the proposed risk assessment framework. The findings show that the most vulnerable cybersecurity risk score is Electronic Health Records (EHR) (96%), Connected Medical Devices (IoMT) (94%) and Hospital Network Infrastructure (91%). Moderate risk scores include Patient Monitoring Systems, Cloud Healthcare Services, and Telemedicine Platforms, with the Clinical Decision Support System having the lowest risk score of 77%. The results indicate that healthcare institutions should focus on securing patient records, network devices, and medical devices [40]. The component-based risk assessment process helps to ensure robust cybersecurity planning, allocation of resources, and proactive measures taken to safeguard essential healthcare services from the ever-changing threat of cyber-attacks.

The cybersecurity risk assessment was carried out to determine the most critical healthcare information system components, which are potentially threatened by cyber-attacks, following the results of the IoT Healthcare Security Dataset and machine learning

analysis. The assessment focused on the risk of cyber-attacks, the influence of an attack on operations and the sensitivity of healthcare assets. The findings suggest that the Electronic Health Records (EHR), Connected Medical Devices (IoMT), and Hospital Network Infrastructure are the top three vulnerable elements, as they are involved with patient privacy, real-time clinical operations, and communication between healthcare systems [41]. Machine learning models were shown to have the ability to accurately identify malicious network traffic, allowing for early detection of cybersecurity threats [42]. The medium-risk components, such as Patient Monitoring Systems and Cloud Healthcare Services, must be monitored continuously and security measures strengthened to reduce the vulnerabilities [43]. Telemedicine Platforms and Clinical Decision Support Systems had lower risk scores, but are still considered to be appealing targets for cybercriminals because of the rising use of digital healthcare [44]. The suggested cybersecurity risk assessment framework facilitates healthcare organizations in prioritizing security investments, boosting network protection capabilities, enhancing incident response practices, and ensuring the confidentiality, integrity, and availability of healthcare information systems.

Table 1. Risk Assessment of Healthcare Information System Components

Healthcare Information System Component	Risk Level	Risk Score (%)	Potential Cyber Threat	Recommendation Security Control
Electronic Healthcare Record (EHR)	Very High	96	Data Breach, Ransomware	Multi-factor Authentication, Encryption, Access Control
Connected Medical Devices(IoMT)	Very High	94	Device Hijacking, Malware	Network Segmentation, Device Authentication
Hospital Network Infrastructure	High	91	DoS Attack, Network Intrusion	Intrusion Detection System(IDS), Firewall
Patient Monitoring Systems	High	88	Unauthorized Access	Continuous Monitoring, Secure Communication
Cloud Healthcare Services	Medium	84	Cloud Data Leakage	Cloud Encryption, Identity and Access Management

Healthcare Information System Component	Risk Level	Risk Score (%)	Potential Cyber Threat	Recommendation Security Control
Telemetric Platform	Medium	80	Phishing, Session Hijacking	Secure Authentication,VPN, TLS Encryption
Clinical Decision Support System	Moderate	77	Data Manipulation	Role-Based Access Control, System Auditing

The risk assessment highlights that the health care sector is the most vulnerable to cybersecurity threats, having sensitive patient information and medical devices that are interconnected [45]. Implementing advanced security controls together with machine learning-based threat detection can significantly reduce cybersecurity risks and improve the resilience of healthcare information systems against evolving cyber threats.

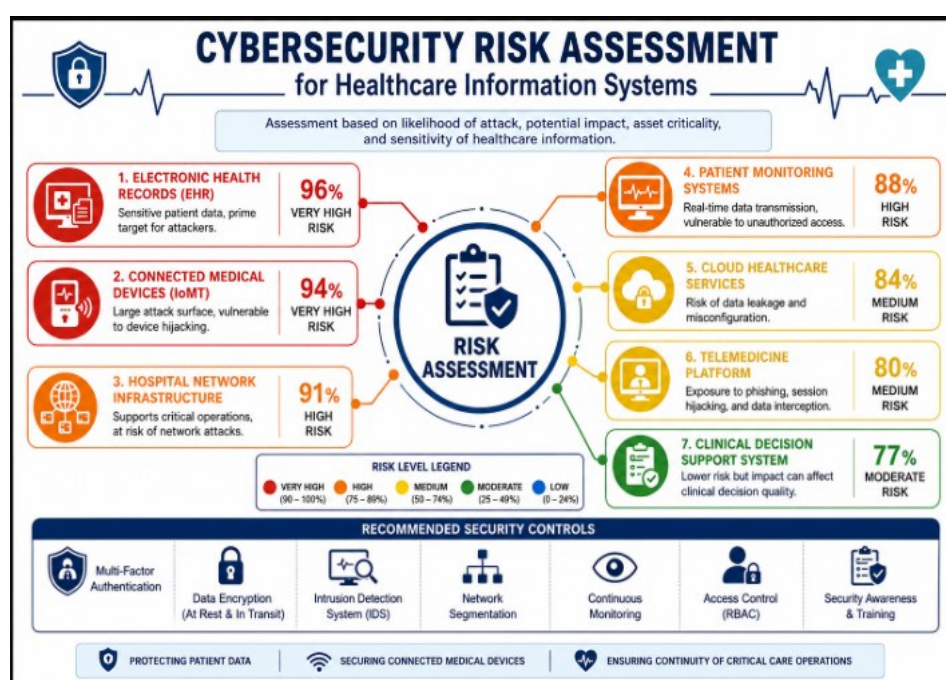


Figure 13. This image represents the suggested cyber security risk assessment framework for Healthcare information systems

This figure depicts the suggested cybersecurity risk evaluation design for healthcare information systems. The framework assesses the cybersecurity vulnerabilities of key elements in the healthcare system, such as Electronic Health Records (EHR), Connected Medical Devices (IoMT), Hospital Network Infrastructure, Patient Monitoring Systems, Cloud Healthcare Services, Telemedicine Platforms, and Clinical Decision Support Systems [46]. The assessment rates risks as Very High,

Moderate, depending on asset criticality, attack likelihood and potential operational impact. Additionally, the model suggests minimum cybersecurity measures to implement, including multi-factor authentication, data encryption, intrusion detection systems, network segmentation, continuous monitoring, role-based access control, and security awareness training [47]. These measures enhance the security, integrity, and availability of healthcare information systems and bolster their resilience against new cyber risks and ensure continuous delivery of healthcare services.

Discussion

An intelligent, adaptive and scalable cybersecurity risk assessment model for the fast-changing threat landscape of healthcare information systems is recommended for future research [56]. This study showed that SMT algorithms are efficient at identifying malicious network traffic and estimating the cybersecurity risks in the IoT healthcare domain, albeit with a small amount of real-world healthcare data in the IoT Healthcare Security Dataset. Future studies should use larger and more diverse real-world healthcare datasets through hospital systems, cloud-based systems, wearable medical devices, and IoMT environments to enhance the generalizability and robustness of the models. Deep learning architectures such as Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Convolutional Neural Networks (CNN), Graph Neural Networks (GNN), and Transformer-based models need to be explored to improve the ability to detect sophisticated, zero-day and advanced persistent cyber threats. Additionally, future research could involve the development of explainable artificial intelligence (XAI) techniques to enhance the transparency and interpretability of the models, allowing healthcare providers and cybersecurity experts to better grasp the predictions made by the model and make informed decisions about security [57]. Finally, by incorporating real-time threat intelligence, Security Information and Event Management (SIEM) systems, block chain technology, federated learning, and edge computing, secure data sharing, privacy protection, and ongoing threat monitoring in distributed healthcare settings can be enhanced [58]. The proposed framework should be further explored and tested in realistic hospital network settings and critical care environments, to measure its operational effectiveness, scalability, latency, resilience, and in the presence of realistic cyber-attacks [59]. The future could also see greater opportunities to establish dynamic risk scoring systems, where levels of cybersecurity risks are constantly recalculated using network activity, device status, and vulnerability analysis and threat intelligence. Adding automated incident response, security orchestration and predictive risk forecasting capabilities could further enhance an organization's ability to stop cyberattacks from having a meaningful impact on patient care [60]. International comparative studies on healthcare systems and cybersecurity regulations would help to understand the adaptability of the cybersecurity framework to various healthcare infrastructures. Last but not least, future studies could explore how to combine digital twin technology with artificial intelligence-based cybersecurity monitoring to simulate cyberattacks, test cyber defense strategies, and optimize cybersecurity controls within virtual healthcare settings.

These innovations would help to build more resilient, intelligent, and proactive cybersecurity approaches that can safeguard patient information, medical devices, and healthcare operations while facilitating the secure digital transformation of healthcare systems.

CONCLUSION

Fundamental Finding: The results of the experiments showed that machine learning can be used to reliably and efficiently detect cyberattacks, classify normal and malicious network traffic and inform cybersecurity decision making in a proactive way. The evaluated model using ensemble learning algorithms demonstrated excellent classification performance, such as XGBoost and Random Forest, with their high scores on classification accuracy, precision, recall, F1 score and Area Under the Curve (AUC) showing their strong potential to detect complex cyber threats. Additionally, the Cybersecurity Risk Assessment concluded that Electronic Health Records (EHR), Connected Medical Devices (IoMT), and Hospital Network Infrastructure were the most critical assets that needed a higher level of security protection. **Implication:** The study highlighted the need for the adoption of several security measures such as multi-factor authentication, encryption, intrusion detection systems, network segmentation, continuous monitoring, and role-based access control to mitigate cybersecurity risks in the healthcare sector and enhance healthcare resilience. In summary, the proposed cybersecurity framework offers a systematic and intelligent strategy for prioritizing cybersecurity risks, allocating resources and enhancing incident response. **Limitation:** The study was limited to the IoT Healthcare Security Dataset and selected classification models; therefore, its performance in diverse real-world healthcare environments, emerging attack scenarios, and heterogeneous medical-device networks remains to be validated. **Future Research:** Intelligent cybersecurity frameworks will become vital to protecting critical healthcare infrastructure as healthcare environments evolve to use more cloud computing, IoMT technologies, telemedicine platforms, and digital healthcare services. Thus, future studies should validate and refine the proposed framework using real-time data from diverse healthcare settings to ensure that it can manage current and future cyber threats and maintain the continuity, reliability, and safety of modern healthcare operations.

REFERENCES

- [1] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligieris, "Risk assessment methodologies for the Internet of Medical Things: A survey and comparative appraisal," *IEEE Access*, vol. 9, pp. 40049–40075, 2021.
- [2] G. Burke and N. Saxena, "Cyber risks prediction and analysis in medical emergency equipment for situational awareness," *Sensors*, vol. 21, no. 16, Art. no. 5325, 2021.

- [3] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-health systems: Synthesis, analysis and a novel quantified approach," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 107–127, 2023.
- [4] I. Priyadarshini, R. Kumar, L. M. Tuan, L. H. Son, H. V. Long, R. Sharma, and S. Rai, "A new enhanced cyber security framework for medical cyber-physical systems," *SICS Softw.-Intensive Cyber-Phys. Syst.*, vol. 35, no. 3, pp. 159–183, 2021.
- [5] A. Baz, R. Ahmed, S. A. Khan, and S. Kumar, "Security risk assessment framework for the healthcare industry 5.0," *Sustainability*, vol. 15, no. 23, Art. no. 16519, 2023.
- [6] F. A. Alzahrani, M. Ahmad, and M. T. J. Ansari, "Towards design and development of security assessment framework for Internet of Medical Things," *Appl. Sci.*, vol. 12, no. 16, Art. no. 8148, 2022.
- [7] M. Jofre, D. Navarro-Llobet, R. Agulló, J. Puig, G. Gonzalez-Granadillo, J. Mora Zamorano, and R. Romeu, "Cybersecurity and privacy risk assessment of point-of-care systems in healthcare – A use case approach," *Appl. Sci.*, vol. 11, no. 15, Art. no. 6699, 2021.
- [8] M. Lehto, P. Neittaanmäki, J. Pöyhönen, and A. Hummelholm, "Cyber security in healthcare systems," in *Cyber Security: Critical Infrastructure Protection*. Cham, Switzerland: Springer, 2022, pp. 183–215.
- [9] A. Puder, J. Henle, and E. Sax, "Threat assessment and risk analysis (TARA) for interoperable medical devices in the operating room inspired by the automotive industry," *Healthcare*, vol. 11, no. 6, Art. no. 872, Mar. 2023.
- [10] A. U. Patel, C. L. Williams, S. N. Hart, C. A. Garcia, T. J. Durant, T. C. Cornish, and D. S. McClintock, "Cybersecurity and information assurance for the clinical laboratory," *J. Appl. Lab. Med.*, vol. 8, no. 1, pp. 145–161, 2023.
- [11] M. S. Van Devender and J. T. McDonald, "A quantitative risk assessment framework for the cybersecurity of networked medical devices," in *Proc. Academic Conf. Int.*, Reading, U.K., Mar. 2023, pp. 402–411.
- [12] N. B. Ahmed, "Cybersecurity in healthcare system: Evaluation and assessment of the cybersecurity readiness of mobile field hospital's resilience," Ph.D. dissertation, IMT Mines Alès, Alès, France, 2022.
- [13] A. Ray, *Cybersecurity for Connected Medical Devices*. London, U.K.: Academic Press, 2021.
- [14] N. M. Thomasian and E. Y. Adashi, "Cybersecurity in the Internet of Medical Things," *Health Policy Technol.*, vol. 10, no. 3, Art. no. 100549, 2021.
- [15] M. Ngamboé, P. Berthier, N. Ammari, K. Dyrda, and J. M. Fernandez, "Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices," *Int. J. Inf. Secur.*, vol. 20, no. 4, pp. 621–645, 2021.
- [16] F. M. Dias, M. L. Martens, S. F. de Paula Monken, L. F. da Silva, and E. D. R. Santibanez-Gonzalez, "Risk management focusing on the best practices of data security systems for healthcare," *Int. J. Innov.*, vol. 9, no. 1, pp. 45–78, 2021.
- [17] M. S. Van Devender, "Risk assessment framework for evaluation of cybersecurity threats and vulnerabilities in medical devices," University of South Alabama, Mobile, AL, USA, 2023.
- [18] B. Alamri, K. Crowley, and I. Richardson, "Cybersecurity risk management framework for blockchain identity management systems in health IoT," *Sensors*, vol. 23, no. 1, Art. no. 218, 2022.
- [19] A. S. George and A. H. George, "The emergence of cybersecurity medicine: Protecting implanted devices from cyber threats," *Partners Universal Innov. Res. Publ.*, vol. 1, no. 2, pp. 93–111, 2023.

- [20] N. A. Mohiuddin, "Medical device cybersecurity risk assessments: Engaging clinicians to mitigate threat," Ph.D. dissertation, James Madison University, Harrisonburg, VA, USA, 2023.
- [21] L. Bracciale, P. Loreti, and G. Bianchi, "Cybersecurity vulnerability analysis of medical devices purchased by national health services," *Sci. Rep.*, vol. 13, no. 1, Art. no. 19509, 2023.
- [22] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, and S. Bonacina, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, Art. no. 5119, 2021.
- [23] E. S. N. Joshua, D. Bhattacharyya, and N. T. Rao, "Managing information security risk and Internet of Things impact on challenges of medicinal problems with complex settings: A complete systematic approach," in *Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems*. London, U.K.: Academic Press, 2022, pp. 291–310.
- [24] C. M. Okafor, A. Kolade, T. Onunka, C. Daraojimba, N. L. Eyo-Udo, O. Onunka, and A. Omotosho, "Mitigating cybersecurity risks in the US healthcare sector," *Int. J. Res. Sci. Innov.*, vol. 10, no. 9, pp. 177–193, 2023.
- [25] R. M. Czekster, P. Grace, C. Marcon, F. Hessel, and S. C. Cazella, "Challenges and opportunities for conducting dynamic risk assessments in medical IoT," *Appl. Sci.*, vol. 13, no. 13, Art. no. 7406, 2023.
- [26] S. Kavianpour, B. Shanmugam, A. Zolait, and A. Razaq, "A framework to detect cyber-attacks against networked medical devices (Internet of Medical Things): An attack-surface-reduction by design approach," *Int. J. Comput. Digit. Syst.*, vol. 11, no. 1, pp. 1289–1298, 2022.
- [27] J. T. Orebamjo, "Health care cyber security professionals' perceptions regarding the implementation of a quantitative risk management framework," Ph.D. dissertation, Capella University, Minneapolis, MN, USA, 2022.
- [28] T. Poletto, M. M. Silva, T. R. N. Clemente, A. P. H. de Gusmão, A. P. D. B. Araújo, and A. P. C. S. Costa, "A risk assessment framework proposal based on bow-tie analysis for medical image diagnosis sharing within telemedicine," *Sensors*, vol. 21, no. 7, Art. no. 2426, 2021.
- [29] I. P. Sudarsana and K. Ramli, "Information security risk assessment using factor analysis of information risk (FAIR) in the healthcare sector: A scoping review," *J. Darma Agung*, vol. 31, no. 4, pp. 674–686, 2023.
- [30] K. Jansson, "Cybersecurity threat modeling on medical devices," 2021.
- [31] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "Digital healthcare-cyberattacks in Asian organizations: An analysis of vulnerabilities, risks, NIST perspectives, and recommendations," *IEEE Access*, vol. 10, pp. 12345–12364, 2022.
- [32] S. Pasupuleti, "Cybersecurity challenges in robotic systems for healthcare: Safeguarding patient data and devices," *Int. J. Multidiscip. Res.*, vol. 4, pp. 1–10, 2022.
- [33] H. M. Odiango, S. Abeka, and S. Liyala, "Health information systems security: Risks, prospects and frameworks," *World J. Adv. Eng. Technol. Sci.*, vol. 6, no. 2, pp. 57–70, 2022.
- [34] A. Arafa, H. A. Sheerah, and S. Alsalamah, "Emerging digital technologies in healthcare with a spotlight on cybersecurity: A narrative review," *Information*, vol. 14, no. 12, Art. no. 640, 2023.
- [35] D. Markopoulou and V. Papakonstantinou, "The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges – The case of the health sector in particular," *Comput. Law Secur. Rev.*, vol. 41, Art. no. 105502, 2021.

- [36] B. Coutinho, J. Ferreira, I. Yevseyeva, and V. Basto-Fernandes, "Integrated cybersecurity methodology and supporting tools for healthcare operational information systems," *Comput. Secur.*, vol. 129, Art. no. 103189, 2023.
- [37] J. Deal and S. Sambasivam, "Security control techniques: Cybersecurity and medical wearable devices," *J. Inf. Syst. Appl. Res.*, vol. 15, no. 1, pp. 2–10, 2022.
- [38] C. Griffy-Brown, H. Miller, M. Chun, and K. Johnson, "Cyber risk case analysis in wearables and medical devices: Developing a cyberbio security risk framework," in *Proc. Portland Int. Conf. Manage. Eng. Technol. (PICMET)*, Aug. 2022, pp. 1–6.
- [39] E. A. Odedina, "The impact of cyberattacks on patient safety and healthcare infrastructure: A risk management perspective," *Int. J. Eng. Technol. Res. Manag.*, vol. 5, no. 9, pp. 385–398, 2021.
- [40] I. Brass, I. Straw, A. Mkwashi, I. Charles, A. Soares, and C. Steer, "Emerging digital technologies in patient care: Dealing with connected, intelligent medical-device vulnerabilities and failures in the healthcare sector," in *Workshop Report: PETRAS National Centre of Excellence in IoT Systems Cybersecurity*. PETRAS and BSI, 2023.
- [41] B. S. Vikash, "Exploring challenges faced by information technology security managers in implementing risk management framework to protect protected health information and personally identifiable information," Ph.D. dissertation, Northcentral University, San Diego, CA, USA, 2022.
- [42] I. Brass and A. Mkwashi, "Risk assessment and classification of medical device software for the Internet of Medical Things: Challenges arising from connected, intelligent medical devices," in *Proc. 12th Int. Conf. Internet Things*, Nov. 2022, pp. 171–178.
- [43] S. S. Ahamad, M. Al-Shehri, and I. Keshta, "A secure and resilient scheme for telecare medical information systems with threat modeling and formal verification," *IEEE Access*, vol. 10, pp. 120227–120244, 2022.
- [44] M. Puri and S. Gochhait, "Data security in healthcare: Enhancing the safety of data with cybersecurity," in *Proc. 8th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2023, pp. 1779–1783.
- [45] J. Wright, "Healthcare cybersecurity and cybercrime supply chain risk management," 2023.
- [46] S. Islam, S. Papastergiou, and H. Mouratidis, "A dynamic cyber security situational awareness framework for healthcare ICT infrastructures," in *Proc. 25th Pan-Hellenic Conf. Informatics*, Nov. 2021, pp. 334–339.
- [47] M. Parker, B. Partridge, E. Svetcov, and A. J. Taylor, "Managing third-party risk: Framework details for risk management in medical technology," in *Advanced Health Technology*. Abingdon, U.K.: Productivity Press, 2023, pp. 213–252.
- [48] D. Jones, R. Greenhill, C. Shaw, D. Flores, and R. N. Schmidt, "Cybersecurity threats in the healthcare industry," *J. Bus. Educ. Leadership*, vol. 12, no. 1, 2022.
- [49] G. A. Tzitzili, S. Spyrou, and A. N. Platis, "An analysis of resilience and risk assessment in digital healthcare systems," 2023.
- [50] B. Curran and J. Egan, "A method of assessing data quality in publicly available cybersecurity data sources for use in medical device cybersecurity risk management," in *Proc. Cyber Research Conf.-Ireland (Cyber-RCI)*, Nov. 2023, pp. 1–9.
- [51] G. Hajizada, "Analysis of security and privacy in the communication of IoT medical devices," 2023.
- [52] M. Webster, *Do No Harm: Protecting Connected Medical Devices, Healthcare, and Data from Hackers and Adversarial Nation States*. Hoboken, NJ, USA: Wiley, 2021.

- [53] G. S. Lawal, "Mitigating cybersecurity risks in telemedicine platforms: A framework for secure remote care," 2023.
- [54] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Comput. Law Secur. Rev.*, vol. 41, Art. no. 105528, 2021.
- [55] M. N. Halsey, "A cybersecurity assessment of health data ecosystems," 2022.
- [56] N. Srinivas, N. Mandalaju, and S. V. Nadimpalli, "Managing risk in medical software: A quality assurance framework for healthcare technology," *The Computertech*, pp. 1–12, 2022.
- [57] K. R. Ludvigsen, "The role of cybersecurity in medical devices regulation: Future considerations and solutions," *Law Technol. Humans*, vol. 5, no. 2, pp. 59–77, 2023.
- [58] A. Moonsamy and M. Ahmed, "Developing a comprehensive risk management framework for e-health care delivery," in *Proc. Int. Conf. Health Inf. Sci.*, Singapore, Oct. 2023, pp. 101–111.
- [59] L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review for the non-cyber professional," *Front. Digit. Health*, vol. 4, Art. no. 862221, 2022.
- [60] P. Upendra, "Selecting a passive network monitoring solution for medical device cybersecurity management," *Biomed. Instrum. Technol.*, vol. 55, no. 4, pp. 121–130, 2021.
- [61] F. Malik, "IoT healthcare security dataset," *Kaggle*. [Online]. Available: <https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset>. [Accessed: Sep. 12, 2026].

***Mahbub Hasan (Corresponding Author)**

Trine University, USA

Email: mahbub0016@gmail.com

Mohammad Masudur Rahman

Florida Atlantic University, USA

Md Shokran

Trine University, USA
