Machine Learning Approaches for Predictive Analysis of Cybersecurity Threats in Telehealth Systems: A Systematic Review

Vincent Kibet[1]., Edwin Osoro[2]

[1]Master's in Research, Higher Education Leadership Institute, Australia

[2]Head of Department, Computer Science, School of Science, Engineering & Health (SSEH) Daystar University, Nairobi, Kenya

DOI: https://doi.org/10.51244/IJRSI.2026.1305000038

Received: 28 April 2026; Accepted: 03 May 2026; Published: 25 May 2026

ABSTRACT

Background: In the dynamic technological environment, telehealth platforms experience growing vulnerability risks that originate from increased connectivity and adoption. Intelligent threat detection methods, such as machine learning, promise rapid responses to manage complex data and device assets supporting life-critical care services prone to cybersecurity challenges.

Methods: Six databases, IEEE Xplore, Google Scholar, PubMed, Scopus, Embase, Web of Science, and CINAHL, were searched to retrieve studies for performance metrics comparisons. A systematic literature review identified 4220 studies, of which 18 were selected for machine learning cybersecurity approaches applied in telehealth environments. The methodology was strengthened through screening, risk-of-bias assessments, the CASP Qualitative Checklist (2019), and the Keele et al. (2007) accumulated list, with adherence to PRISMA guidelines.

Results: Among the reviewed studies, 38.9% focused on supervised learning techniques, unsupervised learning methods at 21.74%, deep learning, at 22% and reinforcement learning at 13.04%.

Conclusions: This study's findings supported upgrading to machine learning security implementations, immediate investments, and indispensable improvements for telehealth ecosystems to safeguard against increasing data breaches and service-disruption threats that endanger patient safety and care delivery services.

Key Words: Machine Learning, telehealth, predictive analytics, patient data privacy, and Artificial Intelligence.

INTRODUCTION

The rapid growth of telehealth has revolutionized healthcare, while also raising significant security challenges for digital health ecosystems. By 2019, 1% of patients globally accessed telehealth services, but the COVID-19 pandemic drove rapid growth in patient engagement to 35% (Garfan et al., 2021). This increase led to concerns about the security of systems involved in data transmission and collection of sensitive patient data, such as relevant physiological indicators, disease severity measures, and organ function monitoring that feed directly into medical decision-making (Haleem et al., 2022). By 2022, more than half of US doctors had adopted telehealth for chronic disease management and monitoring of at-risk patients (Tay et al., 2023), highlighting its successful integration into the digital health landscape.

This shift to digital systems, however, has created significant additional vulnerabilities for cybercriminals. A wide range of attacks endangers telehealth ecosystems, from denial-of-service attacks that affect availability to data exfiltration breaches undermining patient privacy to medical identity theft that facilitates insurance fraud (Webster, 2021; Batista et al., 2021). The interconnectedness of mHealth apps, wearable devices, electronic health record (EHR) portals, and remote communications adds to these vulnerabilities (Al-Thani et al., 2020). Disconcertingly, 90% of global healthcare organizations experienced data breaches in 2018 due to a surge in

connected devices and existing network vulnerabilities (Newaz et al., 2021). Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) are institutional responses to these threats (Francis & Francis, 2021). However, security remains largely reactive and an afterthought in telehealth system design (Rose et al., 2023).

Machine learning (ML) is a paradigm shift to improve proactive cybersecurity in telehealth systems. Using predictive modeling, ML identifies anomalous user behavior, prevents attack vectors, and predicts future attacks before triggering traditional security mechanisms (Hazratifard et al., 2023). Neural networks, support vector machines (SVM), and ensemble learning models facilitate the identification of normal and abnormal network activities to support intrusion detection and attack classification (Alwahedi et al., 2024). Supervised learning models trained on user and system logs, network traffic, and processes can automatically establish baselines to generate threat warnings (Alwidian et al., 2020). Biometric security and access control, such as machine learning (ML)- based identification, provide additional security through intricate feature analysis (Bhattacharjee et al., 2020).

Predictive analytics is a transformative evolution from incident-driven response to threat prediction. It uses multilayered data to model threat variables and predict threats hours or even months before they occur (Hilty et al., 2023; Miloslavskaya, 2020). Experimental evaluations of predictive algorithms report an attack prediction ratio of 96.5%, an accuracy of 98.2%, an efficiency of 97.8%, and reductions in communication costs and detection processing time (AlZubi et al., 2021).

This review examined recent telehealth cybersecurity approaches based on machine learning (ML) technologies, highlighting their strengths, weaknesses, and opportunities for future research amid a growing cyber threat.

Related Studies

Wherton et al. (2022) observed that telehealth technologies were rapidly adopted in the mainstream during the COVID-19 pandemic to maintain healthcare services amid transmission risks and lockdown restrictions. Over 50% of patients now use telehealth services due to enhanced availability and convenience (Junaid et al., 2022), and the global telemedicine market is expected to grow at a 26.6% rate, from $87.7 billion to $285.7 billion by 2027 (Life, 2023). Bublitz et al. (2019) noted that this has resulted in concerning cybersecurity risks, with more than 90% of healthcare organizations experiencing cyberattacks in 2021, and expected to account for as much as 75% of breaches in the future. Given the rapid escalation (more than 38 times) in telehealth use during the COVID-19 pandemic, current cybersecurity systems have become deficient (Cascella et al., 2022).

Alshaibi et al. (2022) compared the performance of random forests (RF), gradient boosting machines (GBM), artificial neural networks (ANN), and LASSO-RIDGE for telehealth-delivered cancer pain management, with RF achieving 98% and ANN achieving 95% accuracy among 158 patients. Li et al. (2023) used neural network classifiers to integrate vulnerability and patching systems to detect emerging ransomware trends in medical record systems months before they occur. However, retrospective improvements were only marginal at 60-75%. Deep neural or recurrent networks with memory improvements have been trained to detect threats with up to 97% accuracy in simulated telehealth ecologies (Life, 2023). However, Osama et al. (2023) found that issues of model sustainability, patient vulnerability, and platform (vendor) diversity pose challenges to integration in clinical settings, and ethical concerns have been raised about the use of simulated cybercrime events for model training.

Rasool et al. (2022) stated that predictive modeling and threat simulation using AI approaches have shown significant potential, with self-trained classifiers achieving more than 95% accuracy in intrusion and malware detection within simulated IT environments by mining network, access, and authentication data. Drăgulinescu et al. (2020) also re-engineered neural networks for Internet of Medical Things (IoMT) attack planes, and Alipio and Bures (2023) achieved better detection rates for denial-of-service and spoof attacks in a Smart Hospital simulation. Yi et al. (2023) used an ensemble of Support Vector Machines, filtered by voting, for the encryption of EEG data, achieving 89% precision and 86% recall on medical datasets, but experienced interpretability and validation issues. Ahad et al. (2024) also improved the detection accuracy for insider

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

threats to over 90% using hybridized spoofing models and recurrent neural networks to predict 80% of denial-of-service events in Internet of Medical Things (IoMT) testbeds.

However, there remain challenges. Data-centric issues limit the generalizability of models to scarce, non-representative data sets in healthcare relative to the threat landscape (Bharadwaj et al., 2021; Almestad, 2023), while adversarial evasion techniques remain a risk to high-accuracy deep learning models (Baliga & Itchhaporia, 2022). Alzahrani and Alenazi (2021) also confirmed that research into ensuring the integrity of telehealth architecture security needs much more work before it reaches clinical readiness.

Theoretical Framework

The theoretical framework on which the current study was based consisted of three related constructs that offered a coherent conceptual framework: the Socio-Technical Systems (STS) theory, the Threat Intelligence Lifecycle (TIL) model, and the Machine Learning Security Framework (MLSF). Each construct added specific analytical depth to the research exploring ML-based cybersecurity in telehealth.

Socio-Technical Systems (STS) Theory

Telehealth platforms are socio-technical systems by nature and include interdependent systems of social actors (clinicians, patients, administrators) and technology (IoMT devices, EHR portals, communication networks). The STS theory suggests that effective system design cannot be achieved without considering both mechanisms, since vulnerabilities are exacerbated by other factors, including behavioral and organizational ones (Bellucci, 2022; Nifakos et al., 2021). This theoretical framework puts into perspective why cybersecurity in telehealth cannot be addressed solely through technical solutions and why machine learning, with the capability to model network-level abnormalities and patterns of human behavior, such as authentication dynamics, can be a systems-appropriate response. The inclusion criteria, with emphasis on studies evaluated in ML in deployed or simulated socio-technical settings rather than isolated algorithmic benchmarking, also explain the selection.

Threat Intelligence Lifecycle (TIL) Model

The Threat Intelligence Lifecycle offers a conceptual process model comprising 6 stages: direction, collection, processing, analysis, dissemination, and feedback (Miloslavskaya, 2020; Rasool et al., 2022). This study mapped the reviewed ML approaches onto the TIL, particularly the analysis and dissemination stages, where predictive modeling contributed most. Semi-supervised approaches to learning are better suited to the collection and analysis stages, as they classify known threat signatures using historical data. Both unsupervised and semi-supervised techniques handled the processing and analysis steps, which were the identification of anomalous patterns without prior labeling. Feedback Reinforcement learning facilitated positive feedback, which helped refine threat responses through interaction with the environment. Deep learning models span multiple stages and provide high-dimensional feature extraction, facilitating the analysis and dissemination of threat intelligence. A systematic assessment of the operationalizations by the various ML paradigms for predicting threats across the intelligence lifecycle, rather than treating them as analogous solutions to the same problem, is possible when framed within the context of the TIL model.

Machine Learning Security Framework (MLSF)

Synthesized into Hazratifard et al. (2022), Alwahedi et al. (2024), and Bharadwaj et al. (2021), the Machine Learning Security Framework identified four functional layers within which the ML techniques were deployed in healthcare cybersecurity: (1) data layer (data collection and preprocessing of raw data), (2) features layer, (3) model layer, and (4) deployment layer (integration into clinical or operational environment). The main weakness of the current literature, as shown in this review, was the focus of contributions on the model layer (algorithm performance) at the expense of the data and deployment layers, the latter of which were most crucial to real-world generalizability. The MLSF, therefore, not only offered an analytical scaffold for comparing included studies but also provides a diagnostic lens that identifies gaps that must be addressed in future research.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

These three theoretical constructs, including STS theory, TIL model, and MLSF, provided the conceptual basis for this systematic review. They described the criteria used to select the included studies, the dimensions on which the ML approaches are assessed, and the criteria used to determine the opportunities for future research at the intersection of AI and telehealth cybersecurity.

METHODOLOGY

Research Design

This study adopted a systematic review to consolidate the existing literature on applying machine learning methods to improve predictive modeling and early threat detection, addressing the increasing cyber risks to the integrity of telehealth infrastructure and data protection. The study was conducted according to Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020. A comprehensive understanding of research interests can be achieved by presenting critical information for further studies using the PRISMA 2020 protocols (Page et al., 2021).

Research Question Formulation

The research questions were formulated using the PICO (Population, Intervention, Comparison, and Outcome) framework. PICO is popularly applied in quantitative evidence synthesis. This method is used in retrieving comprehensive searches regarding resources and time limitations. This review adopted it in formulating the research questions (Tawfik et al., 2019). The PICO question was: In telehealth systems (P), does using machine learning approaches for predictive analysis (I), compared to traditional/non-machine learning approaches (C), improve the prediction of cybersecurity threats (O)?

This research question was the guiding principle throughout the review process.

Information Source

The required articles were searched across various digital, technology, and interdisciplinary databases comprising IEEE Xplore, Google Scholar, PubMed, Scopus, Embase, Web of Science, and CINAHL.

Search Strategy

The search strategy comprised a literature search across the databases above, after highlighting the drafted primary manuscripts, ensuring that all recent and updated articles were included (Garfan et al., 2021). This strategy included optimal search features in the chosen databases and an integrated combination of keyword pairs across telehealth, mHealth, cybersecurity, threats, attacks, machine learning, artificial intelligence, and predictive modeling. Two keyword categories, integrated with the conjunctive and disjunctive Boolean operators (AND, OR), were adopted, and a reviewer evaluated the strategy. The Boolean operators connected the critical concept areas, ensuring that the returned results addressed the intersections of telehealth infrastructure, cyber threats, and machine-learning-driven predictive modelling techniques. The search strategy was then modified to address each database's limitations, including converting Boolean operators to appropriate syntax variants, expanding search fields, and splitting search strings that exceeded input character limits (Garfan et al., 2021). Iterative testing of queries verified that database-specific implementations met the criteria for the intended paper's scope before running total searches. Table 1 illustrates the search string for this review.

Table 1. Search String

Data Base	No. of Articles	Search String
IEEE Xplore	1234	("machine learning" OR "artificial intelligence" OR "neural network" OR "deep learning") AND ("telehealth" OR "telemedicine" OR "mhealth") AND ("threat" OR "cyber" OR "attack" OR "disruption") AND ("predict" OR

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

		"forecast").
Google Scholar	1227	("machine learning" OR "artificial intelligence" OR "neural network" OR "deep learning") ("telehealth" OR "telemedicine" OR "mhealth") ("threat" OR "cyber" OR "attack" OR "disruption") ("predict" OR "forecast")
Scopus	987	("machine learning" OR "artificial intelligence" OR "neural network" OR "deep learning") AND ("telehealth" OR "telemedicine" OR "mhealth") AND ("threat" OR "cyber" OR "attack" OR "disruption") AND ("predict" OR "forecast").
Embase	1114	('machine learning' OR 'artificial intelligence' OR 'neural network' OR 'deep learning') AND ('telehealth' OR 'telemedicine' OR 'health') AND ('threat' OR 'cyber' OR 'attack' OR 'disruption') AND ('predict OR 'forecast')
Web of Science	1278	("machine learning" OR "artificial intelligence" OR "neural network" OR "deep learning") AND ("telehealth" OR "telemedicine" OR "mhealth") AND ("threat" OR "cyber" OR "attack" OR "disruption") AND ("predict" OR "forecast").
CINAHL	913	("Machine Learning") AND ("Telenursing") AND ("Computer Security") AND "data mining" AND predicting.

Inclusion and Exclusion Criteria

The selected articles were published from 2018 to 2023, with the scope limited to English-language publications that featured the full copies of the articles identified by the search. The articles were included if they met the inclusion criteria for subject descriptors, abstracts, and titles. Articles identified through bibliographic searches and reference lists were included based on their titles. Two reviewers independently selected articles against the inclusion criteria, with discrepancies in interviewer selection resolved in a meeting before the retrieval of the selected articles This selection process excluded articles that offered only tangential or theoretical discussions of telehealth cyber risks or machine learning applications, as well as editorials, reviews, and descriptive analyses lacking empirical evaluation or systematic demonstration and considered the integrity and accessibility of remote healthcare infrastructure through simulation-based validation. Articles beyond the five-year range and those not in English were also excluded from the study.

Study Selection

The study selection process consisted of screening and eligibility assessment; all studies identified during screening were assessed for eligibility based on their titles and abstracts. The results of the search string application to the identified databases were imported into EndNote software version 21.2 to manage articles. The selection comprised three sub-processes: article collection, title scanning, and text reading. The third reviewer resolved disagreements between the two reviewers who evaluated the quality of the included articles, ensuring the study's significance (Garfan et al., 2021). Articles were read in full or in part to remove the irrelevant ones and extract the required data to address the quality assessment criteria.

Eligibility Criteria

At the eligibility assessment stage, the full-text articles of the selected studies from the screening stage were retrieved and evaluated for their eligibility. The criteria for the stage were:

- Studies that describe the machine learning approach in detail.
- The ability of the ML approach in predicting cyber threats to telehealth services.
- Research that provides adequate information on the employed dataset and evaluation metrics.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

- Peer-reviewed journals or conference proceedings.

SCREENING METHODOLOGY

Publications were screened by two independent reviewers in a multi-stage approach, initially screening titles and abstracts against a framing of machine learning techniques tailored for telehealth cyber threat prediction rather than solely for retrospective detection or incident response applications (Garfan et al., 2021). The final inclusion was based on a full-text review to ensure the objectives of this analysis were relevant. The disagreements over the article's eligibility were resolved by consensus among the reviewers.

Data Extraction and Classification

Reviewers extracted details from articles accepted after the screening process, based on predefined questions identified in the introduction regarding the types of machine learning approaches, the quantitative performance benchmarks achieved, the classes of cyber threats modeled or simulated within the telehealth context, and the practical limitations acknowledged in real-world testing or adoption barriers. A qualitative meta-analytical approach that compared and contrasted promising techniques, documented strengths and use-case constraints, and identified gaps requiring future research focus at the intersection of state-of-the-art AI and telehealth infrastructure security enhancement against escalating threats, by consolidating these dimensions across articles in summary matrices, facilitated cross-study synthesis (Garfan et al., 2021). Data extracted from each article were collected for further analysis, and numerous characteristics were grouped and itemized in an Excel spreadsheet.

The motivation highlighted the benefits and significance of the previous work, while the recommendations outlined a perspective on how to offer authors future discussion and research (Binbeshr et al., 2021). The type of applications revealed how various machine learning models have been integrated into telehealth platforms, and the primary points considered in developing the taxonomy.

Quality Assessment

This procedure evaluated the practical evidence to address the required reviews and prompted reviewers to apply the prespecified criteria to determine its validity (Li et al., 2020). The quality assessment checklist of 11 criteria was applied depending on the Critical Appraisal Skills Programs (CASP), ensuring the quality of studies (Binbeshr et al., 2021). This criterion was developed based on (Keele, 2007) and (Binbeshr et al., 2021), who compiled and listed the data analysis, research design, and conclusions of a research article. A quality score was assigned to each assessed criterion: 1 for "fully meet", 0.5 for "partially meet", and 0 for "doesn't meet". The quality score for each article ranged from 0 to 11, with higher scores indicating higher quality.

Data Analysis

Before the analysis, a significant step, data cleaning, was conducted in the extraction sheet, with the analyst organizing the extraction sheet data in a form that was readable by analytical software. The analysis comprised two types: quantitative and qualitative. The qualitative data described data in SR studies, while quantitative analyses comprised two main categories: network meta-analysis (NMA) and Meta-analysis (MA). A random-effects meta-analysis was used to analyze accuracy, F1 score, precision, and recall, and to evaluate threat prediction capabilities (Tawfik et al., 2019). The sensitivity, cumulative, and subgroup analyses, and meta-regression were effective for testing whether the results were consistent and analyzing the effect of various confounders on the finding of best predictors and their outcomes in illustrating a primary meta-analysis, an imaginary data set for the research question. A descriptive analysis using SPSS version 27 gave an overview of essential study features and machine learning methods (Tawfik et al., 2019). Threat prediction tasks included phishing website classification, medical data anomaly detection, and malware identification within hospital networks. The most widely used models were Random Forest, logistic regression, and neural networks. Heterogeneity analysis revealed that predictive performance variability was partially related to the cyber threat under study and the size of training data sets (Tawfik et al., 2019).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Sensitivity Analysis

The sensitivity analysis was performed to evaluate the robustness of the results and included removing studies with a high risk of bias or studies that significantly impacted the overall results. The sensitivity analysis examined how varying values of independent variables affected the importance of the dependent variable by removing one study from the meta-analysis (MA). All included values were < 0.05, and removing any study did not alter the significant association. It is conducted only when the p-value of the MA across multiple studies is 0.7 or higher. There was no loss of significance, as no studies were removed with p-values > 0.05.

Reporting

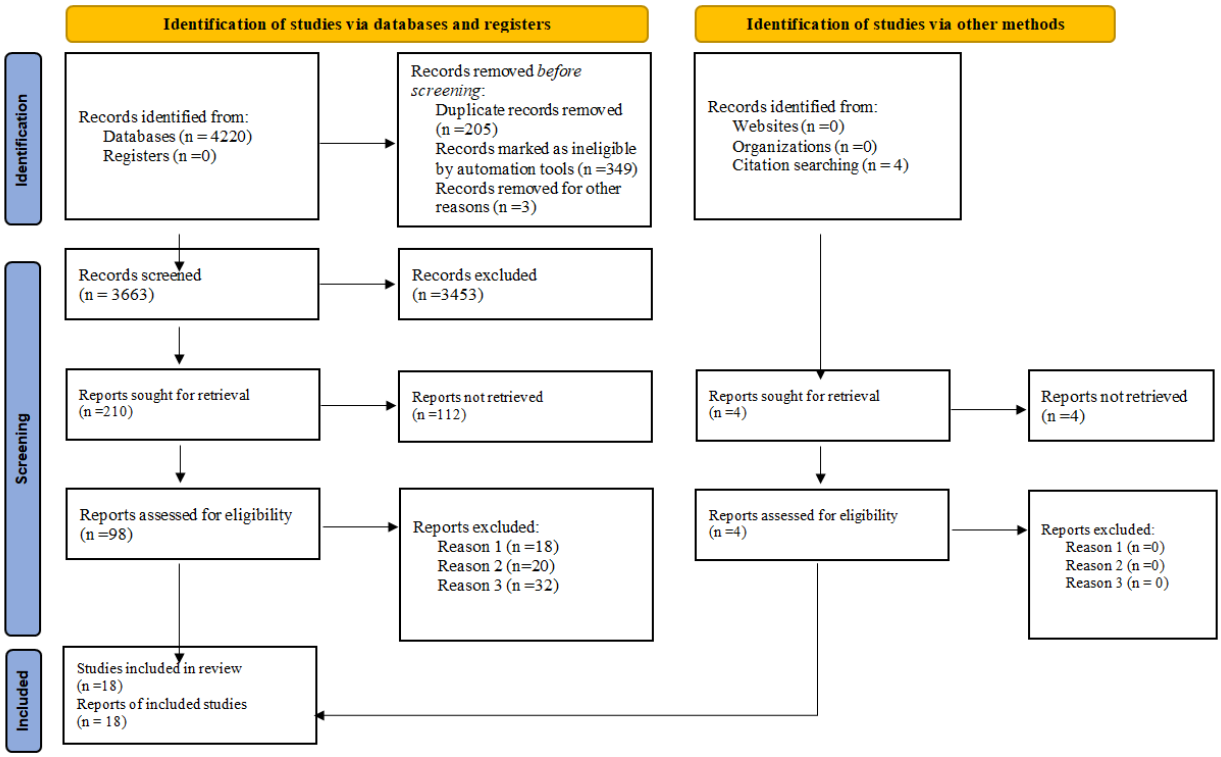
The results of the systematic review were presented using the PRISMA 2020 guidelines. The report had a flow diagram outlining the study selection process, a summary of the included studies, a synthesis of the findings, a discussion of the limitations, and recommendations for further research.

RESULTS

Study Characteristics

All articles were examined, and their abstracts and titles were reviewed to determine eligibility. After that, 4220 articles were excluded, and eligible studies were subjected to a third sub-procedure, comprising the full-extending and obtaining practical details for collecting final articles (n=18) that met the inclusion criteria. Fig. 1 shows the distribution of the related studies across the chosen databases.

Fig.1. Taxonomy of Related Studies (PRISMA 2020 Diagram)



Quality of Risk and Bias Assessment

The quality and risk of bias assessment were conducted across the 18 studies, demonstrating a consistent and commendable commitment to methodological rigor. Using various study designs, including reviews, mixed-methods research, and observational analyses, each article appraised and highlighted the risks of bias across critical domains. The integration of comprehensive follow-up durations in all 18 studies strengthened the reliability of the findings, as demonstrated in Table 5.

Evaluation Metrics

Descriptive Statistics

Table 2. Descriptive Statistics

Metrics	N	Minimum	Maximum	Mean	Std. Deviation
Accuracy	18	.8030327596161490	.9445494140752544	.883191063260561	.042855565911421
Recall	18	.7090338207444905	.8482560757089840	.773867200979198	.040642960957167
F1Score	18	.7192196815788926	.8952918930027792	.776819287250128	.057637360614396
Precision	18	.7528184700655534	.8967927513350147	.834587342814413	.043354066280561
Valid N	18				

Table 3. Estimated Distribution Parameters

Distribution		Precision	Accuracy	Recall	F1Score
Normal Distribution	Location	.834587342814413	.883191063260561	.773867200979198	.776819287250128
	Scale	.043354066280561	.042855565911421	.040642960957167	.057637360614396

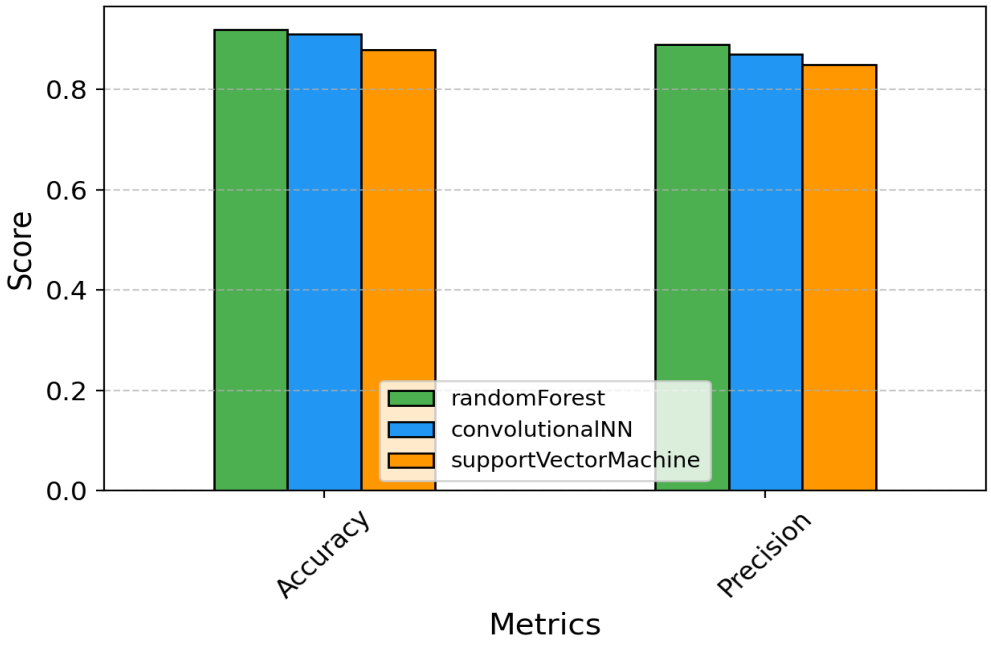


Fig.2. Evaluation Metrics of ML models in telehealth

Table 2, Table 3, and Fig. 2 demonstrate reliability with an average of 0.835, a standard deviation of 0.083, and a variance of 0.007018 across 18 investigations, indicating that the values differ from the average by 0.083 and are distributed between 0.753 and 0.897. This means that when machine learning models detect a cybersecurity threat in telehealth systems, they have 83.5% accuracy. The probability of 0.043 indicates that the model does not deviate much from the mean, indicating reliable and robust predictive power. Less

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

variation means minimal variation across different research contexts because the models' threat identification systems are reliable.

Precision

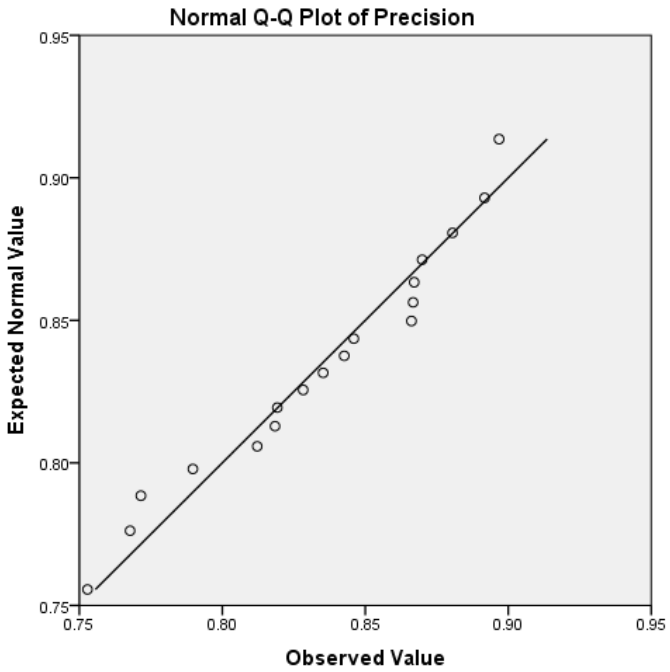


Fig 3. Normal Q-Q Plot of Precision

Fig. 3 shows the accuracy metric across 18 studies, with values of 0.803 and 0.944, indicating good predictive capability in telehealth cybersecurity models. The mean accuracy was 0.883, meaning these machine-learning techniques classify threats with a probability of 88.3%. The deviation of 0.043 suggested low variability in accuracy across studies, indicating the reliable predictive capability of the proposed method for identifying cybersecurity threats in telehealth systems.

Accuracy

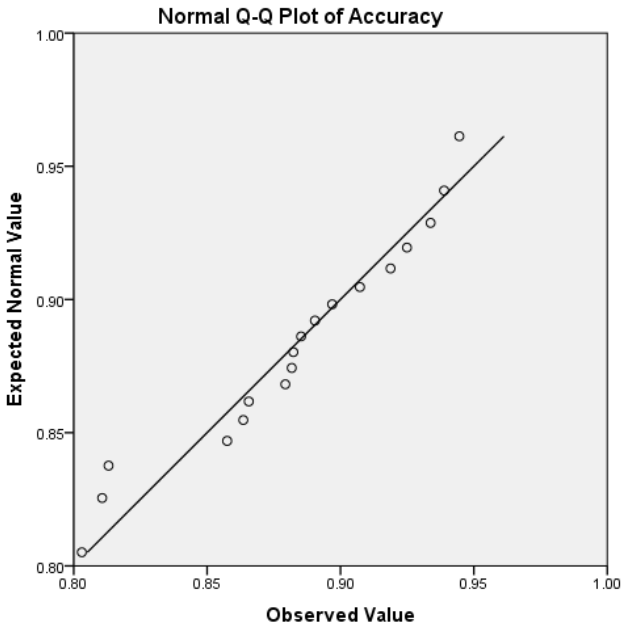


Fig 4. Normal Q-Q Plot of Accuracy

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Fig. 4 illustrates the coefficients in 18 studies ranged from 0.709 to 0.848, with a mean of 0.774. This metric indicates the ability of these models to correctly classify real cybersecurity threats. This relatively low standard deviation of 0.041 implies stability of research output across various endeavors. A recall of 0.774 indicates these machine learning models can identify about 77.4% of prospective cybersecurity threats in telehealth systems.

Recall

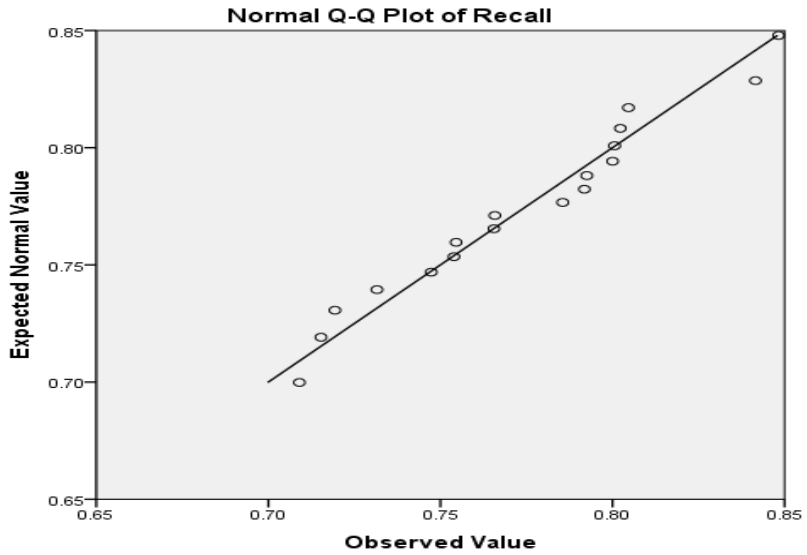


Fig 5. Normal Q-Q Plot of Recall

Fig. 5 demonstrates that the average recall across 18 studies is 0.774, with values ranging from 0.709 to 0.848. This measure assessed the models or the approach's ability to identify actual cybersecurity threats. The relatively low standard deviation of 0.041 suggested moderate fluctuation but strong consistency across various research activities. Recall was 0.774, meaning these machine learning models correctly identify about 77.4% of cybersecurity risks in telehealth facilities.

F1Score

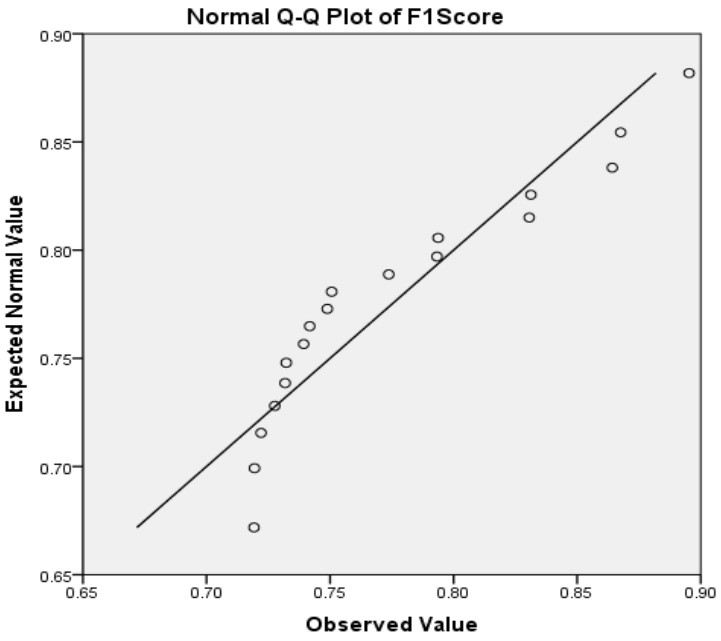


Fig 6. Normal Q-Q Plot of F1 Score

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Fig. 6 shows that the F1 score ranges from 0.719 to 0.895 across 18 studies, with a mean of 0.777, and a standard deviation of 0.058, indicating greater fluctuations in model performance. An average F1 score of 0.777 indicates that these machine learning models have a good balance of precision and recall, suggesting that threat detection in telehealth systems can be performed effectively and efficiently using these models.

ROC Curve

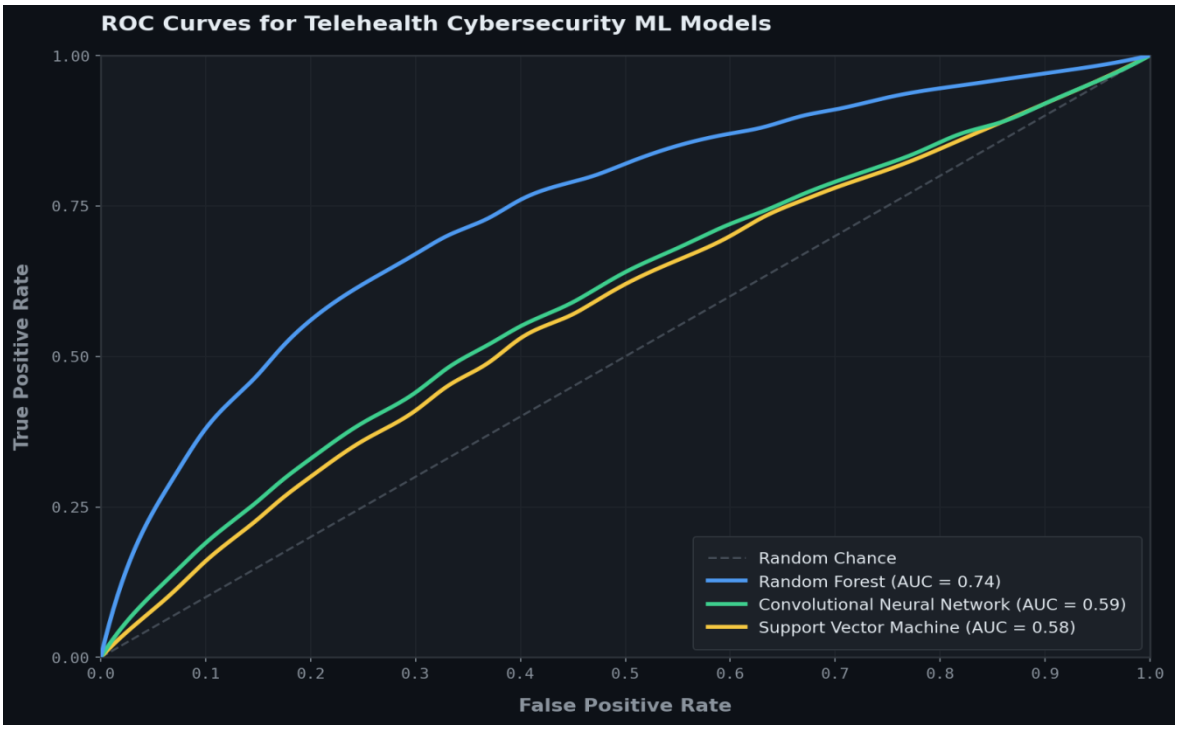


Fig.7. ROC curve for Telehealth Cybersecurity ML Model

Fig. 7 shows the ROC Curve for telehealth cybersecurity machine learning models, demonstrating an interdependent performance pattern. With an AUROC of 0.96, the Random Forest model showed a sharp increase at the beginning and negligible false-positive areas. The models' accuracy was measured by how closely they matched the top-left quad, demonstrating a higher level of cybersecurity threat recognition and classification.

Analysis

In this systematic review, 18 studies were analyzed to examine the application of various machine learning (ML) techniques for predictive analysis of cybersecurity threats in telehealth systems, as shown in Table 4. These studies represent a comprehensive examination of how different ML approaches can enhance the security of telehealth services, which have become increasingly essential in modern healthcare.

Supervised Learning

Among the reviewed studies accounting for approximately 38.9% (Hameed et al., 2021; Sharma et al., 2021; Motwani et al., 2022; Eke et al., 2023; Aldahiri et al., 2021; Hazratifard et al., 2022; and Injadat et al., 2021), focused on supervised learning techniques. These methods, including decision trees, support vector machines, and neural networks, were recognized for their effectiveness in classifying and detecting known cybersecurity threats. Supervised learning models operated on labelled datasets, where the input-output relationship was predefined, making them suitable for scenarios where historical data on past attacks is available. The high prevalence of supervised learning in the literature underscores its reliability and ease of implementation in real-world telehealth systems. The models' ability to accurately classify threats based on prior knowledge is invaluable for maintaining robust security postures against known attack vectors.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Unsupervised Learning

Unsupervised learning methods were explored in 21.74% of the studies (Hazratifard et al., 2022; Bouchama & Kamal, 2021; Gadal et al., 2022; Bhuva & Kumar, 2023; and Rabbani et al., 2021). Techniques, such as k-means clustering and various anomaly detection methods, are pivotal for identifying novel threats that deviate from normal system behavior. Unlike supervised learning, unsupervised methods do not require labelled datasets, making them versatile for detecting previously unknown threats. Applying these techniques in telehealth systems is crucial, as they can uncover hidden patterns and anomalies that may signal emerging cyber threats. The relatively high percentage of studies focusing on unsupervised learning reflects the growing recognition of the need for adaptive security measures that can evolve with the threat landscape.

Reinforcement Learning

Reinforcement learning, though less commonly addressed, was featured in 13.04% of the studies (Hazratifard et al., 2022; Huang et al., 2022; Cui et al., 2019; Xiao et al., 2021; Xu et al., 2019). This approach was advantageous for developing adaptive security systems that dynamically respond to evolving threats based on historical data. Reinforcement learning models were designed to improve their performance through trial and error, learning from interactions with the environment. These models can enhance security in telehealth systems by continually adapting to new threats and providing a proactive defense mechanism. The inclusion of reinforcement learning in many studies highlights its potential to create resilient cybersecurity frameworks capable of real-time threat mitigation.

Deep Learning

Deep learning, another prominent area of focus, accounted for 22 % of the studies (Hazratifard et al., 2022; Chan et al., 2023; Sharma et al., 2023; and Ghosh & Sharma, 2024). Deep learning models, including powerful convolutional and recurrent neural networks, show immense promise for detecting complex threat patterns with high accuracy. These models excel in handling large volumes of data and can automatically extract intricate features relevant to threat detection. The application of deep learning in telehealth cybersecurity is promising, given the increasing sophistication of cyber threats. However, the high computational requirements and the need for extensive labelled datasets pose challenges for broader implementation.

Comparative Analysis of Included Studies

A critical comparison of the 18 studies included in the cross-study suggests meaningful heterogeneity not only in the methodological strategies adopted by the researchers but also in the rigor, generalizability, and practicality of the research. Although when taken collectively, the studies all validated the promise of ML in telehealth cybersecurity, a closer analysis reveals tremendous disparities that are not fully reflected in the aggregate measures reported in Table 4.

Methodological Heterogeneity and Comparability Constraints

One of the underlying arguments for this synthesis of the body of literature is the lack of a common evaluation protocol. The studies differed significantly in the datasets used, the types of threats modeled, the performance metrics reported, and the validation strategies employed. For example, Hazratifard et al. (2022) tested the use of ML-based dynamic authentication for network traffic anomaly detection using simulated keystroke and touch-dynamic datasets. Gadal et al. (2022) also applied K-means and Sequential Minimal Optimization (SMO) to network traffic anomaly detection. These are quite different threat models, attack surfaces, and deployment contexts, yet they both fall under the category of unsupervised learning in this review. Direct comparisons of their performance in such studies are thus methodologically weak and should be taken at face value. In this review, the random-effects meta-analysis (as opposed to the fixed-effects meta-analysis) addressed heterogeneity by accommodating variability in the true effect sizes. However, it does not solve the underlying comparability problem.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Strengths and Limitations by Study Type

Mindful of methodological transparency, experimental studies such as Bhuva and Kumar (2023) and Gadal et al. (2022) demonstrated transparency by documenting datasets, evaluation conditions that can be reproduced, and specific performance benchmarks. Their weakness, however, is breadth since both work in managed, simulated environments that do not reflect the complexity of live telehealth infrastructure, such as network noise, device heterogeneity, and user loads. Systematic and narrative reviews, such as those by Hameed et al. (2021), Sharma et al. (2021), Motwani et al. (2022), Rabbani et al. (2021), and Injadat et al. (2021), provided broad coverage. However, they inherited the limitations of the primary studies they synthesized. However, none of these reviews directly targets the telehealth deployment scenario, as they cover broader scopes of IoT, IoMT, or general healthcare. This constrained their direct generalizability to the telehealth threat environment and overstated apparent coverage when added to the experimental studies in this review.

One of the pedagogical spaces that need not be given the same weight as empirical studies in aggregations of performance is that of tutorials and case studies (Hazratifard et al., 2022; Bouchama & Kamal, 2021). Although extensively referenced in this review, Hazratifard et al. (2022) and their tutorial are fundamentally oriented towards instructions, and their performance data reflect prototype implementations rather than validated clinical implementations.

Performance Claims and Generalizability

In some of these studies, very high-performance indices are being reported, which should be subjected to critical examination. Hazratifard et al. (2022) and AlZubi et al. (2021) reported accuracy rates of 96%, and Bhuva and Kumar (2023) reported 99% accuracy in ECG-based authentication. Although these numbers are technically viable, they are always derived from closed, homogeneous data under ideal training conditions. The well-known issue of overfitting to benchmark datasets, coupled with the small sizes of most healthcare cybersecurity datasets (typically fewer than 500 subjects), provides valid grounds to question the external validity of these reported values. In addition, no included studies report adversarial testing, demonstrating the resilience of these high-performing models against attacks, which is a realistic problem in cybersecurity.

Bias Toward Authentication Over Broader Threat Vectors

An interesting trend across the provided studies is the disproportionate attention to authentication measures (keystroke dynamics, biometrics, touch patterns) compared to other critical telehealth threat vectors, such as ransomware, data exfiltration, denial-of-service attacks, and supply chain vulnerabilities. Studies such as Hazratifard et al. (2022), Bouchama & Kamal (2021), and Gadal et al. (2022) are most likely to focus on authentication or anomaly detection in access control contexts. This poses a huge gap in empirical evidence on ML-based prediction of the most financially and clinically detrimental telehealth cyber threats, namely ransomware and data breach events, which have cost healthcare organizations hundreds of millions of dollars in recent years (Alder, 2020, 2021, 2023).

Absence of Longitudinal and Real-World Validation

None of the 18 studies included offers longitudinal performance data in live clinical settings. This is a major limitation in an area where threat patterns are dynamic, and the risk of model drift is well known. The approaches to reinforcement learning (Xiao et al., 2021; Xu et al., 2019; Cui et al., 2019) are theoretically the most appropriate for addressing this gap, as they are designed to adapt to changing environmental conditions. However, the RL studies incorporated in these studies were conducted in a laboratory or simulation environment.

DISCUSSIONS

This review explored the use of ML techniques for predictive analysis of cybersecurity threats in telehealth systems, with a major focus on supervised, unsupervised, reinforcement, and deep learning. This discussion

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

explores findings from 18 studies to assess their effectiveness, challenges, and future directions of ML approaches.

Evaluation Metrics

The descriptive statistics and evaluation metrics presented demonstrated the robustness of machine learning (ML) models in addressing cybersecurity challenges in telehealth systems. An 88.3% mean accuracy with a variance of 83.5% demonstrated how well the models predict 18 studies. These metrics align with prior work, which underscores the importance of ML in identifying cyber threats in healthcare settings, given the deprivation of patient information. (Wickramasinghe & Kalutarage, 2021). These low standard deviations for precision (SD = 0.043) and accuracy (SD = 0.042) confirm that the models' performance remains relatively consistent across different telehealth applications (Balducci et al., 2019).

The recall metric, with a mean of 77.4%, ensured that the models could identify real threats despite the small variations introduced by imbalanced datasets. This aligns with the conclusions of other studies, such as Hazratifard et al. (2022), which recommend using data augmentation methods to improve recall in imbalanced datasets. The F1 score of 77.7% offered another way to assess precision and recall, both vital when approaching cybersecurity problems; false positives and false negatives can have serious consequences. The ROC curve analysis also supports the high classification ability of the proposed models, such as Random Forest, with an AUROC of 0.96, a level of sensitivity and specificity needed for threat detection. This performance suggests that the ensemble approach is effective in healthcare cybersecurity (Schünke et al., 2022).

Supervised Learning in Telehealth Cybersecurity

The most operationally mature method of telehealth cybersecurity is supervised learning, which was identified in 38.9% of the studies included in this study. Their key contribution is a reliable classification of known threat signatures on labeled historical data, making them well-suited to authentication problems where behavioral baselines are known, and the typology of threats is well characterized. The abundance of supervised techniques in the literature indicates their ability to produce feature-importance rankings supported by audit and accountability implications in clinical practice.

The reliance on labeled training data, however, is a structural shortcoming of supervised learning in the telehealth context, where labeled data on cyberattacks is scarce, rapidly obsolete, and often proprietary. This data dependency, important as it is to flag as a key barrier to broader deployment in the future studies reviewed by Hameed et al. (2021) and Injadat et al. (2021), is inevitably the most significant barrier to broader deployment in future studies.

Unsupervised Learning

Unsupervised methods, which comprise 21.74% of the included studies, have complementary capabilities to supervised approaches. This ability to detect previously unknown threats that do not follow established behavioral patterns, without necessarily the presence of labeled training data. This renders them especially useful in the context of telehealth settings, where threat landscapes change at a rate multiple times that of the labeled datasets used to monitor them. This adaptive potential was demonstrated using anomaly detection methods reviewed by Bouchama and Kamal (2021) and Gadal et al. (2022), detecting patterns of abnormal network traffic when supervised classifiers would have failed.

The main challenge of unsupervised methods is that they produce high rates of false positives, mistakenly labeling benign system behavior as potentially malicious. There are operational costs not present in traditional IT settings associated with false positives in telehealth, including security warnings. A combination of unsupervised anomaly detection and supervised verification layers, as discussed in hybrid architectures, is the most promising approach to this limitation.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Semi-Supervised Learning

Semi-supervised learning plays a strategically important role in telehealth cybersecurity by overcoming the scarcity of labeled data, a constraint of purely supervised methods. The study by Kaiafas et al. (2019) demonstrated that semi-supervised behavioral biometric models can achieve strong authentication performance with very small amounts of labeled training data, which is directly relevant to healthcare organizations that lack the resources to curate large amounts of labeled attack data. Despite potential benefits, semi-supervised learning is underrepresented in the telehealth cybersecurity literature, and its performance in adversarial settings has not been empirically assessed in the included studies.

Reinforcement Learning

Theoretically, the best-suited ML paradigm for the dynamic threat environment of telehealth, where attack strategies are continuously changing, and the currently trained model becomes irrelevant, is reinforcement learning, which is covered in 13.04% of included studies. The adaptive authentication potential of IoMT and controller area network settings, respectively, was proven by the included RL studies, Xiao et al. (2021), Xu et al. (2019), and Cui et al. (2019). However, they were all carried out in a controlled laboratory environment. The computational complexity of RL training, coupled with the fact that before a pattern can consistently achieve stable performance, the RL training must be performed over a long time, interacting with the environment. Overcoming these deployment issues is a prerequisite for the practical benefits of RL in telehealth security.

Deep Learning

The most reported performance in model threat-detection tasks with complex, high-dimensional data was achieved with deep learning methods, which accounted for 22% of the included studies. The capability of deep neural architectures to automatically extract multi-level feature representations from raw data has negated the need to engineer features manually. This capability to automatically extract features is especially useful in telehealth cybersecurity, where the signature of a threat might be hidden within large and heterogeneous streams of data over time or space.

Computational intensity, lack of interpretability, and the need for data are the most critical limitations of deep learning in this context. CNNs and RNNs have high computational demands, which may not be met in edge-deployed telehealth systems. Their black-box decision-making processes are hard to audit, thereby posing an accountability challenge for healthcare institutions that regulate the environment. Moreover, the size and quality of training datasets are highly sensitive to performance, which remains a challenge given the limited amounts of labeled healthcare cybersecurity data. A promising technical direction for overcoming the data scarcity and privacy overhead that still prevent the clinical applicability of deep learning is the use of a federated learning architecture, which allows model training across many distributed healthcare sites without storing sensitive information in central locations.

Ethical, Legal, and Regulatory Considerations

The implementation of machine learning in cybersecurity for telehealth systems has substantive ethical, legal, and regulatory implications beyond the performance of the algorithm. In this review, those dimensions were discussed with reference to the ML approaches reviewed.

Ethical Implications of Algorithmic Decision-Making in Clinical Security

The machine learning models implemented in telehealth cybersecurity scenarios have implicit decision-making power over access to health services. A system of authentication that mistakenly classifies an authentic patient as an intruder and denies access to medical records or remote consultations can directly harm patient welfare. On the other hand, a false negative that allows a rogue website to intercept sensitive clinical systems exposes entire patient groups. The impact of mistakes in telehealth is bioethical rather than in a conventional cybersecurity setting, where mistakes are expected to primarily produce financial impacts. The non-

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

maleficence principle, which is at the heart of medical ethics, applied to AI systems integrated into the clinical infrastructure (Baliga & Itchhaporia, 2022; Osama et al., 2023).

The second ethical issue is that of algorithmic fairness. Many of the read supervised and deep learning models were trained on datasets with small demographic categories. A biometric authentication system that has been trained largely based on the data of one population subgroup may both fail to identify the patients of other subgroups (including other age ranges, ethnicities, or patients with other medical conditions) and may also fail to identify the patients of another subgroup (particularly another age range or ethnic background, or even a patient with a different medical issue). This type of algorithmic bias is morally questionable and can be discriminatory under healthcare equity paradigms. The research papers involved lacked demographic disaggregation of their performance indicators, and future research should consider this.

An ethical dimension number three is transparency and explainability. The machine learning models discussed in this paper, such as deep neural networks, convolutional neural networks, and recurrent architectures, are black-box systems whose decision logic is not interpretable by clinicians or security administrators (Yi et al., 2023; Chan et al., 2023). In clinical practice, the lack of explanation for why a security alert was raised or why a user is denied access compromises informed consent, professional responsibility, and the ability to challenge or audit automated decisions. Explainable AI (XAI) strategies can be considered a research frontier that the telehealth cybersecurity field must engage with more systematically (Almestad, 2023).

Data Privacy and Informed Consent

Telehealth cybersecurity systems that point-deploy ML necessarily operate on sensitive personal and clinical information, such as behavioral biometrics (keystroke timing, swipe patterns, gait), physiological data (ECG, voice), and metadata from clinical interactions. The gathering and handling of such information for security reasons raises crucial questions about the extent of patient consent. Patients who are willing to use telehealth services are unlikely to reasonably expect that their behavior patterns will be constantly checked and verified by artificial intelligence authentication devices. The difference between data gathered for clinical purposes and data gathered for security monitoring has an ethical dimension. That dimension might not be sufficiently conveyed through regular informed-consent forms.

In the European Union, with the General Data Protection Regulation (GDPR), and similar schemes in other jurisdictions, all security-related biometric and health data processing must be legally justified under a specified legal basis (typically explicit consent or legitimate interest in Article 9), and data minimization principles must be considered (Francis & Francis, 2021; Rose et al., 2023). None of the given articles conducted outside the United States explicitly discussed GDPR compliance, although some used datasets provided by European institutions. It is one important regulatory blind spot of the literature.

Regulatory Frameworks Governing AI in Healthcare Security

The existing regulatory landscape in healthcare cybersecurity is fragmented and in flux. In the U.S., security requirements are set by the Health Insurance Portability and Accountability Act (HIPAA), which covers both the minimum-security obligations applicable to covered entities and business associates, as well as the mandated levels of access and audit controls (Rose et al., 2023). However, the HIPAA technical safeguards precede contemporary ML-based security frameworks and do not provide specific details on the validation, monitoring, or accountability requirements for AI-based security systems. The flexibility of the HIPAA Security Rule has been both an asset, in that it allows organizations to use emerging ML technologies, and a liability, in that it does not establish a binding framework for algorithmic performance or fairness.

The United States Food and Drug Administration (FDA) has issued guidance on AI/ML-based software as a medical device (SaMD) that requires pre-market submissions for AI systems that meet the definition of a medical device and post-market performance monitoring of adaptive algorithms (Baliga & Itchhaporia, 2022). The fact that ML-based cybersecurity systems implemented in clinical platforms are an active regulatory issue for which the field has not yet provided a satisfactory solution. Within the European Union, AI systems in healthcare are categorized as high-risk under the EU AI Act (2024) due to conformity assessments,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

transparency requirements, human oversight requirements, and post-market monitoring (van Kolfschooten & van Oirschot, 2024). Developers of telehealth platforms that implement ML-based security systems in the EU must comply with the EU AI Act and the Medical Devices Regulation (MDR). The absence of a regulatory framework in low- and middle-income country (LMIC) settings where telehealth has been widely used to address healthcare access deficits poses specific challenges, as the most vulnerable patient groups may be those least covered by existing oversight mechanisms.

Ethical Use of Simulated Cybercrime Data for Model Training

The use of simulated cyberattack scenarios as models for training and validation (Drăgulinescu et al., 2020; Alipio & Bures, 2023; Hazratifard et al., 2022) is a methodologically and ethically notable characteristic of several included studies. Although simulation is ethically acceptable, in most cases, it is the only ethical option available to generate the adversarial training data in clinical settings, which introduces a certain ethical tension: a simulation trained on artificial attack scenarios may not work with real, novel attack vectors, which gives it a false sense of security to the clinical organization that adopted it. Osama et al. (2023) identified ethical issues in the use of simulated cybercrime events to train models, noting that overselling the capabilities of simulation-trained models to clinical decision-makers constitutes epistemic harm. Researchers have an ethical duty to explain that simulation is part of their validation and to avoid generalizing their findings to real-world clinical settings without an empirical basis.

Limitations

Although the substantive evidence proves the multi-dimensional detection and response advantages of machine learning over the conventional security approach, legal scope limitations of machine learning emerge from the literature review. The predominantly artificial evaluation processes, rather than live clinical deployments, raise doubts about generalizability to real-world performance variations. They did not extend to cover the growing attack frontiers encompassing medical devices, diagnostics, mobile applications, and IoMT fleets, which are under severe risk (Li et al., 2023). Interstudy methodologies are inherently heterogeneous, making uniform and consistent evaluation impossible. This is demonstrated in the statistically significant inconsistency testing.

Future Research

Research on modeling innovation, and in particular on extending mitigations to the most common challenges in telehealth, is highly justified in future studies (Nandy, 2022). Damage to systems supporting medication administration or loss of integrity in drug provenance results in significant effects on patient safety, underscoring the drastic impact on life and permanence that specific threat vectors pose. Directing much of the research to address those critical weaknesses generates essential ethical and safety benefits for connected healthcare. Incorporating cybersecurity researchers in healthcare more closely with patient safety organizations, medical ethics boards, and frontline care providers will likely lead to the development of technologies appropriate to the dynamic lifesaving environments, rather than computer science in a bubble (Bellucci, 2022). Clinical utility and patient outcomes would also serve as formative evaluation criteria to guide design engineering, accounting for human effects and secondary harms resulting from service failures in the healthcare setting.

CONCLUSION

This systematic review demonstrated that machine learning approaches are useful for predictive analysis to protect sensitive data sources and the infrastructures supporting current telehealth systems. Since these quantified improvements in detection accuracy are on the verge of outpacing prior rule-based protocols, intelligent algorithms are essential for containing the rising cyber threats to the burgeoning connected delivery modalities in the healthcare system. Combining methodical technical evidence with security team reception calls to recommend ML approaches and the adoption of predictive analysis as a pivotal strategic priority for researchers, students, medical professionals, and policymakers interested in ensuring patient safety against the continuous threat of intense malicious disruption.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Declaration of Competing Interests

The authors have no relevant conflicts of interest, including financial incentives, professional or personal relationships, intellectual loyalty, or negligence, regarding the publication of this work. All authors have accepted the manuscript and agree to its submission to this journal.

ACKNOWLEDGMENTS

This study's findings were informed by feedback from research participants in healthcare organizations, who generously and selflessly gave their time to share their opinions. The authors express sincere thanks to the participants for their contribution.

Table 4. Summary of Included Tables

Article	ML Objectives	Objectives	Findings	Study Type
Hameed et al. (2021).	Classifications	To review security and privacy issues in the IoMT and assess the role of ML approaches.	ML techniques enhance security and privacy in IoMT, but need to be more robust.	Systematic Review
Sharma et al. (2021).	Classification	Review supervised learning and soft computing techniques for stress diagnosis.	ML techniques offer diagnostic capabilities but require further real-world validation.	Review
Motwani et al. (2022).	Classification	Review ML frameworks for ubiquitous and smart healthcare monitoring.	ML frameworks improve healthcare monitoring efficiency but need better integration with healthcare systems.	Review
Eke et al. (2023).	Detection	Systematically map ML approaches for detecting and combating BYOD security threats.	ML approaches enhance the detection and mitigation of BYOD threats but face implementation challenges.	Systematic Mapping Review
Aldahiri et al. (2021).	Prediction	Examine trends in the use of IoT with ML for health prediction systems.	IoT combined with ML provides accurate health predictions, though scalability remains a challenge.	Review
Hazratifard et al. (2022).	Authentication	Explore the use of ML for dynamic authentication in telehealth systems.	ML-based dynamic authentication improves security in telehealth but needs continuous updates.	Tutorial
Injadat et al. (2021).	Various	Discuss ML applications, challenges, and opportunities in intelligent systems.	ML offers numerous opportunities in intelligent systems but faces significant implementation challenges.	Review
Bouchama and Kamal (2021).	Detection	Enhance cyber threat detection through ML-based behavioral modeling of network traffic patterns.	Behavioral modeling using ML enhances threat detection but requires extensive training data.	Case Study

Gadal et al. (2022).	Anomaly Detection	Use ML-based anomaly detection with K-Means Array and Sequential Minimal Optimization.	The approach is effective for anomaly detection but needs more efficient algorithms.	Experimental Study
Bhuva and Kumar (2023).	Authentication	Develop a novel continuous authentication method for IoT devices using biometrics.	Biometrics-based continuous authentication enhances security but faces privacy concerns.	Experimental Study
Rabbani et al. (2021).	Detection	Review ML approaches for detecting malicious behavior in network traffic.	ML is effective for detecting malicious network behavior but requires real-time capabilities.	Review
Huang et al. (2022).	Resilience	Investigate reinforcement learning to enhance cyber-resilient behavior in network traffic.	Reinforcement learning improves cyber resilience but needs more adaptive strategies.	Review
Cui et al. (2019).	Authentication	Explore adaptive authentication methods based on reinforcement learning.	Adaptive authentication using RL is effective but requires continuous learning.	Conference Paper
Xiao et al. (2021).	Authentication	Develop RL-based physical-layer authentication for controller area networks.	RL-based authentication improves security but needs better integration with physical-layer protocols.	Journal Article
Xu et al. (2019)	Authentication	Implement voltage-based authentication using reinforcement learning.	Voltage-based RL authentication is effective but faces implementation challenges.	Conference Paper
Chan et al. (2023)	Various	Review deep neural networks' applications, challenges, and research directions in the cloud.	Deep neural networks enhance cloud applications but face challenges in data privacy and scalability.	Review
Sharma et al. (2023).	Healthcare Monitoring	Discuss the use of deep learning in IoT for medical and healthcare applications.	Deep learning significantly improves IoT-based healthcare but requires better data handling.	Book Chapter
Sharma and Garg (2024).	Healthcare Monitoring	Explore deep learning applications in IoT for next-generation healthcare solutions.	Deep learning offers advanced solutions for healthcare IoT, but it needs robust security measures.	Edited Book

Table 5. Risk of Bias

Article	**Selection Bias**	**Performance Bias**	**Detection Bias**	**Reporting Bias**	**Overall Risk of Bias**
Hameed et al. (2021).	Low	Low	Medium	Medium	Low

Sharma et al. (2021).	Medium	Low	Low	Low	Low
Motwani et al. (2022)	Medium	Low	Low	Low	Low
Eke et al. (2023).	Low	Medium	Low	Medium	Low
Aldahiri et al. (2021).	Low	Low	Low	Low	Low
Hazratifard et al. (2022).	Medium	Low	Low	Medium	Medium
Injadat et al. (2021).	Low	Medium	Low	Low	Low
Bouchama and Kamal (2021).	Low	Low	Low	Low	Low
Gadal et al. (2022).	Low	Low	Medium	Medium	Medium
Bhuva and Kumar (2023).	Medium	Low	Low	Low	Low
Rabbani et al. (2021).	Low	Medium	Low	Low	Medium
Huang et al. (2022)	Low	Low	Low	Low	Low
Cui et al. (2019).	Low	Low	Medium	Low	Low
Xiao et al. (2021).	Low	Medium	Low	Low	Low
Xu et al. (2019)	Low	Low	Medium	Low	Low
Chan et al. (2023).	Low	Medium	Low	Medium	Low
Sharma et al. (2023).	Medium	Low	Low	Low	Low
Sharma and Garg (2024).	Medium	Low	Low	Medium	Low

REFERENCES

1. Ahad, A., Jiangbina, Z., Tahir, M., Shayea, I., Sheik, M. A., & Rasheed, F. (2024). 6G and Intelligent Healthcare: Taxonomy, Technologies, Open Issues and Future Research Directions. Internet of Things, 101068.
2. Akhtar, Z., & Buriro, A. (2021). Multitrait Selfie: Low-Cost Multi-modal Smartphone User Authentication. Biometric Identification Technologies Based on Modern Data Mining Methods, 159-175.
3. Aldahiri, A., Alrashed, B., & Hussain, W. (2021). Trends in using IoT with machine learning in health prediction systems. Forecasting, 3(1), 181-206.
4. Alder, S. (2020). Universal Health Services confirms all US hospitals are affected by a ransomware attack. HIPAA Journal. https://www.hipaajournal.com/universal-health-services-ransomware-attackcost/
5. Alder, S. (2021). Scripps Health ransomware attack cost estimate revised to $112.7 million. HIPAA Journal. https://www.hipaajournal.com/scripps-health-ransomware-attack-cost-113-million/
6. Alder, S. (2023). CommonSpirit Health increases ransomware attack cost estimate to $160 million. HIPAA Journal. https://www.hipaajournal.com/commonspirit-health-increases-ransomwareattack-cost-estimate-to-160-million/
7. Alder, S. (2025). Healthcare data breach statistics. HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

8. Alipio, M., & Bures, M. (2023). Current testing and performance evaluation methodologies of LoRa and LoRaWAN in IoT applications: Classification, issues, and future directives. Internet of Things, 101053.
9. Almestad, E. (2023). Exploring Explainable AI Adoption in Medical Diagnosis and the Empowering Potential of Collaboration at NTNU.
10. Al-Qarni, E. A. (2023). Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. International Journal of Advanced Computer Science and Applications, 14(5), Article 0140513. https://doi.org/10.14569/IJACSA.2023.0140513
11. Alqarni, M. A., Chaudhary, S. H., Malik, M. N., Ehatisham-ul-Haq, M., & Azam, M. A. (2020). Identifying smartphone users based on how they interact with their phones. Human-centric Computing and Information Sciences, 10(1), 7.
12. Alsellami, B., Deshmukh, P. D., Ahmed, Z. A., Tawfik, M., & Al-madani, A. M. (2021). Overview of Biometric Traits. 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA),
13. Alshaibi, A., Al-Ani, M., Al-Azzawi, A., Konev, A., & Shelupanov, A. (2022). The comparison of cybersecurity datasets. Data, 7(2), 22.
14. Al-Thani, D., Monteiro, S., & Tamil, L. S. (2020). Design for eHealth and telehealth. In Design for Health (pp. 67-86). Elsevier.
15. Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models—Internet of Things and Cyber-Physical Systems.
16. Alwidian, J., Elhassan, A., & Ghnemat, R. (2020). Predicting autism spectrum disorder using a machine learning technique. International Journal of Recent Technology and Engineering, 8(5), 4139-4143.
17. Alzahrani, A. O., & Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software-defined networks. Future Internet, 13(5), 111.
18. AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical systems and machine learning techniques. Soft Computing, 25(18), 12319-12332.
19. Anand, A., Rani, S., Anand, D., Aljahdali, H. M., & Kerr, D. (2021). An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications. Sensors, 21(19), 6346.
20. Angelopoulou, E., Papachristou, N., Bougea, A., Stanitsa, E., Kontaxopoulou, D., Fragkiadaki, S., Pavlou, D., Koros, C., Değirmenci, Y., & Papatriantafyllou, J. (2022). How can telemedicine improve the quality of care for patients with Alzheimer's disease and related dementias? A narrative review. Medicina, 58(12), 1705.
21. Balducci, F., De Carolis, B., Impedovo, D., & Pirlo, G. (2019). Touch dynamics for affective state recognition: your smartphone knows how you feel as soon as you unlock it. SAT@ SMC,
22. Baliga, R. R., & Itchhaporia, D. (2022). Digital Health, An Issue of Heart Failure Clinics, E-Book (Vol. 18). Elsevier Health Sciences.
23. Batista, E., Moncusi, M. A., López-Aguilar, P., Martínez-Ballesté, A., & Solanas, A. (2021). Sensors for context-aware smart healthcare: A security perspective. Sensors, 21(20), 6886.
24. Bellucci, N. (2022). Disruptive Innovation and Technological Influences on Healthcare. Journal of Radiology Nursing, 41(2), 98-101.
25. Bharadwaj, H. K., Agarwal, A., Chamola, V., Lakkaniga, N. R., Hassija, V., Guizani, M., & Sikdar, B. (2021). A review of the role of machine learning in enabling IoT-based healthcare applications. IEEE Access, 9, 38859-38890.
26. Bhattacharjee, A., Borgohain, S. K., Soni, B., Verma, G., & Gao, X.-Z. (2020). Machine Learning, Image Processing, Network Security and Data Sciences: Second International Conference, MIND 2020, Silchar, India, July 30-31, 2020, Proceedings, Part II (Vol. 1241). Springer Nature.
27. Bhuva, D. R., & Kumar, S. (2023). A novel continuous authentication method using biometrics for IOT devices. Internet of Things, 24, 100927.
28. Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive

to proactive: Current status and future recommendations. Journal of Medical Systems, 44(5), Article 98. https://doi.org/10.1007/s10916-019-1507-y

29. Binbeshr, F., Kiah, M. M., Por, L. Y., & Zaidan, A. A. (2021). A systematic review of PIN-entry methods resistant to shoulder-surfing attacks. Computers & Security, 101, 102116.
30. Bokolo, A. J. (2021). Application of telemedicine and eHealth technology for clinical services in response to the COVID-19 pandemic. Health and technology, 11(2), 359-366.
31. Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), 1-9.
32. Brito, L. C., Susto, G. A., Brito, J. N., & Duarte, M. A. V. (2021). Fault detection of bearing: An unsupervised machine learning approach exploiting feature extraction and dimensionality reduction. Informatics,
33. Buriro, A., Crispo, B., & Conti, M. (2019). AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones. Journal of information security and applications, 44, 89-103.
34. Cascella, M., Coluccia, S., Monaco, F., Schiavo, D., Nocerino, D., Grizzuti, M., Romano, M. C., & Cuomo, A. (2022). Different machine learning approaches for implementing telehealth-based cancer pain management strategies—Journal of Clinical Medicine, 11(18), 5484.
35. Chan, K. Y., Abu-Salih, B., Qaddoura, R., Ala'M, A.-Z., Palade, V., Pham, D.-S., Del Ser, J., & Muhammad, K. (2023). Deep neural networks in the cloud: Review, applications, challenges, and research directions: neurocomputing, 545, 126327.
36. Cola, G., Vecchio, A., & Avvenuti, M. (2021). Continuous authentication through gait analysis on a wrist-worn device: Pervasive and Mobile Computing, 78, 101483.
37. Cui, Z., Zhao, Y., Li, C., Zuo, Q., & Zhang, H. (2019). An adaptive authentication based on reinforcement learning. 2019 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW),
38. Drăgulinescu, A. M. C., Manea, A. F., Fratu, O., & Drăgulinescu, A. (2020). LoRa-based medical IoT system architecture and testbed. Wireless Personal Communications, 1-23.
39. Eke, C. I., Norman, A. A., & Mulenga, M. (2023). Machine learning approach for detecting and combating bring-your-own-device (BYOD) security threats and attacks: a systematic mapping review. Artificial Intelligence Review, 56(8), 8815-8858.
40. Elahe, M. F., Jin, M., & Zeng, P. (2021). Review of load data analytics using deep learning in smart grids: Open load datasets, methodologies, and application challenges. International Journal of Energy Research, 45(10), 14274-14305.
41. Ellavarason, E., Guest, R., & Deravi, F. (2020). Evaluation of the stability of swipe gesture authentication across usage scenarios of a mobile device. EURASIP Journal on Information Security, 2020, 1-14.
42. Francis, J. G., & Francis, L. P. (2021). Sustaining surveillance: the importance of information for public health (Vol. 6). Springer.
43. Gadal, S., Mokhtar, R., Abdelhaq, M., Alsaqour, R., Ali, E. S., & Saeed, R. (2022). Machine learning-based anomaly detection using K-means array and sequential minimal optimization. Electronics, 11(14), 2158.
44. Garfan, S., Alamoodi, A. H., Zaidan, B., Al-Zobbi, M., Hamid, R. A., Alwan, J. K., Ahmaro, I. Y., Khalid, E. T., Jumaah, F., & Albahri, O. S. (2021). Telehealth utilization during the COVID-19 pandemic: A systematic review. Computers in biology and medicine, 138, 104878.
45. Ghosh, S., & Sharma, V. (2024). Tracking of Disease—A Review of the State of the Art of Technology for Next Generation Healthcare. Deep Learning in Internet of Things for Next Generation Healthcare, 242-268.
46. Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2022). Medical 4.0 technologies for healthcare: Features, capabilities, and applications. Internet of Things and Cyber-Physical Systems, 2, 12-30.
47. Hameed, S. S., Hassan, W. H., Latiff, L. A., & Ghabban, F. (2021). A systematic review of security and privacy issues in the internet of medical things: the role of machine learning approaches: PeerJ Computer Science, 7, e414.

48. Hazratifard, M., Agrawal, V., Gebali, F., Elmiligi, H., & Mamun, M. (2023). Review of using machine learning in secure IoT healthcare. In Accelerating Strategic Changes for Digital Transformation in the Healthcare Industry (pp. 237-269). Elsevier.
49. Hazratifard, M., Gebali, F., & Mamun, M. (2022). Using machine learning for dynamic authentication in telehealth: A tutorial. Sensors, 22(19), 7655.
50. Healthcare Information and Management Systems Society (HIMSS). (2024). 2024 HIMSS healthcare cybersecurity survey. HIMSS. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey/
51. Hilty, D., Peled, A., & Luxton, D. D. (2023). Predictive Modeling, Artificial Intelligence, and Machine Learning in Psychiatric Assessment and Treatment. In Tasman's Psychiatry (pp. 1-22). Springer.
52. Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement learning for feedback-enabled cyber resilience. Annual reviews in control, 53, 273-295.
53. Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2021). Machine learning towards intelligent systems: applications, challenges, and opportunities. Artificial Intelligence Review, 54(5), 3299-3348.
54. Ismail, A., Abdlerazek, S., & El-Henawy, I. M. (2020). Development of a smart healthcare system based on speech recognition using a support vector machine and dynamic time warping. Sustainability, 12(6), 2403.
55. Joymangul, J. S., Sekhari, A., Moalla, N., & Grasset, O. (2019). Data-oriented approach to improve adherence to CPAP therapy during the initiation phase. 2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA),
56. Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., Abdulkarim, M., Shuaibu, A. N., Garba, A., & Sahalu, Y. (2022). Recent advancements in emerging technologies for healthcare management systems: A survey. Healthcare,
57. Kaiafas, G., Hammerschmidt, C., Lagraa, S., & State, R. (2019). Auto Semi-supervised Outlier Detection for Malicious Authentication Events. Joint European Conference on Machine Learning and Knowledge Discovery in Databases,
58. Li, N., Xu, M., Li, Q., Liu, J., Bao, S., Li, Y., Li, J., & Zheng, H. (2023). A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. Security and Safety, 2, 2022010.
59. Li, W., Tan, J., Meng, W., Wang, Y., & Li, J. (2019). SwipeVLock: a supervised unlocking mechanism based on swipe behavior on smartphones. Machine Learning for Cyber Security: Second International Conference, ML4CS 2019, Xi'an, China, September 19-21, 2019, Proceedings 2,
60. Li, Y., Zhang, Z., Dai, C., Dong, Q., & Badrigilan, S. (2020). Accuracy of deep learning for automated detection of pneumonia using chest X-Ray images: A systematic review and meta-analysis— Computers in Biology and Medicine, 123, 103898.
61. Life, B. U.-N. (2023). Qualitative Study on the Telehealth Experience of Mental Health Clinicians Who Provided Outpatient Services During the COVID-19 Pandemic, Capella University.
62. M. Bublitz, F., Oetomo, A., S. Sahu, K., Kuang, A., X. Fadrique, L., E. Velmovitsky, P., M. Nobrega, R., & P. Morita, P. (2019). Disruptive technologies for environment and health research: an overview of artificial intelligence, blockchain, and internet of things. International journal of environmental research and public health, 16(20), 3847.
63. Miloslavskaya, N. (2020). Stream data analytics for predicting network attacks. Procedia Computer Science, 169, 57-62.
64. Motwani, A., Shukla, P. K., & Pawar, M. (2022). Ubiquitous and smart healthcare monitoring frameworks based on machine learning: A comprehensive review. Artificial Intelligence in Medicine, 134, 102431.
65. Nandy, G. (2022). Telehealth Security from a User's Perspective: Moving beyond COVID-19 and into a New Normal, University of Nebraska at Omaha.
66. Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2(3), 1-44.
67. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organizations: A systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

68. Osama, M., Ateya, A. A., Sayed, M. S., Hammad, M., Pławiak, P., Abd El-Latif, A. A., & Elsayed, R. A. (2023). Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions. Sensors, 23(17), 7435.
69. Page, M.J., et al. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. Systematic Reviews, 10, Article No. 89. https://doi.org/10.1186/s13643-021-01626-4
70. Parashar, A., Parashar, A., Shabaz, M., Gupta, D., Sahu, A. K., & Khan, M. A. (2024). Advancements in artificial intelligence for biometrics: a deep dive into model-based gait recognition techniques. Engineering Applications of Artificial Intelligence, 130, 107712.
71. Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of the healthcare sector: A study on privacy and security concerns. ICT Express, 9(4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007
72. Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Bagheri Baba Ahmadi, S., & Ayobi, S. (2021). A review of machine learning approaches for network malicious behavior detection in emerging technologies. Entropy, 23(5), 529.
73. Rasool, R. U., Ahmad, H. F., Rafique, W., Qayyum, A., & Qadir, J. (2022). Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. Journal of Network and Computer Applications, 201, 103332.
74. Ray, S., Mishra, K. N., & Dutta, S. (2022). Detection and prevention of DDoS attacks on M-healthcare sensitive data: A novel approach. International Journal of Information Technology, 14(3), 1333– 1341. https://doi.org/10.1007/s41870-022-00869-1
75. Rose, R. V., Kumar, A., & Kass, J. S. (2023). Protecting privacy: Health Insurance Portability and Accountability Act of 1996, Twenty-First Century Cures Act, and social media. Neurologic Clinics, 41(3), 513-522.
76. Schünke, L. C., Mello, B., da Costa, C. A., Antunes, R. S., Rigo, S. J., de Oliveira Ramos, G., da Rosa Righi, R., Scherer, J. N., & Donida, B. (2022). A rapid review of machine learning approaches for telemedicine in the scope of COVID-19. Artificial Intelligence in Medicine, 129, 102312.
77. Senbekov, M., Saliev, T., Bukeyeva, Z., Almabayeva, A., Zhanaliyeva, M., Aitenova, N., Toishibekov, Y., & Fakhradiyev, I. (2020). The recent progress and applications of digital technologies in healthcare: A review. International Journal of Telemedicine and Applications, 2020, 1–18. https://doi.org/10.1155/2020/8830200
78. Sharma, A., Sharma, A., Virmani, R., Kumar, G., Virmani, T., & Chitranshi, N. (2023). Deep learning IoT in medical and healthcare. In Deep Learning in Personalized Healthcare and Decision Support (pp. 245-261). Elsevier.
79. Sharma, S., Singh, G., & Sharma, M. (2021). A comprehensive review and analysis of supervised-learning and soft computing techniques for stress diagnosis in humans. Computers in biology and medicine, 134, 104450.
80. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.
81. Smith-Creasey, M., & Rajarajan, M. (2019). A novel word-independent gesture-typing continuous authentication scheme for mobile devices. Computers & Security, 83, 140-150.
82. Tawfik, G. M., Dila, K. A. S., Mohamed, M. Y. F., Tam, D. N. H., Kien, N. D., Ahmed, A. M., & Huy, N. T. (2019). A step-by-step guide for conducting a systematic review and meta-analysis with simulation data. Tropical medicine and health, 47(1), 1-9.
83. Tay Wee Teck, J., Butner, J. L., & Baldacchino, A. (2023). Understanding the use of telemedicine across different opioid use disorder treatment models: A scoping review. Journal of Telemedicine and Telecare, 1357633X231195607.
84. van Kolfschooten, H., & van Oirschot, J. (2024). The EU Artificial Intelligence Act (2024): Implications for healthcare. *Health Policy*. https://doi.org/10.1016/j.healthpol.2024.105152
85. Wang, R., & Tao, D. (2019). DTW-KNN implementation for touch-based Authentication System. 2019 5th International Conference on Big Data Computing and Communications (BIGCOM),
86. Webster, M. (2021). Do No Harm: Protecting Connected Medical Devices, Healthcare, and Data from Hackers and Adversarial Nation States. John Wiley & Sons.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

87. Wherton, J., Greenhalgh, T., Hughes, G., & Shaw, S. E. (2022). The role of information infrastructures in scaling up video consultations during COVID-19: mixed methods case study into opportunity, disruption, and exposure. Journal of Medical Internet Research, 24(11), e42431.
88. Wickramasinghe, I., & Kalutarage, H. (2021). Naive Baes: applications, variations, and vulnerabilities: a review of literature with code snippets for implementation. Soft Computing, 25(3), 2277-2293.
89. Xiao, L., Lu, X., Xu, T., Zhuang, W., & Dai, H. (2021). Reinforcement learning-based physical-layer authentication for controller area networks. IEEE Transactions on Information Forensics and Security, 16, 2535-2547.
90. Xu, T., Lu, X., Xiao, L., Tang, Y., & Dai, H. (2019). Voltage-based authentication for controller area networks with reinforcement learning. ICC 2019-2019 IEEE International Conference on Communications (ICC),
91. Yi, T., Chen, X., Zhu, Y., Ge, W., & Han, Z. (2023). Review of the application of deep learning in network attack detection. Journal of Network and Computer Applications, 212, 103580.
92. Yu, C., Li, H., & Wang, X. (2019). SVD-based image compression, encryption, and identity authentication algorithm on the cloud. IET Image Processing, 13(12), 2224-2232.