Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

Management Strategies and Privacy Law Implementation in Healthcare: A Study of Clinical Data Protection Systems

Balaji Rao[1], Preshni Shrivastava[2], Ajay Kumar Dogra[3], Dhannjay Singh Pundir[4], Vratika Singh[5], Ajay Sudhir Bale[6*], Saurabh Mittal[7*], Mamta B Savadatti[8]

[1.] Professor, Department of Business Administration, Vidyavardhaka College of Engineering, Mysore
[2.] Associate Professor, Department Operations, College IMM New Delhi, India
[3.] Assistant Professor, UIAMS, Panjab University, Chandigarh, India
[4.] Assistant Professor, Department of Law, Maharishi Markandeswar (Deemed to be University), Mullana-Ambala, India
[5.] Assistant Professor, Department of Law, Maharishi Markandeswar (Deemed to be University), Mullana-Ambala, India
[6*.] Dept. of ECE, New Horizon College of Engineering, Bengaluru, India; ajaysudhirbale@gmail.com
[7*.] SCO 367 First Floor Sector 44D, Chandigarh 160047; Saurabhmittal288@gmail.com
[8.] Dept. of ECE, New Horizon College of Engineering, Bengaluru, India
Corresponding Author: Ajay Sudhir Bale and Saurabh Mittal

Cite this paper as: Balaji Rao, Preshni Shrivastava, Ajay Kumar Dogra, Dhannjay Singh Pundir, Vratika Singh, Ajay Sudhir Bale, Saurabh Mittal, Mamta B Savadatti (2024) Management Strategies and Privacy Law Implementation in Healthcare: A Study of Clinical Data Protection Systems. *Frontiers in Health Informatics, 13* (3), 3554-3567

Abstract: *The proliferation of internet of healthcare things and digital health technologies has led to the implementation of privacy laws and data protection systems in the health care settings. The various challenges and strategies in managing healthcare privacy in the digital domain examining the various complex landscapes of clinical data protection systems how been discussed in the study. With the help of a comprehensive review of the current literature and industry practices we investigated the intersection of ioht architecture data privacy frameworks and regulatory compliances in the healthcare settings environment. The research particular emphasis is seen on the challenges faced in implementing the security issues managing the patient data and maintaining the operation C while ensuring that the regulatory compliance are well maintained. Various challenges like technical organisational regulatory legacy system integration staff training resource allocation and complexity of emerging technology is some of the highlights of this study. Besides maintaining accessibility and efficiency in healthcare delivery to study provides inside about effective management strategies and frameworks for protecting sensitive healthcare data*

Keywords: *Privacy, Law, Healthcare, Clinical, Data, Security*

1. Introduction

The Internet of Things (IoT) is a new technology that enables people to exchange information with Internet-connected gadgets. The International Telecommunication Union (ITU) describes the IoT as a network of sensor devices that engage with their surroundings [1]. The scope of IoT has expanded to include multiple uses used in various contexts, including security, autonomous control of appliances that use electricity, military uses, and other gadgets. A major use of IoT is in the field of healthcare, namely the Internet of Healthcare Things (IoHT), which is intended to track, shop, or communicate clinical data. The Internet of Health Things (IoHT) is a subset of the Internet of Things (IoT) that pertains exclusively to healthcare, including devices, services, and software. The Internet of Health Things (IoHT) refers to distinct gadgets linked to the Internet that communicate with one another, used within the medical field. IoHT devices facilitate the monitoring of people' medical status by transmitting clinical data to a remote server or service over mobile network cables [2-3]. Similar to other via the internet gadgets, IoHT devices possess a unique identification, including an IP address, which facilitates their connection to the system and the transmission of information to and from designated devices [4]. The central server oversees the aggregated data and reacts appropriately to diagnose patients' ailments. Figure 1 illustrates a comprehensive workflow model for the installation of the Internet of Health Things (IoHT). The objective is to provide dependable, efficient, and economical healthcare services by enabling doctors and medical personnel to remotely monitor their patients. Implementations of the IoHT facilitate people in the management of their health data and provide guidance on the use of fitness trackers [5-6].

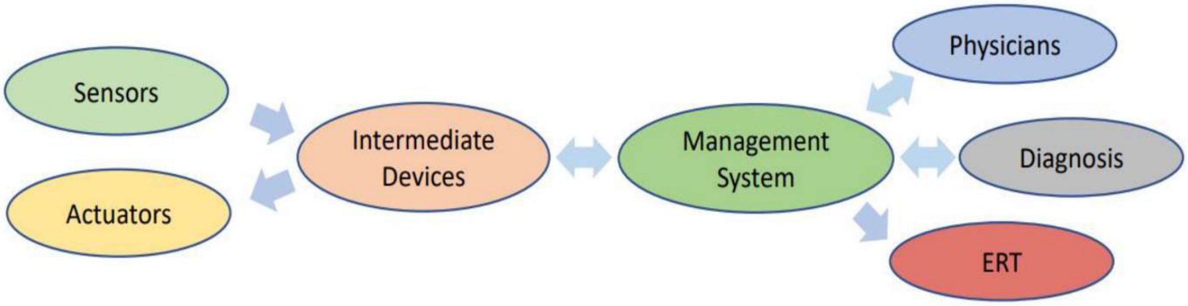

Figure 1: IoHT architecture [1].

Data privacy is seen a key need for customer acceptability, which may be guaranteed by the depiction of data flow, as well as the verification and authorisation of operations including gathering data, preservation [5-6], the process, and transfer. Data privacy issues have to do with unauthorised acquisition, use, availability, preservation, and dissemination of information. These actions may lead to personal data breaches and jeopardise user privacy, particularly with healthcare information, which is prioritised differently and is very important and sensitive. Consequently, suitable protective and safety arrangements are necessary [7-10]. Furthermore, the affordability to and accessibility of individual health data online pose privacy concerns. In June 2015, a critical privacy breach occurred when malware exploited weaknesses in blood gas analyser equipment, infiltrating hospital networks and compromising confidential data. Nonetheless, the confidential structure for IoHT devices and amenities is anticipated to be explicit to patients, providing constant updates to safeguard patients' data [11]. The healthcare systems gather the majority of data from sensing devices and transmit it via intermediary equipment to the administration layer. Various protocols and encoding strategies are used to ensure reliable data communication during this procedure. Utilising engine searches such as as Shodan facilitates the identification of vulnerabilities within various parts of the healthcare system, aiding hackers in locating linked, susceptible equipment on the Internet [12]. A spreadsheet with millions of entries of user medical data may be sent instantaneously, effortlessly, along with leaving a consistent trail [13-14]. Certain

IoT-related safeguards for data measures are implemented to safeguard data and the anonymity of users. Nevertheless, these laws have failed to provide the desired outcomes, and the current degree for medical privacy safeguarding is inadequate for the previously cited concerns [15-16]. Pharmaceutical confidentiality rules exhibit several shortcomings and deficiencies that fail to provide explicit guidelines for the protection of IoHT data.

Health management issues are increasing with the burgeoning population, particularly due to the expanding elderly demographic. The absence of a response from the hospital during crises might lead to societal complications [17-18]. Likewise, medical personnel in rural regions lack enough resources for therapy and possess insufficient competence to detect complex disorders. Consequently, individuals in remote regions prioritise large hospitals for adequate medical care, thereby exacerbating the burden on these facilities. The delayed identification of illnesses and significant health issues in the elderly further complicates the diagnostic procedure. Consequently, it is essential to enhance medical facilities via an optimised healthcare system that incorporates body sensors and medical gadgets for the remote monitoring and diagnosis of medical issues. A general Internet of Health Things (IoHT) architecture comprises IoHT devices, protocols for communication, and networks, as shown in Figure 2. The IoHT devices are categorised as devices that are worn and implantable devices. The data from IoHT devices is transferred via many communication protocols, including IEEE 802.15.6, WBAN, IEEE 802.15.1 Bluetooth, IEEE 802.11 WiFi, and LoRaWAN. The medical data is sent to a cloud service or a distant server intended for high-performance processing operations [19-20].

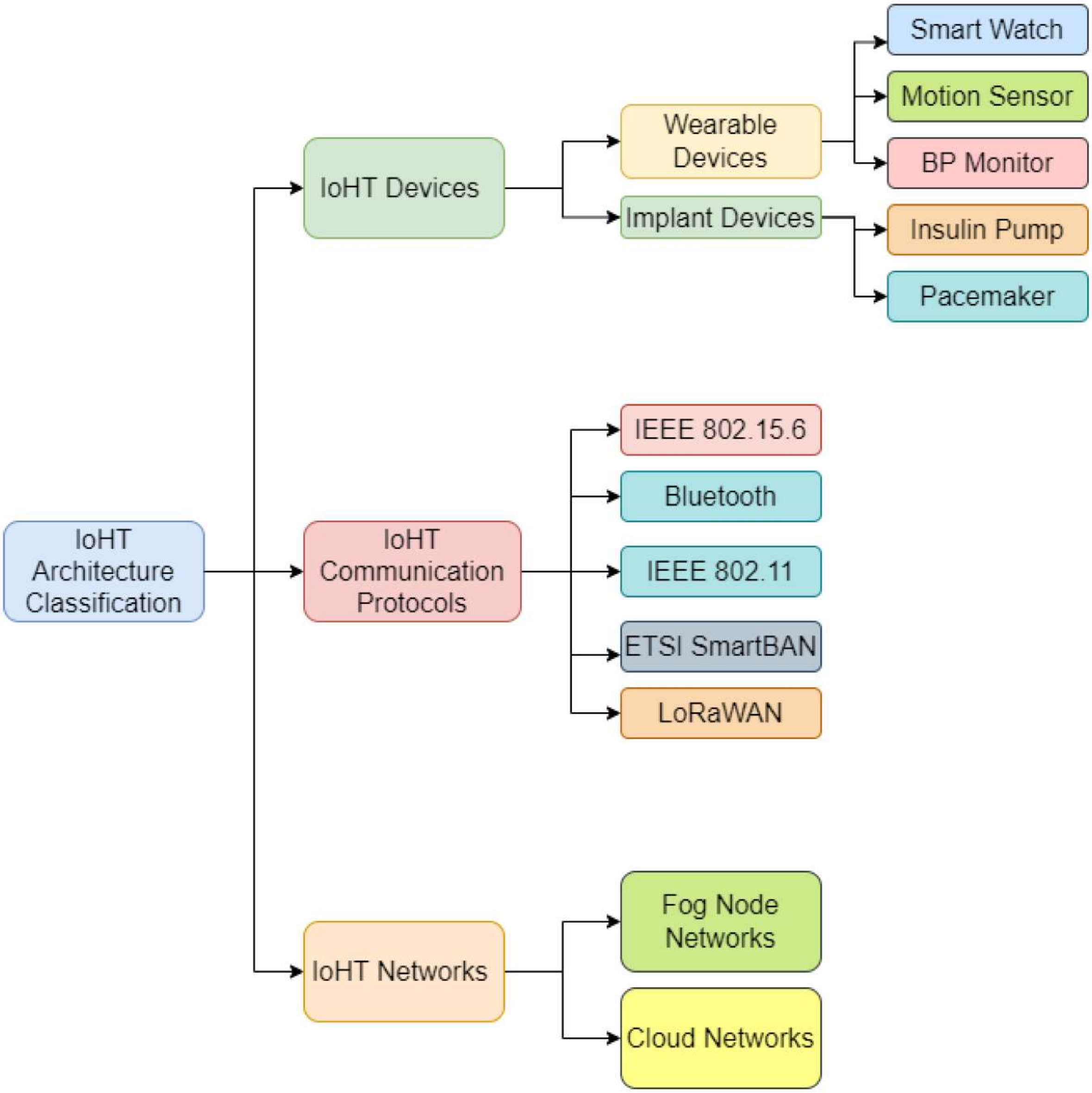

Figure 2: Different components in IoHT [1]

2. Comparative Study

2.1. Data Privacy

The COVID-19 situation necessitates specific solutions for ensuring the emergency care procedure and safeguarding the data collected across all contexts in emergency room (ER). This paper [2] suggested a taxonomy intended to facilitate the creation of privacy protections for healthcare settings. The taxonomy is divided into four categories, each including five qualities; all categories and their corresponding attributes are justified. They [2] created an early version and application for information flow testing that effectively handles key data privacy concerns, despite its simplicity. The program was designed to include registration data inputs and various encryption/hash methods based on environmental parameters. The program interfaces with a wearable device that monitors the patient's temperature and administers therapy according to the patient's febrile condition, facilitating referral to a physician or the option for release [21-23]. The use of scientific definitions and the proficiency of medical professionals in managing patients with suspicious COVID-19 ensures that registration data remains secret via encryption and privacy protocols. Continuous temperature monitoring is essential; if fever persists for a duration specified by the entity, accompanied by other indicative signs, the system recommends patient referral while safeguarding personal data. The study primarily contributes to the examination of various privacy characteristics inside a mobile application that adheres to the principles outlined in our taxonomy. No comprehensive investigation has been conducted about the privacy limitations associated with a mobile application [24-25]. Mobile technologies are widely used by individuals and may assist in the prevention of COVID-19. Furthermore, further research should be conducted, and the resulting taxonomy may be refined to align with real-world applications. Figure 3 illustrates both stationary and portable IoT devices and the application of the settings. All five criteria are employed for both stationary and wearable IoT gadgets [26-28].

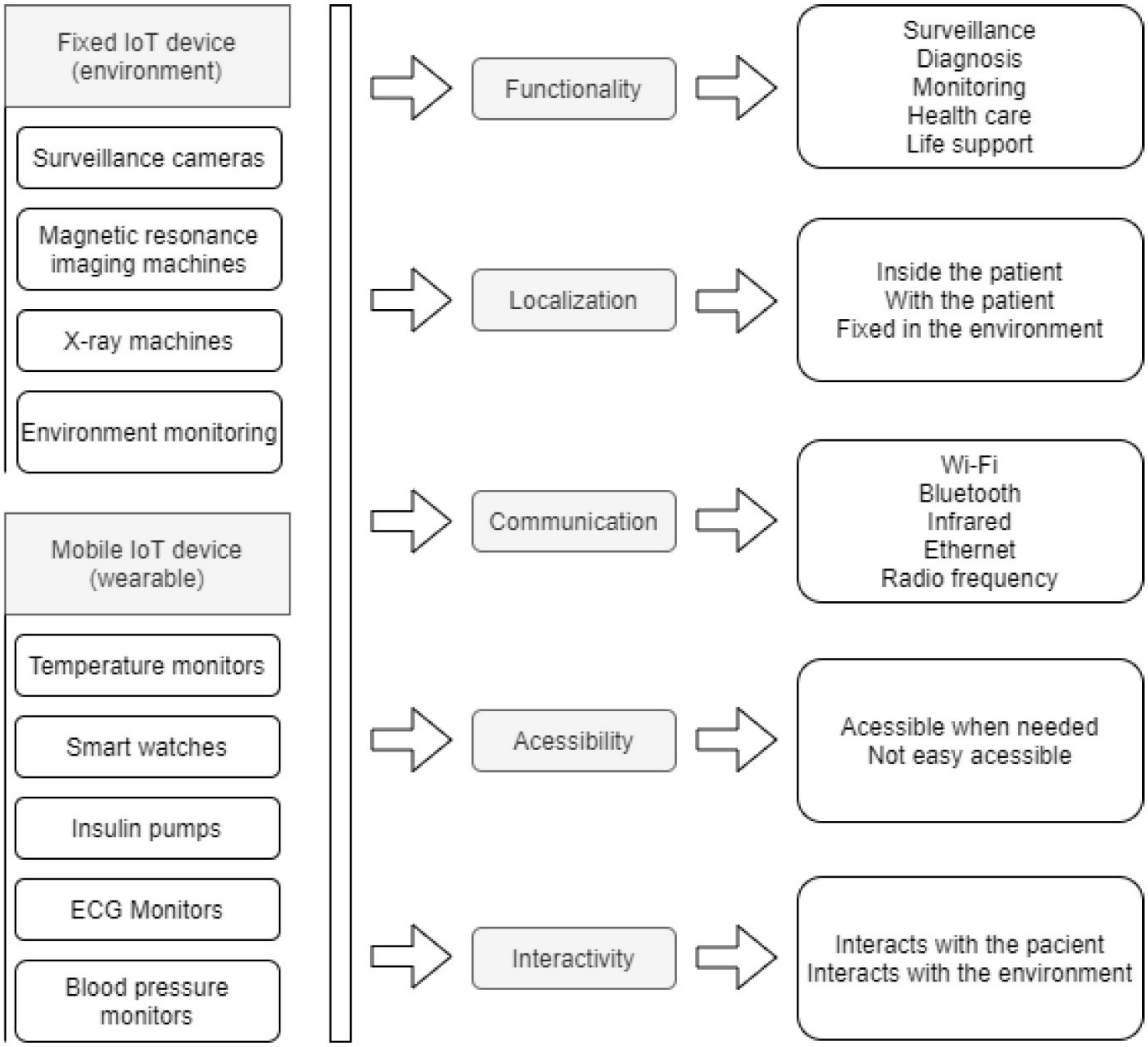

Figure 3: Components integrated in device [2]

The very first scenario illustrates a patient's admission to the EMS centre. The patient engages with the hostess and undergoes certain processes. This use case encompasses many aspects of the suggested taxonomy definition: Privacy, denoted by the data to which the patient consents access and is recorded in the systems [29-31]; The user is represented by the person in need and the secretary; the setting is portrayed by the emergency department, as seen in Figure 4.

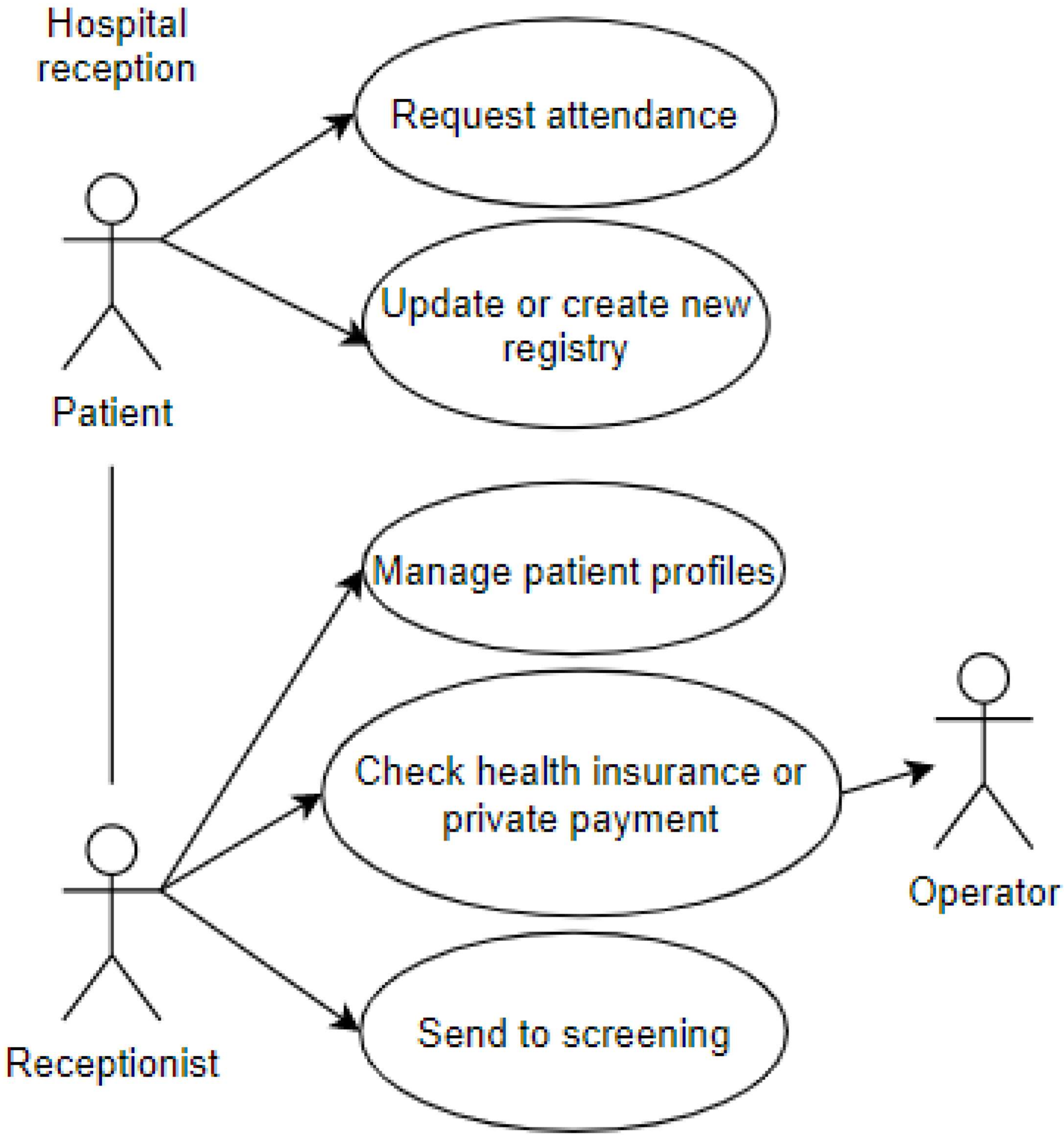

Figure 4: Reception at the Emergency Room [2]

Following initial treatment and enrolment, the patient's transportation to the testing area is shown in the application case depicted in Figure 5. The assessment process seeks to determine the case's priority and danger categorisation. This use case encompasses many properties included in the suggested taxonomy definition: Privacy is denoted by the information for which the patient consents access, recorded in both the systems and the mobile IoT device; the consumer is symbolised by both the individual and the nurse; the setting is characterised by the selection room; the appliance is exemplified by the practical IoT device designed to obtain a code to document the data and classify the patient.

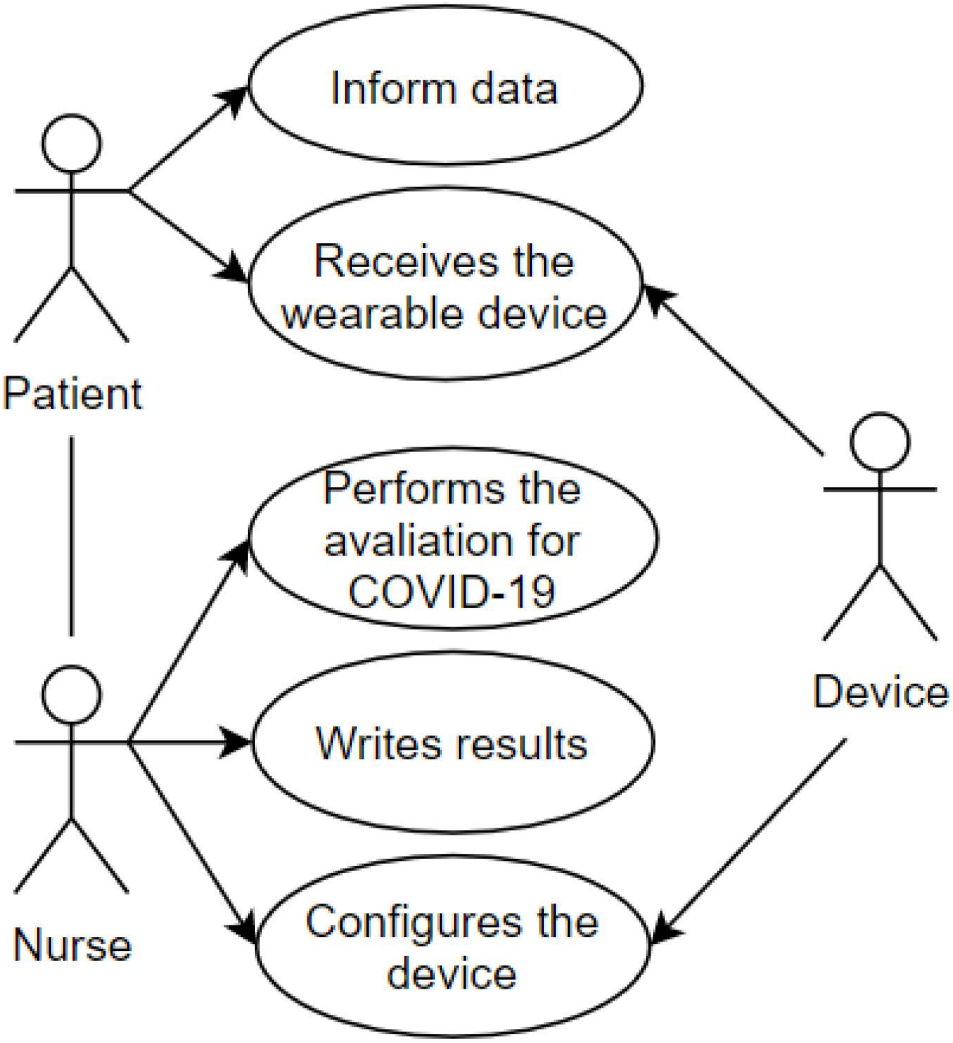
Inform data
Receives the wearable device
Patient
Performs the avaliation for COVID-19
Writes results
Configures the device
Nurse
Device

Figure 5: Scenario in Screening area [2]

Figure 6 shows the first screen of the app's signup process, which has the areas we talked about above.

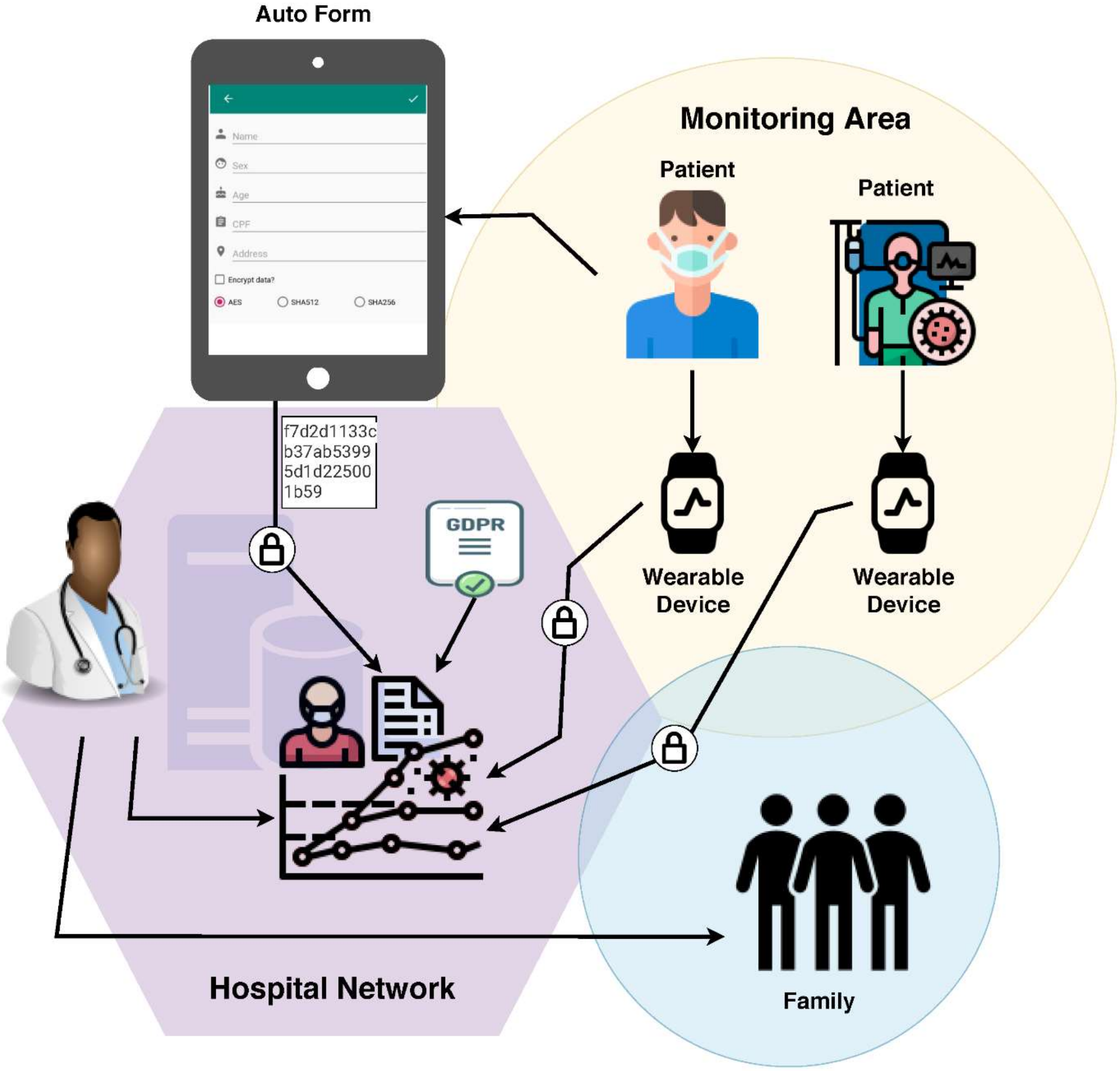

Figure 6: Software flow [2]

1.2. Assessment strategies

Information tools are becoming more and more important in the healthcare field. The electronic health record (EHR) and health information exchange (HIE) networks are two well-known types of health IT (HIT). People think that these tools will make care better, but they have also brought up some important questions and problems with privacy and the law. Putting these processes in place hasn't been easy, and there are still some big problems to solve. This piece talks about EHR and HIE as ways to get around these problems [32-34]. It also looks at how they are developing and being used in different countries around the world right now. Concerns about the law and ethics that EHR users and buyers may face are also talked over. Lastly, the connections and relationships between EHR and HIE and a number of current qualities of care issues in healthcare are looked at. The focus is on EHR and HIE in the emergency department (ED), which has special features that make it a place where implementing this technology may be very good for health, but also presents big problems. At the end of the study, detailed policy consequences and suggestions are talked about based on an analysis of these systems' present flaws [31].

1.3. Challenges:

Data protection systems and privacy laws in healthcare industry implementations faces numerous complex challenges in the field of technology organisation and regulatory domains. There is a impact on maintaining both efficient operations and robust security measures because of the above said challenges. With respect to technical infrastructure health care organisation struggle with the fundamental challenge of integration of the legacy system. With the evolution of New year technologies there are many facilities at operate with updated systems and lack modern security features and hands are incompatible with the latest technology. Due to this there is a challenge for the smaller healthcare products to overcome the cost of system wide updates. This technical depth further complicates the interproability issues various different data formats and systems and managing somehow working in harmony maintaining the security and integrity. There is always a trader of between securing the data transfer between different systems and the efficiency or increased security risks. The human element also present significant challenges in healthcare data protection like training of the staff complaints remains persistent issues even if the turnover rates in the healthcare settings are high 35 -38. Sometimes the medical professionals whose primary focus is patient care may also view the security measures as a burden additional to the already demanding workload. The implementation of security protocols are complicated by wearing levels of technical literacy among the healthcare staff members. Resource allocation also ads on to the above difficulties therefore the health care organisations must balance limited budgets between clinical needs and security requirements. It's a challenge to maintain robust security programs because of shortage of qualified it security personal in the sector. Regulatory compliance also presents other level of complexity in data protection. The organisations must also look through the landscape of overlapping regulations like HIPAA and GDPR and various other state laws each having their own specific requirements. The frequent updates in this regulations require a constant monitoring and modification of the systems. The documentation and auditing of the requirements associated with the above regulations also consume a lot of resources leading to straining of already limited administrative capacity and staff 39 – 42. If third party management ads on to the another dimension of compliance challenge the healthcare organisations must make sure to ensure that the cloud service providers vendors and other business associates also maintain equivalent security standards. The data management poses another challenge and grows exponentially because of increase in the healthcare data volume and variety. Health care organisations face difficulty in managing ever growing array of data types from traditional medical records to latest genetic information and data from variable devices ioht iot etc. the implementation of granular access controls needed for protection of the sensitive information of one conflicts with the need for quick access in emergency situations. Additional complications in data life cycle management because of long term data retention along with the secure data disposal processes. Tera certain inherent security vulnerability is because of the proliferation of mobile health applications and byod policies which has expanded the attacks surface for potential security breaches. With the integration of a and machine learning technology is raising new questions about data privacy algorithm transparency and bias in healthcare decision making. There are various other challenges like patient related challenges from a crucial aspect of healthcare data protection managing patient rights and preferences particularly with the implementation of comprehensive privacy laws 43-46. The health care organisations must also maintain secure communication channels while ensuring the accessibility of the patients. An additional security consideration has been introduced because of the rise of tally health services which has requiring Robert platforms which can protect sensitive medical conversations and data transmission

The various challenges that the health care organisations must invest in our continuous security updates staff training complaints monitoring and maintaining quality patient care 47-50. Financial penalties and loss of patient trust are some of the terms where security breaches in healthcare can be devastating. Their seems and never ending cycle of investment and implementation with rapid evolution of cyber threads to constantly adapt and upgrade the security measures posing an interconnected and often cascading effects throughout healthcare organisations. A sensitive holistic approach to health care data protection is required because addressing one area of frequently impact challenges in another. A balance between security requirements operational efficiency and patient care quality is needed to achieve success in implementing effective data protection systems. There is a need for the organisations to develop flexible and adaptable strategies which can evolve along with the technology like a and ml and other regulatory changes to maintain the fundamental focus on patient care and privacy protection.

Conclusion:

There are various complex challenges in the implementation of data protection and privacy laws in the healthcare industries which are requiring a carefully balanced approach. The comprehensive review in this paper reveals that the healthcare organisations face a lot of significant hurdles in the field of technology human and regulatory dimension. The privacy implementation is becoming a demanding environment considering the technical challenges of integrating the modern security features and the legacy systems in combination with the human factors of staff training and compliance in this industry. There are various challenges evolving around the regulatory landscape like HIPAA and GDPR and various other states specific requirements which the healthcare institutions must navigate in managing with the limited resources. With the evolution of AI and machine learning complicates the abortion landscape further introducing new vulnerability and privacy issues along with the proliferation of internet of healthcare things devices. The healthcare settings must also focus on the financial implications of addressing the above said issues which requires continuous investment in security updates training of this staff and complaints monitoring time to time also maintaining the quality patient care. Maintaining a holistic approach that balances the security issues along with the operational efficiency and patient care quality supported by flexibility adaptable strategies that can evolve with technology and ml and regulatory changes while maintaining the fundamentals on the patient private protection can lead to success in implementing effective data protection systems overall.

References:

1. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. https://doi.org/10.3390/app12041927
2. Verri Lucca, Arielle, et al. "A case study on the development of a data privacy management solution based on patient information." *Sensors* 20.21 (2020): 6030.
3. Sarabdeen, Jawahitha, and Immanuel Azaad Moonesar. "Privacy protection laws and public perception of data privacy: The case of Dubai e-health care services." *Benchmarking: An International Journal* 25.6 (2018): 1883-1902.

4. Kalloniatis, Christos, et al. "Incorporating privacy by design in body sensor networks for medical applications: A privacy and data protection framework." *Computer Science and Information Systems* 18.1 (2021): 323-347.
5. Semantha, Farida Habib, et al. "A conceptual framework to ensure privacy in patient record management system." *IEEE Access* 9 (2021): 165667-165689.
6. Dove, Edward S., and Mark Phillips. "Privacy law, data sharing policies, and medical data: a comparative perspective." *Medical data privacy handbook* (2015): 639-678.
7. Bincoletto, Giorgia. "A data protection by design model for privacy management in electronic health records." *Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7*. Springer International Publishing, 2019.
8. Diamantopoulou, Vasiliki, et al. "Privacy data management and awareness for public administrations: a case study from the healthcare domain." *Privacy Technologies and Policy: 5th Annual Privacy Forum, APF 2017, Vienna, Austria, June 7-8, 2017, Revised Selected Papers 5*. Springer International Publishing, 2017.
9. Di Iorio, Concetta Tania, et al. "Assessing data protection and governance in health information systems: a novel methodology of privacy and ethics impact and performance assessment (PEIPA)." *Journal of medical ethics* 47.12 (2021): e23-e23.
10. Gonçalves-Ferreira, Duarte, et al. "OpenEHR and general data protection regulation: evaluation of principles and requirements." *JMIR medical informatics* 7.1 (2019): e9845.
11. B. C. R, S. Joy, A. S. Bale, A. S. Naidu, V. N and V. S N, "Advanced Computing in IoT for Door Lock Automation," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 565-569, doi: 10.1109/ICEARS53579.2022.9752140.
12. S. S. Kumar, A. Sudhir Bale, P. M. Matapati and V. N, "Conceptual Study of Artificial Intelligence in Smart Cities with Industry 4.0," *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, 2021, pp. 575-577, doi: 10.1109/ICACITE51222.2021.9404607.
13. S. Joy, R. Baby Chithra, A. S. B, N. Ghorpade, S. N. Varsha and A. S. Naidu, "A Comparative Study on Recent Trends in Iris Recognition Techniques," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 1521-1525, doi: 10.1109/ICEARS53579.2022.9752355.
14. Aditya Khatokar, J. *et al.* (2021) “A study on improved methods in Micro-electromechanical systems technology,” *Materials today: proceedings*, 43, pp. 3784–3790. Available at: https://doi.org/10.1016/j.matpr.2020.10.993.
15. S. A. Huddar, B. G. Sheeparamatti, "Study of pull-in voltage of a perforated SMA based MEMS Switch," *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, Vellore, India, 2017, pp. 1-4, doi: 10.1109/ICMDCS.2017.8211584.
16. Tiwari, S. ., Khatokar, A. ., N, V. ., & Mohan M S, K. . (2021). Bio-Inspired Computing-A Dive into Critical Problems, Potential Architecture and Techniques. *Trends in Sciences*, *18*(23), 703. https://doi.org/10.48048/tis.2021.703
17. Kumar, S.S., Kiran Mohan, M.S., Vinay, N. (2022). A Study of Improved Methods on Image Inpainting. In: Johri, P., Diván, M.J., Khanam, R., Marciszack, M., Will, A. (eds) Trends and Advancements of Image Processing and Its Applications. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-75945-2_15

18. Aditya Khatokar, J., Vinay, N., Sanjay, B., *et al.* (2021) “Carbon nanodots: Chemiluminescence, fluorescence and photoluminescence properties,” *Materials today: proceedings*, 43, pp. 3928–3931. Available at: https://doi.org/10.1016/j.matpr.2021.02.582.
19. S. Saravana Kumar, S. Varun Yogi, Swetha Vura, R. Baby Chithra, N. Vinay, P. Pravesh, Chapter 8 - Network and security leveraging IoT and image processing: A quantum leap forward, Editor(s): Prashant Johri, Adarsh Anand, Jüri Vain, Jagvinder Singh, Mohammad Quasim, In Emerging Methodologies and Applications in Modelling, System Assurances, Academic Press, 2022, Pages 123-141, ISBN 9780323902403, https://doi.org/10.1016/B978-0-323-90240-3.00008-4.
20. Ajay Sudhir Bale *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **872** 012008
21. Ben-Assuli, Ofir. "Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments." *Health policy* 119.3 (2015): 287-297.
22. Choi, Young B., et al. "Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules." *Journal of medical systems* 30 (2006): 57-64.
23. Appari, Ajit, and M. Eric Johnson. "Information security and privacy in healthcare: current state of research." *International journal of Internet and enterprise management* 6.4 (2010): 279-314.
24. Hiller, Janine, et al. "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared." *BUJ Sci. & Tech. L.* 17 (2011): 1.
25. Abouelmehdi, Karim, et al. "Big data security and privacy in healthcare: A Review." *Procedia Computer Science* 113 (2017): 73-80.
26. Bale, A.S., Purohit, T.P., Hashim, M.F. and Navale, S. (2022). Blockchain and Its Applications in Industry 4.0. In A Roadmap for Enabling Industry 4.0 by Artificial Intelligence (eds J.M. Chatterjee, H. Garg and R.N. Thakur). https://doi.org/10.1002/9781119905141.ch16
27. Bale, A.S. *et al.* (2021) “Nanosciences fostering cross domain engineering applications,” *Materials today: proceedings*, 43, pp. 3428–3431. Available at: https://doi.org/10.1016/j.matpr.2020.09.076.
28. Sudhir. ., Dhumale, R. B. ., Beri, N. ., Lourens, M. ., Varma, R. A. ., Kumar, Sanamdikar, S. ., & Savadatti, M. B. . (2023). The Impact of Generative Content on Individuals Privacy and Ethical Concerns. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(1s), 697–703. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3503
29. Arushi Gupa *et al.*, "Mobile Cloud Computing - Enabling Technologies and Applications," *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India, 2021, pp. 491-496, doi: 10.1109/ISPCC53510.2021.9609344.
30. A. S. ., Vada, Y. R. ., Oshiojum, B. E. ., Lakkineni, U. K. ., Rao, C. ., Venkatesh (2023). ChatGPT in Software Development: Methods and Cross-Domain Applications. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(9s), 636–643. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3212
31. Ben-Assuli, Ofir. "Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments." Health policy 119.3 (2015): 287-297.
32. Choi, Young B., et al. "Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules." Journal of medical systems 30 (2006): 57-64.
33. Hiller, Janine, et al. "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared." *BUJ Sci. & Tech. L.* 17 (2011): 1.

34. Oetzel, Marie Caroline, and Sarah Spiekermann. "A systematic methodology for privacy impact assessments: a design science approach." *European Journal of Information Systems* 23.2 (2014): 126-150.
35. A. Biswas, S. Malik, E. Uchoi, S. U. Soni and A. Soni, "IoT Applications in Blockchain Technology," *2023 International Conference on Computer Science and Emerging Technologies (CSET)*, Bangalore, India, 2023, pp. 1-6, doi: 10.1109/CSET58993.2023.10346695.
36. Soni, S. U. ., Rajput, D. S. ., R., H. ., Saranya, S. ., Joy, S. ., Chithra R., B. ., & Savadatti, M. B. . (2023). 5G Wireless Communication and Its Adverse Effects on the Human Body: Distinguishing Falsehoods from Reality. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(5s), 101–112. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3870
37. H. R, B. Prakash, P. S. Babu, R. Gupta and S. Malik, "Recent Scientific Achievements and Developments in Software Defined Networking: A Survey," *2023 1st International Conference on Circuits, Power and Intelligent Systems (CCPIS)*, Bhubaneswar, India, 2023, pp. 1-6, doi: 10.1109/CCPIS59145.2023.10291262.
38. Putkuri, T., I. Latva-Korpela, and M. Häkkinen. "Professional support for children or adolescents whose mental well-being is at risk." European Journal of Public Health 34.Supplement_3 (2024): ckae144-1986.
39. Aggarwal, Monica, et al. "Assessing the impact of Canadian primary care research and researchers: Citation analysis." Canadian Family Physician 70.5 (2024): 329-341.
40. Quesada-Puga, Carmen, et al. "Job satisfaction and burnout syndrome among intensive-care unit nurses: A systematic review and meta-analysis." Intensive and Critical Care Nursing 82 (2024): 103660.
41. Davis, Carol M., and Gina Maria Musolino. *Patient practitioner interaction: An experiential manual for developing the art of health care*. Taylor & Francis, 2024.
42. Vinay, N., Bale, A.S., Tiwari, S. and Baby, C.R. (2022). Artificial Intelligence as a Tool for Conservation and Efficient Utilization of Renewable Resource. In Artificial Intelligence for Renewable Energy Systems (eds A.K. Vyas, S. Balamurugan, K.K. Hiran and H.S. Dhiman). https://doi.org/10.1002/9781119761686.ch2
43. M. Rajani, N. Taj, S. A. S, G. Amala and K. Lal, "Connecting Autonomous Engineering Domains with the Shared Language of Deep Neural Networks," *2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*, Namakkal, India, 2024, pp. 1-6, doi: 10.1109/AIMLA59606.2024.10531318.
44. S. Saravana Kumar, P. Rao and A. K. J., "A Recent Trend in DC Microgrid," *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, 2021, pp. 543-546, doi: 10.1109/ICACITE51222.2021.9404668.
45. S. C. Reddy, H. Chandramouli, S. Ponnuru, S. Saranya and K. Lal, "Review on Intelligent Social Networking Algorithms and Their Effects on Predicting the Adequacy of Renewable Energy Sources via Social Media," *2024 Second International Conference on Smart Technologies for Power and Renewable Energy (SPECon)*, Ernakulam, India, 2024, pp. 1-6, doi: 10.1109/SPECon61254.2024.10537390.
46. D. Gowda G and T. U, "Thermoelectric Simulation of a Microresistor Beam," *2019 Global Conference for Advancement in Technology (GCAT)*, Bangalore, India, 2019, pp. 1-3, doi: 10.1109/GCAT47503.2019.8978310.

47. A. S. Bale *et al*., "Advancements of Lab on Chip in Reducing Human Intervention: A Study," *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, 2021, pp. 38-42, doi: 10.1109/ICAC3N53548.2021.9725466.
48. Gomez-Cabello, Cesar A., et al. "Artificial-Intelligence-based clinical decision support systems in primary care: A scoping review of current clinical implementations." European Journal of Investigation in Health, Psychology and Education 14.3 (2024): 685-698.
49. Gill, Neeraj, et al. "Bringing together the World Health Organization's QualityRights initiative and the World Psychiatric Association's programme on implementing alternatives to coercion in mental healthcare: a common goal for action." BJPsych Open 10.1 (2024): e23.
50. Blomqvist, Paula, and Ulrika Winblad. "Have the welfare professions lost autonomy? A comparative study of doctors and teachers." Journal of Social Policy 53.1 (2024): 64-85.