JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 351 – 358 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4142
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

AI-DRIVEN HYBRID ENCRYPTION FOR SECURE ELECTRONIC MEDICAL RECORDS

Edy Prayitno[1*], Basuki Heri Winarno[1], Sri Setyowati[2], Sutono[2], Riyadi[3]
[1]Accounting Information Systems, Universitas Teknologi Digital Indonesia
[2]Nursing, Sekolah Tinggi Ilmu Kesehatan Surya Global
[3]Computer Science, Universitas Teknologi Digital Indonesia
email: [*]edyprayitno@utdi.ac.id

Abstract: In the era of sensitive health data and frequent cyberattacks, securing electronic medical records (EMR) has become a critical challenge. This study proposes a hybrid encryption framework combining Affine and AES algorithms with an AI-based key management module to enhance EMR security while maintaining efficiency. A dataset of 1,000 simulated records was evaluated using five cryptographic configurations: Affine-only, AES-only, RSA-only, Affine–AES, and Affine–AES with AI. Performance was measured through encryption/decryption latency and ciphertext size, while security was assessed under brute-force, SQL injection, and phishing simulations. The AI decision tree for key generation was evaluated using accuracy, precision, recall, F1-score, and entropy metrics. Results show that the AI-enhanced hybrid method eliminates brute-force success, introduces only minor latency overhead, and generates high-entropy keys with reliability above 98%. These findings indicate that integrating AI-based dynamic key regeneration into hybrid encryption can improve EMR security while remaining practical for clinical and cloud-based healthcare systems. Future work should involve real clinical datasets and explore post-quantum cryptographic extensions.

Keywords: AI key management; attack resistance; encryption performance; electronic medical records; hybrid encryption

Abstrak: Di era meningkatnya sensitivitas data kesehatan dan maraknya serangan siber, perlindungan Rekam Medis Elektronik (RME) menjadi tantangan penting. Penelitian ini mengusulkan kerangka enkripsi hibrida yang menggabungkan algoritma Affine dan AES dengan modul manajemen kunci berbasis AI untuk meningkatkan keamanan RME tanpa mengorbankan efisiensi. Dataset simulasi berisi 1.000 entri diuji menggunakan lima konfigurasi kriptografi: Affine-only, AES-only, RSA-only, Affine–AES, serta Affine–AES dengan AI. Performa diukur melalui latensi enkripsi/dekripsi dan ukuran ciphertext, sedangkan keamanan dievaluasi melalui simulasi serangan brute force, SQL injection, dan phishing. Model decision tree untuk manajemen kunci dinilai menggunakan metrik akurasi, presisi, recall, F1-score, dan entropi. Hasil menunjukkan bahwa metode hibrida dengan AI menghilangkan keberhasilan brute force, menambah overhead latensi yang minimal, serta menghasilkan kunci berentropi tinggi dengan reliabilitas di atas 98%. Temuan ini menunjukkan bahwa regenerasi kunci dinamis berbasis AI dalam skema enkripsi hibrida dapat meningkatkan keamanan RME sekaligus tetap praktis untuk sistem klinis dan layanan kesehatan berbasis cloud. Penelitian selanjutnya disarankan menggunakan dataset klinis nyata dan mengeksplorasi kriptografi pascakuantum.

Kata kunci: enkripsi hibrida; ketahanan serangan; kinerja enkripsi; manajemen kunci berbasis AI; rekam medis elektronik

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 351 – 358 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4142
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

INTRODUCTION

Electronic Medical Records (EMRs) and Electronic Health Records (ys) are integral to modern healthcare delivery, improving documentation quality, data accessibility, and care coordination across facilities [1], [2]. However, persistent challenges remain, including privacy concerns, interoperability limitations, and workflow disruptions, particularly in resource-constrained and specialized healthcare environments [3], [4].

As healthcare systems become increasingly digital and distributed, including IoMT-enabled ecosystems, the attack surface expands significantly. These systems face threats such as unauthorized access, ransomware, phishing campaigns, privacy breaches, and operational failures, intensifying the need for robust protection of sensitive medical data [5], [6]. To address these risks, recent approaches combine advanced cryptographic mechanisms—such as homomorphic encryption, attribute-based access control, and secure data-flow authentication—with distributed technologies like blockchain for immutable auditing and consent management, aiming to maintain confidentiality, integrity, and controlled access while preserving operational practicality [7], [8].

Widely used algorithms such as AES and RSA provide strong security but may introduce computational overhead in constrained environments, while lightweight ciphers such as Affine offer efficiency with weaker resistance to brute-force or injection attacks [9], [10]. Recent studies therefore explore optimized cryptographic primitives and learning-assisted mechanisms to balance security and performance in IoT and edge environments [9], [10], [11].

Despite these advances, methodological limitations persist in the literature. Many studies rely on simulated datasets without transparent utility-privacy analysis, omit key technical parameters, or lack standardized benchmarks for evaluating healthcare security and AI-based decision systems, complicating the reproducibility and generalization of results to real EMR environments [12], [13]. Consequently, empirical studies that report both performance and attack resistance under reproducible experimental setups remain necessary.

While previous work has investigated EMR protection using RSA, AES, or hybrid encryption approaches, most studies focus primarily on either algorithmic strength or computational efficiency. The integration of hybrid encryption with AI-driven key management—particularly to balance attack resistance with low-latency requirements in healthcare systems—remains relatively underexplored. Addressing this gap, this study proposes and evaluates a hybrid Affine–AES framework enhanced with AI-based key regeneration to assess its feasibility for securing EMR systems.

This study therefore aims to design and evaluate an EMR security framework integrating the Affine cipher, AES, and AI-based key management. The framework is assessed through encryption–decryption performance, resistance to brute-force and injection-style attacks, and the effectiveness of AI-generated keys measured through accuracy, entropy, and time-cost metrics. Building on advances in neural cryptosystems, decentralized key storage, and trusted key servers, the proposed approach seeks to combine strong security with operational efficiency suitable for clinical environments [14], [15], [16], [9].

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 351 – 358 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4142
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

METHOD

Dataset

This study used a simulated dataset of 1,000 EMR entries designed to approximate realistic clinical record structures while excluding identifiable patient information. Each record contains non-sensitive attributes (e.g., patient ID and demographic data) and sensitive clinical attributes (e.g., diagnoses, medication history, and laboratory results). Disease and medication distributions follow publicly available epidemiological statistics (e.g., WHO/CDC).

The dataset size was chosen to balance statistical reliability and computational feasibility for repeated encryption–decryption experiments across multiple algorithms. Each experiment was repeated 30 times per method, and results are reported as mean ± standard deviation (SD) to represent central tendency and variability.

The mean and standard deviation were calculated using the following expressions:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i, \qquad \sigma = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \mu)^2} \qquad (1)$$

where x_i denotes an observed measurement (e.g., encryption time) and n r epresents the number of repetitions.

Experimental Environment

Experiments were executed on a workstation with Intel Core i7 3.2 GHz CPU, 16 GB RAM, and Ubuntu 22.04 LTS. Implementations used Python 3.11 with PyCryptodome for cryptographic operations, Scikit-learn for AI modeling, and Pandas/Matplotlib for analysis and plotting. Fixed random seeds and consistent runtime conditions were applied to support reproducibility.

Hybrid Cryptographic System Design

The proposed encryption framework combines a lightweight Affine cipher with the Advanced Encryption Standard (AES) to form a layered hybrid cryptographic scheme. The Affine cipher is applied as an initial low-cost transformation to obfuscate plaintext, while AES performs the core encryption due to its well-established security and international standardization [17]. This layered design ensures that even if the preliminary transformation is compromised, AES continues to provide strong protection.

For comparison, the RSA algorithm was also implemented, as it is still used in certain legacy healthcare infrastructures despite its relatively high computational cost [18].

To strengthen key management, the framework integrates an AI-based decision tree model that generates high-entropy cryptographic keys and automatically regenerates them every 24 hours. This mechanism reduces the likelihood of key compromise and improves system resilience. The model choice follows established decision tree learning principles, which offer interpretable and computationally efficient solutions compared with more resource-intensive approaches such as deep neural networks [19].

Performance Testing Procedure

To evaluate system performance, five encryption configurations were tested: Affine-only, AES-only, RSA-only, Affine–AES, and Affine–AES with AI-based key management. Each method was applied to the same dataset of 1,000 EMR records, and experiments were repeated 30 times per configuration to reduce random variation. Results are reported in the Results and Discussion section using the statistical measures defined previously.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 351 – 358 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4142
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Performance was assessed using three metrics: encryption time (ms), decryption time (ms), and ciphertext size ratio relative to plaintext. Encryption and decryption time measure the computational overhead and practical usability of each method, while the ciphertext ratio reflects storage and transmission efficiency.

This evaluation design enables direct comparison across methods and highlights the trade-offs between computational performance and security improvements introduced by the proposed hybrid approach with AI-based key management

Attack Simulation and Resistance Testing

To assess security robustness, the proposed framework was evaluated against three common attack categories: brute force attacks at the cryptographic level, SQL injection targeting the application layer, and phishing injection representing user-level social engineering threats.

The brute force scenario was simulated using 10^6 iterations to approximate realistic computational constraints, while SQL and phishing injections employed standardized payloads commonly used in penetration testing. These attack types were selected because they represent computational-, application-, and user-level vulnerabilities, enabling a broader evaluation than purely cryptographic testing [20].

For each encryption configuration, 50 independent attack trials were conducted. Results are reported in the Results and Discussion section as mean ± standard deviation (SD) using attack success rate as the primary evaluation metric. This design enables assessment of both cryptographic resilience and system-level protection, particularly the contribution of AI-driven key regeneration to long-term resistance.

AI-Based Key Management Implementation

To support dynamic key generation, an AI-based decision tree model was implemented due to its interpretability, low computational cost, and suitability for lightweight security applications [19].

A total of 1,000 randomly generated key samples were used for training and validation. The model was configured with a maximum depth of 10 and evaluated using 5-fold cross-validation to balance complexity and generalization.

Performance was assessed using standard classification metrics (accuracy, precision, recall, and F1-score) together with Shannon entropy to measure key randomness. Results are reported in the Results and Discussion section as mean ± standard deviation (SD) across 30 runs, demonstrating the model's ability to generate high-entropy keys and improve resistance to brute-force and replay-type attacks.

RESULT AND DISCUSSION

Encryption and Decryption Performance

Performance evaluation covered five methods (Affine-only, AES-only, RSA-only, Affine–AES, and Affine–AES + AI). As summarized in Table 1, Affine-only achieves the lowest latency but offers limited protection, while AES-only and RSA-only strengthen security at the cost of higher runtime. The hybrid Affine–AES configuration provides a balanced trade-off between performance and security.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 351 – 358 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4142
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Table 1. Encryption–decryption performance (mean ± SD, n = 30)

Method	Enc (ms)	Dec (ms)	Ciphertext (%)
Affine	40 ± 2	35 ± 2	100 %
AES	420 ± 8	410 ± 9	130 %
RSA	680 ± 11	660 ± 10	145 %
Affine-AES	230 ± 6	220 ± 6	125 %
Affine-AES + AI	250 ± 7	240 ± 7	125 %

The comparative distribution of encryption times is illustrated in Figure 1, showing that the addition of AI-based key management introduces only minor overhead while improving resilience through periodic key regeneration.

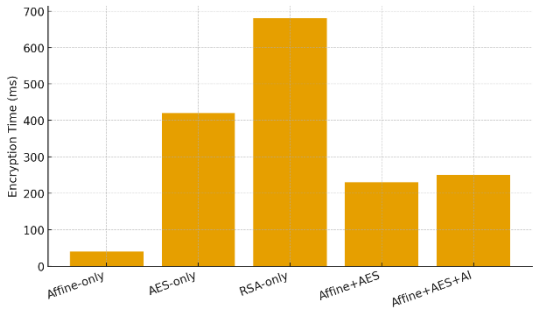

Figure 1. Encryption time across methods (mean ± SD, n = 30).

Affine-only exhibits the lowest latency but provides limited protection in adversarial settings, whereas AES-only and RSA-only strengthen security at the cost of higher runtime. The hybrid Affine–AES approach narrows this gap by retaining much of AES's protection while achieving substantially better runtime than RSA. Integrating AI-based key management introduces only modest overhead while improving resilience through periodic key regeneration, making the configuration suitable for EMR systems that require both low latency and strong confidentiality.

Resistance to Attacks

Security was evaluated using simulated brute force, SQL injection, and phishing injection. As reported in Table 2, Affine-only is highly vulnerable, particularly to brute force, whereas AES-only and RSA-only exhibit low success rates across attacks. The hybrid Affine–AES configuration performs comparably to AES-only and RSA-only, and the AI-enabled variant eliminates brute-force success by enforcing periodic key regeneration, while maintaining comparable resistance to injection-based attacks.

Figure 2 shows the comparative attack success rates across methods. Affine-only exhibits major weaknesses, reaching 78% under brute force and over one-third under injection attacks, whereas AES-only and RSA-only maintain very low success rates (<2% brute force and <10% injection).

Table 2. Attack Success Rates (mean ± SD, %, n = 50)

Method	Brute Force	SQL Inj.	Phishing
Affine	78 ± 2	35 ± 3	40 ± 4
AES	2 ± 1	5 ± 1	8 ± 2
RSA	1 ± 1	4 ± 1	7 ± 1
Affine-AES	3 ± 1	6 ± 1	9 ± 2
Affine-AES + AI	0 ± 0	5 ± 1	7 ± 1

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 351 – 358 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4142
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

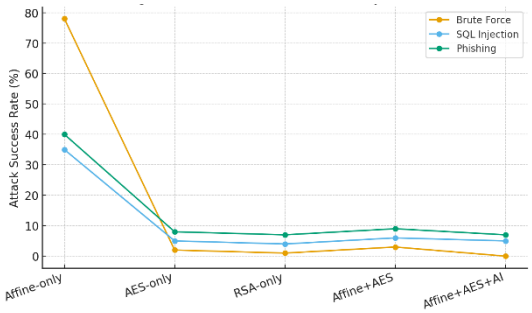

Figure 2. Simulated attack success rates by method (mean ± SD, n = 50).

AI-Based Key Management Evaluation

The performance of the AI-based decision tree for cryptographic key management was evaluated using accuracy, precision, recall, F1-score, and Shannon entropy. Results were obtained from 30 independent runs under a 5-fold cross-validation scheme to ensure stability and reliability.

Table 3. AI key management evaluation (mean ± SD, n = 30)

Metric	Value
Accuracy	98.7% ± 0.4
Precision	98.9% ± 0.3
Recall	98.5% ± 0.5
F1-Score	98.7% ± 0.4
Key Entropy	7.8 / 8 ± 0.1

The prediction distribution is illustrated in Figure 3, which shows the confusion matrix of the decision tree model. The near-diagonal pattern indicates minimal misclassification and confirms the consistency of the reported metrics.

Overall, the results demonstrate that the decision tree produces highly reliable predictions (>98% across metrics) while generating keys with entropy close to the theoretical maximum. This indicates that the AI module can generate statistically robust and unpredictable keys, supporting automated key rotation and improving resistance to brute-force and replay attacks in EMR security environments.

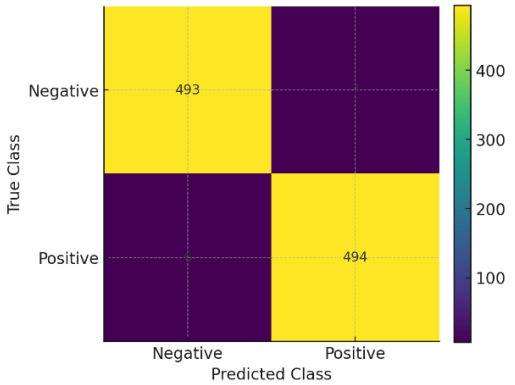

Figure 3. Confusion matrix of the AI decision tree model for key generation.

Discussion Synthesis

Overall, the results show that the hybrid Affine–AES design maintains operational efficiency while providing strong protection through AES. Integrating AI-based key regeneration improves long-term resistance to brute force with minimal overhead, offering a practical security configuration for latency-sensitive EMR systems.

CONCLUSION

This study proposed and evaluated an AI-driven hybrid encryption framework for securing electronic medical records by combining Affine preprocessing, AES core encryption, and decision-tree-based key management with periodic key regeneration. The results indicate that the hybrid design provides a practical balance between operational efficiency and robust protection, while automated key rotation strengthens long-term resilience against brute-force exposure without imposing excessive overhead. Scientifically, the work advances

EMR security by demonstrating an integrated, system-level approach that couples hybrid cryptography with adaptive key management, bridging performance constraints and evolving threat conditions. The proposed framework is applicable to clinical and cloud-based EMR environments that require both low latency and strong confidentiality; future work should validate the approach on real clinical datasets and extend comparisons to next-generation schemes such as post-quantum and privacy-preserving encryption.

ACKNOWLEDGEMENT

The authors acknowledge research funding from the Directorate General of Research and Development, Ministry of Higher Education, Science, and Technology of Indonesia under contract No. 126/C3/DT.05.00/PL/2025, and thank Universitas Teknologi Digital Indonesia and Sekolah Tinggi Ilmu Kesehatan Surya Global for their institutional support.

BIBLIOGRAPHY

[1] F. Wurster *et al.*, "The Analyzation of Change in Documentation due to the Introduction of Electronic Patient Records in Hospitals—A Systematic Review," *J Med Syst*, vol. 46, no. 8, p. 54, Aug. 2022, doi: 10.1007/s10916-022-01840-0.

[2] C. A. Rhoades, B. E. Whitacre, and A. F. Davis, "Higher Electronic Health Record Functionality Is Associated with Lower Operating Costs in Urban—but Not Rural—Hospitals," *Appl Clin Inform*, vol. 13, no. 03, pp. 665–676, May 2022, doi: 10.1055/s-0042-1750415.

[3] J. Kosteniuk *et al.*, "Factors identified as barriers or facilitators to EMR/EHR based interprofessional primary care: a scoping review," *Journal of Interprofessional Care*, vol. 38, no. 2, pp. 319–330, Mar. 2024, doi: 10.1080/13561820.2023.2204890.

[4] D. E. Detmer and A. Gettinger, "Essential Electronic Health Record Reforms for This Decade," *JAMA*, vol. 329, no. 21, p. 1825, Jun. 2023, doi: 10.1001/jama.2023.3961.

[5] A. López Martínez, M. Gil Pérez, and A. Ruiz-Martínez, "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–38, Dec. 2023, doi: 10.1145/3571156.

[6] M. Mahmood *et al.*, "Improving Security Architecture of Internet of Medical Things: A Systematic Literature Review," *IEEE Access*, vol. 11, pp. 107725–107753, 2023, doi: 10.1109/ACCESS.2023.3281655.

[7] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management With Attribute-Based Cryptographic Mechanisms," *IEEE Trans. Netw. Serv. Manage.*, vol. 20, no. 2, pp. 1759–1774, Jun. 2023, doi: 10.1109/TNSM.2022.3186006.

[8] I. Y. B., K. Iriyanta, Hendra, B. T. Sutrisno. Sp., H. Muhrial, and E. Prayitno, "Blockchain-Enabled Secure Federated Learning for Electronic Medical Records: A Scalable and Privacy-Preserving Framework," in *2025 8th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia: IEEE, Dec. 2025, pp. 827–833. doi:

10.1109/ISRITI68345.2025.11393406.

[9] Y. Sun, F. P.-W. Lo, and B. Lo, "Lightweight Internet of Things Device Authentication, Encryption, and Key Distribution Using End-to-End Neural Cryptosystems," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14978–14987, Aug. 2022, doi: 10.1109/JIOT.2021.3067036.

[10] G. Cassiers, L. Masure, C. Momin, T. Moos, and F.-X. Standaert, "Prime-Field Masking in Hardware and its Soundness against Low-Noise SCA Attacks," *TCHES*, pp. 482–518, Mar. 2023, doi: 10.46586/tches.v2023.i2.482-518.

[11] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3559–3591, Aug. 2022, doi: 10.1007/s40747-022-00667-z.

[12] C. A. Stevens *et al.*, "Ensemble machine learning methods in screening electronic health records: A scoping review," *DIGITAL HEALTH*, vol. 9, p. 20552076231173225, Jan. 2023, doi: 10.1177/20552076231173225.

[13] M. Zaresefat and R. Derakhshani, "Revolutionizing Groundwater Management with Hybrid AI Models: A Practical Review," *Water*, vol. 15, no. 9, p. 1750, May 2023, doi: 10.3390/w15091750.

[14] A. Badr, "Instant-Hybrid Neural-Cryptography (IHNC) based on fast machine learning," *Neural Comput & Applic*, vol. 34, no. 22, pp. 19953–19972, Nov. 2022, doi: 10.1007/s00521-022-07539-0.

[15] A. J. Hintaw, S. Manickam, S. Karuppayah, M. A. Aladaileh, M. F. Aboalmaaly, and S. U. A. Laghari, "A Robust Security Scheme Based on Enhanced Symmetric Algorithm for MQTT in the Internet of Things," *IEEE Access*, vol. 11, pp. 43019–43040, 2023, doi: 10.1109/ACCESS.2023.3267718.

[16] M. Li and N. Zhang, "Trajectory-Based Authenticated Key Establishment for Dynamic Internet of Things," *IEEE Access*, vol. 10, pp. 111419–111448, 2022, doi: 10.1109/ACCESS.2022.3215688.

[17] E. Prayitno, N. A. Setiyadi, E. Sofiani, E. Iskandar, B. H. Winarno, and S. Setyowati, "Hybrid Post-Quantum Cryptography (PQC) for Patient-Centric EHR," in *2025 8th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia: IEEE, Dec. 2025, pp. 834–840. doi: 10.1109/ISRITI68345.2025.11393211.

[18] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[19] J. R. Quinlan, "Induction of decision trees," *Mach Learn*, vol. 1, no. 1, pp. 81–106, Mar. 1986, doi: 10.1007/BF00116251.

[20] S. Li, K. Surineni, and N. Prabhakaran, "Cyber-Attacks on Hospital Systems: A Narrative Review," *The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice*, vol. 7, pp. 30–39, Sep. 2025, doi: 10.1016/j.osep.2025.03.002.