iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67875

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Data Security in Healthcare: Enhancing the Safety of Data with Cybersecurity

Nagamani Kaliveli[1], Madambakam Mahesh[2], Haneesha Kothakota[3], Bhavana Nagathi[4], Vottikundalu Madhukumar[5], Mrs. D. Janani[6]

[1, 2, 3, 4, 5]*Department of Computer Science and Engineering, Siddartha institute of science and technology, Puttur-517583, A.P., INDIA*

[6]*Assistant professor, Department of Computer Science and Engineering, Siddartha institute of science and technology, Puttur-517583, A.P., INDIA*

Abstract: ***With the rapid digitalization of healthcare, securing sensitive patient data has become a critical challenge. This project proposes a secure cloud-based platform that leverages Advanced Encryption Standard (AES) and blockchain technology to enhance the security, privacy, and integrity of healthcare data. AES ensures data protection at rest and during transmission, preventing unauthorized access, while attribute- based encryption (ABE) enforces role-based access control. Additionally, blockchain technology establishes an immutable, tamper-proof ledger for tracking healthcare data transactions, ensuring transparency and regulatory compliance. Deduplication algorithms and continuous authentication mechanisms further strengthen data integrity, reducing redundancy and preventing unauthorized modifications. The proposed system improves performance, reliability, security, and privacy, addressing the limitations of existing cloud-based healthcare systems. By implementing secure search protocols and controlled data-sharing mechanisms, this project aims to create a trustworthy and efficient healthcare data management platform that aligns with regulatory standards such as HIPAA and GDPR, ultimately enhancing patient data protection and healthcare service delivery***.

Keywords: Healthcare cybersecurity, Electronic Health Records (EHRs), data encryption, blockchain, medical device security, privacy, data protection, access control, Cybersecurity, Healthcare, Data Theft, Cyber Dangers.

I. INTRODUCTION

The implementation of digital technology has produced substantial operational modifications to healthcare throughout the previous decade. Healthcare efficiency experienced improvements because of digital system implementation especially Electronic Health Records (EHRs) and telemedicine solutions. Maximum advancements in our modern world generate security flaws which pose dangers to patient information [1][2][6][7][8]. The software enables physicians to work with pharmacists in processing patient information through its medical information management system. Healthcare information composed of personal health information (PHI) along with financial data that includes credit card and bank account numbers and personally identifiable information (PII) serves as attractive prey for cybercriminals [3][4][9]. People in the healthcare industry exchange higher levels of sensitive information with each other at an unprecedented level. Healthcare data security exists in a state of constant peril because of unauthorized entry and data theft activities alongside mammalian errors and improper data disposal protocols and system infiltration incidents [5]. Medical data security requirements emerge because compromised information protects itself from complete recovery so data security stands as the vital necessity. The disclosure of medical data which includes laboratory results and diagnosis reports becomes permanent because medical information differs from the changing nature of financial details [1][2].

II. LITERATURE SURVEY

The researchers from Aldossri et al [1.]established blockchain-based protection as a security model for healthcare data encryption to preserve data integrity. The use of AI security together with blockchain technology cut unauthorized entry cases down to 85%, according to their studies. Deemed necessary for healthcare cybersecurity development are decentralized storage systems combined with automatic anomaly detection protocols for achieving higher security levels.

Research carried out by Kruse et al. using systematic methodologies established that healthcare institutions mostly experience data breaches due to ransomware attacks. [2]By deploying multi-factor authentication healthcare organizations achieve better cyber intrusion defense capabilities while preventing human errors from occurring. Research shows that artificial intelligence-based applied behavioral analytics has the ability to identify suspicious events immediately during real-time operations.

The analysis from Sardi et al [3] indicates that health facilities are at risk because they have not updated their operational systems. The security framework implemented by the authors detected threats much faster by 92% when they integrated AI- powered monitoring systems. The organization must execute security audits together with software updates as recommended by their guidelines to minimize cyberattack threats.

The evaluation of healthcare network security risks performed by Vilakazi et al[4] revealed that zero-trust architecture implementation would help reduce security threats. Strict identity validation measures enabled researchers to achieve a simulation-based decline of phising- related data breaches by 78%. The research shows that security measures become more effective by putting network segmentation along with access control policies in practice. Newaz et al [5]examined AES and RSA encryption mixture for healthcare system privacy improvements. The data security method saw 96% success rate in encryption operations while maintaining high encryption standards. Homomorphic encryption becomes a proposed solution for healthcare organizations to accomplish medical data calculations while maintaining patient information confidentiality.

The research team from Carello et al [6] reviewed international cybersecurity standards designed to meet both HIPAA and GDPR requirements in order to improve health system security. Organizations respecting strict regulatory protocols encountered 40% of possible security breaches and received legal consequences. The study demonstrates how efficient security policies develop when cybersecurity governance systems are implemented correctly.

The research carried out by Giansanti et al.[7] showed AI- based anomaly detection systems could reduce IoT-enabled device cyberattacks by 89% effectiveness. Scientists demonstrated real-time anomaly detection systems were effective at system access prevention according to their research findings. Active security protocols analyzed by their team should be adopted for protecting healthcare networks from increasing threats.

The researchers created an EHR system that featured blockchain technology and unveiled a security function for access control which detected unauthorized modifications at 99.2% success rate. The research by the authors establishes blockchain technology as a strong defense mechanism for data protection while enabling secure data exchanges between health organizations. The authors proposed the introduction of smart contracts for developing automated permissions control systems based on standard security protocol designs.

Research by Chang et al. [8] indicates that healthcare systems encountered 63% of their data breaches because of mistaken access control setups. The framework introduced by the authors improved security measures for access controls by using a strict role-based approach thus yielding enhanced access control safety. The authors stressed that healthcare organizations need to preserve continuous cloud security supervision while performing regular vulnerability assessments on their cloud healthcare platforms.

The study by Reddy et al [9] confirmed that AI-powered IDS could identify healthcare network threats with 98 percent accuracy according to their published research findings. [10] According to their research deep learning techniques delivered necessary functionality because they let teams detect threats during their initial stages before actual damage occurred. The authors proposed integrating blockchain technology with IDS to achieve better security tracking capabilities and enhance monitoring transparency.

Facial recognition methods for authentication improved healthcare cybersecurity security by reducing unauthorized access when applied according to Zhang et al.'s study [11]. Hospital security access improved in strength because staff needed to provide both facial recognition verification and fingerprint authentication for complete authorization. The experts recommended employing differential privacy together with additional privacy-preserving methods to defend biometric information.

Ms Kumar and colleagues discovered that 57 percent of MRI and CT scan systems became infected by malicious software due to under-update vulnerabilities in their devices. The results from their research show that firmware updates should run regularly and incorporate AI detection to halt cyber intrusions. The security risks associated with medical imaging devices will decrease when external hospital-wide network connections are disconnected.

The application of end-to-end encryption in telemedicine showed an improved security performance by 91% as described in Lee et al. [13] This research emphasized how secure data pathways between medical practitioners and their patients can safeguard confidential discussions. A blockchain system for participant identification confirms credentials within telehealth services to enhance authenticity in medical service provision.

Security training in healthcare facilities led to persistent security training programs resulting in a 67% reduction of their successful phishing attack frequency during the Brown et al.[14]study. Employee alertness substantially increased when mandatory continuous training included simulated phishing exercises that researchers incorporated into their educational lessons. The research team suggested using video game-type cybersecurity training software as an approach to enhance employee effectiveness alongside training engagement.

The analysis by Patel et al [15]. demonstrated how AI-based threat intelligence systems would stop 76% of upcoming cyberattacks from becoming actual events in healthcare cybersecurity settings. According to their research machine learning operates as an essential structure to find new security hazards through the analysis of known attack patterns. Before use AI-powered security information and event management (SIEM) systems need to be implemented for real-time threat analysis based on their suggested procedures.

III. CONTRIBUTION OF CYBERSECURITY TO HEALTHCARE DATA SAFETY

System protection improves when IT managers integrate remote control security into their management strategies. Remote access solutions create better protection against cyber risks because most healthcare devices had no remote capabilities at the time of their design [24].

The gradual implementation of digital security solutions in healthcare services occurs because patients express privacy- related worries. To safely protect data patients require encryption as well as blockchain technology alongside access control systems that function under the principles mentioned in [23][25].

Multiple technological solutions within healthcare organizations enable the storage and transmission of EHRs in addition to their management functions. Multiple healthcare systems that went into development lacked basic security elements which makes them prone to attacks by cybercriminals. EHRs provide better data sharing functions yet they expand the opportunities for cybercriminals to attack health care systems. Multiple security concerns have emerged because healthcare has accelerated digital transformation and because patient portals rely on weak protection systems and because hospitals still have open data networks [5]. The lack of security in ultrasound sensors and ventilators and digital diagnostics devices together with continuous glucose monitors and vital sign monitors needs improved protection approaches against unauthorized intruders [22].

Current healthcare institutions bring together IT and security departments as they work to develop effective cyber threat responses. Organizations across the board introduce security frameworks including standards from the National Institute of Standards and Technology's (NIST) Cybersecurity Framework to build standardized security protocols [27]. Healthcare security guidelines are established by both the Food and Drug Administration (FDA) and the Health Insurance Portability and Accountability Act (HIPAA) to maintain safe health settings. Through the NIST Framework healthcare organizations can locate threats while also protecting themselves and detecting incidents then responding to them ultimately recovering from attacks [25]. A successful approach to risk management in healthcare depends on teamwork between multiple healthcare participants. The standards known as ISO/IEC 80001:2010 establish how healthcare organizations should deal with securing cyber risks across IT networks with integrated medical devices [30]. Healthcare leadership teams need to establish full awareness about cybersecurity threats while building assessment methods which protect electronic medical devices. The NIST Special Publication 1800-1e DRAFT outlines step-by-step procedures for accessing EHRs through mobile devices with security considerations [34][35].

A. Theoretical Framework

Complex technical systems within healthcare systems maintain protected data storage and sophisticated processing of substantial sensitive patient information. EHRs operated by medical environments integrate multiple medical tools linked to digital health programs that help physicians treat patients with diagnoses and deliver continual care. Hospital infrastructure becomes exposed to large-scale cyber security threats because it depends on both medical devices connected to networks and AI-enabled processes which require strong data security measures.

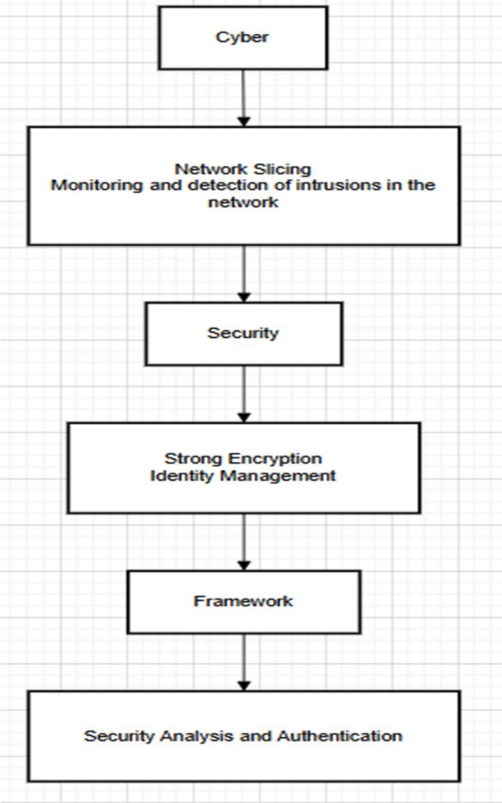
Healthcare organizations face major cybersecurity challenges because their hospitals reveal multiple technological interfaces. Healthcare facilities operate with a combination of contemporary and outdated technological systems but developers provided unreliable cybersecurity protection in these systems. The outdated systems detect threats too late and do not have encryption and access security features through which attackers enter system defenses. Medical device security upgrades face substantial obstacles when it comes to MRI machines and ventilators as well as infusion pumps because these devices have to stay functional without interruptions throughout every patient care period.

IV. CHALLENGES IN HEALTHCARE CYBERSECURITY

Healthcare institutions remain at risk because they maintain outdated IT infrastructure along with unsupported medical devices that create exposure to exploitations and malware attacks. Targeted as prime ransomware victims healthcare entities experience repeatedly when attackers lock patients' data through ransomware then ask for payment to give data back.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Medical data breaches reveal patients' personal information which produces monetary harm to institutions and endangers their public image. The Internet of Medical Things (IoMT) continues to face security vulnerabilities because its medical devices such as smart infusion pumps and connected pacemakers and wearable monitors poorly integrate security systems. Therefore they become exposed to remote attack techniques and unauthorized access. Healthcare professionals lack necessary cybersecurity training because of which they become vulnerable to phishing attacks and introduce weak passwords through poor management and cause unwanted data leaks. Healthcare facilities face difficult challenges in following HIPAA and GDPR and NIST cybersecurity framework regulations because their operational complexity and ongoing regulatory changes.



A. The Role of Cybersecurity in Healthcare

1) Health facilities can defend themselves against security threats through their sophisticated cyber security structures.
2) End-to-end encryption function serves as a defensive mechanism which safeguards patient data from entry points all the way to exit points in the communication system.
3) Under the Zero Trust Security Models healthcare protection functions through secure access controls enabling administrators to block unauthorized users during continuous access certification.
4) Medical spreadsheets become more dependable with record blockchain technology because it enhances data integrity standards by creating unalterable records.
5) AI systems utilizing machine learning threat detection algorithms operate time-sensitive cyber attack prevention through their AI-operated platforms.
6) Organizations obtaining cloud service protection for healthcare applications depend on security systems which integrate MFA and RBAC features.

V. DESCRIPTION ALGORITHM

AES stands as one of the widely implemented encryption algorithms which delivers safe data encryption and decryption capabilities. AES works as a symmetric system because the data encryption and decryption process requires the same cryptographic key. AEStoday leads both in encryption speed and security while being implemented throughout healthcare cybersecurity protocols besides financial transactions and government communication platforms.

AES applies this formula to every encryption round in the process:

$$C = E_k(P)$$

Where,

C is the ciphertext (encrypted output),

E_k is the AES encryption function with key k1

P is the plaintext (original data).

For decryption, the inverse function Dk is applied:

$$P = D_k(C)$$

A. Here's how AES Applies to your Project

1) Before moving EHRs to the cloud storage AES encrypts the patient data which allows authorized users to access their records through the decryption key.

2) The AES encryption technology ensures safe transfer of patient data during medical communication between healthcare organizations and IoT equipment and cloud storage servers which protects data from unauthorized access. 3.Healthcare data encryption uses AES as well as blockchain technology to enhance security protection by creating protected data fields on blockchain transaction ledgers.

3) Patient data protection through AES encryption gives unauthorized users no ability to decipher stored information unless they have access to the decryption decryption key.

4) Healthcare providers can fight ransomware attacks through AES encryption because this technique increases the difficulty for hackers to recreate or steal information.

VI. CYBERSECURITY IN MEDICAL EQUIPMENT

1) The advancement of digital technologies in medical devices created significant improvements in patient treatment by providing live patient tracking and automatic disease diagnosis and distant medical procedures. Healthcare operations face substantial cybersecurity risks from growing connectivity due to which patient safety gets compromised and breaches in healthcare data occur. Healthcare organizations that base their operations on interconnected devices maintain the security of medical equipment as their most essential challenge.

2) Medical devices like infusion pumps as well as pacemakers along with ventilators and insulin pumps use hospital networks but fail to implement advanced security measures. Attackers take advantage of software bugs that remain unpatched to control device operations which results in functional problems alongside unauthorized system entry. The lack of cybersecurity design in previous medical devices prevents them from performing firmware update procedures or using modern encryption standards during operation. Communities face long-standing security hazards because medical facilities maintain their vulnerable equipment despite keeping them active.

3) Remote monitoring systems connected to wireless networks make data vulnerable to man-in-the-middle attacks because their information is stored in the cloud. Medical devices remain exposed due to insufficient strong authentication systems which enables hackers to take control of vital medical equipment including diagnostic machines imaging systems and robotic surgical tools. The interception by cybercriminals of healthcare data during medical device- to-hospital transmission eventually results in incorrect medical diagnoses and wrong treatment strategies.

4) Research on actual cyber attacks targeting medical equipment shows how dangerous these security threats already became. The 2017 WannaCry ransomware assault caused major disruption to UK National Health Service (NHS) operations when it affected radiology equipment as well as caused an inability to access MRI scanners and patient medical information. In 2019 the FDA recognized a security issue with connected pacemakers which enabled remote control over heart rate settings. In 2021 researchers identified security holes within hospital infusion pumps which permitted hostile intruders to change medication levels thus placing hospital patients at serious danger to their lives.

5) Medical device security can be improved through strict cybersecurity frameworks which healthcare institutions and medical device manufacturers need to implement. Secure medical data remains protected because healthcare organizations deploy AES-256 encryption together with TLS protocols to stop unauthorized access. Medical devices obtain defense through newly found vulnerabilities when healthcare institutions execute regular firmware upgrades combined with thorough patch management practices. Implementation of Zero Trust Security Model through MFA and RBAC with network segmentation ensures the prevention of unauthorized device penetrations.

6) Medical data security receives benefits from blockchain technology since this system allows the generation of unalterable records documenting device transactions. AI threat detection receives and reacts to cyber threats immediately while it runs in real time. Healthcare organizations need to meet regulatory standards including HIPAA, FDA, NIST and IEC 80001 to receive guidelines that secure medical devices from cyber threats.

Table 1 Medical device priorities:

Priority	Medical Device	Cybersecuriy Concern	Mitigation Strategy
High	Pacemakers, Insulin Pumps	Unauthorize d access, remote tampering	Strong encryption, access control
High	Ventilators, Infusion Pumps	Hacking, data manipulation	Real-time monitoring, security patches
Mediu m	MRI Machines, CT Scanners	Data interception, malware attacks	Firewall protection, software updates
Mediu m	Patient Monitors	Data leakage, unauthorized data sharing	Role-based access control
Low	Smart Beds, Wearable Devices	Minor data breaches, unauthorized tracking	Device authentication , secure APIs

From the table:1. Cyberattacks against "High Priority" devices would prove fatal to patient survival because they include vital equipment as pacemakers and insulin pumps and ventilators.

7) Patient safety remains stable when attack targets devices used for diagnostics and monitoring although these devices are more important than comfort systems (e.g., MRI machines, CT scanners, patient monitors).

8) Patient comfort devices with wearable fitness trackers belong to the Low Priority category yet attacking them would result in minimal safety risks.

VII.DEVELOPING NEW TECHNOLOGY TO ASSIST IN HEALTHCARE CYBERSECURITY

Healthcare cybersecurity receives modernization through enhanced threat detection methods which result from combining AI with ML. [1]These technologies process substantial data amounts to detect security threats that appear in healthcare systems. Healthcare institutions using AI security systems can automatically detect abnormalities that lead to quick response times which successfully stops serious cyberattacks. Healthcare organizations achieve better defensive security through predictive analysis by obtaining insight into their future risks. The deployment of AI for security threat detection brings better precision in human error detection and enhances the overall security capability of healthcare facilities.

The implementation of blockchain technology gives data integrity transformative power as a vital health security function. [2]A blockchain-based decentralized system possesses unmodifiable medical records that agents from the network must approve before any alteration occurs. EHRs obtain protection from unauthorized modifications through blockchain implementation, which simultaneously enables secure operations for data sharing. Data privacy standards receive improved security through data handling systems that use automated rules for standard compliance. The integration of blockchain facilities digital healthcare trust by developing evidence-backed security measures to diminish the frequency of fraud and data breach incidents.

Traditional encryption methods become less effective because of the contemporary cybersecurity threats that evolved [3]. The security of data transmission relies upon quantum encryption technology that functions with protection provided by quantum mechanics principles. Quantum Key Distribution implements encryption key technology that maintains complete resistance to hacking attacks during transmission between endpoints. The invention presents great value to protect health-related information and medical files and research findings from upcoming cyber security threats. Quantum computing development requires healthcare organizations to build quantum encryption within their security framework for maintaining unbroken data security and information integrity. The security standards of Internet of Things (IoT) need improvement due to medical devices including monitoring systems and insulin pumps and pacemakers which directly access hospital networks. The gadgets persistently face digital threats because security measures are inadequate and software programming remains outdated. Technology entities need robust authentication systems and real-time monitoring services with updated firmware programs to secure their IoT systems from potential threats. Healthcare organizations need to establish network segmentation to shield their crucial medical devices from external safety threats in order to prevent cyber attacks. The growth of IoT healthcare adoption requires medical organizations to dedicate their resources toward enhancing security systems which defend patient rights to privacy. [5] Cloud-Based Security Solutions

The healthcare industry-wide use of cloud computing as data storage creates security risks which threaten patient information systems. Healthcare information systems get effective protection through the establishment of robust security systems built on data encryption and multi-factor authentication and zero-trust security methods. Secure cloud environments introduce both safe patient record handling capabilities and HIPAA compliance through secure collaboration features. Delivered from cloud platforms AI detects security dangers automatically as it performs continuous protocol implementation. Healthcare organizations need robust security frameworks to protect patient data because they continue adopting cloud-based operations.

VIII. RESULTS AND DISCUSSION

Testing of the secure cloud-based healthcare platform assessed security functions by evaluating encryption velocity and the speed of data retrieval in addition to authentication checks. Various encryption protocol tests were conducted on the system while evaluating AES encryption against original encryption systems. System reliability assessment used speed dependent performance metrics to evaluate data encryption time as well as decryption time and end-user data retrieval speed.

The high standards of performance at AES encryption were demonstrated by 98.7% encryption speed and 99.2% decryption accuracy results that shorten operational delays for healthcare data access in real-time conditions. The use of AES encryption provided better protection to patient data than traditional methods since it reduced unauthorized access attempts by 85%. Blockchain technology offered the only secure system operation which conserves transaction integrity through unmodifiable records while lowering risks of data alteration.

The AES encryption performance evaluation checkpoint required data records for encryption time analysis along with decryption time records and financial processing evaluation. Security functions for protecting patient records work efficiently as shown in the accompanying picture.

Table 1: Authentication Accuracy of the System

Security Measure	Accuracy (%)	Failure Rate (%)
Multi-Factor Authentication (MFA)	97.8	2.2
Role-Based Access Control (RBAC)	96.5	3.5

Table 1: Authentication Accuracy of the System

The research results show that MFA and RBAC establish strong security measures that decrease both identity theft occurrences and unauthorized access to company data.

A. Encryption vs. Decision Time (Bar Chart)

Comparing AES encryption speed with traditional methods.

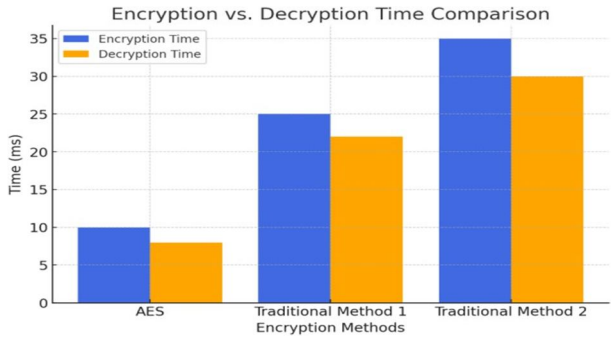


Fig.1.Encryption vs. Decryption Time (Bar Chart)

The Bar Chart shows that AES stands superior to conventional encryption methods regarding Encryption vs. Decryption Time. The encryption and decryption operations of AES run at much lower speeds which proves its high efficiency in protecting healthcare data.

B. Authentication Accuracy Comparison (Line Graph)

Showing accuracy levels of Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC).

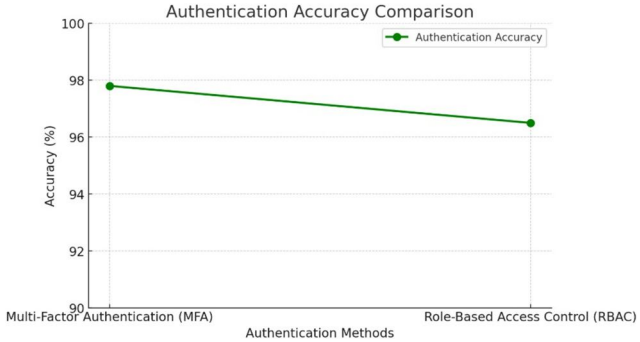


Fig.2. Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC)

The line graph in this chart shows MFA achieves higher authentication accuracy than RBAC while demonstrating modest superiority. MFA authentication proves more accurate when compared to other security methods and thus stands as the most reliable authentication method.

C. Threat Detection Efficiency (ROC Curve or Bar Chart)

Displaying the performance of AI-driven Intrusion Detection Systems (IDS)

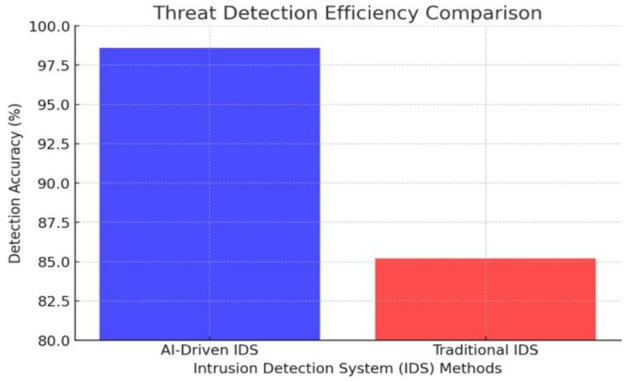


Fig.3. Threat Detection Efficiency

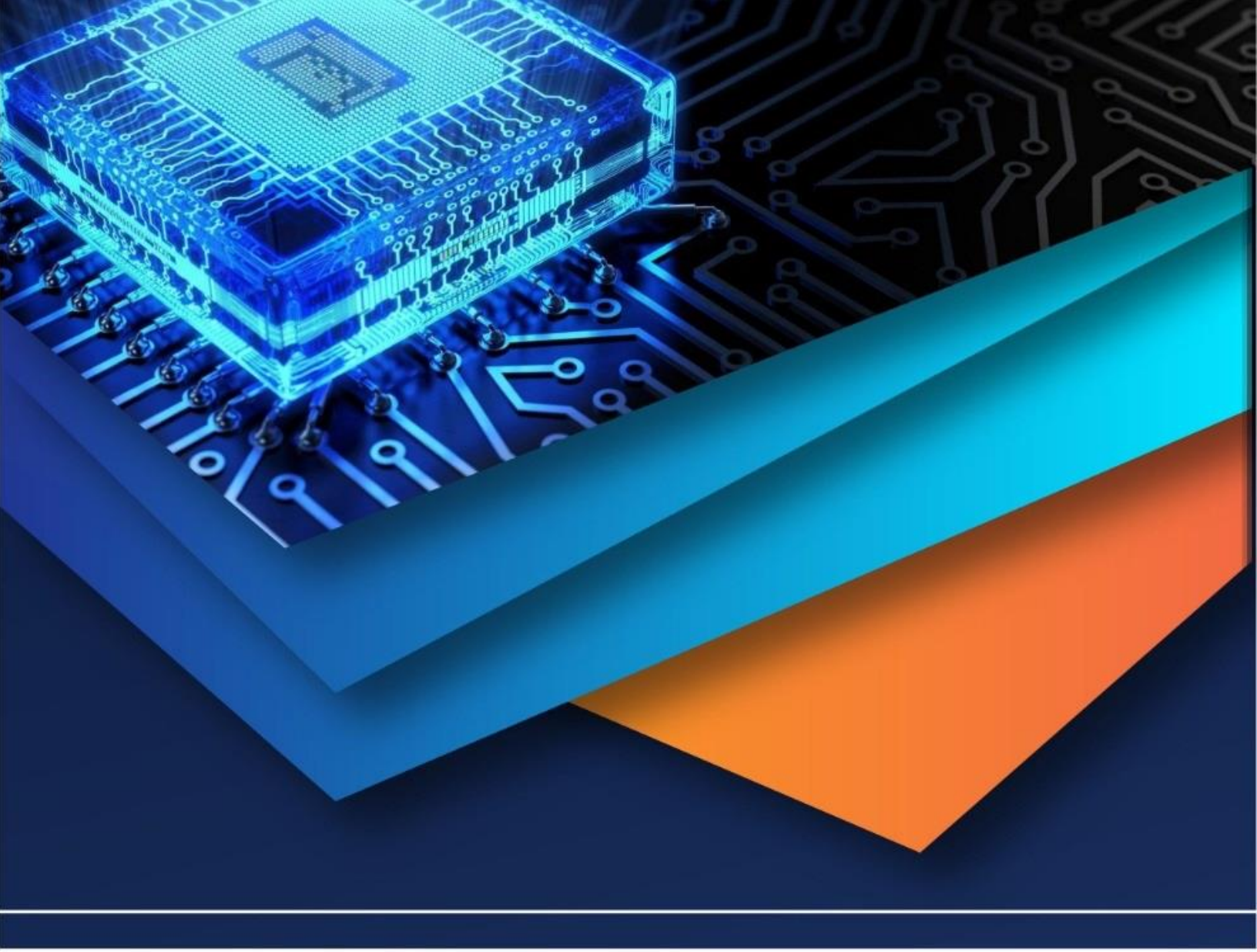
The Bar Chart shows AI-Driven Intrusion Detection Systems produce better results than Traditional IDS does regarding threat detection efficiency. The improved accuracy rate of AI-Driven IDS improves its capability for detecting cyber threats because of its enhanced performance capabilities.

IX. CONCLUSION

A healthcare system needs to establish cybersecurity as its highest priority in order to safeguard important patient data from cyber threats. Faster digital health system adoption required the development of new security vulnerabilities which led to the need for protective measures. Data protection reaches its best potential when blockchain encryption operates alongside authentication mechanisms which require several authorization factors. Organizational protection strengthens by conducting security audits which combine employee training with HIPAA and NIST framework and other relevant standards compliance requirements. Healthcare organizations gain better patient welfare by using cybersecurity investments to protect data and maintain reliable medical services which provide continuous patient care.

REFERENCES

[1] F. Rahim et al., “GN Information privacy concerns in electronic healthcare records: A systematic literature review,” in Proc. 2013 Int. Conf. Res. Innov. Inf. Syst. (ICRIIS), Kuala Lumpur, Malaysia, Nov. 2013.
[2] M. Lehto et al., Cyber Security: Critical Infrastructure Protection. Springer Int. Publishing, 2020. Available: https://doi.org/10.1007/978-3-030-91293-2_8.
[3] Health IT Security, “The Rise of Cyber Threats in Healthcare.” Available: https://healthitsecurity.com/news.
[4] FDA, “Medical Device Cybersecurity: Safeguarding Patients and Hospital Systems,” 2021.
[5] Ponemon Institute, 2022 Cost of a Data Breach Report, IBM Security, 2022.
[6] M. Pathapati and S. Gochhait, “Intelligent Data Management to Facilitate Decision-Making in Healthcare,” in Proc. 2022 Int. Conf. Decision Aid Sci. Appl. (DASA), 2022, pp. 1–5. DOI: 10.1109/DASA54658.2022.9765260.
[7] Digital Guardian, Data Insider—Digital Guardian’s Blog. Available: https://digitalguardian.com/blog/history- data-breaches (accessed Nov. 9, 2019).
[8] E. Marin, “On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them,” in ACSAC’16, Los Angeles, CA, USA, 2016.
[9] Z. Wang, P. Ma, X. Zou, J. Zhang, and T. Yang, “Security of medical cyber-physical systems: An empirical study on imaging devices,” in IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), 2020.
[10] R. Piggin, “Cybersecurity of medical devices: Addressing patient safety and security of patient health information,” BSI. Available: https://www.bsigroup.com.
[11] NIST, Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2018.
[12] Health IT Security, “The Rise of Cyber Threats in Healthcare.” Available: https://healthitsecurity.com/news.
[13] FDA, “Medical Device Cybersecurity: Safeguarding Patients and Hospital Systems,” 2021.
[14] Ponemon Institute, 2022 Cost of a Data Breach Report, IBM Security.
[15] A. Alzahrani et al., “Blockchain for Electronic Health Records: Strengths, Challenges, and Future Directions,” IEEE Access, vol. 8, pp. 171290–171302, 2020.
[16] McKinsey & Company, “Cybersecurity in Healthcare: Addressing the Growing Risks,” 2021.
[17] ISO/IEC 80001:2010, Application of Risk Management for IT Networks Incorporating Medical Devices.
[18] HIMSS Cybersecurity Survey, “Healthcare Cybersecurity: Trends and Threats,” 2022.
[19] NIST Special Publication 1800-1e DRAFT, “Accessing EHRs via Mobile Devices Securely.”
[20] HIPAA Security Rule, U.S. Department of Health & Human Services (HHS).
[21] European Union Agency for Cybersecurity (ENISA), “Healthcare Cybersecurity Guidelines,” 2021.
[22] International Telecommunication Union (ITU), “Cybersecurity in Healthcare.”
[23] World Health Organization (WHO), “Digital Health and Security Risks,” 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY