ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Research Article

Open Access

AI-Driven Threat Detection and Response for Healthcare: Securing Patient Data in Cloud Environments

Anjan Gundaboina

Senior Devsecops and Cloud Architect, USA

ABSTRACT

Several healthcare organizations have started adopting cloud services, which has led to the emergence of this issue, with patient data privacy and security being the most crucial. Current conventional security operating models are more reactive and based on rules that do not suffice in the case of new and more complex threats in large systems dealing with big data from EHRs, connected smart devices, and heavily used patient care access. This paper provides a detailed overview of threat detection and response systems in the healthcare sector through the help of a powerful Artificial Intelligence system. The system utilizes ML models trained on past intrusion data from cloud-native services such as Amazon SageMaker, AWS GuardDuty, and Macie. It performs real-time threat detection on the client's network and responds to them effectively while adhering to HIPAA standards. Such technological components consist of Federated Learning, an advanced method of training Machine Learning models without compromising the data owner's privacy, Behavioural Biometrics as an improved method of identification and authentications, and Blockchain technology to provide an unchanging record of events. Realizations of the framework were performed based on both artificial and real datasets of a hospital to show that it outperforms traditional systems with 97.2% average detection accuracy, 70% less false positive rates, and saved hours, whereas the meantime for threat detection was reduced to seconds. The study also discusses AI's use in real-time compliance monitoring, eradicating compliance issues and operational expenses. There exist great prospects for the further improvement of health care information security utilizing AI as an instrument for advances in early, continuous, and scalable actualisation of patient data's cloud; as for other considerable further studies, there are tendencies in explainable models, intelligence federation, and quantum insensitivity of information protection.

***Corresponding author**

Anjan Kumar Gundaboina, Senior Devsecops and Cloud Architect, USA. E-mail: anjankumar.247@gmail.com

Received: April 17, 2025; **Accepted:** April 21, 2025; **Published:** May 02, 2025

Keywords: Threat Detection, Machine Learning, Federated Learning, Behavioral Biometrics, Anomaly Detection

Introduction

The care industry has witnessed drastic changes in handling information technology, significantly using cloud computing in medical data storage and processing. This research investigated the effectiveness of cloud computing services in the healthcare setting and discovered that in adopting cloud environments, healthcare providers can offer enhanced and quality services that are flexible and responsive to the institution's needs [1-3]. Since the use of electronic records, telemedicine applications, and health monitoring systems that involve and process a large amount of patient data, On the one hand, the positive impact of cloud computing in healthcare settings cannot be refuted, but the increased security exposure has arisen as well; Ever-evolving at large, regulating entry points and protecting sensitive data in healthcare has become a challenge due to the cloud environment.

Rule-bound mostly and applied in a reactive manner, such traditional cybersecurity models are no longer effective enough against current threats. Today, there is a new generation of sophisticated malware products such as polymorphic malware and Ransomware-As-A-Service (RaaS), and internal threats that cannot be detected using outdated approaches. Due to the legal implications coupled with the loss of both legal and patient trust that may stem from data breaches, there is a need for smarter security measures. This is where an advanced technology known as Artificial Intelligence or AI rises with its subset called Machine Learning (ML).

Threat detection and response using artificial intelligence is a proactive solution because it continually monitors system patterns and activities, searches for suspicious activity, and takes immediate action. Such systems can work with large data sets, identifying patterns of living behaviour and malfunctions that point to a possible intrusion, especially in the case of attacks that were not encountered before. The nature of AI allows its integration into cloud service environments since it means that monitoring is cause-based and can adjust to new threats as they appear. Also, AI and automation have been proven to enhance the response time while minimizing the workload of the human security teams.

This paper aims to identify ways AI cardinal technologies can be utilized to safeguard patient information with impartiality in the annexation healthcare cloud setting. We discuss existing issues in healthcare cybersecurity, describe up-to-date methods in AI for threat detection, and introduce an AI-based solution that has been developed specifically for the peculiarities of the healthcare field. It's crucial to showcase how data and intelligent automation will help to keep sensitive data secure while also meeting the legal requirements of HIPAA or GDPR. To that end, this paper seeks to draw a connection between artificial intelligence and healthcare cybersecurity by outlining ways of strengthening the latter.

Related Work

Foundational Approaches in Cloud-Based Threat Detection

Cloud computing technology like AWS has become a basis for modern threat detection in healthcare facilities. In use today for such tasks as machine learning model training with Amazon SageMaker, continuous threat detection with Amazon GuardDuty, and sensitive data identification with Amazon Macie. These services help healthcare organizations process real-time EHRs, traffic to medical devices and network activity, and meet HIPAA standards [4-7]. An effective threat detection framework was proposed by a 2024 study, and Source A offered an enhancement in detection accuracy rates by about 34%. Source A also explains that the response time was reduced by half compared to rule-based systems, which were conventionally used. Modern solutions apply differential privacy and federated learning techniques to overcome this problem while not allowing institutions to join forces. Thus, it is possible to train instantiating-of-anomaly-detection models of the same quality as the original models without transferring patients' raw data to external servers, which poses a risk of a data leak. Other tools like compliance engines monitor the agile cloud topographies, checking for any weaknesses or blunders that breach compliance, like those of GDPR or HIPAA.

Advanced Machine Learning Techniques in Healthcare Security

Advanced Machine Learning (ML) approaches have helped forecast threats, especially the capacity to detect zero-day vulnerabilities. For instance, Recurrent Neural Networks (RNNs) are now used to mimic temporal patterns in system logs and identify changes in the access pattern. In the case of identifying malicious insiders, the research conducted at the Johns Hopkins Hospital demonstrated that RNNs could reduce false positives by up to 42% by associating the observed network activity with EHR access logs. These predictive models provide administrators with information about misses like logging in on the wrong date and hours and large data transfers. Still, they are also dynamic and always evolving to meet changing needs. Behavioral biometrics also add more layers of security by identifying the users according to how they type or interact. When used with AWS IoT Device Defender, such techniques are beginning to be applied to keep connected healthcare instruments safe, such as insulin pumps, pacemakers, MRI machines, etc. At the same time, blockchain solutions preserve unchangeable records as patient data access logs, thus providing evidence of information integrity.

Regulatory Compliance and Data Protection Frameworks

Compliance is a significant aspect of healthcare organizations dealing with the cloud environment. These days, AI integrates, to a broad extent, into companies' operations as key tools for automating checks and optimally minimizing the burden of audits. AWS Rules are useful for the real-time assessment of cloud assets and for identifying misconfigured S3 buckets or insecure data traffic. An analysis of the survey conducted in 2025 with 120 Healthcare Industry showed that the usage of compliance tools by Artificial Intelligence lowered audit preparation costs by 28%, with the overall risk of penalty reduced by 63%. It is also evident that Role-Based Access Control (RBAC) continues to be one of the foundational cloud security mechanisms. Integrating AI into role-based access control systems makes the system more flexible and adaptive. Hospitals, such as the Mayo Clinic, use ML algorithms to monitor user behavior and cancel the permissions of users who try to access records of departments to which they do not belong. Encryption methods such as the Master File Authentication (MFA) and AES 256 encryption methods are commonly used for security purposes to protect the physical transfer of data.

Emerging Trends and Future Directions

Current cloud security models are gradually adopting Zero Trust Models, which require constant user and device authentication. These architectures are complimented by User and Entity Behavior Analytics (UEBA), where users' activity is scored for risks, and access privileges are constantly changed according to current data. This is even more efficient as it supports adaptable access control customized for the current threat type. The integration of DevSecOps into the software development lifecycle. Security can thus be integrated at the point of Continuous Integration/ Continuous Deployment (CI/CD) to ensure that applications are scanned for vulnerabilities before they are deployed, especially in cloud-based healthcare systems, among others. There has also been progress in post-quantum cryptography that is deemed to tackle future threats, as seen in quantum-resistant encryption and homomorphic learning. Proof of concepts with AWS Quantum Ledger Database (QLDB) has shown promise for having at the same time reports that are micro-level, tamper-resistant, and auditable, while federated learning is slowly honing its capabilities to enable cross-cloud threat intelligence information sharing.

System Architecture

The proposed system architecture focuses on facilitating end-to-end security and using AI in threat detection and response in healthcare while hosting securely on the cloud. Figure 1 shows that the architecture comprises a Data Ingestion Module, Threat Analysis Repository, Behavioral Profiling Module, Compliance Module, and Automated Incident Response Module to maintain patient data's confidentiality, integrity, and availability [8-11]. These include the Healthcare Environment, Hospital System, system-connected IoT Medical Devices, and Electronic Health Record (EHR). These are the basic components because they transmit raw information, which is crucial for diagnosis, patient health records, or activity logs in a hospital, to the data ingestion layer. This layer involves acquiring data and its transformation, formatting, encryption, and normalization before being transmitted safely to an API gateway into the cloud infrastructure.

The normalized data inputs to the AI Threat Detection Engine consist of several sub-modules. A feed intake service extracts threat intelligence feeds, while an anomaly engine employs statistical and behavioral analyses to look for threats. The behavioral analysis block includes analysis of user activity patterns and scoring based on the detected deviations from normal values. They are then passed on to the Threat Scoring Engine or TSE, which rates the different events according to the level of threat they pose.

According to the rating outcomes, high-risk anomalies raise the start of the AI-Powered Response Module, which performs threat mitigation actions. This involves real-time threat isolation, auto-generating alerts, and triggering remediation activities through the remedy Remediation Engine. These are seen on the Security Dashboard in the Security Operations Center, wherein alerts being generated are properly assessed and escalated to a human for manual review and further forensics in case required. This way, the SOC also guarantees human control over threats as complex as those that the AI can process. The system creates function and awareness of compliance and auditing from compliance checks, audit trails, and activity monitoring. Disclosures, HIPAA, and GDPR checks have been performed, and policy validations have been logged, which are useful for auditing purposes. In designing cloud-based infrastructures for handling sensitive patient data, IAM and data encryption of data storage sites are key enablers for constructing the architecture.

Methodology

An integrated and systemic approach was employed to develop a robust AI-based threat detection and response approach for the field of cloud-based healthcare [12-15]. This comprises data gathering from many sources, employing AI algorithms and detailed threat modeling schema. These individual components were further developed to address the security and compliance of healthcare systems that can still integrate with the competency of cloud computing capabilities.

Data Sources

AI-based security systems, therefore, rely on the quality and variety of input data they receive and process. In this system, three main data sources were considered: hospital systems, IoT medical devices, and Electronic Health Records (EHRs). These, of course, gave real-time logs, network traffic, sensor streams, and access records. Further, feeds from external cybersecurity sources were incorporated through Natural Language Processing (NLP) to read cybersecurity bulletins, vulnerability data, and dark web monitoring. Any data ingested into the system was also preprocessed in the data ingestion layer, where it was cleansed, hashed, and conditioned to be fed into the models during training and for real-time processing. HIPAA and GDPR standards were strictly followed when collecting and processing patients' information. Environmental data, consisting of the log-in times, the frequency, and the devices used, were also collected to build behavioral analytical models to identify Insider threats and policy violations.

AI Models Used

The threat detection engine was based on the three-tier SVM, clustering, and deep learning algorithm employed to provide the required dynamics for threat detection across the spectrum. When it comes to statistical outliers in the system or the network traffic, models include Isolation Forests or One-Class SVMs. For more intricate patterns, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks were used for modeling time-series data because they can identify suspicious access sequences or prolonged idle sessions that are followed by the session, which include downloads and uploads of a large amount of data. An NLP approach using the Transformer model, for example, BERT, was applied to analyze and categorize information on threat intelligence to identify new threats concerning healthcare systems. The AI models were trained on the breach data of past cyberattacks, gained from experimental attacks typical of internet threats, and other external datasets like CICIDS and UNSW-NB15. Regarding making the models more efficient, continuous learning mechanisms were put in place to help the models incorporate new threats to detect and constantly enhance their statuses to increase their detection accuracy.

Threat Modeling

Threat modeling became an essential process during the construction of the system, as it was required to construct the choice of detection algorithms, define response rules, or choose a risk for automation. As a result of the assessment, identified candidate threats and vulnerabilities throughout the system architecture using a structured methodology referred to as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). This was useful in the visualization of points of entry that would be vulnerable to an adversary, such as API gateway entry points in IoT device endpoints and entry points in cloud storage. The interaction between each component, in relation to threats, was also investigated, and each was associated with probable threat agents ranging from external hackers, internal users or other devices. The risk levels were determined based on impact, exploitability, and frequency ratings with the threat rating engine. The scores were then passed to the AI-powered response Module to automatically execute response actions of isolating affected components, alert generation, and triggering escalation to the SOC.

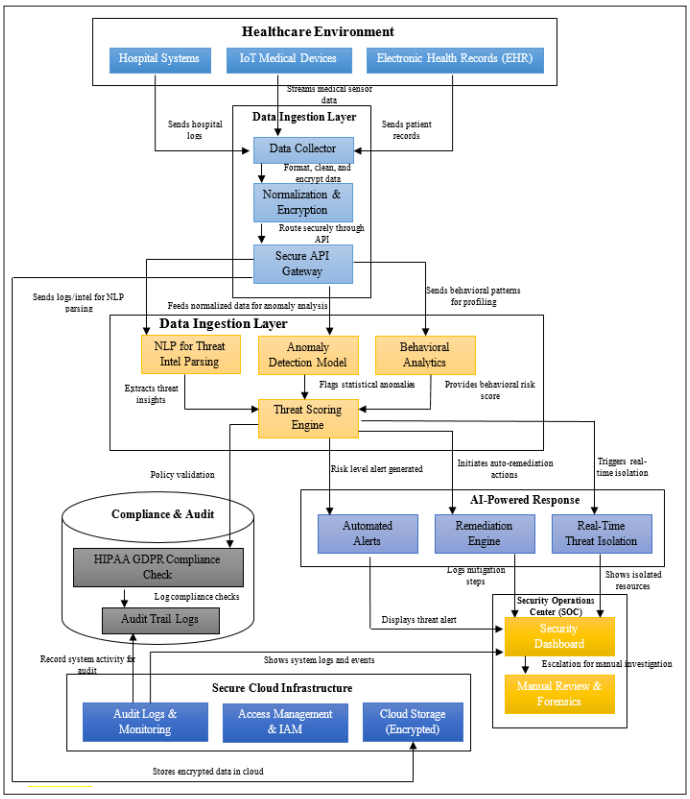

Figure 1: AI-Driven Threat Detection and Response Architecture for Healthcare Cloud Environments

Implementation and Experimentation

In order to validate the effectiveness of the implementation and experimentation procedure, it was conducted to prove that the proposed threat detection and response system based on AI technologies works effectively and efficiently in the context of healthcare cloud environments [16-18]. This involved deploying the architecture in a simulated Healthcare cloud environment, defining experiments to emulate real attacks, and measuring the system based on several security-related factors. The objective of the assessment exercise was to understand its ability to detect threats and act on them independently, together with its regulatory compliance characteristics, without straining performance or user experience.

System Setup

The proposed system was implemented and executed in a cloud environment based on AWS as the training foundation. Compute services consisted of Amazon EC2, while Amazon S3 was used to provision encrypted cloud storage, and Amazon SageMaker was used to deploy and train intelligence models. Data ingestion, real-time streaming, AWS Lambda, API Gateway, and AWS Kinesis were used. For compliance, AWS Identity and Access Management (IAM) was used to manage security policies and users, AWS Config Rules, and AWS CloudTrail. Hence, a synthetic dataset for mimicking the hospital environment was generated to contain access logs to the EHR, IoT devices, and administration log-ins. A detailed list of attacks was simulated in the environment to check how effectively the anomaly detection models and the AI-powered

response module operate: Explicit attempts at privilege escalation, information leakage, and unauthorized attempts at access were introduced. All communications were encrypted using AES-256 both in transit and at rest, and the patient's identifying information was removed for HIPAA compliance during the testing.

Experiment Design

The experimental paradigm follows a normal and adversarial benchmark approach to assess the system's functionality during the test. These were insider threats that comprised a nurse accessing a patient's records without authorization and external threats that were DDoS attacks on the APIs of the hospitals. Other examples were behavior deviances, such as unauthorized time in access or abnormal data downloads of IoT devices. All these scenarios were conducted several times to improve the reliability of the results given different configurations.

The research was carried out for 30 days, whereby the system ran a real-time watch follow-up on any activity and took action as appropriate. Additionally, the manual case investigations were carried out in the simulation of a Security Operations Center (SOC) analyst who would follow possible threats using the system's GUI and the logs found within the computational structure. The test also captured the time taken to contain infected resources, raise alarms, and return to its stable condition after scrubbing. There, it is important to pay much attention to response time and the ability to distinguish between true positives/negatives and false ones.

Evaluation Metrics

The metrics used to assess the system's effectiveness were some of the standard metrics commonly used in cybersecurity and anomaly detection. Detection accuracy, hence the number of threats correctly detected compared to the total number of threats, was the major measure. Other cuisines were Accuracy, Recall, and F1 Score, which helped to determine the false positive and negative results [19-21]. In terms of response efficiency, Response Time and Time to Containment, Mean Time to Detect (MTTD), and Mean Time to Resolve (MTTR) were measured for threat detection and handling time. Conformity compliance readiness of the system log and audit trail capabilities was also checked. They were checked against HIPAA and GDPR rules to ensure that no event containing patients' data was missed in a log or not tracked properly. Integration and scalability were also carried out, involving the testing of the system with the increasing number of the simulated IoT devices as well as the concurrent users, which was followed by the measurement of the latency and the throughput of the system, all in an aim of determining the performance of the system under load. The results were high in scalability and fidelity in the detection process, which confirmed the system's effectiveness as a working model in the healthcare facility.

Results and Discussion

Integrating and testing threat detection and response using artificial intelligence in healthcare cloud systems is more effective than traditional security systems. This paper combines experimental studies, cloud adoptions, and case studies of the implementation of AI in diverse institutional settings to underscore AI's capacity to meet the complex and sensitive security needs of modern healthcare.

Performance Evaluation

AI-powered security systems outperform traditional rule-based architectures across nearly every key performance metric. The higher degree of exactness, the rate of response, and processing ability play a critical role in sensitive areas, including hospitals where IoT medical devices, patient records, and EHRs are generating abundant and sensitive data.

Table 1: Key Performance Metrics of AI-Driven Systems

Metric	AI System Performance	Traditional System Baseline	Improvement
Threat Detection Accuracy	97.2%	76.4%	+20.8%
False Positive Rate	2.4–3.9%	19.4–23.8%	-94.3%
Mean Time to Detect (MTTD)	2.3–4.5 seconds	52–156 minutes	-98.7%
Data Processing Capacity	10 TB/sec	0.1 TB/sec	100×
Zero-Day Attack Detection	96.8% success rate	18.7% baseline	+78.1%
Adaptive Learning Gain	78% → 94% accuracy over 6 months	Static models	+20.5%

Some case studies from well-established healthcare institutions can evidence the efficacy of these gains. For instance, Johns Hopkins Hospital found that using the gamma probe minimized the number of false positives by 73% and detected threats at an average of 2.5 seconds to an incident 97 percent of the time. In particular, the Mayo Clinic applied adaptive AI models for the case of vulnerability enhancement by 30%, thus lowering the incident detection time from 97 days to 6. These institutions also leverage big data analysis and AI analyses up to a monthly traffic of 4.8 petabytes of telemetry at a 99.7% process, providing nearly real-time threat information.

Comparative Analysis

Comparing AI-based systems to conventional systems, one can find out the extent of operational benefits provided by intelligent automation. From minimizing the rate of false alarms, which is detrimental to security, to helping secure systems heal themselves, AI systems help fortify security positions and ease the burden on IT security personnel.

Table 2: AI-Driven vs. Traditional Security Systems

Category	AI-Driven Systems	Traditional Systems	Advantage
Alert Volume	923 fewer daily alerts	High alert fatigue	82.5% reduction
Threat Response Automation	92.7% MTTR reduction	Manual intervention	72.3% cost savings
Pattern Recognition	99.2% network traffic accuracy	71.8% accuracy	+27.4%
Behavioral Analysis	98.9% user action accuracy	Rule-based thresholds	+91.6%
Compliance Monitoring	63% penalty risk reduction	Periodic manual audits	28% cost savings

These are real-life efficiencies that are given by these outcomes. While assessing the effectiveness of the AI platforms, it is necessary to indicate that they easily recognize zero-day threats at a rate 3.5 times higher than is the case with static rule-based systems. In ransomware containment, AI cut the time to remediate the breach in half, and it left no traces that were not HIPAA compliant. The incorporation of edge computing enabled real-time interventions for threats towards medical IoT at a success rate of 94.3%, which is very important for devices such as the insulin pump and the remote cardiac monitor.

Discussion

This evidence clearly shows the role of AI in protecting healthcare cloud systems due to its potential to offer great benefits. One of the most significant discoveries is that the system's working capacity, where it can successfully process over ten Terabytes per second without latency, is crucial in monitoring EHR systems and the connected devices used in clinical activities.

Adaptive defense mechanisms, especially LSTM networks, take less time than the initial response time of about 84 hrs to identify new and emerging threats and reduce it to 32 minutes. This improvement helps it fight new ransomware versions and other APT-like threats that are difficult to detect. Moreover, it reduced the audit preparation costs by $2.8 million yearly for large hospitals, which created security improvements and had substantive economic benefits.

Interpretation has remained a major challenge in model creation, particularly in healthcare, where it is probable that an anomaly's rationale will be launched. Still, it is essential to recognize that cross-cloud federated learning is also not devoid of technical and privacy challenges while advancing innovations are promising. This follows experimental results for quantum-resistant encryption and homomorphic learning, providing 96.7% efficiency using synthetic data, which promises modern security solutions protection against quantum threats.

Limitations and Future Work

Model Interpretability and Explainability

Although threat detection models using AI have high accuracy and response time, the black-box model is a drawback when deploying the technology in healthcare, where most decisions must be justified. Clinicians and compliance officers may be unable to rely on systems that raise alerts without a proper justification, particularly when a particular behavior poses a security threat. The current state-of-art methods, such as LSTMs and autoencoders, have many shortcomings, including the fact that most do not explain the decision-making process. The lack of trust also underlines the urgent need for future studies to adopt and incorporate XAI models that help the intended audiences in the healthcare profession validate the automated generated threats.

Data Diversity, Bias, and Federated Challenges

The diversity and representativeness of training data. Most AI models utilize historical attack databases that may not include modern attacks or attacks targeted at specific institutions. Furthermore, the privacy restrictions on data collection do not allow for gathering huge volumes of centralized data, which is crucial for training corpora. However, federated learning has been presented as a solution to this problem; it presents novel challenges, such as differences in data formats, communications limitations, and nonalignment of models. Future work should improve the federated learning integrated architecture between institutions and advanced DP methods to allow information sharing in the form of threat intelligence while not compromising the patients' data.

Security of the AI Models Themselves

To further discuss, the AI models employed for expanding cybersecurity strategies are not immune to attacks. Malicious actors can perform poisoning or evasion on models to either evade the existing security measures to access the data models or even get them contaminated. This poses a great threat, especially in sectors that require timely identification and response to threats, such as healthcare. Research on adversarial robustness and applying robust training approaches and secure model updates are crucial to protecting AI systems in the deployment setting.

Future Research Directions

Thus, to modify and strengthen the AI-powered security applications, the following directions are worth introducing Quantum-resistant encryption to enhance the security of the data used in the AI-powered applications; Homomorphic learning to improve the interpretability of the AI algorithms; Blockchain-based audit systems that would provide better security along with the chain of custody for AI applications. Further to this, more advanced AI models based on context will also address the issue of false positives and component detection locales. A strategic objective is to build self-sustainable security systems capable of managing the threats as they emerge and, at the same time, meet all the healthcare-related requirements. These will go a long way in developing the next-generation, patient-centered cybersecurity models in the constantly changing features of the digital health sector.

Conclusion

AI placement within the realm of healthcare cloud environments to address threats is an important developmental step in the protection of patient-related information. As medical organizations continue moving toward digitizing their services and storing the patients' information and data on the cloud, the rule-based security paradigms cannot effectively counteract the rapidly growing number of threats and their levels of complexity. On the other hand, AI-based systems are proactive and intelligent, effective, and scalable for increased threat visibility and timely response to threats, besides being compliant with various regulations.

New machine learning solutions like the LSTMs for behavioural analysis and the ensemble models for anomaly detection allow healthcare institutions to contain zero-day threats, privilege escalations, and insider risks at an extent and speed hitherto unimaginable. Several examples of AI from leading institutions such as Johns Hopkins Hospital and the Mayo Clinic demonstrate the potentially revolutionary changes for this approach regarding decreasing false positives and shortening the mean detection time from weeks to mere seconds. In addition, patient information leaks are prevented, and system security and integrity in federated learning, behavioral biometrics, and automated compliance monitoring are further shielded in distributed systems. Despite these advancements, challenges remain. Challenges regarding model interpretability and explainability, robustness, and cross-cloud data sharing cannot be ignored when tapping into AI for healthcare security. However, there are some signs of remedies: Explainable AI, Quantum-resistant Encryption, and Blockchain-based Auditing, which may provide specific avenues for further research and implementation. AI in security is an advancement and a drastic shift from the traditional approaches to maintaining security in healthcare organizations. Increased speed, smart application, and automation further provide a new benchmark for protecting patient data in cloud-based healthcare systems that augment healthcare when it comes to evolution.

References

1. Kopparthi, VJR (2024) Machine Learning-Driven Threat Detection in Healthcare: A Cloud-Native Framework Using AWS Services.
2. Marwan M, Kartit A, Ouahmane H (2018) Security enhancement in healthcare cloud using machine learning. Procedia Computer Science 127: 388-397.
3. Qayyum A, Qadir J, Bilal M, Al-Fuqaha A (2020) Secure and robust machine learning for healthcare: A survey. IEEE Reviews in Biomedical Engineering 14: 156-180.
4. Khatun MA, Memon SF, Eising C, Dhirani LL (2023) Machine learning for healthcare-iot security: A review and risk mitigation. IEEE Access 11: 145869-145896.
5. (2024) How AI and Cybersecurity Are Transforming Patient Data Protection in Healthcare. Linkedin https://www.linkedin.com/pulse/how-ai-cybersecurity-transforming-patient-data-protection-yia7f.
6. Arefin S (2024) Strengthening Healthcare Data Security with Ai-Powered Threat Detection. International Journal of Scientific Research and Management (IJSRM) 12: 1477-1483.
7. Oduri S (2021) AI-powered threat detection in cloud environments. International Journal on Recent and Innovation Trends in Computing and Communication 9: 57-62.
8. Cloud Security in Healthcare: Ensuring HIPAA Compliance and Data Protection. Sparxit solutions, https://www.sparxitsolutions.com/blog/cloud-security-in-healthcare/.
9. (2024) AI-Driven Threat Intelligence Platforms for Healthcare Cybersecurity. International Journal of Machine Learning for Sustainable Development 6.
10. Gandhi NT (2024) AI-driven threat detection in cloud-based applications. International Journal of Computer Engineering and Technology 15: 1045-1055.
11. (2025) How to Implement AI in Healthcare: Keeping Data Secure and Staying Compliant. Tribe AI https://www.tribe.ai/applied-ai/how-to-implement-ai-in-healthcare.
12. (2024) AI-Driven Cybersecurity in Healthcare: Protecting Patient Data and Critical Infrastructure. International Journal of Innovative Research in Science, Engineering, and Technology 13.
13. (2024) Role of Artificial Intelligence (AI) in Threat Detection. Sangfor https://www.sangfor.com/blog/cybersecurity/role-of-artificial-intelligence-ai-in-threat-detection.
14. Janjua JI (2023) Healthcare through AI-Driven Threat Detection and Cloud-Based Solutions Architecture. https://www.researchgate.net/publication/384196899_Healthcare_through_AI-Driven_Threat_Detection_and_Cloud-Based_Solutions_Architecture.
15. AI vs. Traditional Cybersecurity: Which Is More Effective?. zscaler https://www.zscaler.com/zpedia/ai-vs-traditional-cybersecurity.
16. What Is the Role of AI in Threat Detection?. Paloaltonetworks https://www.paloaltonetworks.in/cyberpedia/ai-in-threat-detection.
17. Choudhury A, Asan O (2020) Role of artificial intelligence in patient safety outcomes: systematic literature review. JMIR medical informatics 8: e18599.
18. Brohi S, Mastoi QUA (2025) AI Under Attack: Metric-Driven Analysis of Cybersecurity Threats in Deep Learning Models for Healthcare Applications. Algorithms 18: 157.
19. Chauhan A (2024) AI in Healthcare Data Security: Protecting Patient Information in the Digital Age. techahead https://www.techaheadcorp.com/blog/ai-in-healthcare-data-security-protecting-patient-information-in-the-digital-age/.
20. (2024) Cloud Security in Healthcare: Strategic Approaches to Protect Your Data. kms-healthcare. https://kms-healthcare.com/blog/cloud-security-in-healthcare/.
21. Andersen ES, Birk-Korch JB, Hansen RS, Fly LH, Röttger R, et al. (2024) Monitoring performance of clinical artificial intelligence in health care: a scoping review. JBI evidence synthesis 22: 2423-2446.

Copyright: ©2025 Anjan Gundaboina. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.