Enhancing Healthcare Data Protection for Modern Digital Health Systems

Sura Abdulkareem Abbas, Hassan Jaleel Hassan and Ghaidaa M. Abdulsaheb
Department of Computer Engineering, University of Technology, 10066 Baghdad, Iraq
ce.23.03@grad.uotechnology.edu.iq, hassan.j.hassan@uotechnology.edu.iq, Ghaida.M.Abdulsaheb@uotechnology.edu.iq

Keywords: Healthcare Data Protection, Digital Health Systems, Encryption, Artificial Intelligence, Blockchain Solutions.

Abstract: In addition to transforming healthcare delivery, digital health technologies have also posed significant challenges related to data security and privacy. HIPAA and GDPR compliance, emerging technologies, and best practices are discussed in this paper examining healthcare data protection today. Cryptography, access control, data anonymization, and blockchain-based approaches are key solutions discussed to improve data integrity and security. Moreover, artificial intelligence has the potential to detect and mitigate real-time security threats. This paper proposes strategies for ensuring patient safety, building trust, and protecting sensitive healthcare information as digital health technology continues to develop. Regulatory compliance and robust security measures are key to protecting patient information while fostering digital health innovation. With these challenges addressed, the healthcare industry can enhance patient experiences and maintain patient confidentiality as the landscape becomes increasingly digital.

1 INTRODUCTION

In recent years, digital technologies have transformed the way health data is collected, stored, and processed [1]. Modern digital health systems are revolutionizing patient care with electronic health records, wearable devices, telemedicine platforms, and mobile health applications. The advancement of these technologies has resulted in improved patient outcomes, more efficient workflows, and more personalized treatments. As digital health solutions are increasingly adopted, securing sensitive healthcare data is becoming more challenging. As a sector, healthcare is both valuable and vulnerable [2]. Medical services and the public's trust in electronic health are under threat from this data breach since it threatens not only patient confidentiality, but also medical services. With the proliferation of connected devices and the growing amount of health data being transferred across multiple platforms, healthcare organizations are increasingly forced to implement robust security measures to prevent cyberattacks, unauthorized access, and data misuse.

Besides securing sensitive healthcare information, we comply with regulations like HIPAA and GDPR by incorporating emerging technologies. Interoperability and secure data sharing across healthcare systems can be achieved through blockchain technologies. It will be discussed in further detail how artificial intelligence and machine learning can be used to detect and mitigate threats in real-time [3]. Strengthening healthcare data protection is essential to building trust, ensuring patient safety, and enabling further innovation. An overview of the current state of healthcare data protection is provided in order to provide strategies to safeguard sensitive health information in an increasingly digital and interconnected world. Information and Communication Technology (ICT) has made tremendous advances worldwide, replacing centralized computer systems with distributed networks and computing environments. Different computing systems can be connected over the Internet and through local area networks, which is why many modern applications utilize them. Healthcare, as an example, benefits greatly from a Web-based infrastructure [4].

It should be noted, however, that security is a major concern, particularly since privacy can be compromised in a variety of ways over the Internet. By collecting, processing, and sharing personal data online, the public is putting its privacy at risk, which is its main protection when using the Internet. Further, a Business Week survey [5] indicates that users are more reluctant to use the Internet due to the

lack of privacy than due to costs, difficulty using a service, or unwanted marketing messages. Providing healthcare services in modern medical environments [6], [7] and especially in shared care environments [8] makes the problem worse since multiple healthcare professionals may be located in different, sometimes distant, healthcare facilities. Across the country and/or internationally, networks of general practitioners, hospitals, and social service agencies are designed and developed using standardized electronic patient records. In response to the growth of these networks, sensitive medical information is being collected, stored, shared, and transferred to different places worldwide [9]. These environments may also facilitate telemedicine transactions between the patient and the healthcare organization. The vast majority of these transactions, even those involving personal information or medical records, are done online. It is, therefore, necessary to implement specific measures to ensure that users have access to and process personal data only when it is necessary for them to carry out their authorized tasks and that the purpose of data processing is aligned with the reason for which it was obtained [10].

To maintain integrity, confidentiality, availability, and accountability, a telecommunication network must meet additional technical, procedural, and organizational requirements. It is common for security and privacy to be confused in the literature. Information can be classified as secure or private based on the protection of its contents or the protection of its owner [11]. Security means protecting a piece of information's content, while privacy means protecting the identity of its owner. Technology has been employed to protect privacy in a variety of ways [12]. To ensure that your data is protected, you need more than just a secure infrastructure and a long list of technical countermeasures. Information management means the process of collecting, using, sharing, protecting, renting, and selling information. A society based on information considers privacy a fundamental right [13] - [15].

2 LITERATURE REVIEW

Medical information has become increasingly sensitive, and digital health systems are becoming more prevalent. Data security has therefore become a major concern. A variety of approaches have been used to protect healthcare data, including encryption and access control, as well as advanced technologies like blockchains and machine learning. In this section, we examine how digital health systems can improve the security of healthcare data.

2.1 Threats to Healthcare Data Security

Cyber threats threaten the privacy and security of patient data. As part of the cyber threat landscape, there are ransomware programs that encrypt data and demand a ransom in exchange for its recovery. An insider threat is when an employee misuses or steals sensitive information through phishing emails. Health care organizations need robust security strategies to combat cyber threats. In recent years, healthcare systems have been exposed to increasing levels of cyberattacks [16]. The value of sensitive health information lends itself to an increase in cybersecurity threats in the healthcare sector, which makes it imperative for healthcare organizations to prioritize data protection and cybersecurity [17], [18]. Aside from posing a threat to patients, healthcare providers, and the health system at large, such threats can also have devastating consequences.

In the event of a cyberattack on an electronic health record system or a connected medical device, there can be grave consequences. Since EHRs store so much data, hackers may find them attractive. The digital transformation of healthcare poses cybersecurity risks such as ransomware, data breaches, and other threats [19]. A hacker can also access patient data from Internet-connected devices, such as insulin pumps, pacemakers, and monitoring systems. Cyber security is a concern for healthcare organizations due to modern trends and threats, which require continuous monitoring and adaptive security measures [20], [21]. The healthcare ecosystem is becoming more interconnected, leading to cybersecurity vulnerabilities, emphasizing the need to secure all connected devices [22]. Healthcare organizations need robust security measures to protect EHR systems and connected medical devices from cyberattacks.

2.2 Regulatory and Legal Frameworks for Data Protection

Regulatory and legal frameworks play a significant role in protecting healthcare data. Patient information is protected under a number of legal frameworks, including privacy and security laws. There are many regulations within the healthcare industry, including HIPAA, which aims to protect sensitive patient information. Health care organizations are required to comply with a number of regulations, including

HIPAA, which sets standards for protecting sensitive patient data. In accordance with HIPAA, researchers can use patient data responsibly [23]. Healthcare organizations should adhere to regulatory standards such as HIPAA to maintain efficiency and usability while also taking advantage of cloud computing's benefits [24]. Health care organizations must comply with these regulations while also implementing their security policies and procedures.

Data collectors and processors are required to comply with strict requirements under the General Data Protection Regulation (GDPR). It is possible to develop trustworthy healthcare systems by adhering to standards such as the General Data Protection Regulation (GDPR), which demonstrates a commitment to privacy and security [25]. A robust security system must be implemented to safeguard the personal information of individuals under GDPR. To establish trust and protect sensitive information, secure data management is essential [26].

2.3 Encryption Techniques for Healthcare Data

Encrypting sensitive information is one of the most important security measures in healthcare. When data is encrypted, it can't be read without a decryption key, which is required to restore it to its original form. In this project, AES will be used to enhance the security, privacy, and integrity of healthcare data. Security levels are high because AES-256 encryption is used to protect data. Developing trustworthy systems requires the combination of authoritative artificial intelligence algorithms and strong encryption [25], [27]. The data of patients is encrypted during transit as well as at rest in order to protect their privacy.

For healthcare records, it provides high levels of security through the AES algorithm (Advanced Encryption Standard). An AES block cipher uses keys of 128 bits, 192 bits, or 256 bits to encrypt data. An encryption's security depends on the key's size. Security, privacy, and integrity are enhanced by encrypting healthcare data with Advanced Encryption Standard (AES). Using AES-256 encryption, the proposed system provides high levels of protection against unauthorized access [28]. Developing trustworthy systems requires the combination of authoritative artificial intelligence algorithms and strong encryption. Even though many hardware and software vendors support AES, it is still a practical and cost-effective solution for healthcare encryption.

3 PROPOSED METHODOLOGY

3.1 Proposed Security Management Design in Smart Healthcare Systems

In smart healthcare, advanced encryption techniques, IoT, cloud computing, and security management are integrated to provide secure communication and data privacy.

3.1.1 Data Collection via IoT Sensors

Wearable sensors based on IoT were used to collect data related to COVID-19 on a local and global scale. These devices are needed to support the administration of electronic medical records (EMRs).

3.1.2 Encryption Using Serpent and LRO Algorithms

Using the Serpent encryption algorithm, data is transmitted securely from IoT devices. During the Serpent encryption process, the secure key was generated using the LRO (Lionized Remora Optimization) algorithm.

3.1.3 Cloud Storage and Vulnerabilities

IoT wearable devices collected data that was stored in the cloud. Nevertheless, this setup exposes the system to possible hacker attacks and privacy violations.

3.1.4 Asymmetric Hash Signature Function for Authentication

In order to ensure authentication and validation between sender and receiver, an asymmetric hash signature function has been incorporated. The sender and recipient both possess the same role (for example, medical professionals within the same institution), but only the secret key is sent to the recipient.

3.1.5 Application in Hospital Environments

For hospital-based medical professionals, a similar process was implemented to ensure sensitive patient information was accessible and interpreted only by authorized personnel.

3.1.6 Lionized Remora Optimization Algorithm

Simulated lion behaviours, including hunting, mating, and defence, were used to develop LOA. Organizational behaviour in lions is divided into two types: resident behaviour and nomadic behaviour. Pride is a group of residents. Neither resident nor nomad lions are immune to becoming extinct. LOA generates the initial population randomly over the solution space, where each solution is called a "Lion". Nomad lions make up %N of the population, while residents make up the rest. Most of the population is made up of nomads, while the remainder is made up of residents. A random division of residents is made into pride based on (P). Female lions comprise (%S) of each pride, whereas male lions comprise the rest. Nomadic lions, however, have the opposite proportions.

3.1.7 Initialization

Initial population generation was done randomly by the LOA. A "lion" was assigned to every individual solution. Lions are defined as follows in N_v dimension optimization problems

$$Lion = [x_1, x_2, x_3, \dots., x_{N_v}]. \quad (1)$$

3.1.8 Free Travel (Exploration)

Remoras tend to move with sailfish when they are adsorbed on them. Based on the formula of the SFO algorithm, the following formula represents the elite strategy of the algorithm:

$$X_i^{t+1} = X_{best}^t - (rand * \left(\frac{X_{Best}^t + X_{rand}^t}{2}\right), -X_{rand}^t, \quad (2)$$

There are three current iterations for a remora, t, X_{Best}^t, and X_{rand}^t.

Remoras move around hosts in a small range once they are adsorbed on them, depending on the position of past generations of remoras and their current hosts. As we gain experience, we go through this process. As a mathematical calculation, we use the (3):

$$X_{att} = X_i^t + \left(X_i^t + X_{pre}\right) \times randn. \quad (3)$$

The remora moves tentatively with X_{att}. An experience can be considered. X_{pre}, the position of the previous generation of remora. Last but not least, $randn$ is a random number whose distribution is normal.

According to (4), a remora that is limited in its range of movement will decide whether to switch hosts or not. In (5), the host switching formula is shown:

$$f(X_i^t) < f(X_{att}), \quad (4)$$

$$H(i) = round(rand). \quad (5)$$

Remora adsorbed a host, and $H(i)$ determines the host. A rounding function is a function with rounded values, while $f(X_i^t)$ and $f(X_{att})$ are fitness values for X_i^t and X_{att}, respectively.

The remora moves in synchrony with the host when it is a whale. Here are the (6) - (9) for the calculation:

$$X_i^{t+1} = D * e^t * \cos(2\pi a) + X_i^t, \quad (6)$$

$$D = |X_{best}^t - X_i^t|, \quad (7)$$

$$l = rand * (a - 1) + 1\,, \quad (8)$$

$$a = -\left(1 + \frac{t}{T}\right). \quad (9)$$

3.2 Improved Serpent Algorithm

With the chain ring-based algorithm, 256-bit keys are used to encrypt blocks of size 128 bits. Algorithms consist of three basic functions: initial permutations, rounding, and final permutations. In this cryptosystem, S-boxes are obtained from multiplicative chains of commutative types of the form. $R_8 = \frac{F_2[x]}{<x^8>} = F_2 + xF_2 + x^2F_2 + \cdots \dots x^7F_2$. As can be seen throughout the algorithm, additions and multiplications correspond to chainrings, i.e. R_8 has a multiplication operation corresponding to Z_{2^8}, the local ring of integers modulo, and an addition operation corresponding to the Galois field F_{2^8}. S-box substitutions also differ from literal substitutions. S-boxes are operated with 128-bit blocks, and the results appear in chains. R_8 and S9. Using chain rings as a basis, the SERPENT algorithm is explained in the following sections:

$$B_0^{'} = IP(P), \quad (10)$$

$$B_{i+1}^{'} = LT(S_{imod4})(B_i^{'} \oplus K_i^{'})); 0 \le i \le 20, \quad (11)$$

$$B_{32}^{'} = S_3(B_{21}^{'} \oplus K_{21}^{'}) \oplus K_{22}^{'}\ , \quad (12)$$

$$C = FP(B_{22}^{'})\,. \quad (13)$$

The linear transformations (LT) are derived from the original Serpent algorithm created by Eli Biham and Ross Anderson (Technion Israeli Institute of

Technology, University of Cambridge Computer Laboratory, and University of Bergen, respectively). Divide the given 128-bit input into 4 32-bit blocks. Follow these steps to transform your data:

$$x_0 = x_0 \lll 13$$
$$x_2 = x_2 \lll 3$$
$$x_1 = x_1 \oplus x_0 \oplus x_2$$
$$x_1 = x_1 \lll 1$$
$$x_3 = x_3 \lll 7$$
$$x_0 = x_0 \oplus x_1 \oplus x_3$$
$$x_2 = x_2 \oplus x_3 \oplus (x_1 \lll 7)$$
$$x_0 = x_0 \lll 5$$
$$x_2 = x_2 \lll 22$$

By joining the $x_0, x_1. x_2$ and x_3 As a result of the above equations, we are able to get the LT result.

4 RESULT ANALYSIS AND DISCUSSION

Based on the proposed model, Figure 1 illustrates a comparison of encryption times. Increasing data size naturally increases encryption time. As a result, the proposed technique outperforms traditional methods on various file sizes, such as 100KB, 200KB, 300KB, 400KB, and 500KB, because it is significantly faster than previous encryption methods.

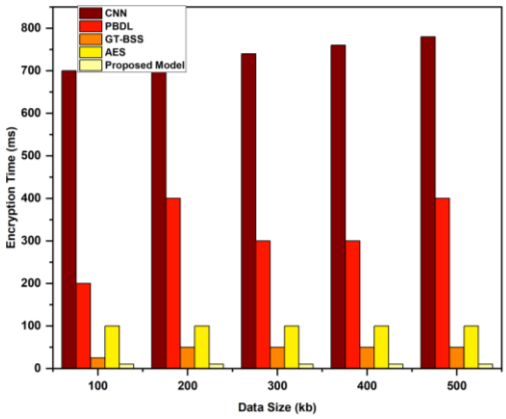

Figure 1: Analysis of variations in encryption time.

According to Figure 2, a proposed model requires a shorter decryption time than any existing model. Decryption times increase proportionally to the size of the data. Based on the results, the proposed method outperforms conventional approaches for files in the 100KB, 200KB, 300KB, 400KB, and 500KB size ranges. The proposed model also offers significant advantages, as it decrypts data substantially faster than previous systems.

While energy consumption decreases with increasing data volume, charge drain increases with increasing data volume, as shown in Figure 3. Cost-effectiveness is observed in addition to resource optimization.

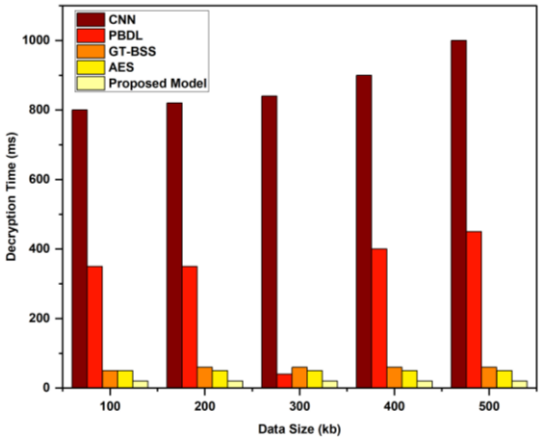

Figure 2: Differences in decryption times.

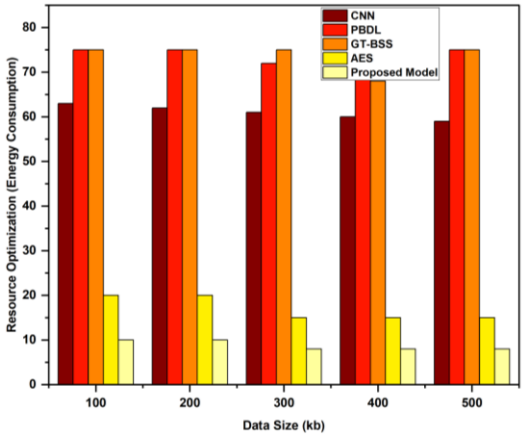

Figure 3: Optimizing energy consumption by reducing data size.

It is apparent from Figures 4 and 5 that data transmission computation and average delay remain relatively constant across all implemented smart hospital management data security systems. Therefore, both the data volume and the number of transmissions are highly scalable using the proposed methodology. Our solution also ensures the secure storage and accessibility of distributed medical records within a smart hospital framework. According to the analysis, the proposed security system outperforms previous methods in most cases.

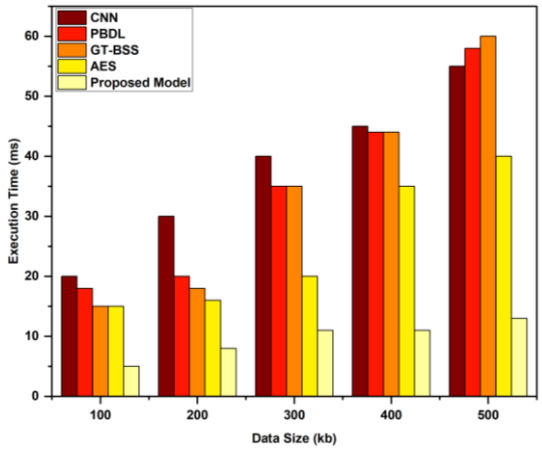

Figure 4: The execution time for a complete data set.

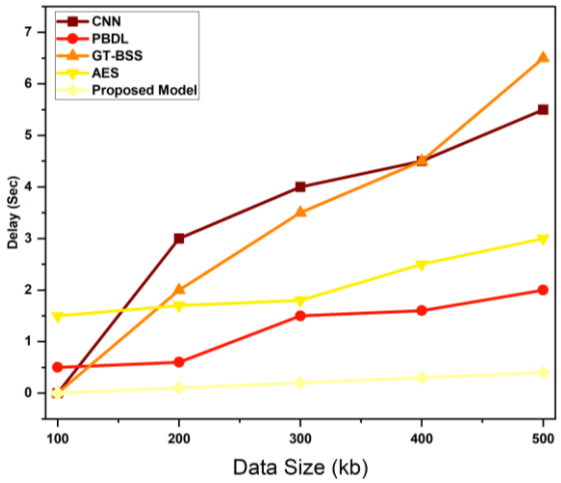

Figure 5: Estimation of the complete data size delay.

5 CONCLUSIONS

The purpose of this paper is to highlight the critical importance of securing healthcare data in a digital and interconnected world. Healthcare organizations are increasingly integrating digital technologies into their operations, which presents a challenge when it comes to protecting sensitive patient data. As for efficiency and scalability, the proposed security system delivers significant improvements over traditional methods thanks to a combination of advanced encryption techniques, AI-driven threat detection, and blockchain technology. The proposed model not only significantly enhances data protection but also optimizes computational resources and reduces overall operational costs cost-effectively, ensuring minimal transmission delays and improved responsiveness. Additionally, due to its inherent scalability, the system is particularly suitable for innovative healthcare environments that require secure storage, efficient management, and rapid access to extensive volumes of sensitive patient data. With robust, scalable data protection mechanisms, healthcare providers can increase patient trust, adhere to strict security and regulatory compliance standards, and effectively support the advancement and innovation of digital health technologies by supporting patient trust. As a result, patients receive better care, clinical outcomes are improved, and healthcare services are more efficient.

REFERENCES

[1] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, “Simulation of the lightweight blockchain technique based on privacy and security for healthcare data for the cloud system,” Int. J. E-Health Med. Commun. (IJEHMC), vol. 13, no. 4, pp. 1–15, 2022.

[2] P. Rani, D. S. Mohan, S. P. Yadav, G. K. Rajput, and M. A. Farouni, “Sentiment Analysis and Emotional Recognition: Enhancing Therapeutic Interventions,” in Demystifying the Role of Natural Language Processing (NLP) in Mental Health, A. Mishra, S. P. Yadav, M. Kumar, S. M. Biju, and G. C. Deka, Eds., IGI Global, 2025, pp. 283–302, doi: 10.4018/979-8-3693-4203-9.ch015.

[3] P. Rani, S. P. Yadav, P. N. Singh, and M. Almusawi, “Real-World Case Studies: Transforming Mental Healthcare With Natural Language Processing,” in Demystifying the Role of Natural Language Processing (NLP) in Mental Health, A. Mishra, S. P. Yadav, M. Kumar, S. M. Biju, and G. C. Deka, Eds., IGI Global, 2025, pp. 303–324, doi: 10.4018/979-8-3693-4203-9.ch016.

[4] F.-A. Allaert, Security Standards for Healthcare Information Systems: A Perspective from the EU ISIS MEDSEC Project, vol. 69. IOS Press, 2002. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=IcuUKU-ElvAC&oi=fnd&pg=PR5

[5] B. Week, “A Little Net Privacy, Please,” 1998.

[6] A. Nadeem, M. Naveed, M. I. Satti, H. Afzal, T. Ahmad, and K.-I. Kim, “Depression Detection Based on Hybrid Deep Learning SSCL Framework Using Self-Attention Mechanism: An Application to Social Networking Data,” Sensors, vol. 22, no. 24, p. 9775, Dec. 2022, doi: 10.3390/s22249775.

[7] S. Gritzalis, C. Lambrinoudakis, D. Lekkas, and S. Deftereos, “Technical guidelines for enhancing privacy and data protection in modern electronic medical environments,” IEEE Trans. Inf. Technol. Biomed., vol. 9, no. 3, pp. 413–423, 2005.

[8] B. Blobel and F. Roger-France, “A systematic approach for analysis and design of secure health information systems,” Int. J. Med. Inf., vol. 62, no. 1, pp. 51–78, Jun. 2001, doi: 10.1016/S1386-5056(01)00147-2.

[9] S. Gritzalis, J. Iliadis, D. Gritzalis, D. Spinellis, and S. Katsikas, "Developing secure Web-based medical applications," Med. Inform. Internet Med., vol. 24, no. 1, pp. 75–90, Jan. 1999, doi: 10.1080/146392399298537.

[10] T. Ahmad, X. J. Li, A. K. Cherukuri, and K.-I. Kim, "Hierarchical localization algorithm for sustainable ocean health in large-scale underwater wireless sensor networks," Sustain. Comput. Inform. Syst., vol. 39, p. 100902, Sep. 2023, doi: 10.1016/j.suscom.2023.100902.

[11] A. K. Ghosh, Security & Privacy for E-Business. John Wiley & Sons, Inc., 2001. [Online]. Available: https://dl.acm.org/doi/abs/10.5555/517043

[12] J. Argyrakis, S. Gritzalis, and C. Kioulafas, "Privacy Enhancing Technologies: A Review," in Electronic Government, R. Traunmüller, Ed., Lecture Notes in Computer Science, vol. 2739. Berlin, Heidelberg: Springer, 2003, pp. 282–287, doi: 10.1007/10929179_51.

[13] A. Deac, "Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of these data," Perspect. Law Public Adm., vol. 7, no. 2, pp. 151–156, 2018.

[14] P. Rani and R. Sharma, "An experimental study of IEEE 802.11n devices for vehicular networks with various propagation loss models," in International Conference on Signal Processing and Integrated Networks, Springer, 2022, pp. 125–135.

[15] R. Clark, "Implications of the EU Data Protection Directive and Council of Europe Recommendations for Healthcare Establishments," in Studies in Health Technology and Informatics, IOS Press, 2001, doi: 10.3233/978-1-60750-910-3-33.

[16] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. K. Gupta, and R. A. Khan, "Analyzing the Big Data Security Through a Unified Decision-Making Approach," Intell. Autom. Soft Comput., vol. 32, no. 2, pp. 1071–1088, 2022, doi: 10.32604/iasc.2022.022569.

[17] K. L. Offner, E. Sitnikova, K. Joiner, and C. R. MacIntyre, "Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation," Intell. Natl. Secur., vol. 35, no. 4, pp. 556–585, Jun. 2020, doi: 10.1080/02684527.2020.1752459.

[18] P. Rani, K. Ur Rehman, S. P. Yadav, and L. Hussein, "Deep Learning and AI in Behavioral Analysis for Revolutionizing Mental Healthcare," in Demystifying the Role of Natural Language Processing (NLP) in Mental Health, A. Mishra, S. P. Yadav, M. Kumar, S. M. Biju, and G. C. Deka, Eds., IGI Global, 2025, pp. 263–282, doi: 10.4018/979-8-3693-4203-9.ch014.

[19] A. A. George, A. O. Ogundipe, and A. B. Bello, "Cybersecurity in healthcare systems: safeguarding electronic health records (EHRs) and medical devices against emerging cyber threats," World J. Adv. Res. Rev., vol. 25, no. 2, pp. 2249–2262, Feb. 2025, doi: 10.30574/wjarr.2025.25.2.0592.

[20] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," Technol. Health Care, vol. 25, no. 1, pp. 1–10, Feb. 2017, doi: 10.3233/THC-161263.

[21] A. Singh et al., "Smart Traffic Monitoring Through Real-Time Moving Vehicle Detection Using Deep Learning via Aerial Images for Consumer Application," IEEE Trans. Consum. Electron., vol. 70, no. 4, pp. 7302–7309, Nov. 2024, doi: 10.1109/TCE.2024.3445728.

[22] M. K. Yusuf et al., "The Growing Cybersecurity Crisis in Healthcare: A Call to Action," Am. J. Innov. Sci. Eng., vol. 3, no. 3, pp. 55–68, Oct. 2024, doi: 10.54536/ajise.v3i3.3576.

[23] S. Mbonihankuye, A. Nkunzimana, and A. Ndagijimana, "Healthcare Data Security Technology: HIPAA Compliance," Wirel. Commun. Mob. Comput., vol. 2019, pp. 1–7, Oct. 2019, doi: 10.1155/2019/1927495.

[24] N. Kaliveli, "Data Security in Healthcare: Enhancing the Safety of Data with Cybersecurity," Int. J. Res. Appl. Sci. Eng. Technol., vol. 13, no. 3, pp. 2857–2865, Mar. 2025, doi: 10.22214/ijraset.2025.67875.

[25] Y. A. Ahmed and M. Mazroub, "Building Trustworthy AI Systems for Secure Digital Health Services," in 2024 25th International Arab Conference on Information Technology (ACIT), Zarqa, Jordan: IEEE, Dec. 2024, pp. 1–7, doi: 10.1109/ACIT62805.2024.10876871.

[26] N. Agarwal, P. K. Kankanampati, S. S. Chamarthy, I. Khan, A. Jain, and M. Almusawi, "Blockchain and Quantum Cryptography-Based Hybrid Security for Healthcare 5.0 Systems," in 2024 3rd International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT), Zhuhai, China: IEEE, Oct. 2024, pp. 376–381, doi: 10.1109/CCPQT64497.2024.00079.

[27] P. Rani and R. Sharma, "Intelligent Transportation System Performance Analysis of Indoor and Outdoor Internet of Vehicle (IoV) Applications Towards 5G," Tsinghua Sci. Technol., vol. 29, no. 6, pp. 1785–1795, Dec. 2024, doi: 10.26599/TST.2023.9010119.

[28] B. S. Swaroop, K. Sowmya, K. N. Rao, M. Z. Shah, and K. Nithin, "Advanced Cloud-Integrated Multi-Layered Security for E-Health Records Protection," Int. J. Res. Appl. Sci. Eng. Technol., vol. 13, no. 3, pp. 1671–1679, Mar. 2025, doi: 10.22214/ijraset.2025.67630.