Research on Securing and Transforming Healthcare System:IoT-Driven E-Health Monitoring Systems

Md. Kamruzzaman*[1], Nisha Sain[2], Shamsul Alam[3]

[1, 2] University Institute of Legal Studies, Chandigarh University, Mohali, Punjab-140413, India
[3] University School of Business, Chandigarh University, Mohali, Punjab-140413, India

*associates.shadhin@gmail.com, nisha.e13418@cumail.in, sohelariba@gmail.com

Abstract. The growth of smart e-health monitoring systems is driven by the rise of the Internet of Things (IoT), transforming healthcare. This evolution relies on real-time updates for patients and stakeholders, as IoT devices generate substantial data. This technology plays a crucial role in modern healthcare monitoring, with various systems emerging to securely track health data. Health data is di- vided into structured and unstructured formats, with structured data adhering to standards and unstructured data being more varied, encompassing elements like emails and media content. To effectively utilize data from these devices in real-time applications, meeting rigorous security requirements is essential. Storing data in a secure environment is crucial, as the volume of data generated by IoT is substantial and requires specialized tools for analysis. The primary goal is to establish an intelligent system for e-health monitoring. This system collects medical data from multiple sensors, filters relevant information about a patient's current state, and integrates their health status. Additionally, the proposed system outlines a secure platform for sharing e-health information and authenticated architecture nodes within the IoT network. Ensuring the security of data generated by IoT devices is crucial for real-time applications. Storing data in a secure environment is essential due to the large volume of data, necessitating specialized tools for processing. The main objective is to create an intelligent e-health monitoring system that collects medical data from multiple sensors, filters relevant patient information, integrates health status, and facilitates secure sharing withinthe IoT network.

Keywords: E-Health Monitoring Systems, Internet of Things, Health Data,Real-Time Security, Secure Data Storage

1 Introduction

Healthcare monitoring, largely embedded within the Internet of Things (IoT), continues to evolve rapidly, significantly influencing daily life [1]. This integration ensures patient care by interconnecting devices within IoT networks. The growing prominence of health monitoring not only reduces costs but also amplifies the quality and accessibility of healthcare services. Moreover, IoT-based health monitoring plays a crucial role in

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_4

disease prevention and enables accurate diagnoses even in the absence of nearby physicians. In rural areas where medical facilities are scarce, locals often seek medical at-attention at distant hospitals or clinics [2]. However, as health conditions escalate to critical stages, accessing timely medical assistance becomes more challenging. In the face of epidemics or in regions where medical professionals struggle to reach easily, IoT-enabled health monitoring stands out, facilitating disease containment while allowing effective remote health monitoring [3].

The research problem in IoT health monitoring systems lies in the multifaceted vul-vulnerabilities posing critical threats [4]. Energy optimization stands as a significant concern as sensors, pivotal for health data analysis, face limitations in continuous data collection due to energy consumption. This limitation leads to compromised functionality and shorter battery life, challenging the seamless operation of the system [5]. Physical attacks further exacerbate the issue, allowing attackers to manipulate or reconfigure data, compromising the integrity of information collected by IoT devices [6]. Privacy breaches emerge as another significant challenge, as health data, transmitted through remote mechanisms, face threats in storage and transmission, impacting the confidentiality of sensitive health information [7]. Moreover, the susceptibility to data manipulation poses a considerable risk, potentially leading to incorrect diagnoses and treatments, endangering patients' lives [8]. Although remote healthcare monitoring systems serve emergency purposes, these vulnerabilities remain largely unsolved, demanding immediate attention and robust solutions to ensure the security, privacy, and integrity of health data within IoT networks.

In contemporary e-health monitoring, the wireless body area network (WBAN) stands out as a prominent application. Using the IEEE802.15.6 standard, this system involves numerous sensors placed across the body, either wearable or implanted, communicating through a centralized device with impressive data rates of 1Mbps and low power consumption at 0.1mW [9]. Additionally, innovations like ProeTEX introduce smart wearable health recording systems mounted on garments for enhanced monitoring [10].

The mobile health care monitoring system, known as mob care health system, incorporates web-based servers, Bluetooth-enabled sensors, and user interfaces [11]. It includes innovations like mobi ECG, transmitting exceptional ECG data to doctors or caregivers over mobile networks. Additionally, systems like C-SMART diagnose falls using Android-based health monitoring, while virtual telemonitoring through next-gen public networks gains popularity [12]. Other research developments involve daily mood assessment via mobile phones and smartphone-based sleep quality measurement [13].

Recent advancements have seen the emergence of cloudbased e-health systems, altering the location of patient data. While these applications offer cloud-backed services, they encounter challenges related to data security and compression [14]. Hybrid cloud solutions have emerged as a remedy to these issues. Another notable area is intelligence in health monitoring, where systems are capable of analyzing previous experiences or hypotheses, predicting and assessing future health states, and preemptively controlling potential health issues [15-16]. Various Artificial Intelligence (AI) techniques such

as artificial neural networks and fuzzy logic contribute to the development of intelligent healthcare systems [17-19].

Although the literature review has provided valuable insights, there is a notable gap in the existing research. Specifically, current research should focus on developing a comprehensive and secure architecture for storing and transmitting medical data while safeguarding patient security and privacy. This research must address emerging security risks in the medical health system, enhance anonymity and traceability of medical nodes and users, and implement a lightweight policy update mechanism. Additionally, there is a need for a user-friendly interface for authorized access to health records. Furthermore, addressing the limitations of real-time health monitoring, such as the need for diverse mechanisms and improved interoperability, especially in rural areas, remains unexplored.

The research novelty stems from its integrative approach towards addressing the burgeoning challenges in e-health data security within the evolving landscape of the Internet of Things (IoT). By focusing on the multifaceted issues, the research devises a comprehensive solution, amalgamating secure data transmission, addressing vulnerabilities in storage, and introducing a user-centric privacy-focused interface. It stands out by not only identifying concerns but also proposing a unified, practical system to combat these issues. This inclusive methodology aims to contribute significantly to the development of more secure and efficient smart health care monitoring systems, crucial in an increasingly IoT-driven healthcare sector.

2 Research Methodology

A. Medical Electronic Health Record (MEHR)

The comprehensive strategy for safeguarding privacy and security in the e-health care system comprises a set of algorithms depicted in Figure 1. Specifically, the MEHR algorithm introduces a robust architectural concept along with a dedicated mobile application [20]–[22].

Figure 1 illustrates the process within the e-health system: the Authentication Unit (AU) generates the Global Secret Key (GSK), used by all nodes and authenticated patients within their respective home networks. Patient data, gathered by medical nodes to form the Medical Electronic Health Record (MEHR), undergoes encryption through the MEHR algorithm. This encryption process incorporates keyword extraction and an update policy defined by the patient before depositing the records in a cloud storage system. Access to view and decrypt these medical records is restricted to authorized users. Any updates or modifications to the record can only occur using the key generated during the patient's registration process, ensuring secure and authorized data alterations within the system.

Authentication Unit execute the user registration segment to generate user key / P S KU KU (public/secret key) which is identical to registration of patient in the IoT network. This part gives a complete authentication to the user registered in the home IoT

network. Algorithm uses a security parameter (k), AU runs this algorithm and give rise to secret key named GSK (Global Secret Key). Patient (PA) register with set of attributes S attr attr □ □1 , n □ the method generates PK SK PA PA (public/ secret key) pairs of patient and thus AU generate algorithm nc SE the symmetric encryption.

PA's-patient's, PKPA (public key) and SKPA (secretkey) need to assemble. Looking at other way the user registered with set of attributes S attr attr = (1 , , nu) which came with health details of patient, staff, or caretakers. Medical node (MN) is also need to register for the same by running the registration module hereby originate MN (medical node's) public/secret key pair MN MN PK SK .

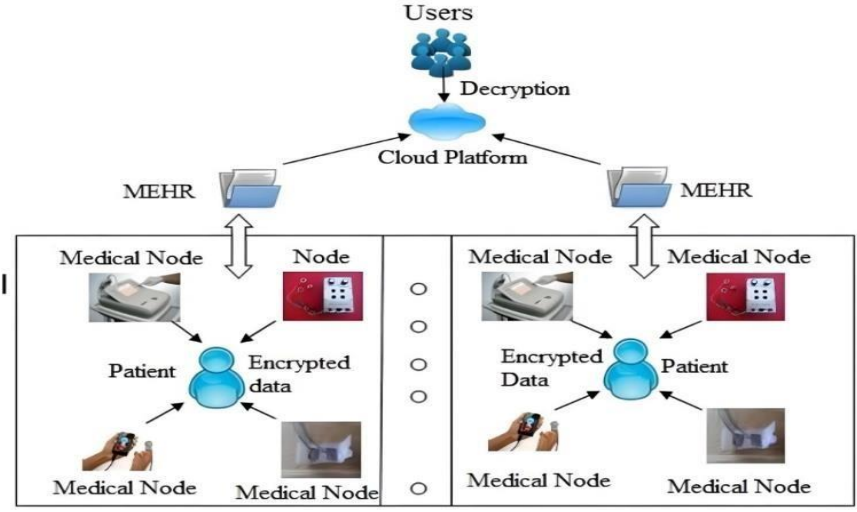

Fig. 1. MEHR process.

When a patient initiates a request to modify access permissions for their Medical Electronic Health Record (MEHR) stored within a secure cloud platform, the process involves the execution of a second algorithm. This algorithm verifies a keyword match for the intended update. Upon acceptance, the update function is activated within the cloud platform. In scenarios where there is a change in both the initial access policy (A, ρ) and the update policy ( ) ' ' A , ρ , the keyword match mechanism operates, updating only the ciphertext. The resultant output provides an updated ciphertext, reflecting the modifications made in the access permissions for the MEHR. ( ) ( ) { ( )} { ( )} ' ' ' ' ' 0 1 2, 3, 4 , , , , , , , 1, , 0, CT A A C C C C i n C j n C ρ ρ M i j = ∈ ∈ ⌈ ⌉

In the event that the keyword match policy fails to meet the specified criteria, resulting in, it denotes that no update has been performed, and consequently, the request is rejected.

B. Security Evaluation

Security assessment in the realm of the Internet of Things (IoT) remains critical due to real-time threats observed in IEEE 802.11 and Mobile Ad-Hoc Networks (MANET),

including the notorious black hole attack. Such vulnerabilities noticeably impact network functionality. To combat security and privacy issues, an elaborate algorithm detailed in the section offers a comprehensive security evaluation [20], [23]. Stringent regulations like HIPAA meticulously oversee healthcare organizations, ensuring strict compliance with standards for safeguarding medical information [24]. Assessing e-health data security highlights challenges such as consistency and repeatability concerns. Even advanced technologies, like smartcard security, grapple with numerous potential attacks, underscoring the intricate nature and broad spectrum of security challenges within healthcare systems [25]. Simulation of attacks is crucial for assessing medical health information security. Realistic network traffic is vital for accurate privacy and security simulations [26], [27].

C. Medical Health Data Encryption

Utilizing private keys within algorithms necessitates secure key exchange. The encryption of medical e-health data by nodes with the Global Secret Key (GSK) ensures privacy and security. Accessible solely with the GSK key, decryption of the data guarantees its confidentiality. Notably, this keycentric approach to preserving privacy and security distinguishes this method from other schemes highlighted in literature [28]–[30], as the significance of this main security thread isn't emphasized in those approaches.

D. Authentication of Medical Data

The different four major areas of authentication are secure communication, a handheld device, smart card and biometric [31]. Sharing the password/ special key in the secure protocol between the user and medical server are typical security features. To prevent Man in the Middle (MITM) attack in medical data is provided with authentication, this is provided in key distribution phase by checking whether the IoT key is sent by authorized node.

E. Policy Update

The scheme outlined in [32]–[34] and the planned work emphasize an updated policy mechanism for medical health data stored in a cloud platform, a feature not addressed in [35], [36]. In the latter systems, the entire data retrieval, decryption, updating, and re-encryption process demands extensive computational resources and time. This intensive process results in repeated decryption and encryption cycles, significantly impacting both computational load and processing time.

TABLE I. COMPARISON OF FUNCTION OVERHEAD.

Scheme						**MEHR**
F1	Y	Y	Y	X	X	Y
F2	X	Y	Y	Y	Y	Y
F3	X	Y	X	X	X	Y
F4	Y	X	X	Y	Y	Y
F5	X	Y	X	Y	X	Y

Table 1 compares various functional overheads denoted by 'X' for not included and 'Y' for included functions. It highlights distinct functionalities: (i) F1 - emphasizing patient anonymity, (ii) F2 - the ability to trace anonymous identities, (iii) F3 - serving medical data encryption, (iv) F4 - facilitating medical data decryption, and (v) F5 - handling access policy updates or modifications. These functionalities encapsulate vital aspects such as identity protection, encryption, decryption, and the dynamic adaptation of access policies within the system.

3. Methodology Simulation and Results for Mehr

Performance measurement and evaluation are crucial for enhancing any system, necessitating quantification and assessment. In the context of health monitoring, performance evaluation considers the behavior of IoT devices, network infrastructure, and patient experiences. Stakeholders with varying objectives and perspectives introduce multiple dimensions and dynamics over time. The simulation setup comprises a computer with a 64-bit Windows 10 Professional operating system, an Intel Core i5 (or equivalent) processor with 2.4/5 GHz core CPU, and 8GB of RAM. The simulation utilizes pairing-based cryptography (PCB) library, and a mobile application is developed using Android Studio as the platform. This approach is fundamental for comprehensive system assessment and improvement.

A. Transmission Efficiency

In the current healthcare system, IoT networks play a vital role in remotely monitoring patients, offering exceptional potential. These networks continuously provide real-time data on crucial health metrics such as pulse rate, diastolic pressure, glucose levels, and oxygen saturation. The choice of secure data transmission methods significantly impacts transmission efficiency. To evaluate system performance, measurements were conducted within the hospital infrastructure, assessing various network configurations and connection speeds. Figure 2 illustrates the transmission cost, with the x-axis representing the number of parameters. The public parameter sizes for different schemes [32-35], including MEHR system, are listed as 0.712KB, 0.528KB, 0.712KB, 0.469KB, and 0.456KB, respectively, reflecting the critical role of these parameters in system behavior and efficiency.

Fig. 2. Transmission cost parameter.

B. MEHR Efficiency

Efficiency in the health record system, as measured by the comparison of outputs to inputs, like cost and time, leads to optimal productivity. Implementing MEHR effectively requires defining and streamlining data flows, enhancing health record efficiency.

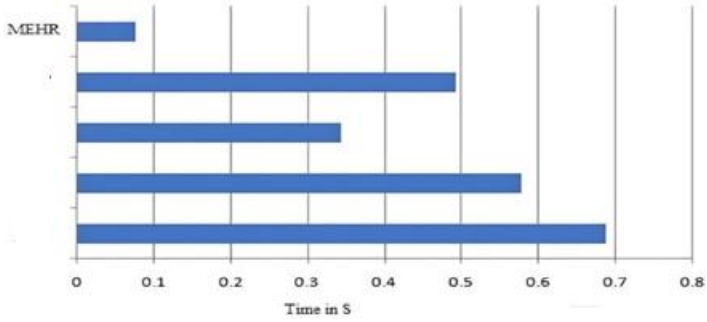

Fig. 3. MEHR Encryption.

Key ways to achieve this include defining and streamlining the health record, focusing on security aspects, and starting with a secure architecture. Figure 3 presents a comparison of medical file encryption computing costs, with the x-axis indicating computing costs and the y-axis showing the current work and various schemes [32]–[34], [36]. The final values, 0.496, 0.342, 0.573s, 0.677s, and 0.687s, collectively confirm the planned system's superior computing cost efficiency.

The sharing of user data is complicated due to the need for cryptographic methods to encrypt it. De-identifying healthcare data involves protecting identifiers in line with privacy rules. Figure 4 displays the MEHR decryption computing costs, with values on the x-axis representing various schemes [32], [33], [35], [36]. Current system's values are 1.496s, 1.594s, 1.520s, 1.439s, and 1.422s, respectively. This comparison underscores the system's primary goal: to enhance privacy and security in medical diagnosis providers, as it excels in decryption computing efficiency compared to other schemes.

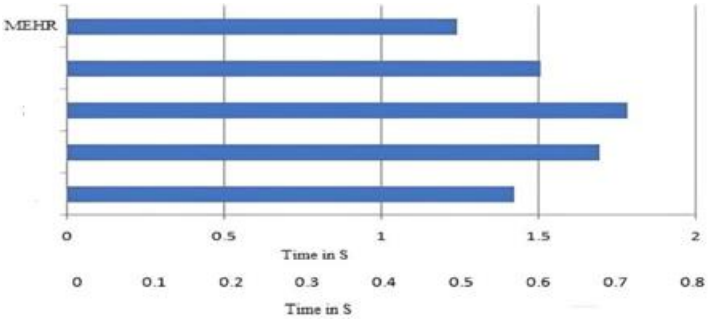

Fig. 4. MEHR Decryption.

C. Discussion

Patient health data undergoes calibration through a microcontroller, with various medical sensors including thermometers, cardiac monitors, room temperature, and humidity sensors integrated into monitoring devices. Following stringent security and privacy measures, this sensor data is transmitted to a secure cloud database server. Authorized users can access the health data through an IoT application platform, ensuring protection against potential security threats while enabling comprehensive health monitoring.

An intricate and secure architectural framework has been meticulously crafted, complemented by a user-friendly mobile application. This dynamic system facilitates remote disease diagnosis and prescription of treatments by medical practitioners based on the received data. This breakthrough allows healthcare professionals to offer medical care and prescribe medications from afar, enhancing patient accessibility to expert guidance. Extensive comparative analysis underscores the system's superior efficiency and security compared to existing solutions within the healthcare industry, marking it as a significant advancement in healthcare technology.

4 Conclusions

In conclusion, the proliferation of IoT connected devices, estimated at over 23 billion globally and projected to reach 60 billion by 2025, signifies a rapidly expanding technological landscape. However, with this growth comes an escalating concern for data privacy and security. The sheer magnitude of these devices necessitates a robust security infrastructure to mitigate the increasing security threats. As we move forward, it is imperative to prioritize and implement comprehensive security measures across the platforms integrating IoT devices to safeguard sensitive data and ensure a secure and resilient IoT ecosystem.

The core objective of the proposed healthcare system is to ensure effective patient monitoring in various settings, including hospitals, clinics, and even at patients' homes. This is achieved by prioritizing the privacy and security of medical records through the development of a robust and secure architectural framework. The integration of an e-

health application, specifically a mobile application programming interface, facilitates the secure storage, access, and sharing of medical records. The performance of the proposed MEHR algorithm is thoroughly evaluated, considering computational, communication, and functional overhead, and it is compared to existing systems. The simulation results convincingly demonstrate that the proposed system outperforms existing medical healthcare systems, marking a significant advancement in the field.

Limitation of the Research

One limitation of the research presented in the current research is the potential lack of empirical validation or real-world implementation of the proposed solution. While the research identifies critical issues and proposes a three-phase approach to enhance privacy and security in storing and transmitting medical health data, the absence of practical implementation or empirical evidence to support the effectiveness of the proposed architecture and mobile application leaves a gap. Without real-world testing or validation, the actual efficacy, usability, and robustness of the proposed system remain theoretical or speculative. This absence of empirical validation could limit the confidence in the proposed solution's practical applicability and its effectiveness in addressing the identified security and privacy concerns in IoT networks, specifically in the context of health-related data.

Scope for Future Research

The future plan involves integrating big data analytics into healthcare, aiming to reduce treatment costs, predict epidemics, prevent diseases, and enhance the quality of life. Artificial intelligence technology is enabling remote patient monitoring, reducing the need for in-person hospital visits. The digital revolution in healthcare and integrated data systems, often referred to as the Internet of Healthcare Things (IoHT), will improve access to patient health data. The future work focuses on developing a real-time, secure IoT framework and demonstrating how to mitigate IoT security threats through wireless network simulations (leveraging 5G communication) while emphasizing the significance of authenticated access to critical information.

References

[1] Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V. Vasilakos, and S. W. Kim, “The Future of Healthcare Internet of Things: A Survey of Emerging Technologies,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1121–1167, Apr. 2020, doi: 10.1109/COMST.2020.2973314.

[2] A. Onasanya and M. Elshakankiri, “Smart integrated IoT healthcare system for cancer care,” *Wireless Networks*, vol. 27, no. 6, pp. 4297–4312, Aug. 2021, doi: 10.1007/S11276-018-01932-1/METRICS.

[3] M. Alshamrani, "IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 4687–4701, Sep. 2022, doi: 10.1016/J.JKSUCI.2021.06.005.

[4] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems," *ACM Trans Comput Healthc*, vol. 2, no. 3, Jul. 2021, doi: 10.1145/3453176.

[5] M. Hartmann, U. S. Hashmi, and A. Imran, "Edge computing in smart health care systems: Review, challenges, and research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3710, Mar. 2022, doi: 10.1002/ETT.3710.

[6] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," *Applied Sciences 2021, Vol. 11, Page 4580*, vol. 11, no. 10, p. 4580, May 2021, doi: 10.3390/APP11104580.

[7] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, Jul. 2021, doi: 10.1016/J.EIJ.2020.07.003.

[8] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, "Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare," *Sensors 2023, Vol. 23, Page 8944*, vol. 23, no. 21, p. 8944, Nov. 2023, doi: 10.3390/S23218944.

[9] T. Benmansour, T. Ahmed, S. Moussaoui, and Z. Doukha, "Performance analyses of the IEEE 802.15.6 Wireless Body Area Network with heterogeneous traffic," *Journal of Network and Computer Applications*, vol. 163, p. 102651, Aug. 2020, doi: 10.1016/J.JNCA.2020.102651.

[10] V. Trovato *et al.*, "A Review of Stimuli-Responsive Smart Materials for Wearable Technology in Healthcare: Retrospective, Perspective, and Prospective," *Molecules 2022, Vol. 27, Page 5709*, vol. 27, no. 17, p. 5709, Sep. 2022, doi: 10.3390/MOLECULES27175709.

[11] D. Kumar, S. Jeuris, J. E. Bardram, and N. Dragoni, "Mobile and Wearable Sensing Frameworks for mHealth Studies and Applications," *ACM Transactions on Computing for Healthcare* , vol. 2, no. 1, Dec. 2020, doi: 10.1145/3422158.

[12] J. T. Thirukrishna, A. Mv, M. Singh,] Mounisha, and N. Kaveri, "A survey on instantaneous data transmission in Wireless Sensor Networks for Healthcare Monitoring," Mar. 2021, doi: 10.21203/RS.3.RS-173273/V1.

[13] J. Lim *et al.*, "Assessing Sleep Quality Using Mobile EMAs: Opportunities, Practical Consideration, and Challenges," *IEEE Access*, vol. 10, pp. 2063–2076, 2022, doi: 10.1109/ACCESS.2021.3140074.

[14] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain Application in Healthcare Systems: A Review," *Systems 2023, Vol. 11, Page 38*, vol. 11, no. 1, p. 38, Jan. 2023, doi: 10.3390/SYSTEMS11010038.

[15] B. Farahani, M. Barzegari, F. Shams Aliee, and K. A. Shaik, "Towards collaborative intelligent IoT eHealth: From device to fog, and cloud," *Microprocess Microsyst*, vol. 72, p. 102938, Feb. 2020, doi: 10.1016/J.MICPRO.2019.102938.

[16] M. Talaat, A. S. Alsayyari, A. Alblawi, and A. Y. Hatata, "Hybrid-cloud-based data processing for power system monitoring in smart grids," *Sustain Cities Soc*, vol. 55, p. 102049, Apr. 2020, doi: 10.1016/J.SCS.2020.102049.

[17] R. Tabbussum and A. Q. Dar, "Performance evaluation of artificial intelligence paradigms—artificial neural networks, fuzzy logic, and adaptive neuro-fuzzy inference system for flood prediction," *Environmental Science and Pollution Research*, vol. 28, no. 20, pp. 25265–25282, May 2021, doi: 10.1007/S11356-021-12410-1/METRICS.

[18] S. Kaur *et al.*, "Medical Diagnostic Systems Using Artificial Intelligence (AI) Algorithms: Principles and Perspectives," *IEEE Access*, vol. 8, pp. 228049–228069, 2020, doi: 10.1109/ACCESS.2020.3042273.

[19]K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar, and A. Khan, "An Intelligent IoT Based Healthcare System Using Fuzzy Neural Networks," *Sci Program*, vol. 2020, 2020, doi: 10.1155/2020/8836927.

[20] D. Moradigaravand Id *et al.*, "Unveiling the dynamics of antimicrobial utilization and resistance in a large hospital network over five years: Insights from health record data analysis," *PLOS Digital Health*, vol. 2, no. 12, p. e0000424, Dec. 2023, doi: 10.1371/JOURNAL.PDIG.0000424.

[21] Madhavi, K. Reddy, Padmavathi Kora, L. Venkateswara Reddy, Janagaraj Avanija, K. L. S. Soujanya, and Prabhakar Telagarapu. "Cardiac arrhythmia detection using dual-tree wavelet transform and convolutional neural network." Soft Computing 26, no. 7 (2022): 3561-3571.

[22] A. T. Kalpally and K. P. Vijayakumar, "Privacy and security framework for health care systems in IoT: originating at architecture through application," *J Ambient Intell Humaniz Comput*, pp. 1–11, Jan. 2021, doi: 10.1007/S12652-020-02676-7/METRICS.

[23] M. Obaidat, M. Khodjaeva, J. Holst, and M. Ben Zid, "Security and privacy challenges in vehicular Ad Hoc networks," *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*, pp. 223–251, Jan. 2020, doi: 10.1007/978-3-030-36167-9_9/COVER.

[24] M. Okpok and B. Kihei, "Challenges and Opportunities for Multimedia Transmission in Vehicular Ad Hoc Networks: A Comprehensive Review," *Electronics 2023, Vol. 12, Page 4310*, vol. 12, no. 20, p. 4310, Oct. 2023, doi: 10.3390/ELECTRONICS12204310.

[25] I. Silva and M. Soto, "Privacy-Preserving Data Sharing in Healthcare: An In-Depth Analysis of Big Data Solutions and Regulatory Compliance," *International Journal of Applied Health Care Analytics*, vol. 7, no. 1, pp. 14–23, Jan. 2022, Accessed: Jan. 04, 2024. [Online]. Available: https://norislab.com/index.php/IJAHA/article/view/39

[26] B. Maqbool and S. Herold, "Potential effectiveness and efficiency issues in usability evaluation within digital health: A systematic literature review," *Journal of Systems and Software*, vol. 208, p. 111881, Feb. 2024, doi: 10.1016/J.JSS.2023.111881.

[27] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020, doi: 10.1109/ACCESS.2020.3016826.

[28] Madhavi, K. Reddy, K. Suneetha, K. Srujan Raju, Padmavathi Kora, Gudavalli Madhavi, and Suresh Kallam. "Detection of COVID 19 using X-ray Images with Fine-tuned Transfer Learning." Journal of Scientific and Industrial Research (2023): 241-248.

[29] T. T. Huynh, T. D. Nguyen, T. Hoang, L. Tran, and D. Choi, "A reliability guaranteed solution for data storing and sharing," *IEEE Access*, vol. 9, pp. 108318–108328, 2021, doi: 10.1109/ACCESS.2021.3100707.

[30] B. Wang and Z. Li, "Healthchain: A Privacy Protection System for Medical Data Based on Blockchain," *Future Internet 2021, Vol. 13, Page 247*, vol. 13, no. 10, p. 247, Sep. 2021, doi: 10.3390/FI13100247.

[31] Kumar, Voruganti Naresh, U. Sivaji, Gunipati Kanishka, B. Rupa Devi, A. Suresh, K. Reddy Madhavi, and Syed Thouheed Ahmed. "A FRAMEWORK FOR TWEET CLASSIFICATION AND ANALYSIS ON SOCIAL MEDIA PLATFORM USING FEDERATED LEARNING." Malaysian Journal of Computer Science (2023): 90-98.

[32] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions," *Journal of Ambient Intelligence and Humanized Computing 2021 14:1*, vol. 14, no. 1, pp. 361–407, May 2021, doi: 10.1007/S12652-021-03302-W.

[33] Avanija, J., K. E. Kumar, Ch Usha Kumari, G. Naga Jyothi, K. Srujan Raju, and K. Reddy Madhavi. "Enhancing Network Forensic and Deep Learning Mechanism for Internet of Things Networks." (2023).

[34] S. Chen *et al.*, "Barriers of effective health insurance coverage for rural-to-urban migrant workers in China: A systematic review and policy gap analysis," *BMC Public Health*, vol. 20, no. 1, pp. 1–16, Mar. 2020, doi: 10.1186/S12889-020-8448-8/TABLES/3.

[35] C. Butpheng, K. H. Yeh, and H. Xiong, "Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review," *Symmetry 2020, Vol. 12, Page 1191*, vol. 12, no. 7, p. 1191, Jul. 2020, doi: 10.3390/SYM12071191.

[36] A. Tahir *et al.*, "A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems," *Sensors 2020, Vol. 20, Page 5392*, vol. 20, no. 18, p. 5392, Sep. 2020, doi: 10.3390/S20185392.