ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

AI-Driven Threat Intelligence in Healthcare Cybersecurity: A Comprehensive Survey

Dr. Sumathy Kingslin[1], Thasleem R[2]

[1]Associate Professor, Department of Computer Science, Quaid-E-Millath Govt College for Women (A), Chennai, India

[2]Research Scholar, Department of Computer Science, Quaid-E-Millath Govt College for Women (A), Chennai, India

DOI: https://doi.org/10.51244/IJRSI.2025.120700106

Received: 15 July 2025; Accepted: 18 July 2025; Published: 05 August 2025

ABSTARCT

This study explores how Artificial Intelligence (AI) can be effectively applied across critical cybersecurity functions in the healthcare domain by analyzing four focused themes. These include real-time threat detection using supervised machine learning, interpretable threat intelligence via explainable AI (XAI), NLP-based cyber threat monitoring from open-source data, and intelligent Identity and Access Management (IAM) systems for insider threat mitigation. Each theme is investigated through selected peer-reviewed studies that collectively demonstrate AI's role in automating threat detection, improving prediction accuracy, enhancing model transparency, and securing access to Electronic Health Records (EHRs). The review also identifies core challenges such as limited real-world deployment, lack of model interpretability, and insufficient multilingual threat processing. Finally, this paper proposes future enhancements including federated AI models, real-time NLP pipelines, and adaptive IAM systems tailored for evolving threats in clinical environments.

Keyword: Artificial Intelligence (AI), Healthcare Cybersecurity Threat Detection Explainable AI (XAI) Natural Language Processing (NLP) Identity and Access Management (IAM) Insider Threats

Scope:

The scope of this research is centered on evaluating and synthesizing the role of AI in enhancing healthcare cybersecurity through four core focus areas:

1. **Real-Time Threat Detection**: Evaluate supervised machine learning techniques applied to detect threats in healthcare systems and EHR environments in real time.

2. **Explainable AI in Cybersecurity**: Explore how XAI techniques like SHAP and LIME improve the interpretability and trustworthiness of machine learning models used for malware and anomaly detection.

3. **NLP-Driven Threat Intelligence**: Analyze the use of Natural Language Processing to mine cyber threat intelligence from forums, dark web sources, and social media for early warning systems.

4. **AI-Enhanced IAM Systems**: Assess the implementation of AI in behavior-based access control, continuous authentication, and insider threat detection within healthcare IAM infrastructures.

INTRODUCTION

Digital transformation in healthcare has brought about significant advancements in patient care and operational efficiency. However, it has also expanded the cybersecurity attack surface, especially with the rise of Electronic Health Records (EHRs), telemedicine, and connected medical devices. Traditional rule-based security systems are no longer sufficient to manage the growing complexity and scale of cyber threats.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

Artificial Intelligence (AI) offers promising solutions by enhancing threat detection, automating response mechanisms, and improving the resilience of healthcare systems. This paper structures the survey around four critical AI applications within cybersecurity:

- First, **real-time threat detection** using supervised machine learning models enables rapid identification of network anomalies and unauthorized behaviors.
- Second, **explainable AI** techniques address the black-box nature of ML models, making threat intelligence interpretable and trustworthy in sensitive healthcare contexts.
- Third, **NLP-driven threat intelligence** captures emerging threats by analyzing unstructured data from forums, social media, and the dark web.
- Finally, **AI-enhanced IAM systems** leverage behavioral analytics for proactive insider threat mitigation and dynamic access control.

Together, these four thematic pillars form the foundation for understanding the current landscape and future potential of AI in safeguarding healthcare infrastructure against cyber threats.

Real-Time AI-Based Threat Detection in Healthcare Networks:

Objective

Real-time AI-based threat detection is crucial in the healthcare domain, where delays in identifying cybersecurity threats can compromise patient safety and data integrity. Gandhi (2025) developed a supervised ML system trained on simulated EHR data, capable of identifying anomalous network behaviors indicative of intrusion attempts. Kohli et al. (2023) extended this approach using real cybersecurity logs, showcasing a practical model for real-time anomaly detection. These approaches demonstrate that AI, particularly supervised learning, significantly improves early threat detection and system responsiveness compared to rule-based methods.

- The application of supervised learning for detecting threats in real-time
- Effectiveness of AI models using simulated and real datasets
- Integration into existing healthcare IT infrastructure
- Practical concerns such as system latency and alert generation accuracy

Combined Analysis:

Application:

Both studies aim to deploy real-time AI models that monitor healthcare systems for threats such as unauthorized access or data exfiltration. Gandhi's model, though tested in simulation, identifies internal threats quickly, while Kohli's implementation works on real-world network logs, generating alerts for suspicious activity with minimal delay.

Techniques:

Gandhi (2025) used supervised ML techniques such as Decision Trees and SVMs to build models trained on synthetic EHR breach data. Kohli et al. (2023) incorporated ensemble methods (Random Forests) and real-time preprocessing pipelines to handle streaming log data, focusing on minimizing false positives while maintaining high sensitivity.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

Research gap:

Gandhi's study lacks scalability testing and was not validated in live environments. Kohli's model, although practical, does not address interpretability, which is essential for clinical integration.

Futurework:

Future work should focus on deploying these models across distributed healthcare environments, incorporating federated learning to preserve data privacy. Integrating these models with IAM and SIEM platforms will further enhance response mechanisms.

Explainable AI for Interpretable Threat Intelligence:

Objective:

As AI becomes deeply embedded in cybersecurity, the need for transparency grows. Siddiqi et al. (2024) demonstrated the use of explainable AI (XAI) frameworks like LIME and SHAP to interpret predictions made by ML models detecting malware in healthcare environments. K.E. (2021) reviewed a wide range of ML algorithms in cybersecurity and underscored the limitations of black-box models. The integration of interpretability tools ensures AI systems not only detect threats but also provide rationale for their decisions—critical in clinical and regulatory contexts.

- Importance of making AI decisions understandable in healthcare
- Integration of XAI tools with ML threat detection models
- Trade-offs between accuracy and interpretability
- Compliance and usability in clinical cybersecurity systems

Combined Analysis

Application:

These studies promote trust and usability in ML-based systems. Siddiqi et al. integrated XAI into malware detection workflows, enabling healthcare IT teams to understand which features triggered alarms. K.E.'s review highlights the need for such transparency across all ML applications in cybersecurity.

Techniques:

Siddiqi used Random Forest classifiers trained on labeled malware datasets (from Kaggle) and applied LIME/SHAP to highlight influential features for each prediction. K.E. categorized different ML approaches (SVM, KNN, RF, Deep Learning) based on complexity and explainability.

Research gap:

Despite high accuracy, Siddiqi's model has not been tested in dynamic environments. K.E. points out a lack of real-world implementations where interpretability tools are used effectively during incident response.

Future enhancement:

Future models should integrate human-in-the-loop systems for collaborative threat validation. Explainable dashboards tailored for healthcare professionals can bridge the AI-user gap, ensuring safer and faster threat mitigation.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

NLP-Driven Cyber Threat Intelligence from Open Sources:

Objective:

Open-source intelligence (OSINT) has become a valuable input for cyber threat detection, especially in healthcare. Ismail (2024) leveraged NLP to analyze social media and dark web discussions for early indicators of cyberattack planning. Meanwhile, Dutta & Kant (2020) proposed an AI-augmented Cyber Threat Intelligence (CTI) framework using honeypots and dark web crawlers. Both studies emphasize the proactive detection of threats before breaches occur.

- Extracting threat signals from social and dark web content
- Classification of textual threat data using NLP + ML
- Integration of threat intelligence with cybersecurity tools
- Ethical and technical challenges of monitoring OSINT

Combined Analysis

Application:

These techniques allow healthcare organizations to anticipate threats by monitoring external sources for attack indicators. Ismail's method detects sentiment and intent shifts in threat actor communication, while Dutta & Kant's system identifies specific Indicators of Compromise (IoCs) via honeypots.

Techniques:

Ismail used NLP methods such as Named Entity Recognition (NER) and sentiment analysis combined with supervised ML classifiers. Dutta & Kant applied Naive Bayes classifiers to structured indicators collected via threat monitoring infrastructure.

Research gap:

Ismail's system is not fully integrated with incident response pipelines. Dutta & Kant's framework lacks multilingual support and real-time capability.

Future enhancement:

Advancements should include real-time NLP pipelines, adaptive threat scoring models, and integration with SIEMs. Multilingual processing and AI ethics in surveillance must also be addressed.

AI-Enabled Identity and Access Management in Healthcare Security:

Objective:

Securing sensitive healthcare data requires stringent control over user access. Balan (2022) investigates AI-enhanced Identity and Access Management (IAM) systems that use behavior-based anomaly detection to identify potential insider threats. Complementing this, Gandhi (2025) emphasizes real-time threat detection in EHR systems, which can be extended to incorporate intelligent IAM. These studies demonstrate how AI can enforce continuous authentication, automate access control decisions, and flag suspicious behavior patterns.

- Leverage AI to automate access control and monitoring
- Detect insider threats based on behavioral deviations
- Strengthen authentication protocols in healthcare systems

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

- Reduce human error and privilege misuse in digital healthcare environments

Combined Analysis

Application:

IAM systems in hospitals can benefit from AI by not just authenticating users at login, but by continuously evaluating their behavior. For instance, an AI-based IAM system may detect if a nurse is accessing patient records outside their assigned department or during irregular hours—potentially flagging an insider threat.

Techniques:

Balan (2022) implemented ML-based anomaly detection using user behavior profiling. Gandhi's work, while focused on general EHR system security, provides an ideal extension point to fuse with IAM mechanisms through supervised learning to analyze login patterns, location, and device trust scores.

Research gap:

Current systems lack context-aware access control—AI models rarely account for environmental or situational variables (e.g., emergency scenarios vs. routine access). There's also a limited number of studies that validate IAM-AI integration in live hospital settings.

Future enhancement:

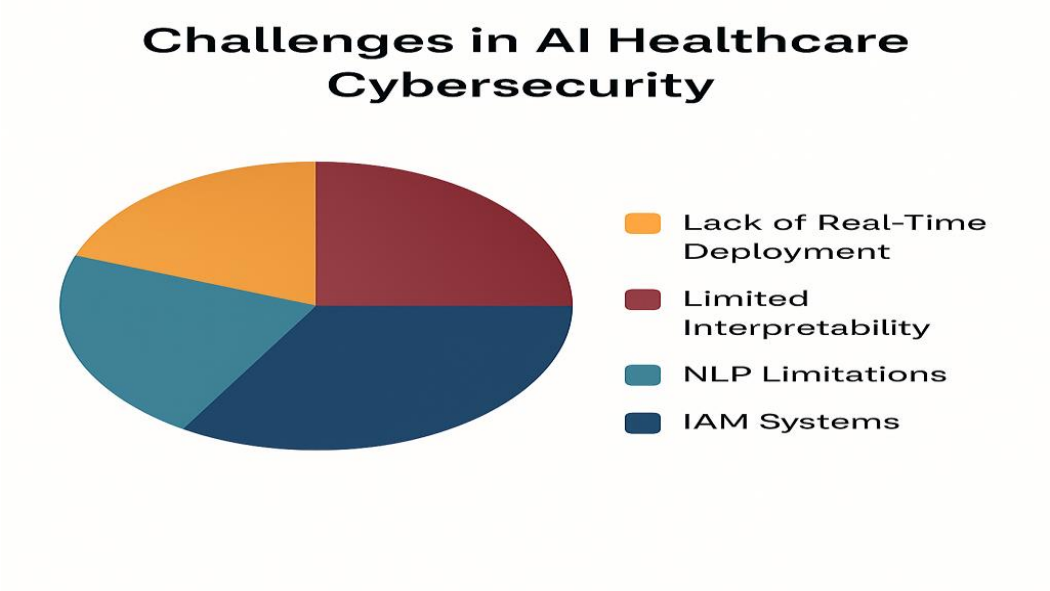
Development of adaptive IAM systems using reinforcement learning could allow real-time policy updates. Moreover, combining federated learning with IAM will allow different hospitals to improve security collaboratively without sharing sensitive patient data.

Comparative Analysis of Eight AI-Based Healthcare Cybersecurity Studies Across Four Core Domains

Pair No.	Ref No.	Core Focus	AI Techniques Used	Dataset	Key Contribution
1	[1] Gandhi (2025)	Real-time threat detection in healthcare systems	Supervised ML (SVM, Decision Tree)	Simulated EHR data	Developed ML models for anomaly detection in EHR systems
	[2] Kohli et al. (2023)	Real-time anomaly detection using live logs	Random Forest, Streaming Pipeline	Real cybersecurity logs	Implemented real-time threat detection system using real hospital network data
2	[3] Siddiqi et al. (2024)	Malware detection with explainability	Random Forest + Explainable AI (LIME, SHAP)	Kaggle malware dataset	Provided interpretable malware detection with high accuracy
	[4] K.E. (2021)	Review of AI applications in cybersecurity	Survey of ML techniques	No dataset (review paper)	Comprehensive review of ML models in cybersecurity contexts
3	[5] Ismail (2024)	Threat intent detection from open-source text	NLP (NER, Sentiment Analysis) + ML	Social media, forums	Detected malicious intent from unstructured online sources

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

	[6] Dutta & Kant (2020)	Threat intelligence from dark web & honeypots	Naive Bayes + CTI Framework	Dark web + honeypot logs	Proposed CTI model generating actionable intelligence using ML
4	[7] Balan (2022)	Insider threat detection via IAM	ML + Behavior Analytics	Behavioral logs (private)	Built IAM system for detecting suspicious access patterns
	[8] Gandhi (2025)	IAM integration for real-time access control	Supervised ML	Simulated EHR	Combined anomaly detection with access control for IAM security enhancement



Challenges And Limitation:

Despite the advancement of AI in healthcare cybersecurity, the literature reveals several pressing limitations across the four core domains:

1. Lack of Real-Time Deployment in Healthcare Environments

Gandhi [1] and Kohli et al. [2] present robust models for real-time threat detection, but both lack real-world deployment in live hospital systems. Their solutions are limited to simulated or static datasets, which do not reflect the operational complexity of healthcare networks.

2. Limited Interpretability in ML Systems

While Siddiqi et al. [3] utilize XAI frameworks such as SHAP and LIME for explaining ML predictions, these are not yet integrated into clinician-facing dashboards. As K.E. [4] notes, most models remain black-box systems that are difficult for non-technical users to understand, limiting trust and usability.

3. NLP Systems Lack Multilingual and Stream-Based Processing

Ismail [5] and Dutta & Kant [6] highlight the potential of NLP for extracting threat intelligence from forums and dark web data. However, current NLP pipelines struggle with multilingual data and cannot process inputs in real time, reducing their ability to provide early warnings.

4. IAM Systems Are Not Context-Aware or Scalable

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

IAM solutions proposed by Balan [7] and Gandhi [8] rely on static behavior-based rules and supervised ML models. These lack adaptability to situational contexts (e.g., emergency overrides, remote access needs) and have not been validated across multi-institutional deployments.

Future enhancement:

To address the above challenges, the following future enhancements are proposed for each research domain:

1. Federated Learning for Real-Time Threat Detection

To ensure privacy while improving accuracy, Gandhi [1] and Kohli et al. [2] should extend their models using federated learning, allowing institutions to collaboratively train AI systems without exposing sensitive patient data.

2. Explainable Dashboards for Clinician Usability

The work by Siddiqi et al. [3] should be extended to include clinician-friendly dashboards that present SHAP/LIME outputs in visual formats. This would enhance trust and allow faster, safer decisions by IT and clinical staff [4].

3. Multilingual, Real-Time NLP Pipelines

Building on the work of Ismail [5] and Dutta & Kant [6], future research should focus on real-time, multilingual NLP engines integrated with Security Information and Event Management (SIEM) systems to extract actionable cyber threat intelligence globally.

4. Context-Aware IAM Using Reinforcement Learning

To adapt access permissions based on real-time risk and context, IAM systems such as those by Balan [7] and Gandhi [8] should be enhanced using reinforcement learning. These systems can evolve policies dynamically based on user behavior, location, and urgency.

CONCLUSION:

This survey examined the transformative role of Artificial Intelligence (AI) in strengthening healthcare cybersecurity through four critical dimensions: real-time threat detection, explainable threat intelligence, NLP-based cyber threat mining, and AI-enhanced Identity and Access Management (IAM).

The review of eight key studies revealed promising applications of supervised learning [1][2], explainable AI [3][4], NLP for CTI [5][6], and behavioral IAM [7][8]. These technologies demonstrate the potential to automate threat detection, detect insider misuse, extract intelligence from open sources, and improve access control.

However, significant challenges remain: limited real-world deployment, poor interpretability, weak NLP generalization, and lack of context-awareness in IAM systems. To advance the field, future research should focus on federated AI deployment, real-time multilingual NLP integration, clinician-friendly explainability tools, and adaptive IAM powered by reinforcement learning.

By aligning technical innovation with ethical design, regulatory compliance, and clinical usability, AI can become a powerful ally in defending healthcare systems against increasingly complex cyber threats.

REFERENCES

1. Gandhi, N. T. (2025). AI-Based Threat Detection in Healthcare Networks. IJCE&T, 57(2), 89–102.
2. Kohli, R. K., Chintha, V., Goel, O., & Goel, P. (2023). Cybersecurity Threat Detection Using Machine Learning. IJCRT, 57(2), 89–102.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

3. Siddiqi, F., et al. (2024). Machine Learning-Based Cyber Threat Detection: Explainable AI Insights. HISI, 6(1), 61–90.
4. K.E. (2021). ML in Cybersecurity: A Technological Review. Computer Science Review, 39, 100317.
5. Ismail, W. S. (2024). Threat Detection Using AI and NLP. JISIS, 14(1), 195–205.
6. Dutta, A., & Kant, S. (2020). Overview of CTI and AI/ML. ICISS 2020, LNCS 12553, 81–86.
7. Balan, M. (2022). AI-Powered IAM and Threat Intelligence in Healthcare. ResearchGate.
8. Gandhi, N. T. (2025). (Same as [1] but also cited under IAM integration).