International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 9 Issue 11 November - 2025, Pages: 46-52

IoT-Based Healthcare Monitoring System: Integrating Data Connectivity, Storage, Security, and Analysis.

Jenny Ebitonere Fawei[1], Damfebo Franklin Ayebagbalinyo[2,] Anyalewechi Chika Juliana3

Department of Electrical and Electronic, Niger Delta University Wilberforce Island, Bayelsa State, Nigeria
*[1] email: jeoebicom@gmail.com
*[2] email: damfebofranklin@ndu.edu.ng
3Department of Electronic Engineering Federal University of Technology Owerri Owerri, Imo State
Email: chika.anyalewechi.futo.edu.ng

Abstract: *IoT (Internet of Things)-based healthcare monitoring systems integrate data connectivity, storage, security, and analytical techniques to enhance patient monitoring, improve data analysis, and support better clinical decision-making, ultimately leading to improved patient outcomes. This paper presents a comprehensive review of techniques in IoT-based healthcare monitoring system that addresses the critical aspects of data connectivity, storage, security, and analysis to improve patient outcomes and enhance healthcare delivery. IoT devices in healthcare collect and transmit data using various connectivity technologies such as Wi-Fi, Bluetooth, and mobile networks to continuously monitor vital signs, medication adherence, and environmental data. Also, this paper explores secure and scalable data storage solutions, including blockchain technology, to ensure the integrity, confidentiality, and availability of patient data. Additionally, the vulnerabilities and threats in IoT healthcare systems and security measures such as encryption and privacy-preserving techniques are discussed. Data analysis techniques such as descriptive analytics, diagnostic analytics, predictive analytics, and anomaly detection are also explored in this review.*

Keywords—component; Internet of Things; data connectivity; Cloud storage; Data Security.

1. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative technology in the healthcare sector, offering unprecedented opportunities to enhance patient care, improve operational efficiency, and reduce healthcare costs. IoT-based healthcare monitoring systems leverage a network of interconnected devices, sensors, and wearables to collect, transmit, and analyze patient data in real-time, enabling continuous and remote monitoring of patients' health status as in [1]. This paradigm shift from traditional healthcare practices to IoT-driven solutions has the potential to revolutionize the way healthcare is delivered, particularly in managing chronic diseases, monitoring elderly patients, and providing personalized treatment plans. The backbone of any IoT-based healthcare monitoring system is its data connectivity. The system relies on wireless technologies such as Wi-Fi, Bluetooth, Zigbee, or cellular networks to transmit data collected from various sensors.

Data from these devices is transmitted to centralized servers, cloud platforms, or local storage systems for analysis. Continuous and uninterrupted connectivity ensures data remains up-to-date and available for real-time monitoring, allowing healthcare professionals to track patients' conditions remotely as in [2].

In an IoT-based healthcare monitoring system, data storage is typically managed through cloud platforms, local servers, or hybrid models. Cloud storage offers scalability, reliability, and remote access to data, while local storage solutions ensure data availability even in the case of internet connectivity disruptions. Proper storage systems are essential to ensure that large volumes of patient data are organized, retrievable, and efficiently maintained over time as in [3]. However, with sensitive healthcare data being transmitted and stored, data security becomes a critical aspect of an IoT-based healthcare system. Protection against unauthorized access, data breaches, and cyberattacks is paramount. Advanced encryption techniques, secure authentication mechanisms, and robust firewalls help safeguard data privacy and integrity as in [4]. Data analysis plays a vital role in deriving meaningful insights from the vast amounts of data collected by IoT devices as in [5]. Machine learning and artificial intelligence algorithms can be employed to analyze IoT healthcare data, providing predictive analytics, anomaly detection, and personalized treatment plans as in [6]. This review aims to provide a holistic view of IoT-based healthcare monitoring systems, highlighting the integration of data connectivity, storage, security, and analytical techniques, as well as their limitations. By addressing these critical aspects, IoT healthcare systems can overcome the challenges associated with data management and security, paving the way for improved patient care and enhanced healthcare delivery.

1.1 IOT-BASED HEALTHCARE MONITORING SYSTEM OVERVIEW

IoT-Based Healthcare Monitoring System (HMS) generally consists of four interconnected layers which are, the Perception Layer, which uses biomedical sensors and wearable devices to collect patient data such as heart rate, blood pressure, and temperature, the Network Layer, which securely transmits this data through communication technologies like Bluetooth, Wi-Fi, or GSM, the Processing Layer, which stores, manages, and analyzes the transmitted

data using cloud computing, artificial intelligence, and data analytics tools to detect anomalies or generate health insights, and the Application Layer, which presents the processed information to end users such as doctors, patients, or healthcare administrators via mobile apps, dashboards, or electronic health record systems for timely diagnosis, monitoring, and decision-making as in [7]. The system overview is described in fig. 1 as shown

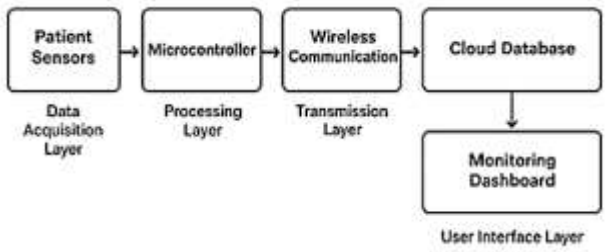

Fig.1. *IoT Healthcare Monitoring System Overview*

1.2 Data Connectivity Techniques

This handles the secure communication between sensing devices and data processing systems by transmitting medical data from the sensory layer to cloud servers or databases using various communication protocols as in [8]. The various data connectivity techniques in healthcare monitoring systems are described in figure 2 as shown;

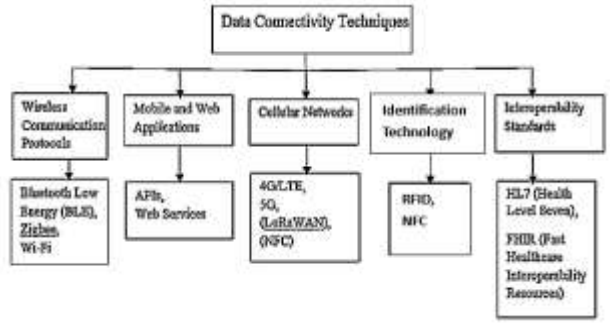

Figure 2. *Data connectivity techniques*

Techniques used in data connectivity may include:

- Mobile and Web Applications: Mobile and Web Applications are usually integrated with wearable devices and electronic health records, mobile and web applications to allow patients to monitor vital signs, track medication adherence, log symptoms, and provide remote access to patient data. Features such as reminders, alerts, and teleconsultations enhance patient engagement and adherence to treatment plans. This enables data exchange between mobile apps and healthcare systems (e.g., Electronic Health Records). Facilitating the integration of healthcare monitoring systems with other applications and services as in [9].
- Cellular Networks: Cellular networks enhance real-time, remote transmission of patient data from wearable devices or mobile health (mHealth) applications to healthcare providers. These networks, include 4G/LTE which provides broadband internet access, 5G for higher speeds, and greater capacity, ideal for advanced healthcare applications such as remote surgery and real-time data analytics. LoRaWAN (Long Range Wide Area Networks) are designed for long-range communication with low data rates, suitable for IoT devices in healthcare as in [10]. Authors in reference [11], demonstrated an IoT-based patient monitoring system using LoRa for efficient long-range data transfer with minimal energy use. The NFC (Near Field Communication) is used for short-range data exchange, such as patient identification and quick data transfer between devices as in [12].
- RFID (Radio Frequency Identification) and NFC (Near Field Communication): RFID and NFC technologies are primarily used for patient identification, tracking, and secure data exchange. Reference [13] implemented an RFID-based hospital management system for tracking patient movement and ensuring medication safety, while authors in reference [14] developed an NFC-based glucose monitoring system for diabetic patients
- Interoperability Standards: These are established protocols and guidelines that enable different systems, devices, applications, or organizations to effectively exchange, interpret, and use data, ensuring that disparate technologies can work together seamlessly, regardless of their manufacturer or platform, promoting consistency, accuracy, and efficiency in data communication. interoperability standards such as HL7 (Health Level Seven) are commonly used in health monitoring system to support the integration, sharing, and retrieval of electronic health information between healthcare providers and applications as in [15], and FHIR (Fast Healthcare Interoperability Resources) enable interoperability between different healthcare systems using RESTful Application Programming Interfaces as in [16].

Each protocol offers unique advantages based on their application. BLE and ZigBee are suitable for wearable and short-range body area networks, Wi-Fi is effective for high-bandwidth data, GSM and LoRa are essential for remote healthcare, and RFID/NFC provide identification and authentication support. The choice of protocol depends on power constraints, required data rate, network range, and environmental factors.

1.3 Data Storage Techniques

Data storage systems play a crucial role in healthcare monitoring by ensuring that patients' medical information is securely stored, efficiently retrieved, and easily shared among healthcare professionals. Data Storage Techniques are described in figure 3 as shown;

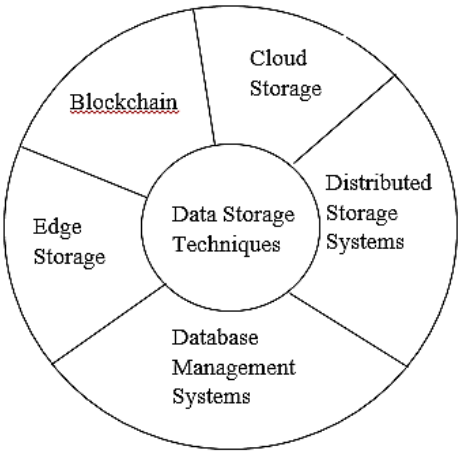

Fig. 3. *Data Storage Techniques*

- Cloud Storage: this provides centralized patient records that prevents data loss due to system failures or cyber-attacks with automatic backups as in [17]. This makes it essential for a modern, efficient, and secure healthcare monitoring system. It enhances data security, real-time data access, scalability, collaboration, AI-driven analytics, and cost-effectiveness. Cloud storage, such as public cloud offers scalable storage solution with robust security features as in [18]. while private cloud, and hybrid cloud allow flexibility in data management as in [19]. Platforms like Google Cloud Healthcare API, Amazon Web Services (AWS) HealthLake, and Microsoft Azure Health Data Services utilizes cloud storage.
- Distributed Storage Systems: Distributed storage systems such as Hadoop Distributed File System (HDFS) and Ceph are used to store data across multiple locations or devices to enhance redundancy and reliability.
- Database Management Systems (DBMS): DBMS efficiently manage large volumes of data, support regulatory compliance, and enable real-time updates and monitoring of patient health as in [20]. DBMS used in IoT healthcare monitoring system such as the relational databases uses structured query language (SQL) for data storage and management, NoSQL database which handle unstructured data and are more flexible for varying data types (e.g., MongoDB, Cassandra) as in [21], data Lakes which facilitating big data analytics and machine learning applications, and lastly data Warehousing for enabling analysis and reporting for generating insights from historical patient data.
- Edge Storage: This is used to stored data locally on devices or edge servers, reducing latency and bandwidth, ensuring continuous operation even if the central cloud is temporarily unavailable. Useful for real-time monitoring and immediate data processing as in [22].
- Blockchain: Provides a decentralized and secure way to store and share healthcare data, ensuring data integrity and privacy. This is also Useful for maintaining a tamper-proof record of patient data.

Each storage system has distinct benefits and limitations. DBMS use for Local storage is suitable for smaller clinics or offline operations that handle moderate amounts of patient data. Cloud systems offer scalability but depend on stable internet, edge and fog systems improve latency but have limited storage capacity, blockchain enhances security but may be slower for large data volumes. Therefore, hybrid architectures combining cloud–edge–blockchain approaches are increasingly being adopted for efficient healthcare data management as in [23].

1.4 Data Analysis Techniques

Data analysis techniques (figure 3) in healthcare monitoring systems enable the extraction of valuable insights from patient data. By effectively analyzing data, providers can identify trends, predict risks, and personalize treatment plans for patients, enabling better decision-making and improved patient care.

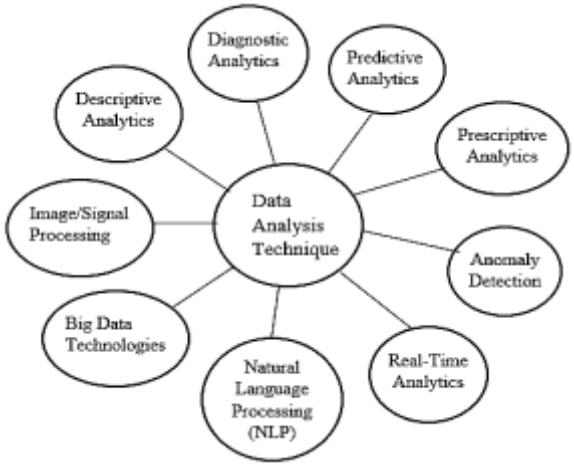

Fig. 4. *Data Analysis Techniques*

- Descriptive Analytics: Statistical analysis is achieved by collecting and organizing data from various sources such as electronic health records, wearable devices, and diagnostic tools to identify patterns, track patient progress, and monitor key health indicators. It also provides clear visualizations and reports, in the form of charts, graphs, and dashboards, enabling healthcare providers to detect early signs of deterioration, and make informed decisions. care A 2024 review of patient-centric healthcare analytics highlights how descriptive statistics and dashboards help healthcare providers track trends in wearable device data, EHR data, and operational metrics as in [24]. Moreover, descriptive analytics typically describe what happened, not why or what will happen next, limiting its scope for proactive intervention as in [25].
- Diagnostic Analytics: This includes root cause analysis which identifies the underlying causes of health issues or anomalies in the data, and correlation analysis conducted to examines the relationships between different parametric, such as the relationship between blood pressure

and heart rate as in [26]. However, many health systems lack interoperability and detailed context, making such analyses weaker or prone to spurious correlations

- Predictive Analytics: Predictive analytics uses machine learning models such as regression, decision trees, random forests, and neural networks, to predict future health outcomes based on historical data, time series analysis to identify trends and patterns over time in other to predicting disease progression or patient deterioration, and risk stratification models to identify patients at risk of adverse events based on various health indicators as in [27].
- Prescriptive Analytics: this utilizes optimization algorithms to provide recommendations for treatment plans or interventions based on predictive models as in [28], simulation models to evaluate the potential outcomes of various treatment options as in [27], and clinical decision support systems (CDSS) algorithms to provide treatment recommendations based on patient data and clinical guidelines as in [29].
- Anomaly Detection: This technique employs Statistical Methods to identify outliers in patient data that may indicate potential health issues (e.g., sudden spikes in heart rate) and machine learning techniques to identify abnormal data patterns that require further analysis as in [30].
- Real-Time Analytics: Real-time analytics uses stream processing tools like Apache Kafka and Apache Flink to analyze data generated, while event detection is conducted to identify significant events or anomalies in real-time data, such as sudden changes in vital signs.
- Natural Language Processing (NLP): This technique employs text analysis to extract meaningful information from unstructured text data, such as patient notes, feedback, and medical reports, and sentiment analysis to analyze patient feedback and reviews to understand their satisfaction and areas for improvement in care.
- Big Data Technologies: Big data technologies include Hadoop and Spark frameworks that handle large datasets, enabling advanced analytics on big data collected from remote monitoring systems as in [31]. Cloud-based analytics solutions for scalable storage and processing of health data.
- Image and Signal Processing: this includes medical imaging analysis for analyzing images from MRI, CT scans, and X-rays to detect abnormalities as in [32], and Signal Processing, which analyzes signals from ECG, EEG, and other medical devices to monitor patient health

1.5 Data Security

Data security challenges in IoT (Internet of Things) encompass a variety of threats that exploit vulnerabilities in connected devices. These attacks can lead to significant data breaches, financial losses, and service disruptions as in [33]. The most common data security attacks in IoT are node capturing adversaries, malicious code injection attacks, eavesdropping, denial-of-service (DoS) attacks, man-in-the-middle attacks, and service interruption attacks. Attackers may gain access to the IoT network, capture data, or deprive legitimate users of using the services of IoT applications as in [34]. Implementing data security techniques in remote healthcare monitoring systems ensures that all devices used in remote monitoring have robust security measures, including regular software updates and patch management to protect patient information and maintaining trust in digital health technologies as in [35]. The techniques to ensure data security are as follows:

- Security Protocols: Security protocols in a health monitoring system are essential for ensuring the confidentiality, integrity, and availability of sensitive patient data. These protocols encompass authentication and authorization mechanisms (like multi-factor authentication and biometric verification), used to verify the identity of users and devices to prevent unauthorized access as in [36], and blockchain technique that provides a secure and transparent way to manage and share healthcare data, ensuring data integrity and privacy. Secure communication protocols are created to secure tunnels for data transmission, especially when accessing remote monitoring systems from external networks using VPNs (Virtual Private Networks). They also ensure that APIs used for data exchange are secured with authentication and encryption measures. For example, authors in reference [37], demonstrated a hybrid cryptography scheme tailored to IoT platforms to secure user information in remote monitoring.
- Encryption: Encryption converts patient data into unreadable formats unless the correct decryption key is used. For instance, hybrid cryptography schemes combining symmetric and asymmetric encryption have been proposed to secure IoT-enabled medical platforms as in [37]. Encryption technique such as Data-at-Rest protects stored data from unauthorized individuals as in [38], and Data-in-Transit, which utilizes protocols like TLS (Transport Layer Security) to safeguard data between devices and servers during transmission as in [39].
- Access Control: Access control Verifying user identity (authentication) and controlling what an authenticated user can access (authorization) are fundamental security controls. Role-based access control (RBAC), multi-factor authentication (MFA), and biometric verification are increasingly recommended in healthcare IoT scenarios to restrict access to those with appropriate clearance as in [40].
- Data Anonymization and De-Identification: This process removes personally identifiable information (PII) from datasets to protect patient identities, especially when using data for research or analysis as in [41].
- Regular Security Audits and Assessments: This uses penetration test to simulate attacks and evaluate system defenses, and conducts periodic audits to identify vulnerabilities and ensure compliance with relevant regulations (e.g., HIPAA).
- Intrusion Detection and Prevention Systems (IDPS): IDPS implements systems that monitor network traffic for suspicious activity, enabling quick responses to potential threats. A hybrid meta-heuristic model proposed in 2023

introduced dynamic reconfiguration of encryption/hashing parameters and integrated blockchain to enhance security performance in Internet-of-Medical-Things (IoMT) networks under attack scenarios as in [42].

- Data Backup and Recovery: This technique is employed to back up data regularly to secure locations to prevent loss due to breaches or system failures, and develop and test disaster recovery plans to ensure quick restoration of services after a security incident.
- Security Awareness Training: this training is employed to educate healthcare staff about security best practices, phishing attacks, and data handling to reduce human error as a vulnerability.
- Compliance with Regulations: Compliance with regulations is employed to ensure IoT healthcare practitioners adhere to regulations such as HIPAA, GDPR, and others that govern data protection in healthcare. This involves enforcing strict controls over data access and handling as in [43].

Limitations in data security systems

Although encryption ensures data confidentiality, it introduces computational overhead and requires substantial processing power especially in resource-constrained IoT medical devices. if encryption keys are lost or compromised, patient data may become inaccessible or exposed as in [44]. While multi-factor and biometric authentication improve access control, they may impact user experience and delay emergency access to patient data, IDSs often generate high false-positive rates, burdening healthcare administrators with irrelevant alerts as in [42].

2. CONCLUSIONS

The integration of IoT-based healthcare monitoring systems, encompassing data connectivity, storage, analysis, and security, represents a transformative advancement in healthcare delivery. These systems enable continuous, real-time monitoring of patients' vital signs and health data through connected devices and sensors, facilitating early detection and intervention for various health conditions. This paper has reviewed the techniques used in data connectivity, such as wireless communication protocols, mobile and web Applications, cellular Networks, and so on. This ensures seamless integration for data transmission between devices and cloud services. The use of cloud-based, blockchain and distributed storage systems discussed in this paper, ensures scalable and secure data management, while advanced analytics techniques such as descriptive analytics, predictive analytics, anomaly detection, natural language processing (NLP) and big data technologies reviewed in this paper provide insights for trend analysis and predictive maintenance. Additionally, the implementation of such systems also presents significant challenges, particularly in ensuring data security and privacy. However, this paper highlights measures, including strong authentication, encryption, and compliance with relevant regulations, that are essential to protect sensitive patient information from potential breaches and unauthorized access. By addressing these challenges, IoT-based healthcare monitoring systems can significantly enhance the quality of patient care, reduce healthcare costs, and improve overall health outcomes. Moving forward, with the right advancements in data connectivity, storage, and analysis, and addressing challenges related to data security, IoT-based healthcare monitoring systems have the potential to transform healthcare into a more efficient, responsive, and patient-centered industry.

3. ACKNOWLEDGMENT

The authors wish to express sincere gratitude to Prof. Gloria Chukwudebe whose guidance and support contributed to the completion of this paper.

4. REFERENCES

[1] Kelly J. T., Campbell L. K., Gong E., and Scuffham P (2020). The Internet of Things: Impact and Implications for Health Care Delivery, Journal of Medical Internet Research, 22(11). https://doi.org/10.2196/20135.

[2] Abdulmalek S, Al-Areeqi W., Almuhaya M., Bairagi A., Al-Masrur K., and Kee, S. (2022). IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. Healthcare. 10.3390/healthcare10101993.

[3] Alhejaili A.D., Alsheraimi M., Alrubaiqi N., Khan M.Z. (2021). A Survey of Data Storing and Processing Techniques for IoT in Healthcare Systems. In: Kumar, S., Purohit, S.D., Hiranwal, S., Prasad, M. (eds) Proceedings of International Conference on Communication and Computational Technologies. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-16-3246-4_34

[4] Ali T.E., Ali,F.I., Dakić,P. and Zoltan D. A (2024). Trends, prospects, challenges, and security in the healthcare internet of things. Computing 107, 28. https://doi.org/10.1007/s00607-024-01352-4

[5] Sharma A., Singh P.K., Nikashina P., Gavrilenko V., Tselykh, A.,and Bozhenyuk, A. (2024). IoT and AI-Based Smart Healthcare Monitoring System. Data Science and Artificial Intelligence for Digital Healthcare. Signals and Communication Technology. Springer, Cham. https://doi.org/10.1007/978-3-031-56818-3_12

[6] Deepa S. K P, Sridhar S. B., Mythili K.B., Reethika A., Hariharan P.R (2022). IoT-enabled smart healthcare data and health monitoring based machine learning algorithms. Journal of Intelligent & Fuzzy Systems. 44. 1-15. 10.3233/JIFS-221274.

[7] Ketu S., and Mishra P. K (2021). Internet of Healthcare Things: A contemporary survey, Journal of Network and Computer Applications. 9(c). https://doi.org/10.1016/j.jnca.2021.103179

[8] Dhanvijay M. M., and Patil S. C. (2019). Internet of Things: A survey of Enabling technologies in healthcare and its applications, Comput. Networks, vol. 153, p 113–131, DOI:10.1016/J.COMNET.2019.03.006

[9] Klochko, O. V., Fedorets, V. M., Mazur, M. V., & Liulko, Y. P. (2023). An IoT system based on open APIs and geolocation for human health data analysis. CTE Workshop Proceedings, 10, 399-413. https://doi.org/10.55056/cte.567

[10] Norbahiah M, Mohammad S. I., Kok B. G., Nowshad A., Mohammad T. I, (2019). IoT Based Health Monitoring System with LoRa Communication Technology 2019 International Conference on Electrical Engineering and Informatics (ICEEI). DOI:10.1109/ICEEI47359.2019.8988869

[11] Bello, K., Ahmed, I., & Musa, L. (2022). LoRa-based IoT architecture for remote patient monitoring in rural environments. IEEE Access, 10, 110213–110225. https://doi.org/10.1109/ACCESS.2022.3201029

[12] Sun, X., Zhao, C., Li, H., Yu, H., Zhang, J., Qiu, H., Liang, J., Wu, J., Su, M., Shi, Y., & Pan, L. (2022). Wearable Near-Field Communication Sensors for Healthcare: Materials, Fabrication and Application. Micromachines, 13(5), 784. https://doi.org/10.3390/mi13050784

[13] Chen, H., & Park, J. (2020). RFID-based patient tracking and health monitoring system. Sensors Journal, 20(14), 3985–3995. https://doi.org/10.3390/s20143985

[14] Li, S., Zhao, P., & Wang, L. (2019). NFC-based portable health monitoring system for diabetic care. IEEE Transactions on Consumer Electronics, 65(4), 512–519.

[15] Harun-Ar-Rashid M, Chowdhury O, Hossain MM, Rahman MM, Muhammad G, AlQahtani SA, Alrashoud M, Yassine A, Hossain MS. (2023). IoT-Based Medical Image Monitoring System Using HL7 in a Hospital Database. Healthcare (Basel). 11(1):139. doi: 10.3390/healthcare11010139. PMID: 36611599; PMCID: PMC9819388.

[16] Ayaz M., Pasha M. F., Alahmadi T. J., Abdullah N. N. B., and Alkahtani, H. K. (2023). Transforming Healthcare Analytics with FHIR: A Framework for Standardizing and Analyzing Clinical Data. Healthcare (Basel, Switzerland), 11(12), 1729. https://doi.org/10.3390/healthcare11121729

[17] Simeone A, Caggiano A, Boun L, Grant R, (2021). Cloud-based platform for intelligent healthcare monitoring and risk prevention in hazardous manufacturing contexts, Procedia CIRP, Volume 99,2021,Pages 50-56,ISSN 2212-8271,https://doi.org/10.1016/j.procir.2021.03.009.

[18] McGuinness T, (2021). Enable the next generation of patient care with Microsoft Cloud for Healthcare. Microsoft. <https://www.microsoft.com/en-us/industry/blog/healthcare/2021/10/19/enable-the-next-generation-of-patient-care-with-microsoft-cloud-for-healthcare/?msockid>

[19] Bamidele A, Kumar A. B, and Barsocchi P. (2021). Hybrid Cloud/Fog Environment for Healthcare: An Exploratory Study, Opportunities, Cha.llenges, and Future Prospects. Hybrid Artificial Intelligence and IoT in Healthcare, (pp.1-20) 10.1007/978-981-16-2972-3_1.

[20] Saleh S, Cherradi B, el Gannour O, Gouiza N, Bouattane O. (2022). Healthcare monitoring system for automatic database management using mobile application in IoT environment. Bulletin of Electrical Engineering and Informatics. 14. 10.11591/eei.v12i2.4282.

[21] Santosh K. S (2024). Transforming Healthcare Data Management with NoSQL: A New Era of Scalability and Efficiency. International Journal of Science and Research (IJSR). Volume 13 Issue 10. DOI: https://dx.doi.org/10.21275/ES241003091413

[22] Singh A., and Chatterjee K. (2021). Securing smart healthcare system with edge computing, Computers & Security, Volume 108. https://doi.org/10.1016/j.cose.2021.102353.

[23] Kumar, R., & Gupta, S. (2020). Hybrid cloud-edge framework for secure healthcare data management. Journal of Healthcare Engineering, 2020, 1–10. https://doi.org/10.1155/2020/8857654

[24] Ibeh, C. V., Elufioye, O. A., Olorunsogo, T., Asuzu, O. F., Nduubuisi, N. L., & Daraojimba, A. I. (2024). Data analytics in healthcare: A review of patient-centric approaches and healthcare delivery. World Journal of Advanced Research and Reviews, 21(2), 1750–1760. https://doi.org/10.30574/wjarr.2024.21.2.0246

[25] Arowoogun, J. O., Babawarun, O., Chidi, R., Adeniyi, A. O., & Okolo, C. A. (2024). A comprehensive review of data analytics in healthcare management: Leveraging big data for decision-making. World Journal of Advanced Research and Reviews, 21(2), 1810–1821. https://doi.org/10.30574/wjarr.2024.21.2.0590

[26] Worku, A., Arage, F.G. & Kebede, F.B. Introduction to health care data analytics- an overview. Discov Health Systems 4, 107 (2025). https://doi.org/10.1007/s44250-025-00291-x

[27] Shukla, S. (2023). Real-time monitoring and predictive analytics in healthcare: Harnessing the power of data streaming. International Journal of Computer Applications, 185(8), 32–37. https://doi.org/10.5120/ijca2023922738

[28] Hassani S and Dackermann, U (2023). A Systematic Review of Optimization Algorithms for Structural Health Monitoring and Optimal Sensor Placement. Sensors (Basel, Switzerland), 23(6), 3293. https://doi.org/10.3390/s23063293.

[29] Chen Z., Liang N., Zhang H., Li H., Yang Y., Zong X., Chen Y., Wang Y., and Shi N. (2023). Harnessing the power of clinical decision support systems: challenges and opportunities. Open heart, 10(2), e002432. https://doi.org/10.1136/openhrt-2023-002432

[30] Tabassum, M., Mahmood, S., Bukhari, A., Alshemaimri B., Daud A., & Khalique F. (2024). Anomaly-based threat detection in smart health using machine learning.

BMC Med Inform Decis Mak 24, 347 https://doi.org/10.1186/s12911-024-02760-4

[31] Alafari, F., Driss, M., & Cherif, A. (2025). Advances in natural language processing for healthcare: A comprehensive review of techniques, applications, and future directions. Computer Science Review, 56, 100725. https://doi.org/10.1016/j.cosrev.2025.100725

[32] Li X., Zhang L., Yang J., Teng F, (2024). Role of Artificial Intelligence in Medical Image Analysis: A Review of Current Trends and Future Directions. J. Med. Biol. Eng. 44, 231–243 https://doi.org/10.1007/s40846-024-00863-x

[33] Kumar S., Sahoo S., Mahapatra A., Swain A. K., and Mahapatra k. (2017). Security enhancements to system on chip devices for iot perception layer. In 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS). IEEE, (151–156).

[34] Li, N., Xu, M., Li, Q., Liu, J., Bao, S., Li, Y., & Zheng, H. (2023). A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. Security and Safety, 2, 2022010. https://doi.org/10.1051/sands/2022010

[35] AlRubaiei M., Jassim sh H., Sharef T. B., Safdar S, Sharef T. Z, Malallah L. F. (2020). 6 - Current vulnerabilities, challenges and attacks on routing protocols for mobile ad hoc network: a review, Swarm Intelligence for Resource Management in Internet of Things, Pages 109-129, https://doi.org/10.1016/B978-0-12-818287-1.00012-7.

[36] Razzaque M. A., Milojevic-Jevric M., Palade A., and Clarke S. (2016). Middleware for internet of things: a survey. IEEE Internet of things journal. 3(70–95)1.

[37] Abikoye, O. C., Oladipupo, E. T., Imoize, A. L., Awotunde, J. B., Lee, C.-C., & Li, C.-T. (2023). Securing critical user information over the Internet of Medical Things platforms using a hybrid cryptography scheme. Future Internet, 15(3), 99. https://doi.org/10.3390/fi15030099

[38] Narula G., Gandhi, B., Sharma, H., Gupta, S., Saini, D., Nagrath, P. (2023). A Novel Review on Healthcare Data Encryption Techniques. In: Gupta, D., Khanna, A., Hassanien, A.E., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 492. Springer, Singapore. https://doi.org/10.1007/978-981-19-3679-1_40

[39] Zarate M., Andrew B., Brandon H., and Ahmad M., (2021). Technology Acceptance for Protecting Healthcare Data in the Presence of Rising Secure Sockets Layer/Transport Layer Security Communications: A Generic Qualitative Inquiry. Capella University. phdthesis{10.5555/AAI28962717.

[40] Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. Sensors, 23(7), 3612. https://doi.org/10.3390/s23073612

[41] Kushida, C. A., Nichols, D. A., Jadrnicek, R., Miller, R., Walsh, J. K., & Griffin, K. (2012). Strategies for de-identification and anonymization of electronic health record data for use in multicenter research studies. Medical care, 50 Suppl (Suppl), S82–S101. https://doi.org/10.1097/MLR.0b013e3182585355

[42] Kanneboina A. and Sundaram G (2023). Improving security performance of healthcare data in the Internet of Medical Things using a hybrid metaheuristic model. International Journal of Applied Mathematics and Computer Science, 33(4), 623–636. https://doi.org/10.34768/amcs-2023-0044

[43] Dunbar, P., Browne, J. P., & O'Connor, L. (2021). Determinants of regulatory compliance in health and social care services: a systematic review protocol. HRB open research, 4, 13. https://doi.org/10.12688/hrbopenres.132

[44] Jawad, L. A. (2024). Security and privacy in digital healthcare systems: Challenges and mitigation strategies. Abhigyan, 42, 23-31. https://doi.org/10.1177/09702385241233073 (scirp.org)