Studies on Internet of Things Powered E-Health Observing Systems for Safeguarding and Revolutionizing the Healthcare Sector

Md. Kamruzzaman
University Institute of Legal Studies
Chandigarh University
Mohali, Punjab, India.
associates.shadhin@gmail.com

Nisha Sain
University Institute of Legal Studies
Chandigarh University
Mohali, Punjab, India.
nisha.e13418@cumail.in

Sringka Dutta
University Institute of Legal Studies
Chandigarh University
Mohali, Punjab, India.
sringkadutta926@gmail.com

***Abstract*— The Internet of Things (IoT) is revolutionizing healthcare and driving the creation of smart e-health monitoring solutions. Since IoT devices create a lot of data, this evolution depends on providing stakeholders and patients with real-time updates. With new technologies emerging to securely manage health data, technology is essential to modern healthcare monitoring. There are two main types for health data: unstructured data is more diverse and includes things like emails and media content, while structured data follows certain guidelines. Meeting strict security criteria is crucial for utilizing data from these devices in real-time applications. Because the Internet of Things generates a significant amount of data that needs to be analyzed with specialized tools, it is imperative to store data in a secure environment. The creation of an intelligent e-health monitoring system is the main objective. This system gathers health data from several sensors, integrates the data, and filters pertinent information about the patient's current condition. The proposed system also describes an authorized architectural node within the IoT network and a secure platform for exchanging e-health data. For real-time applications, it is essential to ensure the security of data generated by Internet of Things devices. Because so much data needs to be processed, it is imperative that it be stored in a secure environment using specialized technologies. The major goal is to develop an intelligent e-health monitoring system that gathers health data from various sensors, integrates health status, filters pertinent patient data, and enables safe sharing within the Internet of Things.**

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

I. INTRODUCTION

The Internet of Things (IoT) is substantially responsible for the rapid evolution of healthcare monitoring, which has a huge impact on daily life [1]. By integrating devices within IoT networks, this integration guarantees patient care. Health monitoring is becoming more and more popular, which boosts the accessibility and quality of healthcare services while also cutting expenses. Furthermore, IoT-based health monitoring makes accurate diagnoses possible even in the absence of close doctors and is essential for illness prevention. People who live in remote places with limited access to healthcare services frequently go to nearby hospitals or clinics for medical care [2]. However, it becomes increasingly difficult to obtain prompt medical attention when health conditions worsen to critical levels.

IoT-enabled health monitoring stands out in the face of epidemics or in areas that are difficult for medical experts to access; it allows for effective remote health monitoring while also facilitating disease control [3].

The intricate vulnerabilities that pose serious risks are the subject of current studies in IoT health monitoring systems [4]. Energy optimisation is a major concern since energy consumption limits the continuous data-gathering capabilities of sensors, which are essential for the interpretation of health data. This restriction puts the system's smooth operation at jeopardy by reducing battery life and impairing functionality [5]. The problem is made worse by physical attacks, which give hackers the ability to alter or rearrange data and jeopardize the accuracy of the data that IoT devices gather [6]. Another major issue that arises is privacy breaches, which affect the security of sensitive health information supplied over remote methods and are caused by threats to data transmission and storage [7]. Furthermore, the vulnerability to data tampering presents a significant concern, possibly resulting in inaccurate diagnosis and treatments that could jeopardize the lives of patients [8]. While remote healthcare monitoring systems are useful in an emergency, there are still many unresolved weaknesses in these systems, which means that strong solutions and prompt attention are needed to guarantee the security, privacy, and integrity of health data on IoT networks.

The wireless body area network (WBAN) is a significant application in modern e-health monitoring. This system makes use of the IEEE802.15.6 standard and consists of several wearable or implanted sensors distributed throughout the body that communicate via a centralized device with astounding data speeds of 1Mbps and low power consumption of 0.1mW [9]. ProeTEX is an example of an innovation that offers smart wearable health recording systems that are installed to clothing for improved monitoring [10].

Mob Care Health System: This mobile health care monitoring system combines Bluetooth-enabled sensors, web-based servers, and user interfaces [11]. It includes breakthroughs like mobi ECG, which uses mobile networks to send superior ECG data to medical professionals or careers. Furthermore, apps such as C-SMART use Android-based health monitoring to diagnose falls, and virtual tele-monitoring via next-generation public networks is becoming more and more common [12].

Additional study advancements include smartphone-based sleep quality measurement and daily mood assessment [13].

Cloud-based e-health solutions have emerged in recent times, changing the placement of patient data. These apps provide cloud-backed services, but they have issues with compression and data security [14]. Solutions for hybrid clouds have surfaced as a fix for these problems. A noteworthy domain of intelligence in health monitoring encompasses

This work is licensed under a Creative Commons Attribution-Noncommercial 4.0 International License

systems that can evaluate past data or theories, forecast and evaluate future health conditions, and proactively manage possible health problems [15], [16]. The creation of intelligent healthcare systems is aided by a number of Artificial Intelligence (AI) techniques, including fuzzy logic and artificial neural networks [17–19].

The literature review has yielded insightful information, yet there is still a sizable vacuum in the field. In particular, current research should concentrate on creating a thorough and secure architecture that protects patient security and privacy during the transmission and storage of medical data. In addition to improving user and medical node anonymity and traceability, this research must address new security threats to the medical health system and put in place a simple process for updating policies. A user-friendly interface is also required for authorized access to health records. Additionally, there is still research to be done on how to overcome the drawbacks of real-time health monitoring, such as the requirement for a variety of mechanisms and enhanced interoperability, particularly in rural areas.

The research is innovative because it takes an integrated approach to solving the growing issues with the security of e-health data in the context of the Internet of Things (IoT). By concentrating on the complex problems, the study develops a complete solution that combines safe data transfer, fixes storage weaknesses, and presents a user-centric, privacy-focused interface. It is unique in that it raises challenges and then offers a cohesive, workable solution to address them. In an increasingly IoT-driven healthcare industry, this inclusive methodology seeks to make a major contribution to the creation of smart health care monitoring systems that are safer and more effective.

II. RESEARCH METHODOLOGY

A. Medical Electronic Health Record (MEHR)

A series of algorithms are part of the all-encompassing plan to protect security and privacy in the e-health care system, as shown in Figure 1. In particular, a specific mobile application and a strong architectural concept are introduced by the MEHR algorithm [20]–[22].

The e-health system's workflow is depicted in Figure 1: the Global Secret Key (GSK), which is utilized by all nodes and verified patients inside their individual home networks, is created by the Authentication Unit (AU). The Medical Electronic Health Record (MEHR) is a collection of patient data that is encrypted using the MEHR algorithm by medical nodes. Keyword extraction and a patient-defined updating policy are included in this encryption procedure before the records are stored in a cloud storage system. Only authorized people are able to see and decode these medical records. The key obtained during the patient's registration process is the only way to update or modify the record, guaranteeing safe and authorized data revisions within the system.

The user registration segment is executed by the authentication unit to generate the user key, also known as the public/secret key, which is the same key used to register a patient in an IoT network. The user who is registered in the home IoT network receives a full authentication from this section. Algorithm runs on AU and generates the secret key known as GSK (Global Secret Key) using a security parameter (k). After a patient (PA) registers with a set of attributes, the method creates patient pairings with public and secret keys, which allows the AU to create a symmetric encryption scheme.

The patient's PA, the public key (PKPA), and the secret key (SKPA) must be assembled. Examining an alternative method in which the user registered with a collection of qualities that included patient, staff, or carer health information. The medical node (MN) must also register for the same by executing the registration module, which generates the public/secret key pair for the MN (medical node).

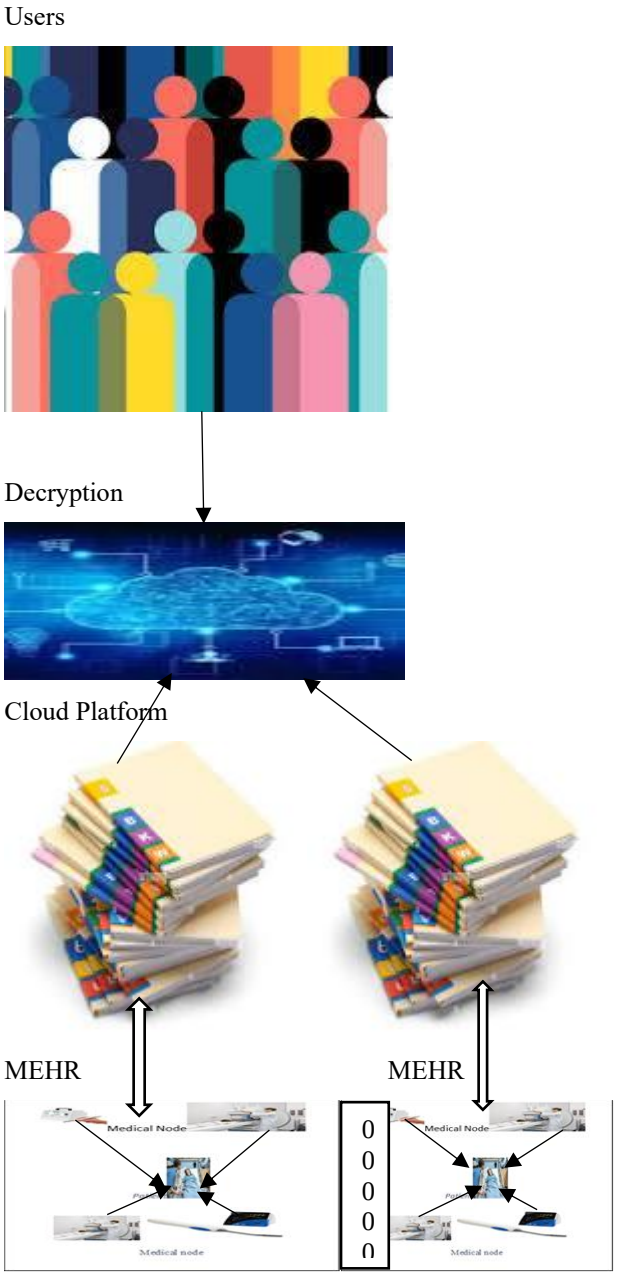

Fig. 1. MEHR process.

A second algorithm is run in response to a patient's request to alter access rights for their Medical Electronic Health Record (MEHR) that is hosted on a secure cloud platform. This method confirms whether the desired update's keywords match. When it is accepted, the cloud platform's update feature gets turned on. The keyword match mechanism updates only the ciphertext when there is a change in both the initial access policy and the update policy. The revised ciphertext that

results from the process reflects the changes made to the MEHR's access rights.

$$CT^{'} = \left[(A, \rho), (A^{'}, \rho^{'}), C_M, C_0, C_1, \{C_{2,i}^{'} \quad i \in (1, n^{'})\}, \{C_{3,j} \quad j \in (0, n)\} C_4 \right]$$

If the keyword match policy does not meet the required standards, which leads to, this indicates that no update has been made, and the request is denied.

B. Safety Assessment

The domain of Internet of Things (IoT) security assessment is still crucial because of the ever-present risks in IEEE 802.11 and Mobile Ad-Hoc Networks (MANET), such as the infamous black hole attack. Network functionality is significantly impacted by these vulnerabilities. An intricate method described in this part provides a thorough security evaluation to address privacy and security concerns [20], [23].

Tight laws such as HIPAA closely monitor healthcare institutions and enforce adherence to requirements for protecting medical records [24]. Evaluating the security of e-health data reveals difficulties such issues with repeatability and consistency. The complexity and wide range of security issues facing healthcare systems are highlighted by the fact that even cutting-edge solutions, such as smartcard security, are vulnerable to multiple possible attacks [25]. To evaluate the security of medical health information, assault simulation is essential. Accurate privacy and security simulations require realistic network traffic [26], [27].

C. Medicinal Fitness Information Encryption

When using private keys in algorithms, safe key exchange is required. Security and privacy are guaranteed when medical e-health data is encrypted by nodes using the Global Secret Key (GSK). The data can only be decrypted using the GSK key, which ensures its privacy. This method is notable for its key-centric approach to privacy and security preservation, which sets it apart from other methods that have been noted in literature [28]–[30]. In previous approaches, the importance of this fundamental security thread is not emphasized.

D. Certification of Medical Information

Smart cards, biometrics, portable devices, and secure communication are the four main categories of authentication [31]. Typical security measures involve the user and medical server sharing a password or secret key in a secure channel. Authentication is provided at the key distribution phase to prevent Man in the Middle (MITM) attacks on medical data. This is achieved by verifying that the IoT key is being transmitted by an authorized node.

E. Plan Upgradation

A revised policy mechanism for medical health data saved in a cloud platform is the focus of the proposed study and the scheme described in [32]–[34]. This is a feature that is not covered in [35], [36]. The process of retrieving, decrypting, updating, and re-encrypting data in the latter systems requires a significant amount of computer power and time. Repeated rounds of encryption and decryption are the outcome of this labor-intensive procedure, which greatly increases processing time and computing strain.

TABLE I. COMPARISON OF FUNCTION OVERHEAD.

Scheme	[33]	[32]	[35]	[36]	[34]	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

The functional overheads are shown in Table 1 as follows: 'X' stands for functions that are not included, while 'Y' stands for functions that are. It draws attention to specific functionalities: F1 emphasizes patient confidentiality; F2 allows anonymous identities to be tracked; F3 serves medical data encryption; F4 makes medical data decryption easier; and F5 manages updates or revisions to access policies. These features encompass essential elements including identity safeguarding, encryption, decryption, and the system's dynamic adjustment of access controls.

III. REPRODUCTION & CONSEQUENCES FOR MEHR

Any system that wants to be improved must measure and evaluate its performance, which calls for quantification and assessment. Performance evaluation in the context of health monitoring takes patient experiences, network architecture, and IoT device behavior into account. Over time, stakeholders with different goals and viewpoints bring in new dynamics and dimensions. A computer running 64-bit Windows 10 Professional, an Intel Core i5 (or similar) processor with 2.4/5 GHz cores, and 8GB of RAM make up the simulation setup. The pairing-based cryptography (PCB) library is used in the simulation, and Android Studio is used as the platform for developing a mobile application. This methodology is essential for thorough system evaluation and enhancement.

A. Diffusion Proficiency

IoT networks have great potential and are essential for remotely monitoring patients in the present healthcare system. Critical health variables including oxygen saturation, glucose levels, heart rate, and diastolic pressure are continuously available in real-time on these networks. Transfer efficiency is greatly impacted by the secure data transfer techniques selected. Measurements of several network configurations and connection speeds were made within the hospital infrastructure in order to assess system performance. The transmission cost is shown in Figure 2, where the number of parameters is represented on the x-axis. The MEHR system is one of the schemes for which the public parameter sizes are specified as 0.712KB, 0.528KB, 0.712KB, 0.469KB, and 0.456KB, respectively. This list illustrates the essential importance that these parameters have in the behavior and efficiency of the system.

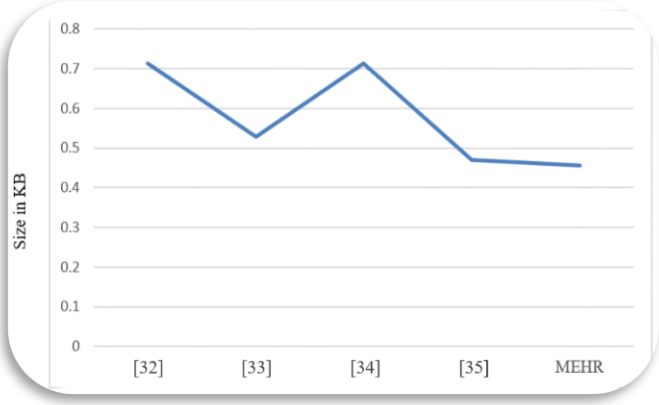

Fig. 2. Transmission cost parameter.

B. MEHR Proficiency

Optimal productivity is achieved in the health record system when efficiency is evaluated by comparing outputs to inputs, such as time and cost. To enhance the efficiency of health records, it is necessary to define and streamline data flows in order to implement MEHR successfully.

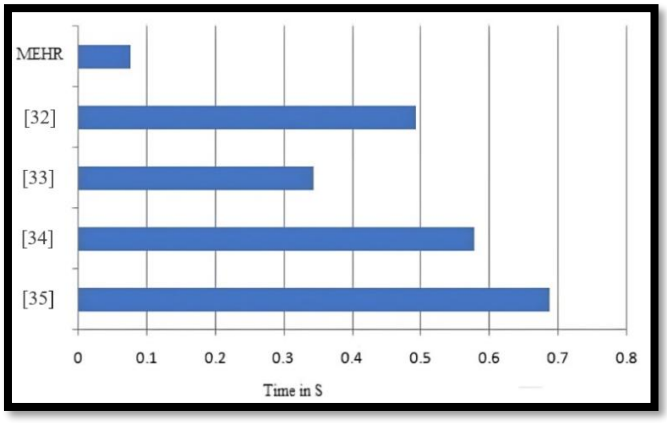

Fig. 3. MEHR Encryption.

The health record should be defined and streamlined, security should be the primary focus, and a secure architecture should be the foundation for achieving this. A comparison of medical file encryption computing costs is shown in Figure 3, where the y-axis displays various schemes and current work, while the x-axis indicates computing costs [32], [34], and [36]. The final results, which are 0.496, 0.342, 0.573s, 0.677s, and 0.687s, all support the higher computational cost efficiency of the planned system.

Because user data must be encrypted using cryptographic techniques, distributing it is difficult. In order to de-identify healthcare data, identifiers must be protected in accordance with privacy regulations. The MEHR decryption computing costs are shown in Figure 4, where different schemes are represented by numbers on the x-axis [32], [33], [35], and [36]. The values of the current system are, in order, 1.496s, 1.594s, 1.520s, 1.439s, and 1.422s. This comparison highlights the system's main objective, which is to improve security and privacy for medical diagnostic providers, because it outperforms other methods in terms of processing efficiency for decryption.

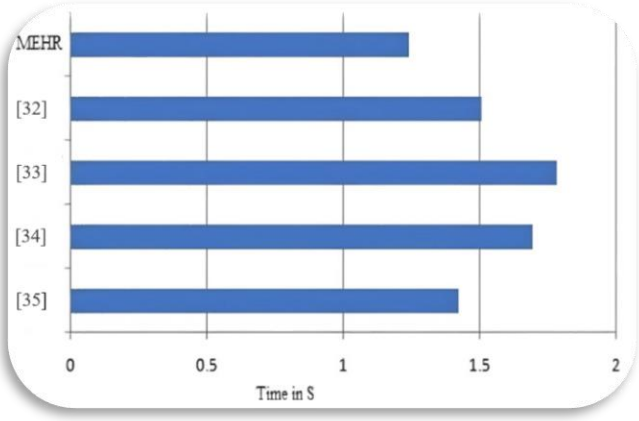

Fig. 4. MEHR Decryption.

C. DISCUSSION

A microcontroller is used to calibrate patient health data, and monitoring devices are equipped with a variety of medical sensors, such as room temperature, humidity, heart monitors, and thermometers. This sensor data is sent to a secure cloud database server via strict security and privacy protocols. Through an IoT application platform, authorized users can access the health data, providing protection against any security concerns and enabling thorough health monitoring.

A sophisticated and safe architecture has been painstakingly designed, and it is enhanced with an intuitive mobile application. Medical professionals can diagnose diseases remotely and prescribe treatments depending on the data they get thanks to this dynamic system. This innovation improves patient accessibility to professional advice by enabling medical practitioners to provide care and write prescriptions from a distance. A thorough comparison examination highlights the system's greater security and efficiency when compared to other healthcare industry solutions, establishing it as a noteworthy development in healthcare technology.

IV. CONCLUSION

In summary, there is a rapidly growing technological landscape indicated by the proliferation of IoT linked devices, estimated to be over 23 billion globally and predicted to reach 60 billion by 2025. But along with this expansion, worries about data security and privacy are growing. These devices are so large that a strong security architecture is required to counteract the growing risks to security. It is essential that we prioritize and deploy all-encompassing security measures on all platforms that integrate IoT devices going forward in order to protect sensitive data and guarantee a safe and robust IoT ecosystem.

The main goal of the suggested healthcare system is to guarantee efficient patient monitoring in a variety of locations, such as clinics, hospitals, and even patients' homes. This is accomplished by giving medical record security and privacy top priority and creating a strong, secure architecture framework. The safe exchange, sharing, and archiving of medical records is made easier with the inclusion of an e-health application, more especially a mobile application programming interface. The suggested MEHR algorithm's performance is carefully assessed in comparison to current systems, taking functional, computational, and communication overhead into account. The simulation findings clearly show that the suggested system performs better than current medical healthcare systems, which represents a major breakthrough in the industry.

V. LIMITATION OF THE RESEARCH

A possible shortcoming of the research reported here is that the suggested remedy may not have been empirically validated or implemented in the real world. The study highlights important concerns and suggests a three-phase strategy to improve security and privacy when transferring and storing medical health data, but there is a gap in the evidence supporting the efficacy of the suggested architecture and mobile application and its practical implementation. The actual effectiveness, usefulness, and robustness of the suggested system stay theoretical or speculative in the absence of real-world testing or validation. The lack of empirical validation may restrict the degree of confidence in the

practical applicability and efficacy of the suggested approach in resolving the security and privacy issues in IoT networks, particularly with regard to health-related data.

VI. SCOPE FOR FUTURE STUDY

Big data analytics will be incorporated into healthcare in the future with the goal of lowering treatment costs, forecasting epidemics, preventing diseases, and improving quality of life. Remote patient monitoring is now possible thanks to artificial intelligence technology, which eliminates the need for in-person hospital visits. Patient health data will be easier to obtain thanks to the digital revolution in healthcare and integrated data systems, sometimes known as the Internet of Healthcare Things (IoHT). In the future, work will concentrate on creating a safe, real-time Internet of Things framework and showcasing how to reduce security risks associated with IoT devices by using wireless network simulations and 5G connectivity, all the while highlighting the importance of authenticated access to vital data.

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] N. Garcelon, A. Burgun, R. Salomon, and A. Neuraz, "Electronic health records for the diagnosis of rare diseases," *Kidney Int*, vol. 97, no. 4, pp. 676–686, Apr. 2020, doi: 10.1016/J.KINT.2019.11.037.

[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] A. K. Pandit, K. Chatterjee, and A. Singh, "Secure fine grained access control for telecare medical communication system," *Telecommun Syst*, vol. 84, no. 1, pp. 1–21, Sep. 2023, doi: 10.1007/S11235-023-01033-1/METRICS.

[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] Z. A. Zukarnain, A. Muneer, and M. K. Ab Aziz, "Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges," *Symmetry 2022, Vol. 14, Page 821*, vol. 14, no. 4, p. 821, Apr. 2022, doi: 10.3390/SYM14040821.

[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] L. Lennox, A. Linwood-Amor, L. Maher, and J. Reed, "Making change last? Exploring the value of sustainability approaches in healthcare: a scoping review," *Health Research Policy and Systems 2020 18:1*, vol. 18, no. 1, pp. 1–24, Oct. 2020, doi: 10.1186/S12961-020-00601-0.

[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.