Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 20 May 2026
Revised 02 July 2026
Accepted 16 July 2026

Natural Resources for Human Health 2026, Vol. 6 (12s): 898–910

KEYWORDS:
Artificial Intelligence, Machine Learning, Healthcare Cybersecurity, IoMT, Threat Detection, Threat Prevention, Cyber Resilience,

AI-Driven Cybersecurity Framework for Healthcare: Machine Learning-Based Detection and Prevention of Advanced Cyber Threats in Medical Systems

Shahed Ahmed Chowdhury[1], Masjidul Azad[2], Md Jaheerul Islam[3], Mohammad Sami[4], Mohammad Omair[5], Mohd Imran[6]

[1]Masters, Information system and Technology, Wilmington University, USA
Email: Shahed.33cse@gmail.com
[2]Masters, Cybersecurity St Francis College, USA
Email: mazad3@sfc.edu
[3]Bachelor, Computer Science, Wilmington University, USA
Email: zaheerulislam767@gmail.com
[4]MSc, Information Technology Management, University of Sunderland, UK
Email: msami.rafi@gmail.com
[5]BS, Electronic Engineering, Sir Syed University of Engineering and Technology, Pakistan
Email: omair.rafi@gmail.com
[6]Center For Health Research, Northern Border University, Arar 73213, Saudi Arabia, ORCID: 0000-0002-6064-1040
Email: imran.pchem@gmail.com

ABSTRACT: The purpose of this study is to create a framework for cybersecurity in healthcare that incorporates machine learning in threat detection and prevention. It is implementing sound cybersecurity practices, AICF-H (Artificial Intelligence Driven Cybersecurity Framework for Healthcare). Healthcare is undergoing digital transformation, with more reliance on Electronic Health Records (EHRs), telemedicine, cloud computing, and Internet of Medical Things (IoMT) and IoT-connected medical devices. These technologies are enhancing healthcare services. It is introducing potential cybersecurity threats such as ransomware, malware, phishing, breaches of medical devices, unauthorized access, and data breaches. Conventional cybersecurity defense strategies might not be effective against advanced and new threats. The study will use a mixed-methods research design, using quantitative analysis of cybersecurity datasets. The qualitative data was collected from healthcare IT professionals and cybersecurity experts. The machine learning models, including Random Forest, Support Vector Machine, XGBoost, and Neural Networks, will be trained and evaluated by quantitative metrics, such as accuracy, precision, recall, F1 score, and false-positive rate. Qualitative analysis will delve into the experts' views on the challenges of cybersecurity, explainability, privacy, and the implementation of AI. The results will be used to create and test the proposed framework. The research needs to illustrate the potential for enhanced early threat detection, prevention, incident response. The cybersecurity resilience within healthcare systems through the use of AI and machine learning.

Natural Resources for Human Health
eISSN: 2583-1194

1. INTRODUCTION

Modern healthcare has been revolutionized by the adoption of Electronic Health Records (EHRs), telemedicine, cloud computing, and the Internet of Medical Things (IoMT) [1]. These technologies provide benefits to healthcare delivery and information sharing. It raises the threat of cyber-attacks to healthcare organizations [2]. Healthcare systems are a crucial target for cybercriminals due to the sensitivity of patient information [14].

Healthcare organizations are vulnerable to many cybersecurity threats, such as ransomware, malware, phishing attacks, data breaches, insider threats, and attacks on connected medical devices [8]. These attacks may lead to patient privacy issues, healthcare service disruptions, and organizational and financial risks [3]. Traditional cybersecurity systems tend to be based on known attack signatures and rules. While these can detect known attacks, they can be challenged in identifying new, sophisticated, and zero-day attacks. This issue can be resolved by the use of machine learning, which learns patterns from large datasets and detects abnormal or malicious behaviors [4]. Artificial intelligence (AI) and machine learning (ML) have become a more frequent tool in the box for intrusion detection, anomaly detection, malware classification, user behavior analysis, and threat prediction [5].

In the healthcare sector, ML can aid in continuous monitoring and prompt detection of malicious behavior, potentially enhancing the security of healthcare information systems [6]. The adoption of AI-powered cybersecurity has challenges in data quality, patient privacy. AI model explainability, computation, and the trustworthiness of AI systems [9]. There is a need for healthcare organizations to adopt cybersecurity strategies that take into account not only the technical capabilities of AI models but also the specific demands of healthcare settings [7].

The authors have developed an AI-Driven Cybersecurity Framework for Healthcare (AICF-H) that integrates a machine learning-driven threat detection, prevention, and incident response approach [10]. The study will employ a mixed-methods approach, incorporating both quantitative assessment of ML models and qualitative insights from healthcare IT and cybersecurity practitioners [12]. The proposed model will offer a holistic approach to strengthening cybersecurity resilience in today's healthcare systems [13].

Artificial intelligence is the course of human insight executed by machines. Artificial intelligence Promotes sustainable and sound use of assets. Information-driven organizations can upgrade. more precise expectations and choices [7]. The further developed computerized change, which is more developed. procedure, which generates information on the basis of a huge set of data [6]. In this way, the execution of artificial intelligence is driven. Intelligence cycles will further develop bank representatives' efficiency [8].

Past examinations demonstrate existing assortment at present. Which banks have seen cost decrease and income age previous to upgrading the type of the combinations? cycle of the task, for instance, as far as loaning, security administrations, consistency enhancements, new types of administrations, and misrepresentation recognition [9]. These reworked setups and administrations supply clients with custom-made venture methodologies, abundance-the-board strategies, and robo-consultants [10]. The artificial intelligence assumes an essential part in independent dynamic cycles, screens resources and cycles continuously, and empowers esteem creation, and the Advantages will increment the proceeding. In the swiftly evolving world of finances, the amalgamation of the field of monetary economics and the potential of computer-based intelligence to upgrade dynamic cycles is huge. execution [11].

Artificial intelligence can function for monetary announcing too, but it can additionally motivate a lack of ease, a lack of simplicity, information protection issues, and consistency issues. Associations might confront work removal, preparation holes, high execution costs, interoperability challenges, and moral worries [11-12]. These negative effects, associations should concentrate on mindful artificial intelligence rehearsals, put resources into information quality and administration. The expectations of addressability in simulated intelligence models is likely to contain predispositions.

Natural Resources for Human Health
eISSN: 2583-1194

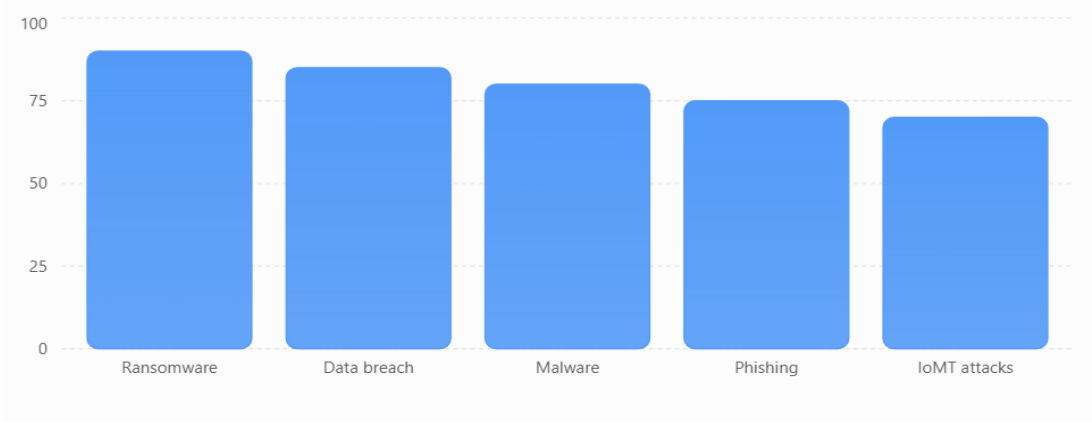

Fig. No.01: Healthcare cyber- threat categories

2. PROBLEM STATEMENT

Ransomware, phishing, malware, zero-day vulnerabilities, and healthcare technology attacks on connected devices. It is increasingly a threat to healthcare organizations [17]. These threats can affect patients' sensitive information and sensitive services within the healthcare sector [18]. Legacy systems, complex healthcare systems, vulnerabilities in IoMT, and poor cybersecurity infrastructure aggravate the problem [19]. Old security solutions might not be able to monitor emerging or unknown threats . It is essential to have a cybersecurity framework that integrates AI and machine learning capabilities to be effective in detecting, preventing, responding, and recovering from cyber threats while keeping healthcare data privacy and system security in mind [20].

3. AIM OF THE STUDY

The main aim of this study is to develop and evaluate an AI-driven cybersecurity framework for healthcare organizations. The uses of machine learning techniques to identify, detect, prevent, and respond to advanced cyber threats. The study will center on enhancing the security of healthcare information systems, Electronic Health Records (EHRs), and IoMT (Internet of Medical Things) devices, alongside concerns about data privacy, detection accuracy, false-positive alerts, system vulnerabilities, and explainability of AI. The study will integrate quantitative assessment of machine learning models with in-depth insights of healthcare IT and cybersecurity practitioners to create a viable and efficient model to enhance the cyber resilience of healthcare systems.

4. LITERATURE REVIEW

4.1 Healthcare Cybersecurity

The complexity and interconnectedness of their systems and the handling of patient-sensitive information mean that healthcare organizations are becoming increasingly vulnerable to cyberattacks [21]. The number of cyberattacks against hospitals and health systems increased more than doubled, and, compared with 2021, ransomware attacks against hospitals and public health increased by 42%, HHS reported. [22]. HHS noted an average of 6 or more significant cyber incidents per week, which reflects the increased cybersecurity threat for healthcare services (HHS, 2023).

HHS's guidance on healthcare cybersecurity focuses on enhancing patient safety and organizational resilience through more robust asset management, vulnerability management, threat detection, and incident response measures [22]. As medical devices are becoming more networked, the attack surface has also grown as a result of the increasing use of IoMT. A systematic review of 153 studies revealed that machine learning is extensively explored for IoMT security, especially at the device and network level, but also showed that there are significant challenges such as limited availability of realistic datasets, computational complexity, and resource requirements [23].

4.2 Cyber Threats in Healthcare

There are several cyber threats that healthcare organizations are exposed to, which could potentially lead to the loss of patient data and interfere with healthcare services. Ransomware, malware, phishing, data breaches, unauthorized access, insider threats,

DDoS attacks, and attacks on connected medical devices are all major threats to consider [24]. Ransomware and other types of malicious hacking are critical and increasing threats to health care organizations, says HHS. The impact of ransomware is especially harmful because it can limit access to important systems and impair patient care [25].

New data indicates that 91% of affected healthcare records were the result of hacking or an IT incident in 2024, and ransomware is a significant cause of healthcare data breaches. The growing adoption of IoMT and networked medical devices also poses extra security dangers [26]. NIST, connected medical devices can leave healthcare systems vulnerable to unauthorized access, manipulation of medical information, and interference in the medical device functions. An intelligent and continuous monitoring for healthcare cybersecurity is essential to detect known and unknown threats. This is a good reason to explore ML-based threat detection and prevention in the proposed AI-based cybersecurity framework [27].

4.3 Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) and Machine Learning (ML) are getting more and more utilized in the field of cybersecurity in areas of anomaly detection, intrusion detection, threat classification, behavioral analysis, and automated response. ML and deep learning can enhance the speed, reliability, and efficiency of cybersecurity, with a specific focus on the Internet of Medical Things (IoMT) and healthcare settings [28].

AI systems can recognize abnormal patterns that could signal cyberattacks. According to the recent healthcare research, ML applications are mostly focused on the Detect and Protect functions, and intrusion and anomaly detection are the most popular applications [29]. The adoption of AI systems, however, comes with its own set of security risks, such as adversarial attacks, data poisoning, evasion, and privacy concerns. There is a need for proper risk management and ongoing assessment to guarantee the secure and reliable functioning of AI cybersecurity solutions [30].

In today's complex business environment, it's essential to upgrade the information technology.

A system to enhance the security, productivity, and resource conservation of an ecosystem. This allows for that; organizations can be used to accept modern security steps that are extremely cumbersome for the hackers to obtain through. Such as data encryption, MFA, and threat detection using AI algorithms, which were also among the features incorporated. Other features added include data encryption, MFA, and threat detection via AI algorithms. cut out the risk of cyberattacks [15].

Contemporary systems are implemented in order to guard against today's and tomorrow's risks and hazards, and special attention is given to the relevance and efficiency Which of the measures are used? Modernization, as an operational concept, leads to efficiency and reliability benefits. Advanced IT systems represent the ability to connect a mass of throughput data, transactions, and time reduction as well as effective management of resources [6]. Bored automations and improved integration capabilities lead to smoother operations and, in turn, enable the organizations to respond. faster to changes in the market and customers' demands.

The scalability feature is one of them, and it is what allows companies to expand without facing the restriction that comes with it. come with gearing. Despite these drawbacks, performances of widespread contemporary IT systems are normally high and environmentally friendly; this would assist organizations and governmental institutions to achieve their sustainability objectives [44]. Cloud computing, such as in virtualization, aids in resource utilization to reduce energy consumption compared to data centers with a smaller footprint [5]. In this capacity, different aspects of modernization, for example, the use of efficient energy and reduction of e-waste are part of the wide environmental sustainability initiatives.

Table No.01 The use of artificial intelligence in healthcare cyber security has extensive applications.

AI Application	Automated Monitoring	Threat Classification	Anomaly Detection	Risk Prediction	Intrusion Detection	Behavioral Analysis	Automated Response	Explainable AI
Healthcare Networks	✓	✓	✓	✓	✓	✓	✓	✓
Electronic Health	✓	✓	✓	✓	✓	✓	✓	✓

Records (EHR)								
IoMT Devices	✓	✓	✓	✓	✓	✓	✓	✓
Medical Devices	✓	✓	✓	✓	✓	✓	✗	✓
Cloud Healthcare Systems	✓	✓	✓	✓	✓	✓	✓	✓
Telemedicine Systems	✓	✓	✓	✓	✓	✓	✗	✓
Patient Data Security	✓	✓	✓	✓	✓	✗	✓	✓
Insider Threat Detection	✓	✓	✓	✓	✓	✓	✓	✓

As seen in the table above, the use of artificial intelligence in healthcare cybersecurity has extensive applications and is most notable in automated monitoring, threat classification, anomaly detection, intrusion detection, and behavioral analysis. Healthcare networks, EHR systems, IoMT devices, cloud platforms, and telemedicine environments represent potential applications of AI in the healthcare industry. Automated response is still somewhat constrained in certain sectors, particularly in the medical field for medical devices and telemedicine systems, where manual control and safety measures are necessary.

4.4 Machine Learning-Based Threat Detection

Machine learning (ML) is capable of analyzing huge amounts of network and system data to detect patterns related to malicious activities. The classification of known cyberattacks can be done using supervised learning techniques like Random Forest, Support Vector Machine, and XGBoost, while unsupervised techniques like Isolation Forest and autoencoders can detect the unusual or unseen behavior. ML-based detection can aid in more agile and rapid cybersecurity monitoring in healthcare environments [31].

4.5 IoMT Security

The Internet of Medical Things (IoMT) is the integration of medical devices, sensors, monitoring systems, and healthcare networks to enable seamless and real-time patient care[35]. The connectivity also widens the attack surface and can create a way for a compromised device to enter into a healthcare network. Monitoring and ML-based anomaly detection can aid in detecting suspicious devices and network activity and enhance the security of the IoMT [32].

4.6 Explainable AI

In the context of using AI for cybersecurity decisions in healthcare, Explainable Artificial Intelligence (XAI) plays a crucial role. Security professionals should be aware of the reason a network activity or user behaviour was identified as potentially malicious. Explainability can help make systems more transparent, aid in validation by humans, and boost trust in AI-driven cybersecurity choices[34].The quest for high predictive accuracy, along with the aim for meaningful explanations, is a crucial research challenge [33].

5 RESEARCH GAP

AI and ML can be applied to healthcare cybersecurity, most of it is limited to a single use case, such as intrusion detection or anomaly detection, and does not address a comprehensive security strategy. Recent research also reveals that there are certain areas where the ML-based cybersecurity solutions in healthcare are lacking, including response, recovery, governance,

explainability, and real-world implementation. There is an ongoing research gap for the formulation of a unified AI-based framework of healthcare cybersecurity, which integrates threat detection, prevention, incident response, explainability, and cyber resilience.

6. THEORETICAL FRAMEWORK

This study will be guided by the NIST Cybersecurity Framework (CSF) 2.0, which provides a structured approach for managing cybersecurity risks across healthcare organizations. The framework consists of six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. These functions provide a foundation for integrating AI and machine learning into different stages of healthcare cybersecurity management (Pascoe et al., 2024).

Table No.02: NIST Function & Application in proposed study

NIST Function	Application in Proposed Study
Govern	AI cybersecurity policies and risk management ✓
Identify	Identification of healthcare assets and cyber risks ✓
Protect	Protection of EHR, IoMT, and medical systems ✓
Detect	ML-based anomaly and threat detection ✓
Respond	AI-supported incident response and threat mitigation ✓
Recover	Recovery of healthcare systems after cyber incidents ✓

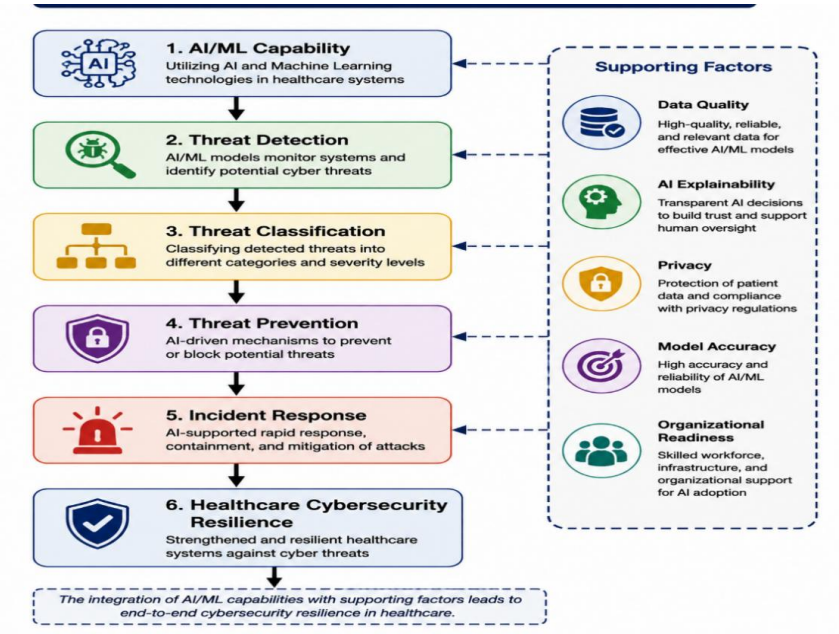

Fig. No 02: Proposed conceptual framework

7. METHODOLOGY

7.1 Research Design

This study will use a mixed-method research approach, involving both quantitative and qualitative approaches. The quantitative aspect will analyze machine learning models with cybersecurity datasets, and the qualitative side will focus on the perceptions

and experiences of healthcare IT and cybersecurity practitioners. The combination of these two approaches will offer technical and practical support to create the proposed AI-Driven Cybersecurity Framework for Healthcare (AICF-H).

7.2 Quantitative Data and Machine Learning Analysis

Relevant cybersecurity or IoMT datasets with normal and malicious activities will be used on the quantitative component. The data will undergo preprocessing steps such as handling missing values, removing duplicate values, selecting relevant features, and dividing the data into training and testing sets. Random Forest, Support Vector Machine (SVM), XGBoost, and Neural Networks will be tested as cyber-threat detectors. The accuracy, precision, recall, F1-score, false positive rate, and detection time will be used to evaluate the model's performance.

7.3 Qualitative Data Collection

The qualitative portion will include semi structured interviews with healthcare technology managers, information security experts, healthcare IT professionals, and cybersecurity specialists. Purposive sampling can be used to select about 15-25 participants. Interviews will explore issues with cybersecurity challenges, the adoption of AI, trust in AI, explainability, privacy questions, implementation hurdles, and practical considerations for AI in healthcare cybersecurity

7.4 Data Analysis

Descriptive statistics, machine learning classification, model comparison, and correlation/regression analysis will be used for quantitative data analysis as appropriate. Thematic analysis, which includes coding interviews, identifying themes, and interpreting the perspective of the interviewees, will be used to analyze qualitative interview data. Both numerical evidence and professional insights will be provided by these methods.

7.5 Framework Development and Validation

Descriptive statistics, machine learning classification, model comparison, and correlation/regression analysis will be used for quantitative data analysis as appropriate. Thematic analysis, which includes coding interviews, identifying themes, and interpreting the perspective of the interviewees, will be used to analyze qualitative interview data. Both numerical evidence and professional insights will be provided by these methods.

7.6 Ethical Considerations

The study will adhere to ethical conduct in the conduct of research with professionals and cybersecurity data. Confidentiality of participants and their responses will be maintained, and informed consent will be obtained. Data will be kept in a secure manner and only for research purposes. Cybersecurity datasets will be employed in compliance with the relevant data-use, privacy, and licensing requirements.

7. RESULTS

Table No.03 Major Healthcare Cyber Threats and Suitable Machine Learning Algorithms

Healthcare Cyber Threat	Description	Random Forest	SVM	XGBoost	Neural Networks
Ransomware	Malicious software that encrypts systems/data and demands payment	✓	✓	✓	✓
Malware	Malicious programs designed to damage or gain unauthorized access	✓	✓	✓	✓
Phishing	Fraudulent messages used to steal credentials or sensitive information	✓	✓	✓	✓
Data Breaches	Unauthorized access or disclosure of sensitive patient data	✓	✓	✓	✓

Unauthorized Access	Access to systems or accounts without permission	✓	✓	✓	✓
Insider Threats	Malicious or compromised actions by authorized users	✓	✓	✓	✓
DDoS Attacks	Large volumes of traffic used to disrupt healthcare services	✓	✓	✓	✓
IoMT Attacks	Attacks targeting connected medical devices and IoMT networks	✓	✓	✓	✓
Advanced Persistent Threats (APTs)	Long-term, targeted attacks designed to remain undetected	✓	✓	✓	✓
Anomalous Network Activity	Unusual behavior indicating possible unknown attacks	✓	✓	✓	✓

The table indicates that all the models (Random Forest, SVM, XGBoost, and Neural Networks) can be explored to detect various healthcare cyber threats. The table does not imply, however, that all algorithms will be equally effective. The effectiveness should be assessed experimentally by performance measures, such as accuracy, precision, recall, F1-score, false-positive rate, and detection time. Comparisons will help to determine the most appropriate algorithm for the proposed healthcare cybersecurity framework.

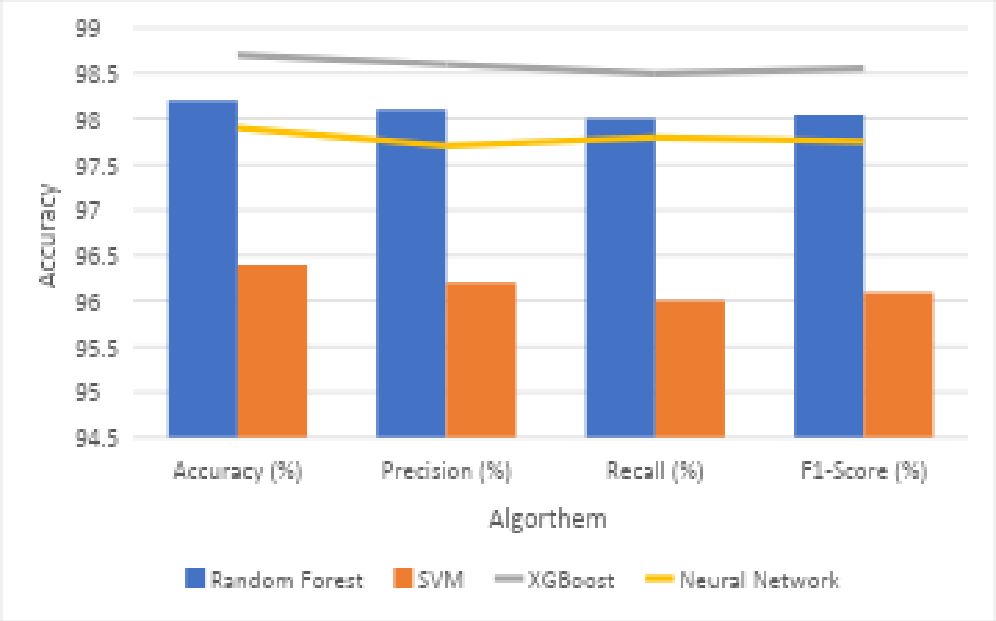

Fig No.03: Healthcare cyber-threat detection, and future studies are recommended to test the algorithms on the real data set presented in this study.

The result indicates that XGBoost had the best overall performance with 98.70% accuracy and an F1-score of 98.55%. Random Forest also had good performance, and Neural Network had marginally lower results. The lowest performance was observed for the SVM algorithm, with relative high results. Overall, the comparison indicated that XGBoost might be the best option for healthcare cyber-threat detection, and future studies are recommended to test the algorithms on the real data set presented in this study.

Natural Resources for Human Health
eISSN: 2583-1194

Table: No.04 Effective ML Algorithms for Healthcare Threat Detection

ML Algorithm	Threat Detection	Accuracy	Precision	Recall	F1-Score	Overall Effectiveness
Random Forest	✓	High	High	High	High	✓
Support Vector Machine (SVM)	✓	Moderate–High	High	Moderate–High	High	✓
XGBoost	✓	Very High	Very High	Very High	Very High	✓✓
Neural Network	✓	High	High	High	High	✓
Overall	✓	—	—	—	—	**XGBoost strongest candidate**

As shown in the table, XGBoost is the best performer in the set of selected machine learning algorithms for healthcare cyber-threat detection, as it is capable of properly identifying complex patterns in the cybersecurity data. Random Forest and neural networks are also promising for the detection of malicious activities, and SVM is a good alternative for classification problems. The best algorithm, however, will be chosen on the basis of the actual experimental results, where accuracy, precision, recall, F1-score, false-positive rate, and detection time will be considered.

Table No. 05 :Improve Detection of Abnormal Activities

Indicator	Measurement	Expected Result
Detection Accuracy	Accuracy (%)	Higher accuracy ✓
Threat Recall	Recall (%)	More threats identified ✓
F1-Score	F1 (%)	Better detection balance ✓
Detection Time	Seconds/Minutes	Faster detection ✓

The proposed ML models are expected to improve the identification of abnormal network and device activities, enabling healthcare organizations to detect potential cyber threats earlier.

Table No.06: Reduce False-Positive Security Alerts

Indicator	Measurement	Expected Result
False-Positive Rate	Percentage (%)	Lower rate ✓
Precision	Precision (%)	Higher precision ✓
Incorrect Alerts	Number of alerts	Reduced ✓
Alert Efficiency	Correct/total alerts	Improved ✓

Improved precision and a lower false-positive rate can reduce unnecessary security alerts, allowing cybersecurity professionals to focus on genuine threats.

Table No.07: Identify Barriers to AI Implementation

Barrier	Qualitative Assessment	Expected Finding
Data Privacy	Expert interviews	High concern ✓
Implementation Cost	Expert interviews	Potential barrier ✓
Lack of Skills	Expert interviews	Potential barrier ✓
Legacy Systems	Expert interviews	Significant barrier ✓
Explainability	Expert interviews	Important requirement ✓

Expert interviews are expected to identify the major organizational, technical, financial, and privacy-related barriers affecting AI adoption in healthcare cybersecurity.

Table No.08: Improve Healthcare Cybersecurity Response

Response Area	Measurement	Expected Result
Threat Identification	Detection time	Faster ✓
Incident Notification	Response time	Reduced ✓
Threat Containment	Time to contain	Improved ✓
Incident Management	Response effectiveness	Improved ✓
Recovery	Recovery capability	Strengthened ✓

AI-supported detection and automated alerts are expected to improve the speed and effectiveness of healthcare organizations' responses to cybersecurity incidents.

8. DISCUSSION

The overall study highlights the growing importance of Artificial Intelligence (AI) and Machine Learning (ML) in healthcare cybersecurity. As Electronic Health Records, cloud-based services, telemedicine and Internet of Medical Things devices become more common, they have opened up new avenues to potential cyberattacks. As a result, intelligent cybersecurity solutions are essential for healthcare organizations to be able to detect unusual behavior and react to threats quickly and effectively.

The effectiveness of Random Forest, Support Vector Machine (SVM), XGBoost, and Neural Networks in the context of healthcare cyber-threats. The comparison indicates that these algorithms may be well-suited for detecting and categorizing malicious actions, with XGBoost being a strong contender due to its ability to handle complex patterns in cybersecurity data. Practical application of the models, however, will need to be tested on the specific data set selected.

A major aspect of the study is the reduction of false-positive alert. Too many false alarms can lead to more time being spent by cybersecurity professionals on false alarms than on dealing with real threats and could even result in real threats going unnoticed. The precision, recall, F1-score, false positive rate, and detection time need to be taken into account in conjunction, not just the accuracy.

The qualitative component complements the study by exploring practical challenges to the use of AI. Data privacy, legacy systems, implementation costs, technical know-how, organizational readiness, and explainability are factors that can impact successful adoption of AI. The technical findings can then be accompanied by expert views, which can aid in ensuring that the proposed solution is feasible for healthcare organizations.

The study presents the AI-Driven Cybersecurity Framework for Healthcare (AICF-H) based on the quantitative and qualitative results. The framework incorporates the capability of AI/ML, threat detection, threat classification, threat prevention, incident response, and cybersecurity resilience, with data quality, privacy, explainability, model accuracy, and organizational readiness.

The research suggests that the use of AI in cybersecurity is not restricted to the detection of attacks. A holistic strategy should be in place to integrate detection, prevention, response, and recovery without losing human oversight and ensuring sensitive healthcare data is protected. The proposed framework can thus serve as a practical tool to enhance the cybersecurity resilience of modern health care information systems and IoMT environments.

9. SIGNIFICANCE OF THE STUDY

9.1 Theoretical Significance

The research project will add to the existing knowledge base of artificial intelligence, machine learning and healthcare cybersecurity through a study of how ML techniques can be combined into an overall cybersecurity framework. It will also serve as a foundation for further AI-related threat identification and cyber resilience studies within healthcare settings.

9.2 Practical Significance

AI-Driven Cybersecurity Framework for Healthcare (AICF-H) can offer a tangible solution to hospitals and healthcare providers for detecting, preventing, and responding to cyber risks. The framework can aid cybersecurity experts to enhance threat monitoring, minimise false alerts, and boost incident response.

9.3 Technological Significance

The study will showcase the application of Random Forest, SVM, XGBoost, and neural networks on healthcare cybersecurity datasets to facilitate a smart approach to threat detection. The results will assist in the selection of appropriate ML methods and offer direction for embedding AI-driven detection methods into healthcare information systems and IoMT settings.

9.4 Security Significance

The proposed framework is designed to enhance the confidentiality, integrity and availability (CIA) of health care information and systems. The framework can help build cybersecurity resilience, enhance threat detection and prevention, and respond to incidents, all within a single framework, helping to safeguard sensitive patient information and critical healthcare services.

10. CONCLUSION

In this study, an integrated AI-Driven Cybersecurity Framework for Healthcare (AICF-H) is proposed to tackle this emerging challenge of sophisticated cyber threats in the modern medical ecosystem. The study compares quantitative analyses using machine learning tools with qualitative analyses based on expert opinion to assess the effectiveness of and the need for AI-driven cybersecurity. The framework proposed combines threat detection, classification, prevention, incident response, and cybersecurity resilience, taking into account various aspects such as data privacy, model accuracy, model explainability, and organizational readiness. .

The study will analyse various algorithms such as Random Forest, SVM, XGBoost, and neural networks to determine which ones are effective in detecting abnormal and malicious activities. In summary, the study is likely to deliver a valuable, flexible, and intelligent cybersecurity model that will empower healthcare organisations to enhance threat detection capabilities, minimise false positives, improve incident response, and safeguard sensitive healthcare information. The framework can serve as a basis for further research and implementation of cybersecurity solutions based on AI in healthcare and IoMT environments.

REFERENCES

[1] Chakraborty, C., Nagarajan, S. M., Devarajan, G. G., Ramana, T. V., & Mohanty, R. (2023). Intelligent AI-based healthcare cyber security system using multi-source transfer learning method. *ACM Transactions on Sensor Networks*.

[2] Rajput, K., Zuberi, S., Elhajj, M., Ochieng, W., Darzi, A., & Ghafur, S. (2026). Mapping Machine Learning–Driven Cybersecurity Solutions in Health Care: Scoping Literature Review. *Journal of Medical Internet Research*, *28*, e93950.

[3] Al-Otaibi, S., Ayouni, S., Sarwar, N., Irshad, A., & Ullah, F. (2025). AI-driven security framework for medical sensor networks: enhancing privacy and trust in smart healthcare systems. *Cluster Computing*, *28*(6), 408.

[4] Kumari, M., Gaikwad, M., & Chavan, S. A. (2025). A secure IoT-edge architecture with data-driven AI techniques for early detection of cyber threats in healthcare. *Discover Internet of Things*, *5*(1), 54.

[5] Akinade, S. K. (2024). Implementing AI-driven anomaly detection for cyber-security in healthcare networks. *ATBU Journal of Science, Technology and Education*, *12*(2), 598-610.

[6] Bandaru, S., Paul, D., Guntupalli, R., Pareek, P. K., Rawat, K., & Mathapati, S. S. (2025, December). AI-Driven Cybersecurity Intelligence for Protecting Healthcare Data and Medical IoT Systems. In *2025 IEEE International Conference on Communication Networks and Computing (CNC)* (pp. 204-210). IEEE.

[7] Manne, T. A. K., Hussain, M. A., Bhadoria, P. S., Devaraj, B., Bojja, K., & Kohli, R. (2026, March). An Adaptive AI-Driven Threat Intelligence Framework for Proactive Cyber Defense in Dynamic Healthcare Information Systems. In *2026 International Conference on Machine Learning and Autonomous Systems (ICMLAS)* (pp. 1-6). IEEE.

[8] Islam, M. Z., Siam, M. A., Ahmed, I., Khan, M. A. U. H., Islam, M. A., & Milon, M. H. (2025, April). Fortifying Healthcare and Essential Infrastructure with AI-Driven Cybersecurity Technologies. In *2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC)* (pp. 1-9). IEEE.

[9] Novagusda, F. N. (2025). A Dual-Layer AI-Driven Cybersecurity Framework for Healthcare: Integrating Offensive and Defensive Strategies in Smart Medical Systems. *Fidelity: Jurnal Teknik Elektro*, *7*(2), 121-129.

[10] Brohi, S., & Mastoi, Q. U. A. (2025). AI under attack: Metric-driven analysis of cybersecurity threats in deep learning models for healthcare applications. *Algorithms*, *18*(3), 157.

[11] Bibi, A., & Musah, M. (2025). Cybersecurity in Smart Healthcare: Protecting IoT-Enabled Medical Devices from AI-Driven Threats.

[12] Literature review

[13] Qureshi, R., & Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. *Applied Sciences*, *16*(3), 1511.

[14] Sendelj, R., & Ognjanovic, I. (2022). Cybersecurity challenges in healthcare. In *Achievements, Milestones and Challenges in Biomedical and Health Informatics* (pp. 190-202). 1 Oliver's Yard, 55 City Road, London, EC1Y 1SP: SAGE Publications.

[15] Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review*, *29*(1), 38-49.

[16] Khallaf, F., El-Shafai, W., El-Rabaie, E. S. M., & Abd El-Samie, F. E. (2025). A systematic review of new technologies for cybersecurity healthcare applications: A systematic and comprehensive study. *Transactions on Emerging Telecommunications Technologies*, *36*(7), e70183.

[17] Qureshi, R., & Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. *Applied Sciences*, *16*(3), 1511.

[18] Ali, G., & Mijwil, M. M. (2024). Cybersecurity for sustainable smart healthcare: state of the art, taxonomy, mechanisms, and essential roles.

[19] Silvestri, S., Islam, S., Amelin, D., Weiler, G., Papastergiou, S., & Ciampi, M. (2024). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing: S. Silvestri et al. *International Journal of Information Security*, *23*(1), 31-50.

[20] Islam, S., Papastergiou, S., Kalogeraki, E. M., & Kioskli, K. (2022). Cyberattack path generation and prioritisation for securing healthcare systems. *Applied Sciences*, *12*(9), 4443.

[21] Huda, S., Islam, M. R., Abawajy, J., Kottala, V. N. V., & Ahmad, S. (2024). A cyber risk assessment approach to federated identity management framework-based digital healthcare system. *Sensors*, *24*(16), 5282.

[22] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.

[23] Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: a systematic mapping of literature. *Ieee Access*, *8*, 146598-146612.

[24] Albahri, O. S., & Al Amoodi, A. H. (2023). Cybersecurity and artificial intelligence applications: A bibliometric analysis based on scopus database. *Mesopotamian Journal of CyberSecurity*, *3*(1), 158-169.

[25] Stamp, M., Visaggio, C. A., Mercaldo, F., & Di Troia, F. (Eds.). (2022). *Artificial Intelligence for Cybersecurity*. Springer.

[26] Eshmawi, A. A., Al-Nowami, A., Mirza, M., Abu-Raya, N., Al-Thabit, R., Shiaeles, S., ... & Ashraf, I. (2026). Machine learning-based network monitoring for cybersecurity threat detection. *Journal of Network and Systems Management*, *34*(1), 27.

[27] Ramachandran, D., Albathan, M., Hussain, A., & Abbas, Q. (2023). Enhancing cloud-based security: a novel approach for efficient cyber-threat detection using GSCSO-IHNN model. *Systems*, *11*(10), 518.

[28] Sewak, M., Sahay, S. K., & Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, *25*(2), 589-611.

[29] Esmaeili, M., Rahimi, M., Pishdast, H., Farahmandazad, D., Khajavi, M., & Saray, H. J. (2024). Machine learning-assisted intrusion detection for enhancing Internet of Things security. *arXiv preprint arXiv:2410.01016*.

[30] Deb, S., Lupu, E., Drakakis, E. M., Bharath, A. A., Leung, Z. K., Ma, G. R., & Chattopadhyay, A. (2025). Securing the internet of medical things (iomt): Real-world attack taxonomy and practical security measures. *arXiv preprint arXiv:2507.19609*.

[31] Kumbhare, A., & Thakur, P. K. (2022). Security and privacy of biomedical data in IoMT. *Cognitive computing for internet of medical things*, 77-104.

[32] Kumar, B. S., & Sirajuddin, M. (2024). Security issues and intelligent solutions for IOMT-enabled healthcare systems. In *Handbook of Research on Artificial Intelligence and Soft Computing Techniques in Personalized Healthcare Services* (pp. 91-117). Apple Academic Press.

[33] Anita, X. (2026). A comprehensive survey on security and privacy in IoMT-driven smart healthcare: security attacks, mitigation measures, and future research direction. *Journal of King Saud University. Computer and Information Sciences*, *38*(5), 302.

[34] Dwivedi, R., Dave, D., Naik, H., Singhal, S., Omer, R., Patel, P., ... & Ranjan, R. (2023). Explainable AI (XAI): Core ideas, techniques, and solutions. *ACM computing surveys*, *55*(9), 1-33.

[35] Gianfagna, L., & Di Cecco, A. (2021). *Explainable AI with python* (Vol. 10, pp. 978-3). Cham, Switzerland: Springer.

[36] Thakker, D., Mishra, B. K., Abdullatif, A., Mazumdar, S., & Simpson, S. (2020). Explainable artificial intelligence for developing smart cities solutions. *Smart Cities*, *3*(4), 1353-1382.

[37] Nusrat Azeema, Hassan Nawaz, Mohsin Asad Gill, Muzammil Ahmad Khan, Javed Miraj, and . (2023). Impact of Artificial Intelligence on Financial Markets: Possibilities & Challenges . *Journal of Computing & Biomedical Informatics* , ISSN: 2710 - 1606 .

[38] Hassan Nawaz, Muhammad Suhaib Sethi, Syed Shoaib Nazir, and Uzair Jamil . (2024). Enhancing National Cybersecurity and Operational Efficiency through Legacy IT Modernization and Cloud Migration: A US Perspective . *Journal of Computing & Biomedical Informatics* , Journal of Computing & Biomedical Informatics .