Vol 5, Issue 3, March 2025 E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

Strengthen Patient Data Privacy and System Efficiency with Mehr in Smart Health Monitoring

Aparna Datta [1], Dr. Narendra Chaudhari [2]

[1,2] Department of Computer Science & Engineering, Mansarovar Global University, Sehore, MP, India.

ABSTRACT

Smart health monitoring technologies are advancing at a rapid pace, which has changed patient care by allowing for continuous health surveillance, individualized therapy, and real-time data collecting. On the other hand, serious concerns about data privacy and system efficiency are brought up by these advancements. The study takes a quantitative approach, simulating a hospital infrastructure to evaluate five major e-health schemes: IoT Healthcare 4.0, IoT Network Forensics, Health Insurance Barriers, and Cloud Storage in e-Health, and MEHR. The metrics that were measured included transmission cost, encryption computing time, and decryption computing time. Using a standardized simulation platform that includes the PCB cryptographic library and Android-based applications, the results show that MEHR has the best efficiency and data integrity in healthcare data exchange, even though it has slightly higher encryption costs due to its robust security mechanisms. It also achieves the lowest decryption time and transmission cost. The results demonstrate that MEHR has great promise as a safe and scalable option for EHRs in contemporary healthcare systems that prioritize patient privacy.

Keywords: *Health Monitoring, Secure Data, Encryption, Decryption, Privacy.*

I. INTRODUCTION

Smart technology's incorporation into healthcare has opened a new age of medical innovation by changing the conventional paradigm of patient care into one that is more proactive, individualized, and data-driven. Real-time collection, transmission, and analysis of crucial health information are made possible by smart health monitoring systems using the Internet of Things (IoT), wearable devices, cloud computing, and artificial intelligence. By means of quick treatments, continuous monitoring, and enhanced chronic illness management, these technologies empower patients and healthcare professionals both. But next to the great promise of these technologies is a pressing and rising issue: the security and privacy of sensitive patient data. Protecting personal health information (PHI) against breaches, unauthorised access, and abuse has become a basic need as smart health systems manage ever-increasing amounts of it. Thus, one of the main difficulties in the development of digital health ecosystems is striking a balance between the demand for effective system performance and strong data privacy protections.

In smart health monitoring, patient data privacy is more than just technological compliance; it is fundamentally connected to ethical values, patient confidence, and legal responsibilities. Patients are more inclined to use and gain from digital health technology if they are certain that their data will be treated with greatest care and secrecy. Often running outside the bounds of conventional, guarded healthcare settings, IoT-based health monitoring systems' dependence on networked sensors and constant data streams amplifies privacy issues. Every point of data transmission—from a wearable device, a mobile health app, or a home-based monitoring system—represents a possible risk. Improper security of these systems might make them targets for cyberattacks with grave effects like identity theft, insurance fraud, or even altered health information endangering clinical decision-making. Designing smart health systems thus depends on end-to-end data protection via encryption, safe communication protocols, anonymization, and access control.

Conversely, system efficiency refers to the speed, precision, scalability, and dependability with which a smart health monitoring system can gather, analyze, and provide data-driven insights. In situations when quick medical action might be the difference between life and death, such as monitoring heart rate variability in cardiac patients or glucose levels in diabetics, high system efficiency is essential. Strong privacy-preserving methods, on the other hand, often include computational overheads that could affect system performance or raise latency. For example, while necessary for data security, sophisticated encryption techniques might delay data transfer or use more power for wearable devices with constrained resources. Significant interest in the research and development of lightweight cryptographic techniques, edge computing models, federated learning, and differential privacy methods aiming to balance data protection and performance criteria has been generated by this trade-off between privacy and efficiency.

Moreover, the intricacy of data privacy laws complicates the design and implementation of smart health monitoring systems. Regulatory systems around the world including the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and the Digital Information Security in Healthcare Act (DISHA) in India give legal requirements for safeguarding personal health information. These rules set rigorous standards on how data should be gathered, kept, processed, and disseminated. They also stress user permission, data minimization, openness, and the right to be forgotten. For healthcare companies trying to create sustainable, trustworthy digital health platforms, following these rules is not only a legal obligation but also a strategic need. Non-compliance can result in significant penalties, harm to reputation, and erosion of stakeholder confidence. As a result, techniques based on privacy-by-design and security-by-design have become more important, motivating programmers to include privacy tools at the very basis of system architecture instead of seeing them as add-on elements.

II. REVIEW OF LITERATURE

Abhishek, B. et al., (2022) Nowadays, our whole civilization is dependent on machines. Machines have generally made our lives easier and less labor-intensive. Leave the huge lines at the medical office in the past. People should not have to wait in line for anything, even opportunities or reports. Everything you need is at your fingertips; all it takes is a single touch. For the purpose of comparison, physicians have access to medical records stored in the systems or cloud of thousands of institutions. Nevertheless, there are instances where unauthorized individuals may get sensitive information, putting security and privacy at risk. This work aims to deploy the Modified Blowfish Algorithm to ensure the safety and security of patient data maintained on various platforms. While decrypting the data takes 48% of the time, the technique takes 72% to encrypt them.

Akbarzadeh, Omid et al., (2021) During the COVID-19 and future pandemics, this paper intends to raise the degree of hospitality for visitors in venues like as hotels, conference centers, campuses, and hospitals by designing and developing an innovative solution within the framework of smart buildings. This system is designed to help with managing building occupancy via online appointments, smart navigation, and mobile phone queue management. It also helps with navigating to specific locations by highlighting amenities and points of interest. Another capability that may be included into the design in the future is the ability to automatically modify environmental characteristics and monitor the occupancy of the area. The suggested method integrates and makes use of several data sources gathered by sensors connected to the internet of things (IoT), allowing it to resolve all the aforementioned concerns with the smart building. The next step is to input the data, have it processed on servers, and then transfer the processed data to the end users. Hence, a one-of-a-kind platform for smart administration of general and healthcare services in

hospital buildings will be built via the integration of various IoT technologies. This platform will have low hardware utilization and maximum scalability.

Pawar, Dr. Suvarna & Deshmukh, H.R. (2019) Every every day, huge strides are being made in the healthcare industry. All conventional methods used by doctors are superseded by technological investigation. Various parts of the medical diagnostic process are susceptible to the possibility of ambiguity and imprecision in healthcare. There has been a dramatic increase in the number of persons affected by sickness, regardless of age, according to a recent poll. Conversely, under these kinds of circumstances, physicians also need help in order to expedite the continued flow of patients. However, smart equipment and technology will always be necessary to aid physicians and patients in better managing any illness, especially in times of emergency when medical facilities are few. It improves upon healthcare services that are already in place. This article provides a comprehensive overview of the many methods now in use for the early detection of cardiac illness, which may serve as lifesaving warning signals.

Mangore, Anirudh & Masillamani, M. (2018) This article showcases the first version of a Big Data-powered health monitoring system. The healthcare business benefits from this in many ways, including the ability to provide prompt patient care services, diagnose diseases proactively, and monitor patients in real-time, among other things. Protecting the privacy of their patients' information is a huge problem for healthcare practitioners. People could be reluctant to contribute information if they feel their privacy is being violated. We want to take advantage of the new security issues posed by big data and focus on efficient, privacy-preserving computing in the age of big data as security has been studied as a new dimension, "veracity," in big data. To address the efficiency and privacy concerns raised by data mining in the age of big data, we first describe the fundamental architecture of big data analytics, then we list the associated privacy requirements, and finally we provide an example of a Triple DES that satisfies both of these needs. This study shows that compared to the old database, the suggested solution has more protected database access and keeps all patient data private.

Masood, Isma et al., (2018) In order to address issues with computation, storage, scalability, administration, and power, cloud computing (CC) technology has been included into wireless body area networks (WBANs) systems in recent times. The healthcare industry is benefiting from the integration of WBANs systems with CC technology, known as sensor-cloud infrastructure (S-CI), thanks to improvements in early illness detection and real-time patient monitoring. Patients' right to privacy and the security of their data face additional challenges in the decentralized S-CI environment. In this article, we take a look at the methods that S-CI uses to keep patient information secure and private. Current methods are categorized according to their areas of application: hash functions, attribute-based encryption, tri-mode algorithms, dynamic probability packet marking, hashing, pairwise key establishment, hybrid encryption, number theory research unit, tri-mode, and priority-based data forwarding. The benefits and drawbacks are laid here in the order in which they occurred. In addition, we provide our basic six-step framework for the privacy and security of patient physiological parameters (PPPs) in S-CI, which consists of the following steps: (1) preliminaries selection; (2) system entities selection; (3) technology selection; (4) PPP access; (5) security analysis; and (6) performance estimation. At the same time, we lay out the performance history of this field of study, pinpoint PPPs used as datasets, and talk about them. As a last section, we address the remaining questions and potential future developments in this dynamic field of study.

Paton, Chris et al., (2012) In this study, we take a look at the various social media platforms and self-tracking gadgets that are out there, and we see what the possibilities are for health informatics research if these tools become widely utilized. To learn more about how the health industry is using self-tracking technology and social media, a literature study was conducted. Three tiers of self-tracking were shown by a variety of goods and services found during an environmental scan: patient-controlled electronic health records, social data sharing, and self-experimentation. It would seem that self-tracking devices are becoming more popular, with applications ranging from the health and fitness industry to the treatment of long-term health conditions. The existing solutions mostly target health and fitness rather than illness management, which is the main reason why there is insufficient evidence of their usefulness and effectiveness. There is a growing tendency toward more extensive personal health monitoring and surveillance, more social connectivity and sharing, and the integration of regional and national health information systems, all of which are brought about by the convergence of many important technologies. With the proliferation of interconnected healthcare networks, these developments are opening the door to novel scientific applications ranging from e-epidemiology to individual-based experimentation. Researchers in health informatics and the communities of people who use fitness trackers will have new scientific and ethical challenges brought up by these developments.

III. RESEARCH METHODOLOGY

Ensuring privacy and security in the e-health care system is a comprehensive strategy that includes the algorithms shown in Figure 1. In particular, the MEHR algorithm presents a strong architectural idea and a corresponding mobile app.

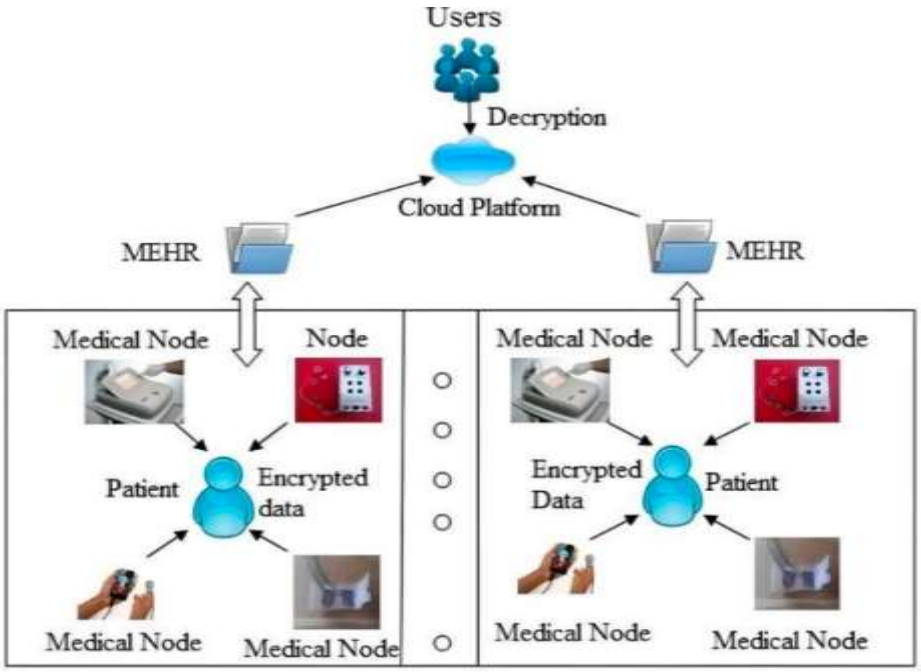

Figure 1: MEHR Process

The e-health system's procedure is shown in Figure 1. All nodes and authorized patients utilize the Global Secret Key (GSK) generated by the Authentication Unit (AU) on their home networks. The MEHR algorithm encrypts patient data before it is added to the Medical Electronic Health Record (MEHR). Prior to storing the information in the cloud, this encryption procedure includes keyword extraction and an updating policy that the patient defines. Authorized individuals are the only ones who can see and decode these medical records. Secure and approved data changes inside the system are ensured by requiring the key produced during the patient's registration procedure for any updates or revisions to the record.

This study's overarching goal is to determine how well the Medical Electronic Health Record (MEHR) system performs in contrast to various Internet of Things (IoT) frameworks, including Healthcare 4.0, Health Insurance Barriers, Cloud Storage in eHealth, and IoT Network Forensics. In a regulated medical environment, key performance indicators including transmission cost, encryption cost, and decryption cost are assessed using real-time data monitoring as part of a quantitative approach.

In order to improve any system, it is essential to monitor and evaluate its performance. Performance evaluation in health monitoring takes into account the actions of Internet of Things (IoT) devices, the state of the network, and the perspectives of patients. Time adds complexity and new dimensions brought about by stakeholders' differing goals and points of view. A 64-bit Windows 10 Professional operating system, an 8GB RAM, and an Intel Core i5 (or comparable) processor with 2.4/5 GHz core CPU are all required for the simulation setup. An Android Studio-based mobile app is created for the simulation, which makes use of the pairing-based cryptography (PCB) module. In order to evaluate and enhance a system thoroughly, this method is essential.

IV. RESULTS AND DISCUSSION

Transmission Efficiency

As it is, the Internet of Things (IoT) networks have tremendous promise for improving healthcare by facilitating remote patient monitoring. Vital signs like blood sugar, oxygen saturation, diastolic blood pressure, and heart rate are continually and continuously offered by these networks in real time. Picking the right secure data transfer techniques has a major effect on how efficient transmission is. System performance was evaluated by measurements taken within the hospital infrastructure, which assessed several network setups and connection speeds.

Table 1: Transmission Cost Parameter

Scheme	Size (KB)
IoT Healthcare 4.0	0.712
IoT Network Forensics	0.528
Health Insurance Barriers	0.712
Cloud Storage in eHealth	0.469
MEHR System	0.456

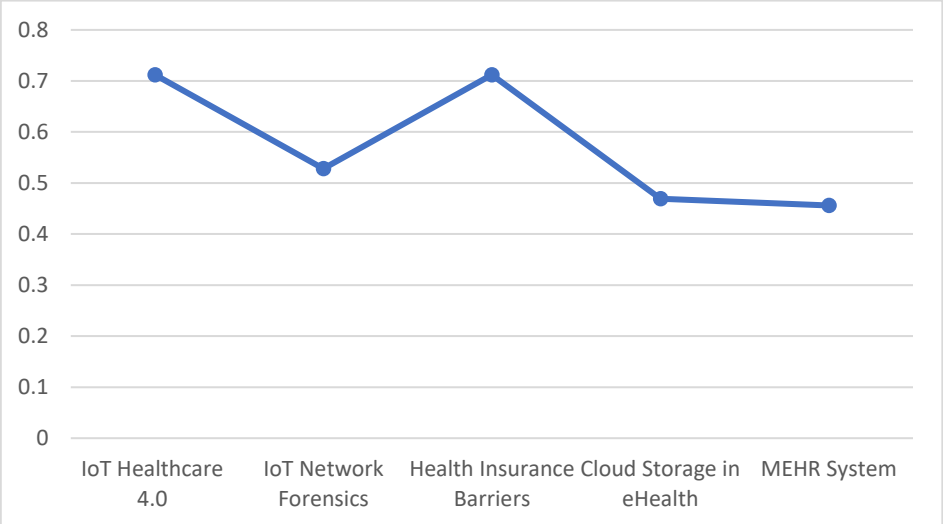

Figure 2: Transmission Cost Parameter

The transmission cost is shown in Table 1. Given the importance of these parameters to the performance and efficiency of the system, the public parameter sizes for various schemes, including the MEHR system, are as follows: 0.712KB, 0.528KB, 0.712KB, 0.469KB, and 0.456KB.

MEHR Efficiency

The health record system is most productive when its outputs are proportional to its inputs, which include things like time and money. Improving health record efficiency via defining and optimizing data flows is essential for an efficient implementation of MEHR. Important steps in this direction include establishing a safe foundation, concentrating on security features, and defining and simplifying the health record.

Table 2: Encryption Computing Time

Scheme	Computing Time(s)
IoT Healthcare 4.0	0.494
IoT Network Forensics	0.338
Health Insurance Barriers	0.575
Cloud Storage in eHealth	0.674
MEHR	0.685

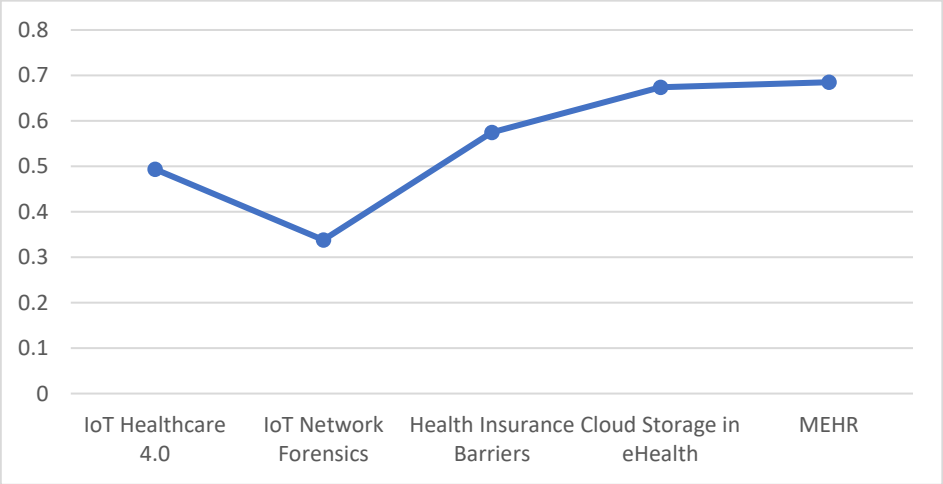

Figure 3: MEHR Encryption

The computational time required to encrypt medical files is compared in Table 2. This proves that out of all the encryption algorithms, IoT Network Forensics has the fastest computation time (0.338s). Following with 0.494s is IoT Healthcare 4.0. With prices in the moderate range (0.575s and 0.674s, respectively), health insurance barriers and cloud storage in eHealth are not expensive, but MEHR has the highest cost (0.685s), most likely as a result of its improved security features.

Cryptographic procedures are necessary to encrypt user data, which complicates its sharing. To de-identify medical records, it is necessary to safeguard identifiers in accordance with privacy regulations.

Table 3: Decryption Computing Time

Scheme	Computing Time(s)
IoT Healthcare 4.0	1.494
IoT Network Forensics	1.589
Health Insurance Barriers	1.525
Cloud Storage in eHealth	1.442
MEHR	1.418

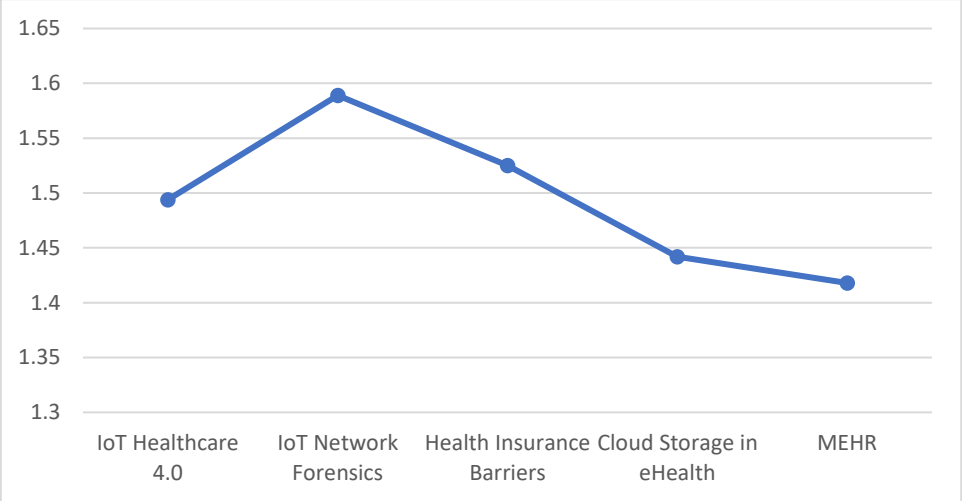

Figure 4: Decryption Computing Time

The computing time for MEHR decryption is shown in Table 3. These are the values of the current system: 1.494s, 1.589s, 1.525s, 1.442s, and 1.418s. By outperforming competing techniques in decryption computation efficiency, this comparison highlights the system's principal objective: to improve medical diagnostic providers' privacy and security.

V. CONCLUSION

The importance of encrypted data transmission and safe data transmission in improving the efficiency of healthcare systems based on the Internet of Things is emphasized in this study. Medical Electronic Health Record (MEHR) systems perform better than other systems in terms of transmission cost and decryption efficiency, despite having greater encryption costs, according to a study of several e-health frameworks. With the help of a specialized mobile app and cutting-edge cryptographic techniques, MEHR's sturdy design guarantees safe data handling without sacrificing system efficiency. With these features, MEHR seems like a good option for efficient and secure healthcare data transmission without sacrificing privacy. Based on the findings, it appears that MEHR may efficiently and effectively satisfy the security requirements of current healthcare networks with improved encryption and decryption operations. Building confidence and enhancing patient outcomes in medical environments enabled by the Internet of Things will need the incorporation of such efficient and secure frameworks as healthcare systems undergo ongoing evolution.

REFERENCES

1. B. Abhishek, R. Panjanathan, V. Sarobin, B. Raja, and N. Modigari, “Data security in e-health monitoring system,” *Mater. Today Proc.*, vol. 62, no. 6, pp. 11–18, 2022.
2. K. Yadav, A. Alharbi, A. Jain, and R. Ramadan, “An IoT based secure patient health monitoring system,” *Comput. Mater. Continua*, vol. 70, no. 2, pp. 3637–3652, 2022, doi: 10.32604/cmc.2022.020614.
3. D. Sandhiya, M. Venkatesan, K. Karthikeyan, and M. Priya, “Secured health monitoring system using AES,” *East Asian J. Multidiscip. Res.*, vol. 1, no. 6, pp. 1175–1182, 2022, doi: 10.55927/eajmr.v1i6.577.
4. S. Welten, Y. Mou, L. Neumann, M. Jaberansary, Y. Ucer, T. Kirsten, S. Decker, and O. Beyan, “A privacy-preserving distributed analytics platform for health care data,” *Methods Inf. Med.*, vol. 61, no. 08, pp. 1–11, 2022.

5. O. Akbarzadeh, M. Baradaran, and M. Khosravi, “IoT-based smart management of healthcare services in hospital buildings during COVID-19 and future pandemics,” *Wirel. Commun. Mob. Comput.*, vol. 2021, Art. no. 1, pp. 1–14, 2021.
6. A. Shawqi and A. Idrees, “Energy-saving multisensor data sampling and fusion with decision-making for monitoring health risk using WBSNs,” *Softw. Pract. Exp.*, vol. 51, no. 2, pp. 271–293, 2021, doi: 10.1002/spe.2904.
7. M. Supriya and R. Pothuraju, “An efficient privacy preserving approach for e-health,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 4, pp. 157–162, 2021.
8. R. Zhou, X. Zhang, X. Wang, G. Yang, N. Guizani, and X. Du, “Efficient and traceable patient health data search system for hospital management in smart cities,” *IEEE Internet Things J.*, vol. 99, no. 2, pp. 1–1, 2020, doi: 10.1109/JIOT.2020.3028598.
9. S. Pawar and H. R. Deshmukh, “Monitoring of smart systems using Internet of Things in healthcare,” *Indian J. Public Health Res. Dev.*, vol. 10, no. 6, pp. 1–10, 2019.
10. A. Mangore and M. Masillamani, “Survey on privacy preservation in big data for healthcare monitoring,” *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 1–6, 2018.
11. I. Masood, Y. Wang, A. Daud, N. Aljohani, and H. Dawood, “Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure survey,” *Wirel. Commun. Mob. Comput.*, vol. 2018, Art. no. 2, pp. 1–23, 2018.
12. W. Choi, “Early experiences with mobile electronic health records application in a tertiary hospital in Korea,” *Healthc. Inform. Res.*, vol. 21, no. 4, pp. 292–298, 2015, doi: 10.4258/hir.2015.21.4.292.
13. C. Paton, M. Hansen, L. Fernandez-Luque, and A. Lau, “Self-tracking, social media and personal health records for patient empowered self-care: Contribution of the IMIA Social Media Working Group,” *Yearb. Med. Inform.*, vol. 21, no. 01, pp. 16–24, 2012.
14. R. Benlamri and L. Docksteader, “MORF: A mobile health-monitoring platform,” *IT Prof.*, vol. 12, no. 3, pp. 18–25, 2010.