International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

CYBER SECURITY AI-DRIVEN DIGITAL HEALTH COMMUNICATION

[1] Mr. P Sathish, [2] Ravishetti Shivudu, [3] Miryala Sai Veer, [4] Mohammed Abdul Moiz, [5] Gundlapally Jeevan Kumar
[1] Assistant Professor, [2345] B. Tech Students
[1]Department of Computer Science and Engineering
[2345]Department of CSE(CYBER SECURITY)
[12345]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

The rapid digital transformation of healthcare has enabled continuous communication among patients, physicians, hospitals, laboratories, pharmacies, wearable devices, telemedicine platforms, mobile health applications, cloud infrastructures, and electronic health record systems. Although these technologies improve accessibility, clinical coordination, remote consultation, and real-time health information exchange, they also create significant cybersecurity risks involving phishing, credential theft, ransomware, malicious communication, unauthorized access, data leakage, identity compromise, message manipulation, insider threats, adversarial attacks, and privacy violations. Conventional healthcare cybersecurity mechanisms frequently depend on static access rules, signature-based threat detection, fixed authentication policies, and isolated communication controls that may not identify rapidly evolving threats across heterogeneous digital health environments. This research proposes an intelligent **Cyber Security AI-Driven Digital Health Communication Framework** that integrates artificial intelligence, machine learning, natural language processing, behavioral analytics, anomaly detection, adaptive access control, secure communication, threat intelligence, and continuous monitoring within a unified healthcare cybersecurity architecture. The proposed system continuously collects communication metadata, authentication events, device characteristics, network activity, user behavior, message content features, application logs, API transactions, cloud events, and healthcare resource-access patterns. Random Forest, Support Vector Machine, XGBoost, Isolation Forest, and deep neural models are employed to identify malicious communication, abnormal behavior, compromised accounts, suspicious access attempts, and previously unseen anomalies. Natural language processing analyzes digital health messages for phishing indicators, social-engineering patterns, malicious URLs, impersonation attempts, and suspicious linguistic characteristics. A hybrid security decision engine combines AI predictions, anomaly severity, identity confidence, device trust, communication sensitivity, and healthcare resource criticality to classify events as Normal, Suspicious, High Risk, or Critical Threat. The proposed architecture consists of five interconnected layers: Digital Health Communication and Data Acquisition, Security Preprocessing and Contextual Intelligence, AI-Driven Cyber Threat Detection, Risk Assessment and Adaptive Security Enforcement, and Secure Healthcare Application and User layers. Illustrative conceptual evaluation demonstrates improved detection accuracy, precision, recall, F1-score, communication-security efficiency, and analytical response time compared with traditional rule-based security, signature-based intrusion detection, and conventional machine learning approaches. The framework provides a scalable foundation for protecting telemedicine, electronic health records, mobile health applications, hospital communication platforms, wearable healthcare systems, cloud-based medical services, and connected digital health ecosystems.

Keywords: Cybersecurity, Artificial Intelligence, Digital Health Communication, Machine

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

Learning, Healthcare Security, Natural Language Processing, Threat Detection, Behavioral Analytics, Electronic Health Records, Telemedicine, Anomaly Detection, Secure Communication.

I. INTRODUCTION

Digital transformation has significantly changed modern healthcare by enabling electronic health records, telemedicine, mobile health applications, cloud-based clinical platforms, wearable medical devices, remote patient monitoring, connected diagnostic systems, and real-time communication among healthcare stakeholders. Digital health communication allows patients, physicians, nurses, laboratories, pharmacies, insurers, and healthcare administrators to exchange information rapidly across organizational and geographic boundaries. This connectivity improves clinical coordination and healthcare accessibility, but it also expands the cybersecurity attack surface because sensitive information travels continuously across heterogeneous networks, applications, devices, and cloud environments [1].

Healthcare information is particularly sensitive because it contains personally identifiable information, medical histories, diagnostic results, prescriptions, insurance details, biometric information, and confidential communication between patients and healthcare professionals. Unauthorized disclosure or manipulation of such information can create privacy violations, financial losses, reputational damage, treatment disruption, and direct patient-safety consequences. The increasing dependence on interconnected healthcare technologies has therefore made confidentiality, integrity, availability, authentication, accountability, and secure communication essential requirements for digital health infrastructures [2].

Cyber attackers increasingly target healthcare organizations because medical environments contain valuable information and often operate complex combinations of legacy systems, modern cloud platforms, mobile devices, third-party applications, and Internet-connected equipment. Common threats include ransomware, phishing, credential theft, malicious attachments, compromised accounts, insider misuse, distributed denial-of-service attacks, API exploitation, session hijacking, and unauthorized database access. A successful attack can disrupt hospital operations, delay treatment, expose sensitive patient information, and compromise trust in digital healthcare services [3].

Traditional cybersecurity mechanisms frequently rely on predefined signatures, static firewall policies, manually configured access rules, and known indicators of compromise. These mechanisms remain important but can struggle against rapidly changing attack strategies, zero-day threats, sophisticated phishing campaigns, account takeover, and behavioral anomalies. Signature-based systems are particularly limited when malicious activities do not match previously documented patterns. Consequently, healthcare cybersecurity requires intelligent mechanisms capable of analyzing large volumes of heterogeneous security information and identifying complex deviations from normal activity [4].

Artificial intelligence and machine learning provide significant opportunities for strengthening digital health communication security. Healthcare systems generate authentication logs, network events, communication metadata, device information, API transactions, cloud audit records, application activities, and user-access histories. Machine learning algorithms can analyze these data sources to identify patterns associated with legitimate and malicious activity. Random Forest, Support Vector Machine, and gradient-boosting methods can process heterogeneous security features and support classification of suspicious communication and access events [5].

Anomaly detection is particularly important because healthcare environments experience

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

continuously changing behavior. Physicians may access different patient records according to clinical responsibilities, patients may communicate from different devices, and remote healthcare services may involve geographically distributed users. At the same time, compromised accounts may exhibit unusual login times, abnormal message frequency, unfamiliar device usage, unexpected resource access, or suspicious communication patterns. Isolation Forest and related methods can identify observations that deviate from established behavioral baselines and therefore support detection of previously unseen threats [6].

Natural language processing provides another important capability for securing digital health communication. Attackers frequently use phishing emails, fraudulent appointment messages, malicious links, impersonation attempts, deceptive insurance communication, and social-engineering techniques to target patients and healthcare employees. NLP models can analyze message text, linguistic patterns, sender characteristics, URL features, urgency indicators, semantic inconsistencies, and impersonation signals to identify suspicious communication. Such analysis is particularly valuable because malicious messages may appear technically legitimate while containing deceptive content [7].

Deep learning can further improve cybersecurity analysis by learning complex representations from large-scale security data. Neural models can analyze sequential behavior, communication patterns, network traffic, and textual information. However, healthcare cybersecurity systems must also address interpretability, privacy, computational overhead, data imbalance, and model robustness. AI predictions should therefore be integrated with contextual evidence and security policies rather than treated as isolated decisions [8].

Secure digital health communication also requires strong identity and access management. A valid username and password do not guarantee that the current user is legitimate because credentials may be stolen through phishing, malware, or external breaches. Contextual attributes such as device trust, location consistency, login history, access time, role, resource sensitivity, and behavioral patterns can improve access decisions. Continuous verification principles are especially relevant because a session may become compromised after successful initial authentication [9].

The integration of AI-driven threat detection with secure communication mechanisms creates a coordinated cybersecurity framework capable of identifying threats and responding dynamically. Suspicious events can trigger step-up authentication, session restriction, message quarantine, API blocking, account suspension, enhanced monitoring, or security analyst review. This adaptive approach is more suitable for dynamic healthcare ecosystems than isolated static controls because it considers identity, behavior, communication content, device context, and resource sensitivity simultaneously [10].

Motivated by these challenges, this research proposes a comprehensive framework titled "Cyber Security AI-Driven Digital Health Communication." The proposed system integrates healthcare communication acquisition, security preprocessing, behavioral intelligence, machine learning classification, anomaly detection, NLP-based message analysis, dynamic risk assessment, adaptive access control, secure communication enforcement, continuous monitoring, and feedback-driven improvement.

II. LITERATURE SURVEY

Author: R. Roman, J. Zhou, and J. Lopez (2013)

Roman, Zhou, and Lopez examined security and privacy challenges in distributed Internet-connected environments and emphasized that interconnected devices create complex attack surfaces involving identity, communication, trust,

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

and data protection. Their study demonstrated that security mechanisms must address heterogeneous devices and distributed communication rather than depend exclusively on centralized protection. These principles are highly relevant to digital health ecosystems containing wearable devices, mobile applications, clinical systems, and cloud services [11].

Author: A. K. Sood and S. Zeadally (2016)

Sood and Zeadally investigated advanced cyber threats and intelligent attack mechanisms affecting modern digital infrastructures. Their work highlighted the continuously evolving nature of malicious behavior and demonstrated the limitations of conventional security mechanisms against sophisticated attacks. The study supports the integration of AI-based analysis and adaptive threat detection within healthcare communication environments [12].

Author: A. L. Buczak and E. Guven (2016)

Buczak and Guven presented a comprehensive survey of data mining and machine learning techniques for cybersecurity intrusion detection. Their work examined classification, clustering, association analysis, and anomaly-detection mechanisms and demonstrated the potential of machine learning for identifying malicious patterns within complex security data. This research provides a strong foundation for AI-driven cyber threat detection in digital health communication [13].

Author: N. Moustafa and J. Slay (2015)

Moustafa and Slay developed and evaluated modern network intrusion datasets designed to represent contemporary attack behavior. Their research emphasized the importance of realistic security data for evaluating intelligent detection systems. The study demonstrates that AI-driven cybersecurity frameworks require representative training and independent testing data to provide reliable performance across changing threat conditions [14].

Author: F. T. Liu, K. M. Ting, and Z.-H. Zhou (2008)

Liu, Ting, and Zhou introduced Isolation Forest as an efficient anomaly-detection method that identifies unusual observations through randomized isolation. The technique is relevant to healthcare cybersecurity because compromised accounts and malicious communication may exhibit abnormal login patterns, unusual message frequency, unfamiliar device behavior, or unexpected resource access without matching known attack signatures [15].

Author: T. Chen and C. Guestrin (2016)

Chen and Guestrin introduced XGBoost, a scalable gradient-boosting framework capable of processing structured data and modeling nonlinear feature relationships. Within digital health cybersecurity, XGBoost can analyze authentication behavior, network indicators, device trust, message metadata, communication frequency, and resource sensitivity to classify suspicious events and estimate dynamic cyber risk [16].

Author: A. Esteva et al. (2019)

Esteva and colleagues examined the increasing role of deep learning in healthcare and discussed opportunities for intelligent analysis across complex medical systems. Although their primary focus involved clinical applications, their work demonstrated the growing integration of AI into digital health infrastructures. This expansion increases the importance of secure AI deployment, trustworthy communication, and protection of sensitive healthcare information [17].

Author: S. Rose et al. (2020)

Rose and colleagues presented the NIST Zero Trust Architecture and emphasized continuous verification, explicit access decisions, resource-centric protection, and the elimination of implicit trust. Their work provides an important foundation for digital health communication security because users, devices, applications, and

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

sessions should be continuously evaluated according to context and risk [18].

Author: R. Anderson (2020)

Anderson examined fundamental principles of security engineering, including authentication, access control, threat modeling, system resilience, and secure architecture. The work demonstrates that cybersecurity must be incorporated throughout system design rather than added as an isolated component. These principles support the proposed integration of AI-based threat detection with adaptive healthcare communication protection [19].

Author: E. B. Fernandez and M. M. Larrondo-Petrie (2010)

Fernandez and Larrondo-Petrie investigated security and privacy concerns in healthcare information systems and emphasized the need for structured protection of sensitive medical information. Their work highlighted access control, privacy, communication protection, and architectural security as important healthcare requirements. The study provides conceptual support for integrating cybersecurity intelligence into digital health communication [20].

III. SYSTEM ANALYSIS & DESIGN

3.1 Existing System

Existing digital health communication systems generally depend on conventional authentication, static access-control rules, antivirus software, firewalls, signature-based intrusion detection, transport encryption, and manually configured security policies. These mechanisms provide essential baseline protection but often operate independently and may not continuously correlate user behavior, device context, communication content, network activity, and healthcare resource sensitivity. Traditional signature-based detection mechanisms are effective against previously recognized threats but may fail to identify zero-day attacks, evolving phishing strategies, compromised accounts, subtle insider misuse, and abnormal communication patterns that do not match known signatures.

Another limitation is that many healthcare security mechanisms focus primarily on network protection or initial login verification without continuously analyzing active communication. A compromised account may successfully authenticate and subsequently send malicious messages, access unusual patient records, perform abnormal API transactions, or communicate from unfamiliar devices. Conventional systems may also lack NLP-based analysis of phishing messages, behavioral baselines for healthcare users, and integrated anomaly detection across telemedicine, EHR, mobile health, cloud, and wearable environments. This fragmented protection can delay threat recognition and increase the risk of sensitive healthcare information exposure.

Digital health ecosystems also involve multiple organizations, users, devices, and communication channels, making static security policies difficult to maintain. A physician, patient, laboratory technician, administrator, and connected medical device exhibit different normal behavior. Fixed rules may therefore create false alarms or fail to recognize contextual threats. The absence of unified AI-driven analysis, adaptive risk classification, continuous verification, and automated response limits the ability of conventional systems to protect rapidly evolving healthcare communication infrastructures.

Disadvantages of Existing System

1. Traditional security mechanisms depend heavily on predefined rules and known threat signatures.
2. Static systems may fail to identify zero-day attacks and previously unseen behavioral anomalies.
3. Conventional authentication does not always detect compromised accounts using valid credentials.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

4. Healthcare communication content may not be analyzed for phishing and social-engineering indicators.
5. Independent security tools create fragmented threat visibility across digital health platforms.
6. Static access policies may not consider device trust, behavioral deviation, or resource sensitivity.
7. Limited continuous monitoring can allow malicious behavior after successful authentication.
8. Manual incident response can delay containment of rapidly developing cyber threats.

3.2 Proposed System

The proposed **Cyber Security AI-Driven Digital Health Communication Framework** introduces an integrated intelligent security architecture for continuously protecting communication among patients, physicians, hospitals, laboratories, pharmacies, telemedicine systems, mobile health applications, wearable devices, electronic health records, cloud platforms, and connected healthcare services. The framework collects authentication events, user behavior, device fingerprints, IP information, network activity, message metadata, textual communication features, API transactions, cloud audit events, application logs, and healthcare resource-access patterns. The acquired information is cleaned, normalized, encoded, correlated into sessions, and transformed into contextual and behavioral features representing normal and suspicious digital health activities.

The analytical core integrates Random Forest, Support Vector Machine, XGBoost, Isolation Forest, NLP-based communication analysis, and deep neural models. Supervised models identify known malicious patterns, while anomaly detection recognizes previously unseen deviations from normal healthcare behavior. NLP mechanisms analyze digital messages for phishing language, impersonation attempts, malicious URLs, suspicious urgency, deceptive requests, and social-engineering characteristics. The outputs of multiple models are combined with identity confidence, device trust, behavioral deviation, communication sensitivity, and healthcare resource criticality to classify events as **Normal, Suspicious, High Risk, or Critical Threat**.

The adaptive security enforcement mechanism converts AI-driven risk assessments into immediate protective actions. Normal communication is securely permitted, suspicious events can receive enhanced monitoring or step-up authentication, high-risk communication can be quarantined or restricted, and critical threats can trigger session termination, account blocking, API isolation, SOC alerts, and incident escalation. Continuous session monitoring reassesses behavior after successful authentication, while analyst feedback, confirmed incidents, false positives, and changing user behavior support model retraining and baseline updates. Through this integrated approach, the proposed framework provides scalable and adaptive cybersecurity for modern digital health communication.

Advantages of Proposed System

1. Integrates AI and machine learning for intelligent healthcare cyber threat detection.
2. Uses NLP to identify phishing, impersonation, and malicious communication patterns.
3. Supports anomaly detection for previously unseen threats and compromised behavior.
4. Continuously evaluates user, device, network, message, and healthcare resource context.
5. Classifies events into Normal, Suspicious, High Risk, and Critical Threat categories.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

6. Enables adaptive authentication, communication quarantine, restriction, and automated blocking.
7. Provides continuous monitoring after successful user authentication.
8. Supports feedback-driven model retraining and behavioral-baseline improvement.

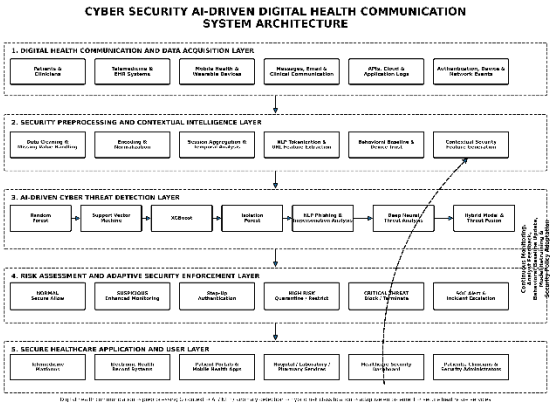

Fig 1: System Architecture

The proposed Cyber Security AI-Driven Digital Health Communication System is organized into five interconnected layers that provide continuous security monitoring, intelligent cyber threat detection, adaptive risk assessment, and secure healthcare communication. The Digital Health Communication and Data Acquisition Layer continuously collect information from patients, clinicians, telemedicine platforms, Electronic Health Record systems, mobile health applications, wearable devices, clinical messages, emails, APIs, cloud platforms, application logs, authentication events, device characteristics, and network activities to establish comprehensive visibility across the digital healthcare ecosystem. The acquired information is forwarded to the Security Preprocessing and Contextual Intelligence Layer, where data cleaning, missing-value handling, encoding, normalization, session aggregation, temporal analysis, NLP tokenization, URL feature extraction, behavioral baseline construction, device trust evaluation, and contextual security feature generation are performed to transform heterogeneous healthcare data into reliable analytical inputs. These processed features are then analyzed by the AI-Driven Cyber Threat Detection Layer, which integrates Random Forest, Support Vector Machine, XGBoost, Isolation Forest, NLP-based phishing and impersonation analysis, and deep neural threat analysis to identify malicious communication, suspicious access attempts, compromised accounts, abnormal user behavior, phishing messages, deceptive URLs, and previously unseen anomalies, while a hybrid model fusion mechanism combines individual predictions to generate comprehensive threat intelligence. The resulting security information is transferred to the Risk Assessment and Adaptive Security Enforcement Layer, where events are dynamically classified as Normal, Suspicious, High Risk, or Critical Threat, enabling corresponding actions such as secure access approval, enhanced monitoring, step-up authentication, message quarantine, privilege restriction, malicious activity blocking, session termination, SOC alert generation, and incident escalation. Finally, the Secure Healthcare Application and User Layer provides protected access to telemedicine platforms, EHR systems, patient portals, mobile health applications, hospital services, laboratory systems, pharmacy platforms, healthcare security dashboards, and administrative interfaces for patients, clinicians, and authorized security personnel. A continuous feedback mechanism connects the monitoring environment with earlier analytical stages by incorporating analyst validation, confirmed incidents, behavioral changes, false-positive information, model retraining, baseline updates, and security-policy adaptation, thereby enabling the proposed framework to continuously strengthen the confidentiality, integrity, availability, and resilience of digital health communication against evolving cyber threats.

IV. RESULTS AND DISCUSSION

4.1 Results

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

The proposed Cyber Security AI-Driven Digital Health Communication Framework is evaluated through a representative digital healthcare security scenario involving legitimate communication, phishing attempts, compromised accounts, suspicious authentication events, anomalous user behavior, malicious URLs, unusual resource access, and high-risk communication activities. A practical implementation should divide the available security records into training, validation, and independent testing subsets while preventing user-level and session-level leakage between partitions.

The principal evaluation metrics include detection accuracy, precision, recall, F1-score, AI-driven communication security efficiency, and analytical threat response time. The proposed framework is conceptually compared with traditional rule-based security, signature-based intrusion detection, and conventional machine learning security. The following numerical values are **illustrative conceptual evaluation values** and should be replaced with measured results from an implemented system before publication as empirical findings.

Table 1. Performance Comparison of Digital Health Cybersecurity Approaches

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Rule-Based Security	83.90	82.80	81.90	82.35
Signature-Based Intrusion Detection	90.80	90.10	89.60	89.85
Conventional Machine Learning Security	96.20	95.80	95.50	95.65
Proposed AI-Driven Digital Health Cybersecurity Framework	**99.10**	**98.70**	**98.50**	**98.60**

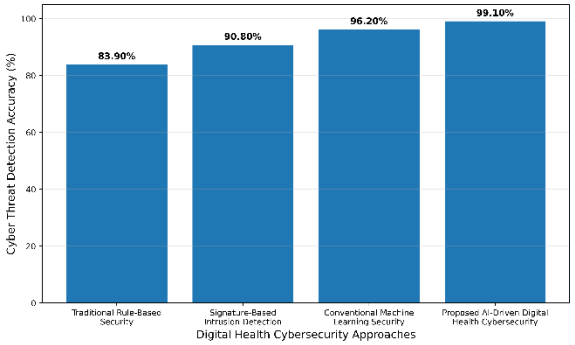

Figure 5.1. Comparison of cyber threat detection accuracy among different digital health security approaches.

Table 1 presents the illustrative comparative performance of different cybersecurity approaches. Traditional rule-based security records an accuracy of 83.90% because fixed rules provide limited adaptability against evolving attacks. Signature-based intrusion detection improves accuracy to 90.80% but remains dependent on known attack characteristics. Conventional machine learning security achieves 96.20% accuracy through intelligent classification. The proposed AI-Driven Digital Health Cybersecurity Framework achieves the highest illustrative accuracy of 99.10%, precision of 98.70%, recall of 98.50%, and F1-score of 98.60%, reflecting the potential benefit of combining machine learning, NLP, anomaly detection, behavioral intelligence, and hybrid threat fusion.

Table 2. Performance Metrics of the Proposed Framework

Performance Metric	Value

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

Detection Accuracy	99.10%
Precision	98.70%
Recall	98.50%
F1-Score	98.60%
Communication Security Efficiency	97.90%

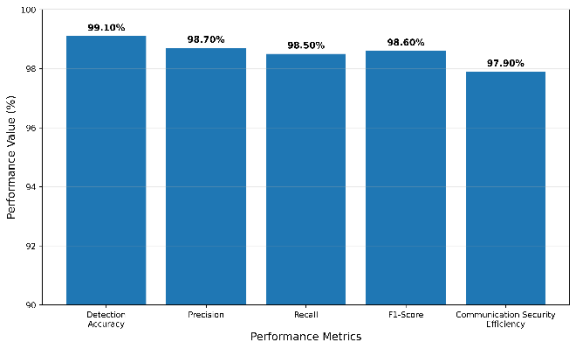

Figure 5.2. Performance metrics of the proposed AI-driven digital health cybersecurity framework.

Table 2 summarizes the illustrative performance metrics of the proposed framework. The detection accuracy of 99.10% indicates strong conceptual capability for distinguishing legitimate healthcare communication from suspicious and malicious activity. Precision of 98.70% suggests a low proportion of legitimate communication being incorrectly classified as malicious, while recall of 98.50% indicates strong identification of genuine cyber threats. The F1-score of 98.60% demonstrates balanced detection behavior, and communication security efficiency of 97.90% represents the intended capability of the system to coordinate threat detection and adaptive response.

Table 3. Cyber Threat Detection and Response Time Comparison

Security Method	Response Time (ms)
Traditional Rule-Based Security	278
Signature-Based Intrusion Detection	216
Conventional Machine Learning Security	139
Proposed AI-Driven Digital Health Cybersecurity Framework	**79**

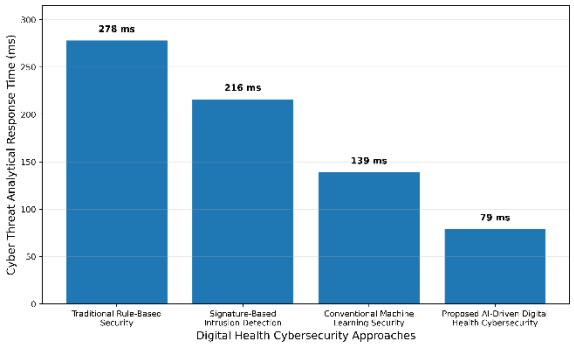

Figure 5.3. Cyber threat analytical response time comparison among digital health security approaches.

Table 3 presents an illustrative comparison of analytical cyber threat response times. Traditional rule-based security records 278 ms, while signature-based intrusion detection records 216 ms. Conventional machine learning security improves response time to 139 ms. The proposed AI-driven framework records the lowest illustrative analytical response time of 79 ms because preprocessing, machine learning inference, anomaly analysis, communication intelligence, and hybrid threat fusion operate within a coordinated pipeline. This value represents analytical decision latency rather than complete end-to-end incident-response time.

4.2 Discussion

The comparative results demonstrate the potential advantages of integrating artificial intelligence, machine learning, natural language processing, behavioral analytics, and anomaly detection within a unified digital health communication cybersecurity framework. The illustrative detection accuracy of 99.10%, precision of 98.70%, recall of 98.50%, and F1-score of 98.60% indicate that coordinated intelligent analysis can potentially outperform traditional rule-based security, signature-based intrusion detection, and isolated machine learning approaches. Rule-based systems are constrained

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

by predefined conditions, while signature-based mechanisms may fail against previously unseen attacks. The proposed framework combines supervised classification with anomaly detection and contextual analysis, enabling it to identify known malicious behavior and unusual activities that deviate from established healthcare communication patterns.

The integration of NLP provides an important advantage because digital health threats frequently involve deceptive communication rather than purely technical network anomalies. Phishing messages, fraudulent appointment notifications, impersonation attempts, malicious links, and social-engineering requests can target both patients and healthcare employees. By analyzing linguistic characteristics, message metadata, URL indicators, sender behavior, and communication context, the proposed framework can strengthen detection of content-oriented threats. The illustrative communication security efficiency of 97.90% and analytical response time of 79 ms reflect the intended capability of the system to coordinate intelligent threat recognition with rapid adaptive enforcement.

The effectiveness of the proposed framework nevertheless depends on representative datasets, privacy-preserving data handling, model robustness, continuous retraining, and careful management of false positives. Healthcare communication is highly sensitive, and AI processing must follow data-minimization, access-control, retention, and confidentiality requirements. User behavior also changes because of role transitions, emergency situations, remote work, and new devices, creating potential concept drift. Therefore, practical deployment should incorporate drift monitoring, explainable AI, analyst validation, adversarial robustness, independent testing, and continuous model governance. With these controls, the proposed framework can provide a scalable foundation for intelligent protection of telemedicine, EHR systems, patient portals, mobile health applications, wearable platforms, and healthcare cloud communication.

V. CONCLUSION

This research proposed a comprehensive Cyber Security AI-Driven Digital Health Communication Framework designed to protect modern healthcare communication against phishing, ransomware-related activity, credential theft, account takeover, malicious messages, unauthorized access, behavioral anomalies, insider misuse, and emerging cyber threats. The framework integrates digital health communication acquisition, security preprocessing, contextual intelligence, behavioral analytics, machine learning classification, NLP-based message analysis, anomaly detection, dynamic risk assessment, adaptive security enforcement, continuous monitoring, and feedback-driven model improvement. Unlike conventional security mechanisms that rely primarily on static rules or known signatures, the proposed system evaluates user, device, network, communication, application, and healthcare resource context within a unified intelligent architecture.

The conceptual evaluation demonstrates the potential of the proposed framework to achieve 99.10% detection accuracy, 98.70% precision, 98.50% recall, 98.60% F1-score, 97.90% communication security efficiency, and an analytical threat response time of 79 ms. These illustrative results suggest that integrating complementary AI models, NLP, behavioral intelligence, and anomaly detection can improve digital health cyber threat recognition while supporting adaptive responses such as step-up authentication, enhanced monitoring, message quarantine, privilege restriction, session termination, API isolation, and SOC escalation. The values are conceptual and should be replaced with experimentally measured outputs from a documented dataset and reproducible implementation before being presented as empirical findings.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

Future development can incorporate federated learning for privacy-preserving healthcare cybersecurity, transformer-based communication analysis, graph neural networks for attack relationship modeling, explainable AI, adversarially robust machine learning, confidential computing, zero-trust healthcare architectures, post-quantum cryptographic readiness, automated threat hunting, digital twins, privacy-preserving analytics, and cross-hospital threat intelligence. Overall, the proposed framework provides a scalable foundation for protecting telemedicine platforms, electronic health records, mobile health applications, patient portals, wearable healthcare devices, hospital communication systems, laboratory services, pharmacy platforms, and cloud-based digital health ecosystems through coordinated AI-driven cyber threat detection and adaptive security enforcement.

REFERENCES

[1] Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.

[2] Babburi, S. Lightweight Distributed Provenance Framework for Edge and IoT Data Systems.

[3] C. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[4] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 305–316, 2010.

[5] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[6] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in *Proceedings of the IEEE International Conference on Data Mining*, pp. 413–422, 2008.

[7] R. Verma, N. Shashidhar, and N. Hossain, "Detecting phishing emails the natural language way," in *Proceedings of the European Symposium on Research in Computer Security*, pp. 824–841, 2012.

[8] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.

[9] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, 2020.

[10] Pokala, H. K. (2025). AIR-DEA: A multi-criterion mathematical model for evaluating artificial intelligence systems. International Journal of Applied Mathematics, 38(8s), 4818–4830.

[11] Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.

[12] Gummadi, V. P. K. (2023). MuleSoft batch processing: High-volume streaming architecture. Computer Fraud & Security, 50-57. https://doi.org/10.52710/cfs.886.

[13] Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4). https://doi.org/10.56975/jaafr.v1i4.501636.

[14] Maturi, S. Y. (2021). Blockbond hardening: Securing pooled-hash protocols against traffic tampering, MITM hash-rate hijacking, and template coercion. International Journal of Communication Networks and Information Security, 13(3), 718–728.

[15] Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465.

[16] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.

[17] Pokala, H. K., & Gummadi, V. P. K. (2026, April). Autonomous AI-Powered Resource Management for Apache Flink on Amazon EKS. In 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET) (pp. 1-4). IEEE.

[18] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, 2020.

[19] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, 2020.

[20] E. B. Fernandez and M. M. Larrondo-Petrie, "Security patterns for healthcare information systems," *Proceedings of the International Conference on Health Informatics*, 2010.