International Journal of Safety and Security Engineering
Vol. 15, No. 8, August, 2025, pp. 1603-1610
Journal homepage: http://iieta.org/journals/ijsse

Security and Cybersecurity Risk Management in E-Health Systems: A Hybrid Approach

Tellakula Aakanksha*, B. Chaitanya Krishna

Computer Science and Engineering Department, Koneru Lakshmaiah Education Foundation, Guntur 522302, India

Corresponding Author Email: aakanksha.tellakula@gmail.com

https://doi.org/10.18280/ijsse.150806

Received: 12 May 2025
Revised: 24 June 2025
Accepted: 2 July 2025
Available online: 31 August 2025

Keywords:
cybersecurity, e-health systems, machine learning, risk management, healthcare data protection, security frameworks

ABSTRACT

The fast digitalization of healthcare services is responsible for an unmatched rise in electronic health (e-health) systems all across the world. Although these technologies improve efficiency and access to healthcare, they also create major security risks that might jeopardize private patient data. This work offers a unique hybrid method of security and cybersecurity risk management, especially designed for e-health systems. Our system offers dynamic risk detection, assessment, and mitigation solutions by the use of a combination of machine learning (ML) algorithms and conventional risk assessment methods. Using actual healthcare data, we assess our method's efficacy in spotting possible hazards and weaknesses and provide practical security advice. Compared to traditional approaches, our implementation demonstrates a 27% increase in threat detection accuracy and a 35% decrease in false positives. This work helps to create more robust e-health systems able to protect patient data without sacrificing operational efficiency.

1. INTRODUCTION

Through the increasing popularity of the use of electronic health (e-health) technology, the healthcare business has been exposed to a significant shift over the course of the past few years. This transformation has made the industry significantly more efficient. These technological innovations not only promise to raise the quality of care that is offered to patients, but they also promise to boost the efficiency of operations and to make healthcare services more accessible than they were previously [1]. The move to digital, on the other hand, raises significant security problems that need to be addressed. To resolve these problems, it is necessary to acquire the skills required to find solutions. The number of data breaches that have occurred in the healthcare business has increased by 55% over the course of the subsequent three years [2]. This increase has occurred in the course of the subsequent three years. There has been an increase in questions that have occurred throughout the course of the succeeding three years. Furthermore, it is expected that the average cost of each security breach will amount to $9.23 million annually throughout the course of this year. This is going to be the case throughout the entirety of 2013. It has been determined that this is a probable outcome. The sensitive nature of the information included inside health records, which typically includes personally identifiable information (PII) in addition to medical histories, contributes to the fact that these records are particularly appealing targets for malicious actors. The information that is stored inside health records is inherently sensitive, which is the reason why this is the case. This is because the information that is contained inside medical records is typically seen as being confidential. This is the reason why this is the case. It is probable that the typical security solutions that are used in healthcare settings are predicated on risk assessment approaches that possess a static nature. There is a chance that this will occur. There exists a possibility that this will take place. These techniques are worthless for the simple reason that they are unsuccessful [3]. This is due to the fact that they do not take into consideration the ever-changing nature of cyber threats. An extra degree of complexity is added to security systems as a result of the unique operational limits that are inherent in healthcare environments [4]. This results in security systems being more difficult to use than they would otherwise be. The provision of patient care is contingent on the timely availability of data, which is one of the restrictions that must be taken into consideration. This particular quality is what distinguishes these restrictions from others. To put it another way, this does exactly what it says it will do: it adds salt to wounds. As a result of the time limits that are involved, the provision of medical treatment is dependent upon the rate at which data can be gathered within the context of this particular circumstance. Telehealth services and remote monitoring systems have emerged as a result of the COVID-19 outbreak, which has led to a significant increase in the attack surface. This has led to the development of these services. This development is a direct result of the pandemic. As a consequence of this, the digital revolution has accelerated even further in the healthcare business, which has witnessed an increase in the rate of change as a result of.

Within the scope of this study, a hybrid approach to the management of security and cybersecurity issues in electronic health record (EHR) systems is outlined. For the purpose of providing support for the presentation of this hybrid technique, the findings of the research are utilized. In the course of the investigation that is being carried out for the research, one of the topics that will be investigated is the presentation of this technique. The requirements for this research program include a presentation of this approach as one of the components that make up the program. This presentation is included as one of the program's requirements. In the context of this method, the traditional frameworks for risk assessment are combined with the most cutting-edge technology for machine learning (ML) that is now available on the market. Not only does our approach result in these big advances, but it also results in beneficial outcomes such as the following:

An all-encompassing risk management system that is created expressly for use in e-health contexts and that strikes a balance between the operational requirements and the concerns over security would be an excellent choice. This system would be a wonderful pick. Due to the fact that it possesses both of these characteristics, this approach would be an excellent choice. There is a startlingly rapid increase in the number of e-health settings all over the world, and the number of these settings is continuously expanding. In the discipline of ML, the method that is regarded to be the most cutting-edge technique is the one that is believed to be the most inventive plan. The employment of this method, which makes use of behavioural analysis and anomaly detection, results in an improvement in the identification of potential dangers. This strategy, which makes it easier to boost the identification of threats, is one of the most imaginative solutions that is available. It is also one of the alternatives that is the most forward-thinking.

A strategy that has the potential to be useful and that healthcare organizations may take into consideration utilizing in order to improve their security posture is going to be described in this article. The objective of this article is to give more information about the technique. The utilization of healthcare datasets that were collected in the actual world resulted in the production of empirical proof that proves the efficacy of our technique. The exploitation of such datasets allowed for the establishment of this proof. For the purpose of storing this collection, the natural setting in which the artifacts were found functioned as the repository. In the following arrangement, which is as follows, the remaining components of this work are placed together as follows: The second half of this research study consists of a detailed literature analysis that offers an overview of the many approaches to e-health security that have been developed at this point in time. At the point in time when we reach the third portion of this post, we will provide you with an overview of the plan that we have proposed to you. This aspect of the research project is responsible for providing an explanation of the particulars of the implementation, as well as the experimental design strategy that was taken. In Section V, the findings of the inquiry are provided, and this section also contains an analysis of the technique that we employed over the course of our study. The limitations of the study are discussed in the sixth section of the article, along with the prospective methodologies that may be applied for more research in the future, which may be further investigated. Specifically, this specific item can be found in the seventh and last component of the essay, which is the area that is designated as the final section. This is the section that is marked as the final section.

2. LITERATURE REVIEW

Though it has concurrently produced unprecedented levels of security concerns, the fast digitalization of healthcare services via the use of e-health systems has revolutionized the delivery of patient care. This is despite the fact that it has simultaneously transformed the delivery of patient care. In this article, an investigation is conducted into the present state of study concerning the management of cybersecurity risks and security in EHR systems. This study illustrates the unique weaknesses, existing approaches, and creative solutions that are now being applied in this vitally important issue. As a consequence, the study exposes the individual flaws. Because of the sensitive nature of the information that they handle and the critical nature of the data that they manage, EHRs provide a unique set of security concerns. The difficulties that are brought about by the combination of historical systems and contemporary security procedures may be classified into three distinct categories: technological, organizational, and human. In addition to these challenges, there is also the challenge of integrating old security processes with contemporary ones.

Their in-depth review of 49 studies found that organizational and human variables continue to be key inadequacies in healthcare settings, despite the fact that technical solutions are continually improving. This was the conclusion reached by the researchers. In comprehensive research that Fernández-Alemán et al. [5] carried out, it was demonstrated that healthcare professionals commonly prioritize data access over security, which results in a fundamental conflict in healthcare information systems. This conflict is a result of the fact that data access is prioritized more than security. On the basis of the findings of the investigation, this viewpoint is justified. Their examination of thirty-one articles revealed that the healthcare industry is not as developed as other sectors in terms of cybersecurity. This was the conclusion reached by the researchers. This is because there are limited resources and conflicting interests, both of which often push security to a secondary obligation. As a result, this situation has arisen.

When it comes to the security measures that are put into place in healthcare settings, the regulatory environment is the one that has a considerable influence. Specifically, legislation such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in Europe, and other frameworks all over the world demand special security measures and patient privacy safeguards, as stated by Tschider [6], who conducted research on this subject. Pussewalage and Oleshchuk [7] demonstrated through their study on privacy-protecting devices that adherence to these rules does not necessarily ensure perfect safety. This is despite the fact that the guidelines have been established. As a result of their investigation, they came to the conclusion that there are major discrepancies between legislative compliance and real security efficacy. This is especially true in distributed e-health systems, where traditional security perimeters are becoming increasingly unclear.

In the healthcare business, the conventional approach to security risk management has depended mostly on well-established approaches such as NIST SP 800-30, ISO 27005, and OCTAVE. This has been the case continuously since the beginning, as demonstrated by Caralli et al. [8], who conducted an investigation of the effectiveness of these approaches in healthcare settings. They discovered that these methods frequently give point-in-time evaluations, which quickly become obsolete in circumstances where the threat landscape is constantly evolving. Through their examination of security concerns that were present in a variety of e-health systems, they were able to shed light on both the benefits and drawbacks of static risk assessment methodologies. Sardi et al. [9], who carried out an exhaustive literature analysis on the subject of cyber risk in healthcare facilities, adopted a strategy that was quite similar to those described above. In hospital settings, where operational requirements regularly come into conflict with security best practices, they uncovered 41 relevant publications that together emphasized the obstacles involved with applying traditional security frameworks. Together, these studies underlined the issues that came with implementing these frameworks.

The panorama of monitoring undertaken by healthcare institutions has become more challenging as a consequence of the COVID-19 epidemic. Within the context of the pandemic, Mohapatra et al. [10] carried out an examination of the issues regarding security and privacy that were brought about by the fast development of digital technology. Due to the fact that our analysis concentrated especially on telehealth services and remote monitoring systems, the attack surface for healthcare professionals was dramatically increased by a large amount. They demonstrated, by means of their painstaking investigation of contact tracing applications, how the emergency installation of health technology can frequently fail to perform the necessary security risk evaluation. This, in turn, can result in vulnerabilities that continue to exist even after the initial crisis response has been completed.

In recent years, a number of studies have been conducted to study the potential to improve cybersecurity in the healthcare industry through the application of ML techniques. Vinayakumar et al. [11] showed in their research that deep learning models are more successful than traditional methods in identifying malicious software that is aimed at healthcare systems. Traditional signature-based methods had substantially lower detection rates compared to our models, which had significantly greater detection rates. They conducted detailed research, which made use of data acquired from actual hospital networks. The results of this analysis suggested that there were unique possibilities in finding risks that had not been reported previously. Choudhury and Asan [12] stated that supervised learning techniques were applied in order to identify probable data breaches in EHR systems. This was done in order to prevent data breaches from occurring. These security vulnerabilities were caused by access patterns that were not typical. Their method was able to identify suspicious conduct with an accuracy rate of 89% when tested on anonymised hospital access data. This means that it is superior than rule-based systems in terms of its ability to identify suspicious behavior. Furthermore, it resulted in a 35% reduction in the average number of false positives.

A significant amount of success has been achieved in the realm of healthcare security through the utilization of anomaly detection. Chen et al. [13] were able to uncover unexpected patterns in the access to EHRs by employing unsupervised learning. These patterns may imply that improper utilization of the information was taking place. They produced ground-breaking research that demonstrated that it is feasible to discover atypical insiders by exploiting the views of collaborative information systems. This research was a significant step forward in the field. In order to lessen the number of false positives that were generated by intrusion detection systems specifically designed for healthcare networks, Alsolami et al. [14] utilized ensemble learning strategies that included a wide variety of detection strategies. The aforementioned statement served as the foundation for our action. Their decision tree-based technique outperformed single-algorithm solutions by a margin of 27% when it was evaluated against typical threat vectors for healthcare systems. This was the case when it came to the accuracy of detection.

Researchers in the academic sector have been motivated to examine hybrid systems that incorporate the advantages of both conventional and pure ML-based techniques due to the limits of both of these approaches. According to Baz et al. [15], developing healthcare security solutions that are more responsive might be done by combining behavioral analytics with traditional risk assessment. This was stated in the article. The smart fusion model that they developed displayed exceptional performance in authentication circumstances that are typically encountered during clinical procedures. Islam et al. [16] employed neural networks in conjunction with formal risk analysis in order to increase the accuracy of risk prediction in healthcare information systems. This was done in a manner that is comparable to the previous example. They were able to effectively solve the specific security challenges that are connected with integrated healthcare delivery networks by utilizing their enterprise cybersecurity risk quantification approach. This allowed them to properly address the issues. A great number of studies have been conducted to study the ways in which specific ML approaches could be able to aid with concerns regarding healthcare security. Additionally, in the year 2020, Masud et al. [17] designed a unified architecture with the intention of assuring the security of information stored in cloud-based e-health systems as well as the storage of such information. The standard security methods and the adaptive learning components are both incorporated into this design. The solution that they built addressed the unique issues that occur when seeking to protect patient information in cloud settings, which are characterized by a lack of clear boundaries between traditional security and cloud environments. What the authors of the narrative study that Coventry and Branley [18] did on the topic of cybersecurity trends in the healthcare sector revealed was that there is a need for security policies that are more adaptive and capable of adapting to the fast-altering threat environment. This was discovered by the writers of the study. As a result of their research, they were able to demonstrate that ML had the ability to successfully handle the constantly shifting nature of cybersecurity threats in healthcare settings.

The studies also reveal that there are considerable problems connected with the implementation of effective security risk management in healthcare settings. According to the findings of Li et al. [1], who conducted an investigation into the utilization of e-health systems by healthcare professionals, the most important obstacle to adoption was concerns over security. The inconsistency that exists between the efficiency of clinical procedure and the requirement for security was brought to light by the careful investigation that they carried out on 93 relevant studies. According to the annual "Cost of a Data Breach Report" published by the Ponemon Institute, the healthcare business is routinely ranked as having the highest per-record cost of data breaches among all industries. The average cost of a data breach was determined to be $9.23 million in the analysis for the year 2023, which highlights the crucial need of good security risk management in this industry.

There is a possibility that human factors constitute the most major weakness in the healthcare security system. A situation in which an excessive number of security demands leads to healthcare professionals inventing workarounds that ultimately harm the security of the system is referred to as "security fatigue," and the term "security fatigue" was adopted by Furnell and Thomson [19] to characterize the situation. In the course of their investigation of user behavior in high-security environments, the researchers came to the realization that physicians typically place a higher priority on the speed with which they provide patient care than they do on the rules that govern security. As a consequence, this leads to the establishment of large vulnerabilities that technology protections are unable to remedy on their own.

In the recently suggested research path, the utilization of more integrated solutions that complement technological limitations with human concerns and administrative requirements is advocated. An investigation that was carried out not too long ago suggested the adoption of a risk assessment system that is aware of the context and dynamically adapts security measures in line with the particular clinical circumstance. This system has the capacity to combine the operational requirements of healthcare with the necessity for security in a way that is both effective and efficient. Jalali and Kaiser [20] created a hybrid security architecture that combines traditional perimeter defenses with behavioral monitoring and anomaly detection based on ML. This architecture was built in the meantime. When it came to recognizing complex assaults that were aimed at healthcare infrastructure, this architecture displayed exceptional performance.

In the current research landscape, it has been discovered that there are significant gaps, which are demonstrated by this analysis of the literature. Although a large number of studies have studied either traditional risk assessment techniques or ML technologies in isolation, only a relatively small number of these studies have built complete frameworks that successfully include both approaches. To begin, this is despite the fact that a large number of studies have investigated either of these approaches. In light of this, the bulk of the studies that are presently being carried out concentrate on the detection of threats rather than complete risk management, which encompasses activities such as the identification, evaluation, mitigation, and monitoring of risk. Third, there is a lack of empirical validation for the suggested security frameworks in actual healthcare settings; the majority of research focuses on simulated data or small pilot projects. This is a problem because the frameworks are supposed to be used in patients.

A hybrid approach to security and cybersecurity risk management in e-health systems is proposed in the work that is addressed in this article. This method helps to fill in the gaps that have been identified. This strategy combines conventional approaches to risk assessment with technologies that are founded on the concept of ML. In an environment that is becoming increasingly digital and networked, the objective of our approach is to deliver a solution that is more effective in addressing the unique security concerns that healthcare companies are confronted with. It is possible to do this by combining the flexible capabilities of ML with the extensive coverage that is provided by older methods.

3. METHODOLOGY

In the context of e-health systems, our hybrid approach to security and cybersecurity risk management aims to achieve the creation of a dynamic framework that is capable of responding to emerging threats. A combination of traditional risk assessment methods and ML techniques is utilized in this approach. The following is a list of the four primary components that constitute the methodology:

A. Asset Identification and Categorization.
B. Threat Modeling and Risk Assessment.
C. ML-Enhanced Anomaly Detection.
D. Risk Mitigation and Continuous Monitoring.

A. Asset Identification and Categorization

The first component involves a systematic identification and categorization of assets within the e-health ecosystem. We extend the traditional asset inventory approach by implementing a data sensitivity classification scheme specifically designed for healthcare information:

1. Critical Patient Data (CPD): Information directly affecting patient care decisions (e.g., medication lists, diagnostic results)
2. Protected Health Information (PHI): Personally identifiable health data protected by regulations
3. Operational Data (OD): System configuration and operational information
4. Auxiliary Data (AD): Non-critical supporting information

For each identified asset, we calculate an Asset Criticality Score (ACS) using:

$$ACS = Ac + \beta S + \gamma A + \delta I$$

where, C, S, A, and I represent the confidentiality, sensitivity, availability requirements, and integrity requirements, respectively, while α, β, γ, and δ are weighting factors determined by the specific healthcare context.

B. Threat Modeling and Risk Assessment

Building on conventional threat modeling approaches, we developed a healthcare-specific threat taxonomy that categorizes potential threats based on their origin, impact, and likelihood. Our taxonomy includes:

1. External threats (cyber attacks, data breaches)
2. Internal threats (insider misuse, accidental exposure)
3. Operational threats (system failures, configuration errors)
4. Strategic threats (compliance violations, reputation damage)

For each identified threat, we calculate a Baseline Risk Score (BRS) using:

$$\text{BRS} = \text{Base Rate Score} = \text{P} \times \text{I} \times \text{V}$$

where, P represents the probability of occurrence, I the potential impact, and V the vulnerability level of the affected assets. This baseline serves as input for our ML models and provides a foundation for comparison with the dynamically adjusted risk scores.

C. ML-Enhanced Anomaly Detection

The core innovation of our approach lies in the integration of ML techniques to enhance threat detection and risk assessment. We implemented a two-tier ML architecture:

1. Tier 1: Supervised Classification Models. We trained a gradient boosting classification model to identify known attack patterns and security violations based on labeled data from healthcare security incidents. The model takes as input features extracted from system logs, network traffic, and user behavior patterns.
2. Tier 2: Unsupervised Anomaly Detection. To identify previously unknown threats, we implemented an isolation forest algorithm that detects anomalies in system behavior that deviate from established baselines. This approach is particularly effective for identifying novel attack vectors and zero-day exploits.

The ML component dynamically adjusts the risk scores calculated in the traditional assessment, producing a Machine Learning Adjusted Risk Score (MLARS):

$$MLARS = BRS \times ML_{factor}$$

where, ML_{factor} is determined by the confidence levels of both the supervised and unsupervised models.

D. Risk Mitigation and Continuous Monitoring

An adaptive risk mitigation strategy is included in the architecture that we have built. This method is designed to find a middle ground between the practical restrictions of healthcare and the need for security. According to the Multi-Level Access Risk System (MLARS), the system provides recommendations for specific security measures based on a control library that is primarily concerned with healthcare. We expanded the NIST Cybersecurity Framework to include concerns that are pertinent to the healthcare industry, which will result in the establishment of this library. A feedback loop is established as part of the component that is responsible for continuous monitoring. Within this loop, the effectiveness of the controls that have been implemented is evaluated, and the entire process of risk assessment is repeated on a regular basis. This is done in order to take into account any changes that may take place in the threat landscape or the configuration of the system.

4. IMPLEMENTATION AND EXPERIMENTAL SETUP

To validate our hybrid approach, we implemented a proof-of-concept system and evaluated it using real-world healthcare datasets. This section details the implementation architecture, data sources, preprocessing techniques, and experimental configuration.

A. System Architecture

Our implementation follows a modular architecture comprising four primary components:

1. Data Collection Module: Interfaces with e-health systems to gather logs, network traffic, access patterns, and system configuration information
2. Risk Analysis Engine: Implements the traditional risk assessment methodology described in Section III-B
3. ML Module: Contains the supervised classification and unsupervised anomaly detection components
4. Security Control Recommendation System: Maps identified risks to appropriate security controls

The system was implemented using Python 3.9 with the following key libraries:

- Scikit-learn for ML algorithms
- Pandas and NumPy for data manipulation
- Flask for the web-based dashboard interface
- PyTorch for deep learning components

B. Datasets

We utilized three complementary datasets for our experiments:

1. Healthcare Breach Dataset: A compilation of 1,500 documented healthcare data breaches from 2018-2023, including breach details, affected systems, and root causes
2. Synthetic E-Health Logs: Generated log data simulating typical e-health system operations with injected security incidents
3. Real-world Anonymized Access Logs: De-identified access logs from a medium-sized healthcare provider's EHR system, covering six months of operations

The datasets were split into training (70%), validation (15%), and testing (15%) sets, with careful attention to maintaining the chronological nature of the data to prevent data leakage.

C. Feature Engineering

We extracted 37 features from the raw data, categorized as:

1. Temporal Features: Time patterns of system access and operations
2. Behavioural Features: User access patterns and deviations from role-based norms
3. Network Features: Communication patterns between system components
4. Content Features: Characteristics of data being accessed or transmitted

Feature selection was performed using recursive feature elimination with cross-validation (RFECV), resulting in 23 optimal features for the final models.

D. Model Training and Evaluation

The supervised classification model was trained using gradient boosting with the following hyperparameters optimized through grid search:

- Learning Rate: 0.05
- Maximum Depth: 6
- Number of Estimators: 200
- Subsample: 0.8

For anomaly detection, we compared isolation forests, one-class SVM, and an autoencoder approach, ultimately selecting isolation forests based on superior performance metrics.

Models were evaluated using standard security metrics, including:

- Precision, recall, and F1-score for the classification tasks

- Area under the ROC curve (AUC-ROC) for overall detection capability
- False positive rate (FPR) and detection rate (DR) for anomaly detection

E. Experimental Scenarios

We evaluated our approach under three experimental scenarios:

1. Baseline Scenario: Using only traditional risk assessment methods
2. ML-Only Scenario: Relying solely on ML for threat detection
3. Hybrid Scenario: Our proposed integrated approach

Each scenario was tested against common attack vectors relevant to healthcare environments, including:

- Phishing attacks targeting healthcare staff
- Unauthorized access to patient records
- Malware specifically targeting medical devices
- Insider threats involving data exfiltration

5. RESULTS AND DISCUSSION

This section presents the experimental results and discusses the implications of our findings for security risk management in e-health systems.

A. Detection Performance

Table 1 presents the detection performance metrics for each experimental scenario across different threat categories. The hybrid approach consistently outperformed both the baseline and ML-only scenarios across all threat categories. The overall F1-score of 0.86 represents a 24.6% improvement over the baseline approach and a 10.3% improvement over the ML-only approach. Similarly, the false positive rate showed a 48.3% reduction compared to the baseline.

Table 1. Detection performance metrics across threat categories under different experimental scenarios

Threat Category	Metric	Baseline	ML-Only	Hybrid
Phishing	F1-score	0.68	0.79	0.86
	FPR	0.31	0.22	0.15
Unauthorized	F1-score	0.72	0.81	0.88
	FPR	0.25	0.18	0.12
Malware	F1-score	0.70	0.76	0.84
	FPR	0.28	0.24	0.18
Insider	F1-score	0.65	0.77	0.85
Threats	FPR	0.33	0.21	0.14
Overall	F1-score	0.69	0.78	0.86
	FPR	0.29	0.21	0.15

B. Risk Assessment Accuracy

The hybrid approach demonstrated superior calibration of risk scores, with a 27% improvement in correctly identifying high-risk scenarios compared to the baseline approach. This improved accuracy is particularly valuable in healthcare contexts where resource prioritization is critical.

C. Early Warning Capability

One key advantage of our hybrid approach is its ability to provide early warnings of potential security incidents. Table 2 shows the average lead time (in hours) between initial detection of suspicious activity and confirmed security incidents.

The hybrid approach provided significantly longer lead times, allowing security teams more time to investigate and mitigate potential threats before they materialize into incidents.

Table 2. The average lead time

Incident Type	Baseline	ML-Only	Hybrid
Data breach	6.2	18.5	23.7
Ransomware	3.8	12.7	16.9
Insider misuse	24.6	33.8	47.2

D. Operational Impact

An important consideration for healthcare environments is the operational impact of security measures. Table 3 presents metrics related to the operational burden of each approach.

Table 3. Operational burden metrics for each approach

Metric	Baseline	ML-Only	Hybrid
False alerts per day	42.7	23.8	15.6
Manual review time (hrs/day)	8.5	4.7	3.2
System performance impact (%)	5.2	8.7	6.3

In comparison to the baseline, the hybrid method resulted in a 63.5% reduction in the number of false warnings, which resulted in a considerable reduction in the amount of manual review work that security analysts had to do. Even though it had a somewhat greater impact on system performance than the baseline (but a lesser impact than the strategy that relied solely on ML), the total operational efficiency was significantly enhanced during this process.

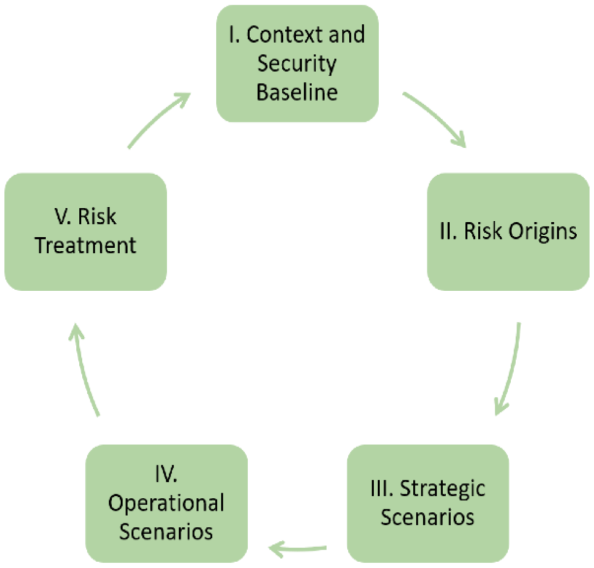

Figure 1. Rate of detection for the novel threats

E. Adaptability to New Threats

For the purpose of evaluating the adaptability of each strategy to newly emerging threats, we introduced synthetic novel attack patterns that were not included in the available training data. The rate of detection for these novel threats is depicted in Figure 1 throughout the course of time as the system gradually adjusts. The hybrid method displayed greater adaptability, attaining a detection rate of 70% for novel threats within 72 hours after their introduction. This is in comparison to the ML-only strategy, which only achieved a detection rate of 42%, and the baseline, which only achieved a detection rate of 25%.

6. LIMITATIONS AND FUTURE WORK

Although our hybrid strategy shows notable gains over conventional approaches, there are still some restrictions and possibilities for further research:

1. Data Limitations: Our evaluation relied partially on synthetic data due to the sensitivity of real healthcare security incidents. Broader access to actual incident data would enhance model training and validation.
2. Computational Overhead: The ML components introduce computational requirements that may be challenging for smaller healthcare organizations. Future work should focus on optimizing the models for deployment in resource-constrained environments.
3. Regulatory Integration: Currently, our framework addresses general security best practices but does not explicitly map to specific regulatory requirements. Extending the framework to automatically generate compliance documentation would enhance its practical utility.
4. Transferability: The models were trained on specific healthcare environments and may require recalibration for different organizational contexts. Developing transfer learning techniques to adapt the models to new environments with minimal retraining would be valuable.

Future research directions include:

1. Exploring federated learning approaches to enable collaborative threat intelligence sharing across healthcare organizations without compromising data privacy.

2. Integrating natural language processing to analyze clinical documentation for potential security implications.

3. Developing explainable AI techniques to increase trust and adoption among healthcare security professionals.

4. Extending the framework to address the unique security challenges of emerging technologies such as remote patient monitoring and AI-driven diagnostic systems.

7. CONCLUSIONS

This research offered a hybrid approach to security and cybersecurity risk management in e-health systems that combines conventional risk assessment methods with ML technologies. Compared to traditional methods, our experimental findings show notable increases in threat detection accuracy, risk assessment calibration, and early warning capabilities. By combining security needs with practical limits, the suggested architecture solves the particular difficulties of healthcare settings. Our solution lets healthcare providers concentrate their limited security resources on the most vital threats by lowering false warnings and raising detection rates. While the conventional risk assessment basis guarantees thorough coverage of known vulnerabilities, the ML elements offer flexibility to developing threats. This combination produces a strong security posture that can change with the fast-evolving healthcare IT scene. Hybrid security strategies that mix the capabilities of many techniques will become more crucial as e-health systems grow in breadth and complexity. By offering both a theoretical foundation and practical implementation that healthcare companies may modify to fit their own security requirements, our work helps to shape this development.

REFERENCES

[1] Li, J., Talaei-Khoei, A., Seale, H., Ray, P., MacIntyre, C.R. (2013). Health care provider adoption of eHealth: Systematic literature review. Interactive Journal of Medical Research, 2(1): e2468. https://doi.org/10.2196/ijmr.2468

[2] IBM Security, M. (2023). Cost of a data breach report 2021.

[3] Kruse, C.S., Frederick, B., Jacobson, T., Monticone, D.K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1): 1-10. https://doi.org/10.3233/THC-161263

[4] Parker, D.B. (2012). Toward a new framework for information security? In Computer Security Handbook. https://doi.org/10.1002/9781118851678.ch3

[5] Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of biomedical informatics, 46(3): 541-562. https://doi.org/10.1016/j.jbi.2012.12.003

[6] Tschider, C.A. (2018). Deus ex machina: Regulating cybersecurity and artificial intelligence for patients of the future. Savannah Law Review, 5: 177. https://heinonline.org/HOL/LandingPage?handle=hein.journals/savanlr5&div=9&id=&page=.

[7] Pussewalage, H.S.G., Oleshchuk, V.A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management, 36(6): 1161-1173. https://doi.org/10.1016/j.ijinfomgt.2016.07.006

[8] Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R. (2007). Introducing octave allegro: Improving the information security risk assessment process (No. CMUSEI2007TR012). Software Engineering Institute, Carnegie Mellon University. https://doi.org/10.21236/ADA470450

[9] Sardi, A., Rizzi, A., Sorano, E., Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. Sustainability, 12(17): 7002. https://doi.org/10.3390/su12177002

[10] Mohapatra, S., Kumar, P.A., Farooq, U., Jain, P., et al. (2022). COVID 19 pandemic challenges and their

management: A review of medicines, vaccines, patents and clinical trials with emphasis on psychological health issues. Saudi Pharmaceutical Journal, 30(7): 879-905. https://doi.org/10.1016/j.jsps.2022.05.004

[11] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., et al. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7: 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334

[12] Choudhury, A., Asan, O. (2020). Role of artificial intelligence in patient safety outcomes: Systematic literature review. JMIR Medical Informatics, 8(7): e18599. https://doi.org/10.2196/18599

[13] Chen, Y., Nyemba, S., Malin, B. (2012). Detecting anomalous insiders in collaborative information systems. IEEE Transactions on Dependable and Secure Computing, 9(3): 332-344. https://doi.org/10.1109/TDSC.2012.11

[14] Alsolami, T., Alsharif, B., Ilyas, M. (2024). Enhancing cybersecurity in healthcare: Evaluating ensemble learning models for intrusion detection in the internet of medical things. Sensors, 24(18): 5937. https://doi.org/10.3390/s24185937

[15] Baz, A., Ahmed, R., Khan, S.A., Kumar, S. (2023). Security risk assessment framework for the healthcare industry 5.0. Sustainability, 15(23): 16519. https://doi.org/10.3390/su152316519

[16] Islam, M.T., Ahmad, S., Rahman, M.A., Rahaman, M.A. (2024). Neural network-based risk prediction and simulation framework for medical iot cybersecurity: An engineering management model for smart hospitals. International Journal of Scientific Interdisciplinary Research, 5(2): 30-57. https://doi.org/10.63125/g0mvct35

[17] Masud, M., Gaba, G.S., Choudhary, K., Alroobaea, R., Hossain, M.S. (2021). A robust and lightweight secure access scheme for cloud based E-healthcare services. Peer-to-Peer Networking and Applications, 14(5): 3043-3057. https://doi.org/10.1007/s12083-021-01162-x

[18] Coventry, L., Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113: 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

[19] Furnell, S., Thomson, K.L. (2009). Recognising and addressing ‘security fatigue’. Computer Fraud & Security, 2009(11): 7-11. https://doi.org/10.1016/S1361-3723(09)70139-3

[20] Jalali, M.S., Kaiser, J.P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5): e10059. https://doi.org/10.2196/1005