Mahadeo D. Kokate, Satish N. Gujar, Sunil L. Bangare, Dharmesh Dhabliya, Parth Sharma, Mukesh Patil, Securing the Future: Technological Innovations for Social Medical Public Healthcare Security. Submitted: 22-02-2024 Accepted: 22-04-2024 Posted: 24-05-2024, Vol. (XXIII)

Securing the Future: Technological Innovations for Social Medical Public Healthcare Security

Mahadeo D. Kokate[1], Dr. Satish N. Gujar[2], Dr. Sunil L. Bangare[3], Dharmesh Dhabliya[4], Parth Sharma[5], Dr. Mukesh Patil[6]

[1]Department of Electronics and Telecommunication Engineering SNJBs K B Jain College of Engineering, Chandwad Email Id: mdkokate66@gmail.com

[2]Professor, Dept. Of Computer Engineering, Navashyandri Education Soc. Group of Institute faculty of Engineering, Pune, Maharashtra, India. Email: satishgujar@gmail.com

[3]Associate Professor, Department of Information Technology, Sinhgad Academy of Engineering, Savitribai Phule Pune University, Pune, India, sunil.bangare@gmail.com

[4]Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: dharmesh.dhabliya@viit.ac.in

[5]Assistant professor, Symbiosis Law School, Nagpur Campus, Symbiosis International (Deemed University), Pune, India. Email: parthsharma@slsnagpur.edu.in

[6]NIT Graduate School of Management, Mahurzari, Nagpur, Maharashtra, India. Email: 10mukeshpatil@gmail.com

KEYWORDS

Social Medical, healthcare technologies , Public Healthcare Security

ABSTRACT

The public healthcare sector is currently experiencing significant changes, characterized by a growing dependence on technology to improve efficiency, accessibility, and the quality of patient care. Nevertheless, the swift process of digitization presents unparalleled challenges in healthcare security. This review paper explores the complex relationship between technological advancements and the need to strengthen the security of social medical public healthcare. The paper commences by examining the historical progression of healthcare security concerns, emphasizing the insights gained from previous occurrences, and clarifying the urgent requirement for a comprehensive security framework. An exhaustive analysis of the present healthcare security scenario exposes weaknesses in the current systems and emphasizes the need for flexible solutions. The literature review examines the most recent progressions in healthcare technologies, specifically emphasizing pioneering innovations such as blockchain, artificial intelligence, and Internet of Things (IoT) devices. Concrete examples of successful technology implementations in different healthcare settings are provided through real-world case studies, offering practical insights into their effectiveness. Nevertheless, the incorporation of these technological solutions presents difficulties, encompassing privacy apprehensions, adherence to regulations, and the intricate endeavor of aligning with existing systems. The paper examines these challenges closely and suggests strategies for reducing cybersecurity risks. The advantages of technological advancements in healthcare security are outlined, highlighting how these advancements contribute to heightened data security, enhanced patient care and monitoring, and streamlined healthcare procedures. The narrative is enhanced by the inclusion of case studies that demonstrate successful implementations on a global scale. The paper progresses by predicting forthcoming risks to healthcare security, offering a strategic plan for policymakers and healthcare practitioners to foresee and tackle emerging challenges. The potential impact of emerging

technologies, such as quantum computing and genomics, on healthcare security is being investigated. The recommendations for policymakers include policy reforms, regulatory frameworks, and incentives to promote the adoption of secure technologies. In addition, the paper promotes the implementation of training and education initiatives to enhance cybersecurity awareness among healthcare professionals. Ultimately, this review paper combines historical viewpoints, present circumstances, and future possibilities to emphasize the crucial importance of technological advancements in ensuring the future of social medical public healthcare. The purpose of this paper is to provide policymakers, healthcare practitioners, and researchers with valuable information and suggestions. The goal is to encourage a shared dedication to strengthening healthcare security for the betterment of society.

1. Introduction

The convergence of technology and public healthcare has become progressively intricate in the modern era. The present condition of public healthcare security is characterized by a precarious equilibrium between the advantages of technological progress and the increasing perils presented by cybercriminals. The process of converting health records into digital format, the extensive incorporation of interconnected medical devices, and the rapid expansion of telemedicine have all increased the susceptibility of healthcare systems. These vulnerabilities not only endanger the security of patient data but also present a significant threat to the provision of essential medical services. With the ongoing development and growth of healthcare systems' digital presence, it is crucial to thoroughly assess the current security measures and explore inventive strategies to strengthen these systems against new and emerging risks[1].

The significance of safeguarding healthcare systems extends well beyond the boundaries of data security. The security of healthcare systems is fundamentally interconnected with the social welfare of communities. Security breaches in the healthcare sector not only jeopardize the confidentiality of highly sensitive medical data but also disrupt the smooth provision of patient care. The consequences encompass the erosion of public confidence in healthcare institutions, which could potentially impede individuals from seeking prompt medical care. Therefore, ensuring the security of healthcare systems is crucial for promoting societal well-being, emphasizing the necessity for comprehensive strategies to protect the integrity of these systems[2], [3].

Technological advancements are powerful resources in strengthening the security of public healthcare. These innovations offer exceptional opportunities, including cutting-edge encryption methods to protect patient data confidentiality and artificial intelligence-driven threat detection mechanisms to enhance proactive defense. The review aims to thoroughly explore these technological advancements, emphasizing their potential to fundamentally reshape the healthcare security landscape. The paper aims to promote the inclusion of these innovations as essential elements of a strong healthcare security framework by demonstrating their effectiveness[4], [5].

This review aims to address and analyze the complexities of the current healthcare security paradigm by recognizing the presence of challenges. A thorough examination is necessary to fully understand the complex interplay between privacy concerns and regulatory compliance, as well as the technical difficulties involved in integrating new

technologies with existing legacy systems. The paper seeks to analyze these challenges in order to enhance our comprehension of the barriers that need to be overcome in order to establish a robust healthcare security infrastructure[6], [7].
In order to understand the current situation and plan for the future, it is crucial to examine the historical development of concerns regarding security in healthcare. This section offers a reflective perspective, clarifying the significant events and critical moments that have influenced the current state of affairs.
The healthcare security concerns have existed throughout different periods of history, reflecting the changes in medical practices and technological advancements. The evolution of healthcare security has paralleled the progress of technology, starting from basic protection of physical medical records to the introduction of electronic health records. Gaining insight into this evolutionary trajectory is crucial for identifying patterns, foreseeing obstacles, and mapping out a direction for future healthcare security initiatives[8], [9].
The history of healthcare security is marked by incidents that provide significant lessons for the current and future times. The review seeks to extract valuable insights that can guide current strategies by analyzing significant events and their consequences. Whether it is a breach caused by insufficient encryption protocols or a failure in cybersecurity frameworks, every incident adds to the shared understanding required for constructing robust healthcare security systems. Building upon historical perspectives, the review then delves into a comprehensive analysis of the current healthcare security landscape. This section highlights the current weaknesses in healthcare systems and presents the latest developments that can strengthen these systems[10].
The present healthcare security environment is marked by a variety of weaknesses that present significant dangers to the confidentiality of patient information and the uninterrupted provision of medical services. The increasing number of interconnected devices, the larger vulnerable area provided by telehealth platforms, and the growing complexity of cyber threats exacerbate the difficulties. The review seeks to gain a comprehensive understanding of the multifaceted challenges that require immediate attention by conducting a thorough examination of these vulnerabilities.

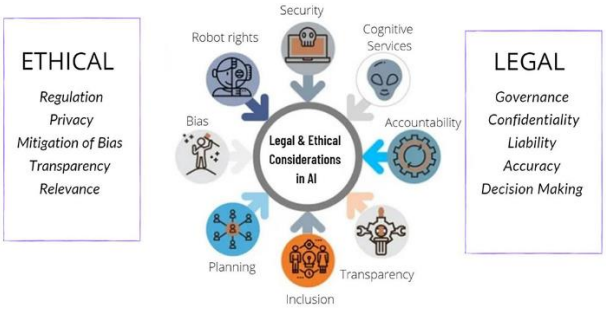

Figure 1 Concern related to AI in healthcare[11]

The figure-1 presents the “Legal and Ethical Considerations in Artificial Intelligence." The content is categorized into four primary segments: Ethics, Regulation, Privacy & Transparency, and Security. The sections are comprised of multiple sub-sections that delve deeper into the specific factors that must be considered during the development and utilization of AI.
Located at the uppermost part of the diagram, the Ethics section primarily centers around the possible advantages and disadvantages of AI. The subsections within this section encompass the principles of fairness, accountability, transparency, and human oversight. These factors are crucial in the development of AI to guarantee that AI systems are free from bias or discrimination, that they are responsible for their decisions, and that they operate in a transparent manner.
The Regulation section is positioned on the left side of the diagram and specifically addresses the legal framework and regulations that oversee the advancement and utilization of AI. The subsections within this section encompass data privacy, intellectual property, and product

liability. These factors are crucial when creating AI, as it is imperative to adhere to all relevant laws and regulations.

The Privacy & Transparency section is positioned adjacent to the diagram and emphasizes the protection of personal data and the clarity of AI systems. The subsections within this section encompass the processes of data collection, data utilization, and algorithmic bias. When developing AI, it is crucial to prioritize safeguarding individual privacy and mitigating biases in AI systems.

The Security section is positioned at the lowermost part of the diagram and specifically addresses the safeguarding of AI systems. The subsections within this section encompass cyber security, physical security, and data security. These factors are crucial in AI development to guarantee the resilience of AI systems against potential attacks and safeguard them against unauthorized intrusion.

Generally, the diagram offers a comprehensive outline of the legal and ethical factors that must be considered during the development and utilization of AI. In order to create AI that is secure, equitable, and advantageous to society, it is crucial to take into account all of these variables.

In spite of the difficulties, there is a domain of potentiality due to recent breakthroughs in healthcare technologies. The possibilities range from innovative blockchain solutions that guarantee secure health records to artificial intelligence algorithms that identify unusual activities. This section thoroughly examines these technological advancements, providing a glimpse into the array of tools and resources that can be utilized to strengthen healthcare security. By comprehending the functionalities of these technologies, individuals involved in the healthcare ecosystem can make well-informed decisions regarding their integration and implementation.

The essence of the review centers around a thorough examination of technological advancements that are crucial in transforming the security of public healthcare. In a society where data holds significant value and medical information is considered sacred, these advancements provide a powerful safeguard against emerging dangers.

Overview of Cutting-Edge Technologies

- Blockchain in Healthcare: The decentralized and secure nature of blockchain technology has led to significant applications in the healthcare industry. Blockchain technology guarantees the integrity and immutability of health records, effectively addressing concerns regarding data tampering and unauthorized access. This section explores the fundamental principles and practical uses of blockchain technology in ensuring the security of healthcare data. It clarifies how blockchain acts as an immutable record for patient information, resistant to tampering or corruption.
- Artificial Intelligence for Threat Detection: The interdependent connection between artificial intelligence and healthcare security is revolutionary. Machine learning algorithms possess the ability to analyze extensive datasets and detect patterns that may indicate potential security risks. This section explores the impact of artificial intelligence on threat detection in healthcare, covering topics such as anomaly detection and predictive analytics. By utilizing these capabilities, healthcare systems can actively detect and reduce security risks.
- IoT Devices for Patient Monitoring: The healthcare sector has been significantly impacted by the Internet of Things (IoT), which provides advanced solutions for remote patient monitoring and data collection. The interconnected nature of IoT devices presents security challenges despite the immense opportunities it offers

for enhancing patient care. This segment explores the impact of IoT on healthcare security and provides strategies to reduce related risks. Healthcare practitioners can optimize the advantages of IoT while ensuring the integrity of patient data by finding a harmonious equilibrium between innovation and security.

The purpose of the review is to provide a clear and concise explanation. This review has two main objectives: firstly, to emphasize the crucial importance of technological innovations in improving the security of public healthcare, and secondly, to tackle the complex challenges that exist in the current healthcare security landscape.

his review aims to provide valuable insights to researchers, policymakers, and healthcare professionals by exploring the complex intersection of technology and healthcare security. The paper seeks to examine the past, present, and future aspects of healthcare security in order to promote a shared dedication to strengthening the basis of healthcare systems for the benefit of society. As we approach the beginning of a new era in digital healthcare, we must consider the knowledge gained from the past and the advancements made in the present.

2. Exiting work analysis

The literature review covers a wide range of studies that examine the use of advanced technologies, specifically artificial intelligence (AI), neuroimaging, blockchain, and Internet of Things (IoT), in different areas of healthcare. These studies examine the techniques used, important discoveries, and observed restrictions in the effort to improve medical diagnostics, disease categorization, and healthcare decision-making assistance. The synthesis of these findings enhances our comprehensive comprehension of the present condition and prospective advancements in utilizing technology for enhancing healthcare. Table-1 represents the major related works.

Table 1 Major related works

Study	Focus	Methodology	Key Findings	Limitations
Chen et al.[12]	Overview of AI applications in healthcare	Literature review	AI can improve efficiency, safety, and access to healthcare, but leaders need to understand its limitations and ethical considerations.	Limited to published literature and may not capture all emerging AI applications.
Cossy-Gantner et al.[13]	Potential of AI for global health, especially in resource-poor settings	Case studies and expert interviews	AI can address healthcare challenges in resource-poor settings, but requires addressing data privacy, infrastructure limitations, and ethical concerns.	Limited scope to specific case studies and expert opinions.
Asgharzadeh-Bonab et al.[14]	AI-based method for Alzheimer's disease classification using MRI data	Proposed and evaluated a deep learning model for Alzheimer's disease classification.	Achieved high accuracy in classifying Alzheimer's disease, but needs validation on larger datasets and in clinical settings.	
Amini et al.[15]	Comparison of different neuroimaging techniques for	Review of existing literature on	Combined neuroimaging techniques (e.g., MRI and PET) may offer better	Focuses on existing techniques, may not capture advances in

	Alzheimer's disease detection	neuroimaging for Alzheimer's disease.	accuracy than single modalities, but further research is needed.	emerging AI-based methods.
Bütün et al.[16]	AI-based method for automatic detection of cancer metastasis in lymph nodes	Proposed and evaluated a deep learning model for lymph node metastasis detection.	Achieved promising results, but requires further validation with larger datasets and in clinical practice.	Limited to specific cancer type and dataset, may not generalize to other cancers.
Chaudhury et al.[17]	Blockchain-based IoT system for breast cancer detection	Proposed a conceptual framework for using blockchain and IoT in breast cancer detection.	Offers potential for secure and transparent data sharing in cancer diagnosis, but needs real-world implementation and validation.	Conceptual framework, lacking practical implementation and evaluation.
Fekri-Ershad et al.[18]	AI-based method for cervical cancer diagnosis using combined deep learning models	Proposed and evaluated a hybrid model for cervical cancer diagnosis.	Achieved high accuracy, but requires validation with larger datasets and diverse patient populations.	Limited data and focus on single cancer type, may not generalize to other settings.
Fernandes et al.[19]	AI-based methods for automatic decision support in cervical cancer screening	Literature review and evaluation of existing automated colposcopy analysis methods.	Various automated methods show promise for improving accuracy and efficiency of cervical cancer screening, but require further development and clinical validation.	Focuses on existing methods, may not capture recent advancements in AI for colposcopy analysis.
M. Hussain et al.[20]	Diagnosis of disc degenerative diseases using MRI	Systematic review	Deep learning can be used to effectively diagnose disc degenerative diseases using MRI.	Limited number of studies, need for further validation
M. Jardon et al.[21]	Foraminal stenosis evaluation	Retrospective study	Deep learning can be used to reconstruct high-resolution 3D cervical spine MRI for foraminal stenosis evaluation.	Small sample size, need for further clinical validation
H. Hosseinzadeh et al.[22]	COVID-19 detection	Proposed deep learning model	Deep multi-view feature learning can be used to effectively detect COVID-19 based on chest X-ray images.	Limited dataset, need for multi-center validation
M. Hemalatha[23]	COVID-19 and pneumonia detection	Proposed hybrid model	The proposed hybrid model can effectively detect COVID-19 and pneumonia.	Need for real-world validation, computational complexity
M. S. Patil et al.[24]	Diabetic retinopathy classification	Systematic review	Data augmentation techniques can improve the performance of deep learning models for diabetic retinopathy classification.	Limited focus on specific data augmentation techniques, need for further research
S. A. Patil et al.[25]	Diabetic retinopathy classification	Proposed distributed deep learning model	Pipeline parallelism can improve the performance of distributed deep learning	Complexity of implementation, need for larger datasets

			models for diabetic retinopathy classification.	
S. Muhammad Usman et al.[26]	Epileptic seizure prediction	Comparative study of deep learning models	Deep learning can be used to predict epileptic seizures with high accuracy.	Limited generalizability, need for patient-specific models
M. Mursalin et al.[27]	Epileptic seizure classification	Proposed feature selection algorithm	The proposed feature selection algorithm can improve the performance of epileptic seizure classification.	Need for validation on larger datasets, limited focus on deep learning

The studies that were examined provide valuable insights into the changing use of technology in healthcare. The utilization of AI, neuroimaging, and cutting-edge frameworks like blockchain and IoT offers potential opportunities for improving diagnostic precision, automating disease identification, and revolutionizing healthcare decision-making procedures. Nevertheless, the studies also emphasize the inherent difficulties and restrictions, encompassing limitations in the dataset and the requirement for validation and application in real-world clinical settings.

The advancements in healthcare technology highlight the significance of a careful and incremental approach. Continual research and validation are crucial to closing the current gaps and ensuring the smooth incorporation of technology into clinical practice. These insights provide a basis for future efforts, directing researchers, practitioners, and policymakers towards the efficient and ethical application of advanced technologies to achieve better healthcare results.

3. Technological Innovations in Public Healthcare Security

In the ever-changing field of public healthcare, the merging of technology and security is crucial for guaranteeing the honesty, availability, and privacy of sensitive health data. With the increasing intricacy of healthcare systems, there is a corresponding demand for inventive measures to protect against emerging risks. This section examines state-of-the-art technologies that have emerged as powerful factors in strengthening the security of public healthcare. The emergence of advanced technologies provides a unique chance to completely transform the field of public healthcare security. This section explores three fundamental elements of technological innovation that have attracted considerable interest due to their capacity to fundamentally transform the security paradigm:

- Blockchain technology[28]–[30]: The healthcare sector has been captivated by the decentralized and tamper-resistant nature of blockchain technology. The utilization of blockchain technology in the healthcare sector offers the potential to improve the reliability of data, guarantee secure exchange of information between different systems, and create a clear and verifiable record of medical transactions. The incorporation of blockchain technology has the potential to significantly enhance the security of public healthcare by ensuring the protection of electronic health records and enabling efficient drug traceability.
- Artificial Intelligence[12], [31]: Artificial Intelligence (AI) has become a powerful ally in the ongoing fight against cybersecurity threats in the healthcare sector. AI serves as a proactive defense mechanism by leveraging its capacity to analyze extensive datasets, detect patterns, and forecast potential security breaches. AI technologies enable healthcare systems to proactively address evolving cyber threats,

ranging from anomaly detection to predictive analytics. This section examines the profound influence of AI in enhancing the ability to detect threats and strengthening the resilience of security frameworks in public healthcare.

- Internet of Things (IoT)[32], [33] : The widespread adoption of Internet of Things (IoT) devices has introduced a new era of patient care and monitoring. Interconnected medical devices, which include wearables and remote monitoring tools, provide immediate and accurate information about the health of patients. Although these innovations improve the quality of care, they also bring about new security vulnerabilities. This section explores the role of IoT devices in patient monitoring, highlighting their potential advantages and the necessary security measures to reduce related risks.

As we explore these advanced technologies, it becomes clear that incorporating them into public healthcare security can strengthen protection against cyber threats and also drive a transformation towards more efficient, transparent, and patient-focused healthcare systems. Table-2 summarized the advance technologies used in healthcare.

Table 2 Summarize table for various technologies in social health services

Technology	Description	Security Benefits	Examples
Blockchain in healthcare	Securely stores and shares patient data across providers and institutions.	Enhances data privacy, auditability, and prevents unauthorized access.	MedRec for patient-controlled records, Hyperledger Fabric for supply chain tracking.
Artificial intelligence (AI) for threat detection	Analyzes healthcare data to identify suspicious activities and potential breaches.	Detects fraud, malware, and anomalous behavior, reduces vulnerability to cyberattacks.	AI-powered intrusion detection systems, anomaly detection algorithms.
IoT devices for patient monitoring	Collects real-time patient data like vitals and location.	Improves patient safety by enabling remote monitoring, identifying critical events, and alerting healthcare professionals.	Smart beds with fall detection, wearables for chronic disease management.

4. Major Medical/Healthcare Regulatory Compliance in India

Regulation/Act	Focus	Purpose	Key Compliance Requirements
Drugs & Cosmetics Act 1940 & Rules 1945	Pharmaceutical products	Ensure drug quality, safety, and efficacy	- Licenses (manufacturing, import, distribution, sale) - Quality control measures - Adverse drug reaction reporting
Clinical Trials Rules 2012	Clinical research	Protect patient safety, rights, and data privacy	- Informed consent procedures - Ethical conduct - Accurate reporting of study results
Biomedical Waste Management Rules 2016	Biomedical waste	Prevent environmental and public health hazards	- Segregation of waste - Treatment and disposal protocols

Digital Health Data Protection Bill (Proposed)	Digital healthcare data	Regulate collection, storage, and use of personal health data	- Data privacy measures - Patient consent - Breach notification protocols
Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002	Medical professionals	Maintain ethical standards and professional conduct	- Patient-doctor relationships - Informed consent - Conflict of interest avoidance
National Health Mission	Public healthcare delivery	Improve quality and access to healthcare	- Service standards - Quality guidelines - Performance monitoring

5. Conclusion, discussion and future scope

The investigation into state-of-the-art technologies such as Blockchain, Artificial Intelligence (AI), and Internet of Things (IoT) in the field of public healthcare security uncovers a promising landscape filled with significant possibilities for change. The utilization of blockchain technology in safeguarding health records and guaranteeing transparent data transactions establishes a strong basis for trust in healthcare systems. Artificial intelligence, equipped with its ability to analyze data and identify unusual patterns, serves as a proactive defense against constantly changing cyber risks. Simultaneously, the incorporation of IoT devices for patient monitoring not only improves healthcare provision but also introduces fresh obstacles that require careful security deliberations.

The combined use of these technologies is set to fundamentally change the models of healthcare security. Nevertheless, like any form of progress, these advancements come with their own set of difficulties and factors to take into account. Privacy issues, adherence to regulations, compatibility, and the necessity for consistent education and training are crucial factors that require continuous focus.

Discussion

The discussion clarifies the complex relationship between technological advancements and the diverse landscape of public healthcare security. Blockchain, characterized by its distributed and unchangeable record, guarantees the integrity of data and the security of transactions. The blockchain technology has the potential to be used not only for keeping records, but also for building trust in the pharmaceutical supply chain, improving the ability of different systems to work together, and giving patients more control over their health data.

Artificial Intelligence is becoming a powerful tool in identifying threats, as it has exceptional abilities to analyze large amounts of data and forecast possible security breaches. Nevertheless, the conversation highlights the significance of ethical deliberations, openness, and ongoing surveillance to guarantee the conscientious and impartial implementation of AI in healthcare security.

The incorporation of IoT devices introduces a novel aspect to patient care, facilitating instantaneous monitoring and tailored health insights. However, the conversation underscores the weaknesses linked to the interconnectedness of these devices, underscoring the urgent requirement for strong security measures to safeguard against potential cyber risks.

During the discussion, the focus is not only on the potential advantages but also on the ethical, legal, and practical difficulties that come with these technological advancements. The importance of adopting a comprehensive and interdisciplinary approach is emphasized, acknowledging that effective execution

necessitates cooperation among healthcare practitioners, policymakers, technologists, and cybersecurity specialists.

Potential for Future Expansion

The intersection of technological advancements and public healthcare security offers numerous opportunities for future exploration and improvement. The following areas are identified as crucial focal points for the future:

- Ethical and Regulatory Frameworks: It is crucial to establish strong ethical and regulatory frameworks in order to ensure the responsible implementation of these technologies. Ensuring a harmonious equilibrium between fostering innovation and protecting patient rights will be pivotal in shaping the future of healthcare security.
- Interoperability and Standardization: Interoperability and standardization are crucial for improving the compatibility of various technologies and implementing standardized procedures. This will make it easier to integrate these technologies into existing healthcare infrastructures without any complications. This is especially vital for ensuring a unified and interconnected healthcare system.
- Continuous Education and Training: Continuous education and training programs for healthcare professionals and IT personnel are of utmost importance as technologies continue to advance. It is crucial to have a proficient workforce capable of managing these advancements in order to maximize their advantages and minimize potential hazards.
- Patient Empowerment: Enhancing patient education and empowerment in the management of their health data will be crucial. Incorporating technologies that empower patients to have more authority over their information, while also guaranteeing privacy and security, will enhance a healthcare model that prioritizes the needs and preferences of patients.

As these technologies further develop and become more integrated into healthcare systems globally, their influence on the security of public healthcare will become more noticeable. The future of healthcare security hinges on the intricate interplay among technological advancements, ethical deliberations, and a steadfast dedication to enhancing the welfare of individuals and communities. By employing strategic planning, conducting research initiatives, and demonstrating a collective commitment to the responsible utilization of technology, the future guarantees a healthcare landscape that is more secure, efficient, and focused on the needs of patients.

References

[1] L. Yardley *et al.*, "The Agile Co-production and Evaluation framework for developing public health interventions, messaging and guidance," *Front. Public Heal.*, vol. 11, no. June, pp. 1–6, 2023, doi: 10.3389/fpubh.2023.1094753.

[2] The Lancet, "Universal health care in 21st century Americas," *Lancet*, vol. 393, no. 10181, p. 1570, 2019, doi: 10.1016/S0140-6736(19)30864-5.

[3] A. Odone, S. Buttigieg, W. Ricciardi, N. Azzopardi-Muscat, and A. Staines, "Public health digitalization in Europe," *Eur. J. Public Health*, vol. 29, pp. 28–35, 2019, doi: 10.1093/eurpub/ckz161.

[4] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, p. 101660, 2019, doi: https://doi.org/10.1016/j.scs.2019.101660.

[5] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[6] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.018.

[7] Z. Lv and L. Qiao, "Analysis of healthcare big data," *Futur. Gener. Comput. Syst.*, vol. 109, pp. 103–110, 2020, doi: https://doi.org/10.1016/j.future.2020.03.039.

[8] N. Rieke *et al.*, "The future of digital health with federated learning," *npj Digit. Med.*, vol. 3, no. 1, pp. 1–7, 2020, doi: 10.1038/s41746-020-00323-1.

[9] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 511–521, 2019, doi: https://doi.org/10.1016/j.future.2018.12.044.

[10] J. Xu *et al.*, "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, 2019, doi: 10.1109/JIOT.2019.2923525.

[11] N. Naik *et al.*, "Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?," *Front. Surg.*, vol. 9, no. March, pp. 1–6, 2022, doi: 10.3389/fsurg.2022.862322.

[12] M. Chen and M. Decary, "Artificial intelligence in healthcare: An essential guide for health leaders," *Healthc. Manag. Forum*, vol. 33, no. 1, pp. 10–18, 2020, doi: 10.1177/0840470419873123.

[13] A. Cossy-Gantner, S. Germann, N. R. Schwalbe, and B. Wahl, "Artificial intelligence (AI) and global health: How can AI contribute to health in resource-poor settings?," *BMJ Glob. Heal.*, vol. 3, no. 4, pp. 1–7, 2018, doi: 10.1136/bmjgh-2018-000798.

[14] A. Asgharzadeh-Bonab, H. Kalbkhani, and S. Azarfardian, "An Alzheimer's disease classification method using fusion of features from brain Magnetic Resonance Image transforms and deep convolutional networks," *Healthc. Anal.*, vol. 4, no. June, p. 100223, 2023, doi: 10.1016/j.health.2023.100223.

[15] M. Amini, M. M. Pedram, A. Moradi, M. Jamshidi, and M. Ouchani, "Single and Combined Neuroimaging Techniques for Alzheimer's Disease Detection," *Comput. Intell. Neurosci.*, vol. 2021, 2021, doi: 10.1155/2021/9523039.

[16] E. Bütün, M. Uçan, and M. Kaya, "Automatic detection of cancer metastasis in lymph node using deep learning," *Biomed. Signal Process. Control*, vol. 82, no. December 2022, p. 104564, 2023, doi: 10.1016/j.bspc.2022.104564.

[17] S. Chaudhury and K. Sau, "A blockchain-enabled internet of medical things system for breast cancer detection in healthcare," *Healthc. Anal.*, vol. 4, no. April, p. 100221, 2023, doi: 10.1016/j.health.2023.100221.

[18] S. Fekri-Ershad and M. F. Alsaffar, "Developing a Tuned Three-Layer Perceptron Fed with Trained Deep Convolutional Neural Networks for Cervical Cancer Diagnosis," *Diagnostics*, vol. 13, no. 4, 2023, doi: 10.3390/diagnostics13040686.

[19] K. Fernandes, J. S. Cardoso, and J. Fernandes, "Automated Methods for the Decision Support of Cervical Cancer Screening Using Digital Colposcopies," *IEEE Access*, vol. 6, pp. 33910–33927, 2018, doi: 10.1109/ACCESS.2018.2839338.

[20] M. Hussain, D. Koundal, and J. Manhas, "Deep learning-based diagnosis of disc degenerative diseases using MRI: A comprehensive review," *Comput. Electr. Eng.*, vol. 105, no. December 2022, p. 108524, 2023, doi: 10.1016/j.compeleceng.2022.108524.

[21] M. Jardon *et al.*, "Deep-learning-reconstructed high-resolution 3D cervical spine MRI for foraminal stenosis evaluation," *Skeletal Radiol.*, vol. 52, no. 4, pp. 725–732, 2023, doi: 10.1007/s00256-022-04211-5.

[22] H. Hosseinzadeh, "Deep multi-view feature learning for detecting COVID-19 based on chest X-ray images," *Biomed. Signal Process. Control*, vol. 75, no. February, p. 103595, 2022, doi: 10.1016/j.bspc.2022.103595.

[23] M. Hemalatha, "A hybrid random forest deep learning classifier empowered edge cloud architecture for COVID-19 and pneumonia detection," *Expert Syst. Appl.*, vol. 210, no. June, p. 118227, 2022, doi: 10.1016/j.eswa.2022.118227.

[24] M. S. Patil and S. Chickerur, "Study of Data and Model parallelism in Distributed Deep learning for Diabetic retinopathy classification," *Procedia Comput. Sci.*, vol. 218, pp. 2253–2263, 2022, doi: 10.1016/j.procs.2023.01.201.

[25] S. A. Patil, M. S. Patil, S. Giraddi, S. Chickerur, V. M. Boormane, and G. Gamanagatti, "Pipeline Parallelism in Distributed Deep Learning for Diabetic Retinopathy Classification," *Procedia Comput. Sci.*, vol. 215, pp. 393–402, 2022, doi: 10.1016/j.procs.2022.12.041.

[26] S. Muhammad Usman, S. Khalid, and M. H. Aslam, "Epileptic Seizures Prediction Using Deep Learning Techniques," *IEEE Access*, vol. 8, pp. 39998–40007, 2020, doi: 10.1109/ACCESS.2020.2976866.

[27] M. Mursalin, S. S. Islam, M. K. Noman, and A. A. Al-Jumaily, "Epileptic seizure classification using statistical sampling and a novel feature selection algorithm," pp. 1–9, 2019.

[28] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 34, no. 14, pp. 11475–11490, 2022, doi: 10.1007/s00521-020-05519-w.

[29] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, p. 102407, 2020, doi: https://doi.org/10.1016/j.jisa.2019.102407.

[30] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 935–949, 2020, doi: https://doi.org/10.1016/j.future.2018.02.023.

[31] O. Baclic, M. Tunis, K. Young, C. Doan, and H. Swerdfeger, "Challenges and opportunities for public health made possible by advances in natural language processing," *Canada Commun. Dis. Rep.*, vol. 46, no. 6, pp. 161–168, 2020, doi: 10.14745/ccdr.v46i06a02.

[32] A. Ali and S. AlshmranyArshad Ali, "Health Monitoring and Management System by Using Wireless Sensor Network and Internet of Things (IoT) Un-Interrupted Glucose Monitoring and Prediction by Using Smart Sensor System View project Health Monitoring and Management System by Using Wireless Sens," *Artic. Int. J. Comput. Netw. Inf. Secur.*, vol. 19, no. 12, 2019, [Online]. Available: https://www.researchgate.net/publication/338689945.

[33] M. Dadkhah, M. Mehraeen, F. Rahimnia, and K. Kimiafar, "Use of internet of things for chronic disease management: An overview," *J. Med. Signals Sens.*, vol. 11, no. 2, pp. 138–157, 2021, doi: 10.4103/jmss.JMSS_13_20.