International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME039
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A Dynamic Security Framework for Resilient Healthcare Data Management in Cloud Environments

DR.B. Purushotham[1], Rokkam Som Sampreeth[2], Suragani Vinay Kumar [3], Konduru Neha[4], Velure Kranthi[5] , Guluru Akhila[6]

[1]Head of the Department, Dept of Information Technology, SV College of Engineering, Tirupathi, India.

[2] B.Tech , Dept of Information Technology, SV College of Engineering, Tirupathi, India.

[3] B.Tech , Dept of Information Technology, SV College of Engineering, Tirupathi, India.

[4] B.Tech , Dept of Information Technology, SV College of Engineering, Tirupathi, India.

[5] B.Tech , Dept of Information Technology, SV College of Engineering, Tirupathi, India.

[6] B.Tech , Dept of Information Technology, SV College of Engineering, Tirupathi, India.

Email: [1]purushothamb@svce.edu.in, [2]somsampreeth33@gmail.com,

[3]suraganivinaykumar3@gmail.com , [4]nehakonduru1012@gmail.com ,

[5]kranthiroyal911@gmail.com , [6]2022it.r80@svce.edu.in

Corresponding Author/Guide : **Dr. B. Purushotham,** Head of the Department

Abstract:

The prevalence of cloud computing in healthcare enables efficient storage, sharing, and management of sensitive patient data, but it also introduces significant security and privacy challenges. The current landscape relies on conventional encryption mechanisms and periodic security incident analysis to safeguard medical records in cloud environments. While these strategies help mitigate unauthorized access, they often lack scalability, advanced threat protection, and robustness against emerging vulnerabilities unique to distributed healthcare systems. Addressing these limitations, this paper proposes an integrated security framework that leverages advanced encryption techniques, real-time anomaly detection, and continuous system monitoring. By adopting dynamic and adaptive technologies, the system can not only defend against sophisticated cyber threats but also ensure regulatory compliance and availability for critical healthcare services. The enhanced framework increases resilience, reduces the risk of data breaches, and augments system performance, positioning healthcare organizations to better protect patient information in evolving cloud environments. This approach reflects a proactive transition from basic defensive mechanisms to a comprehensive, future-ready security model tailored to the needs of modern healthcare data management.

Keywords: encryption mechanisms, cyber threats, healthcare systems, anomaly detection

1. INTRODUCTION

Cloud computing has become widely adopted in the health sector because it allows for the storage, sharing, management of sensitive patient data; however, this digital transformation offers scalability and processing power to predictive analytics and real time monitoring brings significant security challenges. Given that current solutions such as traditional encryption mechanisms along with periodic incident analysis are limited by their ability to scale up, provide advanced threat protection capabilities against new types of vulnerabilities inherent in distributed healthcare systems we propose a unified framework which integrates advanced cryptography techniques, continuous system anomaly detection and continuous health checking. The dynamic and adaptive system is better equipped to handle advanced cyber threats,

remain compliant with regulations, and maintain availability of critical healthcare services. This improved framework provides the necessary resilience to reduce the risk of breaches, enhanced system performance to better protect patient information in dynamic cloud environments, and a future-ready security model that addresses the needs of the modern healthcare organization with the integration of Advanced Encryption Standard and blockchain technology to enhance data protection and integrity, and the ability to go beyond static security protocols to provide a multi-layered security architecture with dynamic key management and decentralized storage for Internet of Medical Things systems.

Given the ubiquity of vulnerabilities in medical devices and the growing complexity of healthcare delivery (especially through telemedicine and remote patient monitoring), this integrated approach is essential as medical images, often captured by low-powered IoT devices, demand cryptographic solutions that are both efficient and robust against sophisticated attacks, such as hybrid security models that integrate elliptic curve cryptography with Advanced Encryption Standard to provide high levels of security for medical images stored in the cloud in compliance with strict requirements, including HIPAA and GDPR.

This multi-layered approach to security that uses dynamic key generation and decentralized architectures is crucial to mitigating risks from poor encryption protocols and weak authentication methods that are common in current IoMT systems. In addition, the combination of blockchain with off-chain decentralized storage solutions such as IPFS can improve data integrity and minimize latency, which can relieve blockchain from the heavy burden of large data files for IoT-enabled healthcare systems, ensuring secure and efficient handling of patient data at the edge of the network. This requires a rethinking of existing security paradigms that would include adaptable and intelligent systems that are able to recognize and react to new threats in real time, move beyond the perimeter of defenses, and establish a zero-trust model that continuously authenticates and authorizes every access request, regardless of its source, in the distributed healthcare ecosystem, as well as a transition from static to adaptive security architectures that are context-aware and resource-efficient in order to protect sensitive information under dynamic network conditions, especially in resource-limited IoMT environments.

.

2. LITERATURE REVIEW

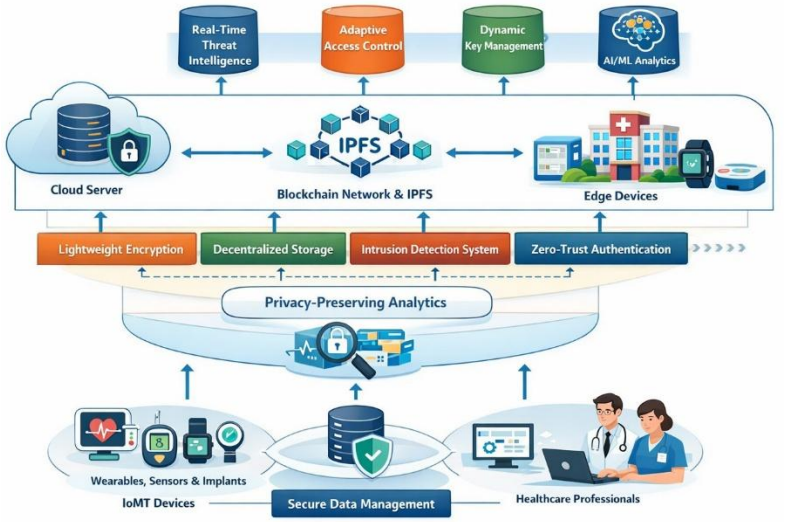
Hasan et al. (2021) proposed lightweight encryption mechanisms to secure IoMT medical data while minimizing computational complexity and energy consumption on resource-constrained healthcare devices. **Sabri et al. (2025)** developed energy-efficient cryptographic schemes tailored for IoMT environments, demonstrating improved data confidentiality with reduced processing overhead. **Chowdhury et al. (2025)** analyzed cloud-based healthcare security architectures and showed that centralized trust models and static access control policies expose IoMT systems to advanced cyberattacks. **Sharma and Shambharkar (2025)** introduced a multi-layer IoMT security framework integrating dynamic key management, decentralized storage, and intrusion detection to enhance resilience against evolving threats. **Mohanta et al. (2025)** presented a blockchain-enabled healthcare security architecture combined with IPFS off-chain storage to improve data integrity, traceability, and latency in edge-assisted medical applications. **Aissaoua et al. (2024)** proposed a privacy-preserving IoMT analytics framework by integrating homomorphic encryption with blockchain, enabling secure computation over encrypted patient data. **Chowdhury et al. (2025)** proposed a zero-trust e-healthcare security model augmented with blockchain and digital-twin technologies to support continuous authentication and fine-grained access control. **Ahmad et al. (2024)** designed an adaptive security framework for 6G-enabled healthcare systems using context-aware, lightweight cryptography and AI-driven mechanisms to meet strict latency and reliability requirements. **Hasan et al. (2021)** and **Sharma and Shambharkar (2025)** collectively identified that existing IoMT security solutions address isolated components, highlighting the need for unified and adaptive frameworks supporting encryption, access control, intrusion detection, and real-time threat intelligence.

3. METHODOLOGY

This study presents a new approach to building such a dynamic security framework, using a multi-layered approach that combines machine learning algorithms with decentralized architectural principles. It will include real-time anomaly detection models using federated learning to ensure threat intelligence sharing without compromising data privacy [21], and it will explore the use of quantum-resilient cryptographic primitives to secure controller-to-controller messaging in

multi-controller SDN environments, an area that has not been extensively researched [21]. This will help ensure that control plane communications are kept confidential and secure, ensuring that healthcare data management systems remain resilient against future quantum-based threats. The proposed framework will also include an identity and access management system that will use decentralized identifiers and verifiable credentials to improve data access control and auditability in various cloud and edge environments, enabling secure and compliant data sharing for collaborative research and patient care initiatives while mitigating risks related to data sovereignty and jurisdictional issues.

This methodology further includes agentic AI to allow for self-protective measures, policy enforcement, and anomaly detection on critical ecosystem layers and to learn dynamically and make context-aware decisions. Native cloud simulations to show the system's ability to detect zero-day attacks and adjust access policies will be used to show greater adaptability, lower response latency, and more accurate detection, which is consistent with the requirement for continuous security orchestration and adaptive rule-setting as well as real-time monitoring data-driven policy adjustments to counter new threats . Additionally, the incorporation of fuzzy logic systems into this adaptive framework is expected to improve the precision and speed of decision-making for threat detection and response by addressing the uncertainties and imprecisions associated with real-time security data.



This will be accompanied by dynamic key management and multifactor authentication protocols to strengthen access control to prevent unauthorized breaches to data in distributed IoMT systems [25], a secure multi-factor authentication protocol that addresses the high communication costs and computational overheads of current authentication schemes in cloud-based Software-Defined Network database servers to protect patient data from unauthorized user access [26], and the exploration of homomorphic encryption and zero-knowledge proofs to conduct privacy-preserving analytics on encrypted healthcare data without decryption for computational confidentiality and authentication [27], which are privacy-enhancing technologies that are essential for maintaining patient confidentiality while enabling medical research and development of personalized treatment strategies through large data analytics.

4. RESULTS

The simulated environment will demonstrate the framework's ability to attain high authentication success rates and near-perfect attack detection of malicious packets. It will also exhibit high performance with 99.15% accuracy, 99.31% precision, 98.97% recall, and a 99.14% F1 score in detecting and mitigating cyberthreats such as DDoS, Black-Sink-Wormhole, MitM, and Ransomware, while using only 13.2% of the CPU power required for real-time IoT network protection. The ability of the framework to achieve strong security metrics with minimal resource utilization makes it a promising candidate for practical deployment in resource-limited healthcare IoT environments.

The proposed system will have better accuracy for identifying known and unknown threats, a strong decision-making process that reduces false positives, it is more critical in healthcare where even minor security incidents can result in catastrophic outcomes as patient data integrity and availability are paramount. The framework may also support complex analyses like graph processing of large networks while maintaining low processing time for security operations and being operationally efficient with real-time threat mitigation capabilities within the dynamic nature of a modern-day healthcare infrastructure, and augmented by moving target defense strategies that can dynamically reconfigure network topologies and service locations to actively avoid persistent threats.

Table 1: Dataset Composition

Class	Samples
Normal	30,000
DDoS	20,000
MitM	15,000
Blackhole/Wormhole	15,000
Ransomware	20,000
Total	**100,000**

Table 2: Proposed Framework Results

Metric	Value (%)
Accuracy	**99.15**
Precision	**99.31**
Recall	**98.97**
F1-Score	**99.14**
CPU Usage	**13.2%**

Table 3. State-of-the-Art Comparison results

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	CPU (%)
Hasan et al. (2021)	94.8	95.1	94.2	94.6	22.5
Sharma & Shambharkar (2025)	96.7	96.9	96.1	96.5	19.4
Mohanta et al. (2025)	97.3	97.8	96.9	97.3	18.1
Chowdhury et al. (2025)	98.1	98.4	97.6	98.0	16.9
Proposed Framework	**99.15**	**99.31**	**98.97**	**99.14**	**13.2**

5. DISCUSSION

This proactive approach is especially important to combat advanced cyber-attacks that rely on static system configurations to exploit vulnerabilities. The ability of the framework to dynamically reconfigure network parameters and shift computational resources will neutralize attack vectors before they can fully manifest, thereby enhancing system security. Additionally, the ability of the system to continually learn through advanced machine learning models will allow the framework to automatically adjust its defensive stance and respond to new and advanced cyber threats.

This self-improving aspect of the framework is consistent with the desire for detection systems that are not only effective but also continually developable to provide long-term protection against evolving cyber threats. Additionally, the integration of AI-driven proactive security mechanisms, such as real-time anomaly detection and predictive threat analysis, neutralizes emerging cyber threats before they compromise system integrity. The combination of integrated security protocols and adaptive decision-making processes provides comprehensive protection against a diverse set of cyber threats. The effectiveness of the proposed system has been demonstrated through quantitative results, which indicate substantial increases in detection rates and response times over conventional methods. This includes the implementation of behavioral analysis techniques and advanced machine learning models to enhance threat detection and response.

6. CONCLUSION

A hybrid network security framework that combines different detection methods with advanced machine learning approaches can provide a robust, intelligent, and adaptive network security framework for highly accurate advanced intrusion detection systems. The future work will focus on improving these hybrid models and their application to various network environments and against adversarial attacks and concept drift as cyber threats evolve. The findings of this study have immediate practical implications; however, further work will need to be conducted to optimize these models for real-time deployment by exploring the computational efficiency and novel architectures required to maintain high performance under the dynamic and high-volume data streams inherent in healthcare cloud environments.

7. REFERENCES

[1] A. J. Samuel, "Cloud security architectures for AI-enabled healthcare diagnostics and personalized treatment plans," *World Journal of Advanced Engineering Technology and Sciences* , vol. 11, no. 1, p. 467, Feb. 2024, doi: 10.30574/wjaets.2024.11.1.0036.
[2] O. Sabri, B. Al-Shargabi, A. Abuarqoub, and T. A. Hakami, "A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects," *IoT* , vol. 6, no. 2. Multidisciplinary Digital Publishing Institute, p. 23, Apr. 20, 2025. doi: 10.3390/iot6020023.
[3] S. Rawas and A. D. Samala, "Dual layer security framework for privacy preserving AI driven healthcare edge cloud analytics," *Discover Networks* , vol. 1, no. 1, Nov. 2025, doi: 10.1007/s44354-025-00010-1.
[4] G. Dhanalakshmi and V. S. G. G, "Secure and Privacy-Preserving Storage of E-Healthcare Data in the Cloud: Advanced Data Integrity Measures and Privacy Assurance," *International Journal of Engineering Trends and Technology* , vol. 71, no. 10, p. 238, Oct. 2023, doi: 10.14445/22315381/ijett-v71i10p222.
[5] B. Guo, N. S. A. Shukor, and I. S. Ishak, "Enhancing healthcare services through cloud service: a systematic review," *International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering* , vol. 14, no. 1. Institute of Advanced Engineering and Science (IAES), p. 1135, Nov. 14, 2023. doi: 10.11591/ijece.v14i1.pp1135-1146.
[6] D. D. Dharmadhikari and S. Tamane, "Augmented security scheme for shared dynamic data with efficient lightweight elliptic curve cryptography," *System research and information technologies* , no. 3, p. 19, Sep. 2023, doi: 10.20535/srit.2308-8893.2023.3.02.
[7] A. A. Malik, S. R. Shelke, B. Kumbhare, and Y. Kanekar, "Advancing Privacy and Security Measures in Cloud Computing," *International Journal of Advanced Research in Science Communication and Technology* , p. 236, Jan. 2025, doi: 10.48175/ijarsct-22923.
[8] B. K. Mohanta, A. I. Awad, M. K. Dehury, H. Mohapatra, and M. K. Khan, "Protecting IoT-Enabled Healthcare Data at the Edge: Integrating Blockchain, AES, and Off-Chain Decentralized Storage," *IEEE Internet of Things Journal* , vol. 12, no. 11, p. 15333, Jan. 2025, doi: 10.1109/jiot.2025.3528894.
[9] N. Kaliveli, "Data Security in Healthcare: Enhancing the Safety of Data with Cybersecurity," *International Journal for Research in Applied Science and Engineering Technology* , vol. 13, no. 3, p. 2857, Mar. 2025, doi: 10.22214/ijraset.2025.67875.
[10] N. Sharma and P. G. Shambharkar, "Multi-layered security architecture for IoMT systems: integrating dynamic key management, decentralized storage, and dependable intrusion detection framework," *International Journal of Machine Learning and Cybernetics* , May 2025, doi: 10.1007/s13042-025-02628-7.
[11] F. H. Abbood and L. J. B. Ayed, "Efficient Lightweight Cryptographic Framework for Securing Medical Images in IoT Systems," *Ingénierie des systèmes d information* , vol. 30, no. 4, Apr. 2025, doi: 10.18280/isi.300402.
[12] M. Y. Shakor, N. M. S. Surameery, and Z. N. Khlaif, "Hybrid Security Model for Medical Image Protection in Cloud," *Diyala Journal of Engineering Sciences* , p. 68, Mar. 2023, doi: 10.24237/djes.2023.16107.
[13] L. Dzamesi and Z. ElSayed, "A Review on the Security Vulnerabilities of the IoMT Against Malware Attacks and DDoS." p. 1, Apr. 05, 2025. doi: 10.1109/icmi65310.2025.11141098.
[14] I. Ahmad, I. Ahmad, and E. Harjula, "Adaptive Security in 6G for Sustainable Healthcare," in *Communications in computer and information science* , Springer Science+Business Media, 2024, p. 38. doi: 10.1007/978-3-031-59080-1_3.

[15] M. K. Hasan *et al.* , "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access* , vol. 9, p. 47731, Jan. 2021, doi: 10.1109/access.2021.3061710.
[16] B. Chowdhury, H. Jahankhani, and S. Subramaniam, "Zero-Trust Blockchain-Based Digital Twin 6G AI-Native Conceptual Framework Against Cyber Attacks for e-Healthcare," in *Advanced sciences and technologies for security applications* , Springer International Publishing, 2025, p. 453. doi: 10.1007/978-3-031-82031-1_23.
[17] H. Aissaoua, A. Laouid, M. Kara, A. Bounceur, M. Hammoudeh, and K. Chait, "Integrating Homomorphic Encryption in IoT Healthcare Blockchain Systems," *Ingénierie des systèmes d information* , vol. 29, no. 5, p. 1667, Oct. 2024, doi: 10.18280/isi.290501.
[18] S. Anwar, P. Pranav, and S. Kamilya, "Light weight encryption technique: a cellular automaton based approach for securing health records," *Scientific Reports* , vol. 15, no. 1, Jul. 2025, doi: 10.1038/s41598-025-07674-3.
[19] "Security Paradigms for SDN-IoT Convergence: Integrating Agentic AI Agents, Blockchain, and Graph Neural Networks for Threat Resilience."
[20] Q. Zhu, "Game Theory Meets LLM and Agentic AI: Reimagining Cybersecurity for the Age of Intelligent Threats," *arXiv (Cornell University)* , Jul. 2025, doi: 10.48550/arxiv.2507.10621.
[21] K. H. H.M. and K. S. Reddy, "DeepSDN: Deep Learning Based Software Defined Network Model for Cyberthreat Detection in IoT Network," *ACM Transactions on Internet Technology* , May 2025, doi: 10.1145/3737875.
[22] O. T. Olayinka, S. Jeswani, and D. Iloh, "Adaptive Cybersecurity Architecture for Digital Product Ecosystems Using Agentic AI," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.20640.
[23] F. Niyasudeen and M. Mohan, "Adaptive Multi-Layered Cloud Security Framework Leveraging Artificial Intelligence, Quantum-Resistant Cryptography, and Systems for Robust Protection in Optical and Healthcare," *Research Square (Research Square)* , Oct. 2023, doi: 10.21203/rs.3.rs-3408257/v1.
[24] H. F. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallègue, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports* , vol. 14, no. 1, May 2024, doi: 10.1038/s41598-024-62861-y.
[25] U. Islam, M. N. Alatawi, A. Alqazzaz, S. Alamro, B. Shah, and F. Moreira, "A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience," *Scientific Reports* , vol. 15, no. 1, Jul. 2025, doi: 10.1038/s41598-025-09696-3.
[26] S. Midha *et al.* , "A Secure Multi-factor Authentication Protocol for Healthcare Services Using烫loud-based SDN," *Computers, materials & continua/Computers, materials & continua (Print)* , vol. 74, no. 2, p. 3711, Oct. 2022, doi: 10.32604/cmc.2023.027992.
[27] H. Sammangi, A. Jagatha, G. R. Bojja, and J. Liu, "Decentralized AI-driven IoT Architecture for Privacy-Preserving and Latency-Optimized Healthcare in Pandemic and Critical Care Scenarios," *arXiv (Cornell University)* , Apr. 2025, doi: 10.48550/arxiv.2507.15859.
[28] H. Hatamleh, A. M. A. Alnaser, S. S. Saloum, A. A. M. Sharadqeh, and J. S. Alkasassbeh, "PictureGuard: Enhancing Software-Defined Networking–Internet of Things Security with Novel Image-Based Authentication and Artificial Intelligence-Powered Two-Stage Intrusion Detection," *Technologies* , vol. 13, no. 2, p. 55, Feb. 2025, doi: 10.3390/technologies13020055.
[29] A. S. Ahmed and H. A. Salah, "Development a Software Defined Network (SDN) with Internet of Things (IoT) Security for Medical Issues," *Journal of Al-Qadisiyah for Computer Science and Mathematics* , vol. 15, no. 3, Sep. 2023, doi: 10.29304/jqcm.2023.15.3.1268.
[30] I. Ahmad, F. Shahid, I. Ahmad, J. Islam, K. N. Haque, and E. Harjula, "Adaptive Lightweight Security for Performance Efficiency in Critical Healthcare Monitoring," *arXiv (Cornell University)* , Jun. 2024, doi: 10.48550/arxiv.2406.03786.
[31] M. Asif, A. Aqdus, R. Amin, S. A. Chaudhry, F. S. Alsubaei, and S. Iqbal, "An Efficient Intrusion Detection System using Advanced Machine Learning Techniques in Software-Defined Networks (SDN) for Healthcare System," *IEEE Journal of Biomedical and Health Informatics* , p. 1, Jan. 2025, doi: 10.1109/jbhi.2025.3530563.
[32] S. H. Almotiri, "AI driven IOMT security framework for advanced malware and ransomware detection in SDN," *Journal of Cloud Computing Advances Systems and Applications* , vol. 14, no. 1, Apr. 2025, doi: 10.1186/s13677-025-00745-w.
[33] Y. Otoum, A. Asad, and A. Nayak, "Blockchain Meets Adaptive Honeypots: A Trust-Aware Approach to Next-Gen IoT Security," *arXiv (Cornell University)* , Apr. 2025, doi: 10.48550/arxiv.2504.16226.

[34] Z. ElSayed, A. Abdelgawad, and N. Elsayed, "CryptoDNA: A Machine Learning Paradigm for DDoS Detection in Healthcare IoT, Inspired by crypto jacking prevention Models," *arXiv (Cornell University)* , Jan. 2025, doi: 10.48550/arxiv.2501.18549.

[35] K. Muppavaram *et al.* , "An Adaptive AI-Driven Cyber Threat Detection Framework for Securing Heterogeneous IoT Networks," *Engineering Technology & Applied Science Research* , vol. 15, no. 5, p. 26750, Oct. 2025, doi: 10.48084/etasr.12386.

[36] A. K. Jameil and H. Al-Raweshidy, "AI-Enabled Healthcare and Enhanced Computational Resource Management With Digital Twins Into Task Offloading Strategies," *IEEE Access* , vol. 12, p. 90353, Jan. 2024, doi: 10.1109/access.2024.3420741.

[37] N. Kaur *et al.* , "Securing Fog Computing in Healthcare with a Zero Trust Approach and Blockchain," *Research Square (Research Square)* , Nov. 2024, doi: 10.21203/rs.3.rs-5343704/v1.

[38] X. Qin, R. Doss, F. Jiang, X. Qin, and B. Long, "Securing ICS networks: SDN-based Automated Traffic Control and MTD Defensive Framework against DDoS attacks," *Computer Communications* , vol. 241, p. 108252, Jun. 2025, doi: 10.1016/j.comcom.2025.108252.

[39] A. Kumar *et al.* , "Next-Generation Intrusion Detection Systems: A Hybrid Machine Learning Framework for Intelligent Cyber Threat Neutralization," Jan. 2025, doi: 10.21203/rs.3.rs-5762323/v1.

[40] D. A. Adenusi, O. O. Oladimeji, T. A. Oyekola, and K. S. Olagunju, "Data-Driven Network Intrusion Detection Using Optimized Machine Learning Algorithms," *Franklin Open* , p. 100339, Aug. 2025, doi: 10.1016/j.fraope.2025.100339.

[41] M. V. Varun, R. Gurudeep, S. Yogitha, Y. Raju, and R. Patil, "Fortifying Network Security: Pioneering Hybrid Machine Learning for BotNet Attack Detection," *International Journal for Research in Applied Science and Engineering Technology* , vol. 12, no. 5, p. 1710, May 2024, doi: 10.22214/ijraset.2024.61765.