Jayalaxmi Dash, Sheetal Sachin Barekar, Ratnaprabha Ravindra Borhade, Sharayu Ikhar, Ahmar Afaq, Shailesh P. Bendale, Next-Gen Security: Leveraging Advanced Technologies for Social Medical Public Healthcare Resilience.
Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

Next-Gen Security: Leveraging Advanced Technologies for Social Medical Public Healthcare Resilience

Jayalaxmi Dash[1], Dr. Sheetal Sachin Barekar[2], Dr. Ratnaprabha Ravindra Borhade[3], Sharayu Ikhar[4], Dr. Ahmar Afaq[5], Dr. Shailesh P. Bendale[6]

[1]*Department of Computer Science and Engineering, Sudhananda Group of Institutions, Balianta, Bhubanrswar, India. Email: dash.jayalaxmi11@gmail.com*

[2]*Assistant Professor, Department of Computer Engineering, Cummins college of engineering for women Pune, Maharashtra, India. Email: sheetal.barekar@gmail.com*

[3]*Assistant Professor, Department of Electronics and Telecommunication, Cummins College of Engineering for Women, Pune, Maharashtra, India. Email: rrborhade11@gmail.com*

[4]*Department of Artificial Intelligence & Data Science, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: sharyu.ikhar@gmail.com*

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

[6]*Head and Assistant Professor, Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune, Maharashtra, India. Email: bendale.shailesh@gmail.com"*

KEYWORDS

Healthcare Resilience, Advanced Technologies, Social Medical Public Healthcare, Security Infrastructure, Cyber Threats, Artificial Intelligence (AI) in healthcare

ABSTRACT

The healthcare industry is undergoing a significant change as it incorporates advanced technologies to strengthen its security infrastructure and improve its ability to withstand current challenges and explores the important overlap between security, technology, and public health. The introductory section presents a thorough overview, highlighting the current status of public healthcare and emphasizing the crucial importance of security in protecting confidential medical data. This statement highlights the current difficulties encountered by social medical public healthcare systems and emphasizes the urgent need to utilize advanced technologies to strengthen their ability to adapt and recover. The systematic literature review explores a wide range of studies, providing insight into the various aspects of healthcare security. This text examines conventional security methods, exposes their constraints, and advances the discussion by examining cutting-edge technologies such as Artificial Intelligence (AI), Machine Learning, Blockchain, Internet of Things (IoT), and Biometric Security Solutions. Every technology is carefully examined to determine its ability to strengthen healthcare systems against cyber threats and breaches, guaranteeing the confidentiality and accuracy of patient data. The methodology section provides a clear explanation of the research design, the process of selecting participants, and the strategies used for analyzing the data. The research seeks to evaluate the present security situation and determine the best methods for incorporating advanced technologies into healthcare systems, using either qualitative or quantitative methods. The following sections elucidate the security challenges inherent in social medical public healthcare, encompassing cyber threats and privacy concerns. Drawing on case studies, the paper illustrates successful implementations of advanced technologies in healthcare security, distilling valuable lessons and best practices. The recommendations

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

section goes beyond the technical domain, exploring the policy implications and strategies for technological implementation. The exploration of regulatory frameworks, legal considerations, and ethical dimensions is conducted to provide guidance for the smooth integration of advanced technologies into healthcare systems. Healthcare professionals are encouraged to participate in training and awareness programs to ensure a comprehensive and efficient implementation. To summarize, the paper combines the results, highlighting the importance of utilizing advanced technologies to strengthen the security framework of social medical public healthcare. The significance of healthcare resilience is emphasized, and potential areas for future research are delineated. This research is an important resource that offers valuable insights and guidance for stakeholders, policymakers, and technologists who are dealing with the intricate field of healthcare security in the age of advanced technologies.

1. Introduction

The public healthcare sector is currently experiencing a significant change, marked by the merging of medical practices and cutting-edge technologies. The growing need for healthcare services, along with the digitalization of patient records, signifies a significant shift in the field. To address the current difficulties encountered by public healthcare systems, it is imperative to strategically incorporate cutting-edge technologies in order to guarantee easy access, effectiveness, and the provision of high-quality healthcare services. With the growing dependence of the healthcare industry on technology, the necessity for strong security measures becomes more evident[1], [2].

The importance of security in the healthcare sector is extremely significant. Ensuring patient confidentiality, maintaining the integrity of medical data, and safeguarding sensitive information are essential aspects of providing efficient healthcare. Given the prevalence of cyber threats, it is imperative for healthcare systems to prioritize security measures in order to protect the well-being of patients and uphold public confidence. The convergence of security measures and advanced technologies is crucial for enhancing resilience in the field of social medical public healthcare, as the value and susceptibility of healthcare data continue to increase.

1.1.Overview of Healthcare Security

The historical progression of healthcare security can be traced from the manual documentation of medical records to the digitalization of health records. The historical context provides valuable understanding of the difficulties encountered by conventional security measures and the urgent need for flexible solutions. Gaining insight into the historical foundations of healthcare security is essential for placing the current state of security frameworks into context and envisioning future progress[3].

When examining the present state of healthcare security, it is crucial to identify the primary concerns and weaknesses. The interconnectivity of healthcare networks, combined with the rapid expansion of healthcare data, provides an ideal environment for potential security breaches. These vulnerabilities go beyond external risks and also include internal obstacles such as staff awareness, training, and the ever-changing nature of cyber threats.

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

- **Current security protocols: Conventional Security Methods**

Historically, conventional security methods like firewalls, antivirus software, and access controls have played a crucial role in ensuring healthcare security. Although these measures offered some degree of protection, they frequently failed to adequately address the intricacies of contemporary cyber threats. Understanding the need for a shift towards adaptive and proactive solutions requires recognizing the limitations of traditional security mechanisms[4].

1.2.Advanced technologies in healthcare security

- **Artificial Intelligence and Machine Learning :** The emergence of Artificial Intelligence (AI) and Machine Learning (ML) brings about a fundamental change in healthcare security. Artificial intelligence algorithms have the capability to analyze large amounts of data, identify irregularities, and forecast possible security breaches in real-time. This integration not only improves the ability to identify potential dangers, but also enables healthcare systems to react quickly to emerging difficulties, guaranteeing a proactive approach to dealing with evolving threats[5], [6].
- **Blockchain technology:** The decentralized and immutable nature of blockchain technology is utilized to ensure the security of healthcare data. Blockchain guarantees the integrity and traceability of medical records by establishing a tamper-resistant ledger of transactions. In addition to ensuring data security, blockchain has the potential to improve data interoperability and promote trust within healthcare ecosystems[7], [8].
- **Internet of Things (IoT) in the healthcare industry:** The widespread adoption of Internet of Things (IoT) devices in healthcare creates multiple vulnerabilities that can be exploited by security threats. Nevertheless, when effectively controlled, IoT can enhance real-time surveillance of patients, optimize healthcare provision, and streamline data administration. Ensuring the optimal utilization of IoT in healthcare requires a careful equilibrium between innovation and security[9]–[11].
- **Enhancing Healthcare Data Security through Cloud Computing:** Cloud computing provides scalable and adaptable solutions for the storage and processing of healthcare data. Nevertheless, significant apprehensions regarding the protection and confidentiality of data persist. It is crucial to thoroughly examine the intricate execution of cloud solutions specifically designed for healthcare requirements in order to minimize risks and maximize the advantages of cloud computing, all while ensuring the privacy and security of healthcare data[12].

1.3.Constraints and deficiencies

Comprehending the limitations of advanced technologies is vital, despite their significant potential. Important factors that require careful handling include ethical considerations, potential biases in AI algorithms, and challenges in integrating diverse technologies with interoperability. Recognizing these constraints is crucial to guaranteeing a comprehensive and morally sound integration of cutting-edge technologies in healthcare security[13].

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

The complex difficulties in ensuring the security of social medical public healthcare systems arise from the interrelated and data-driven characteristics of these networks. The escalating complexity of cyber threats, combined with the vast amount of patient data, results in an intricate security environment. Recognizing and comprehending these obstacles is fundamental for devising efficient and enduring security strategies customized to the distinct circumstances of social medical public healthcare.

The Importance of Utilizing Advanced Technologies to Strengthen Resilience given the inherent constraints of conventional security methods, it is imperative to adopt cutting-edge technologies to bolster the durability of social medical public healthcare systems. This entails a deliberate amalgamation of artificial intelligence, blockchain, Internet of Things (IoT), and cloud computing to strengthen security protocols. Adopting these technologies is not just a reaction to current challenges, but a proactive measure to strengthen healthcare security for the future.

1.4. The research aims to achieve the following objectives

- To evaluate the present security situation in the public healthcare sector of social media. The research aims to thoroughly evaluate the current security situation in the field of social medical public healthcare. This entails a comprehensive examination of existing vulnerabilities, strengths, and weaknesses within healthcare security frameworks, establishing the basis for well-informed enhancements.
- The main goal is to identify and assess cutting-edge technologies that have the potential to improve the resilience of social medical public healthcare systems. This entails a detailed examination of the uses, advantages, and difficulties linked to the integration of AI, blockchain, IoT, and cloud computing. The research aims to offer practical insights for healthcare stakeholders to strategically adopt advanced technologies in a way that optimizes their influence on healthcare resilience.

To summarize, the introduction establishes the context for a thorough examination of the complex interplay between healthcare security and advanced technologies. By basing the research on the current status of public healthcare, highlighting the significance of security, and outlining the existing measures and technological advancements, a solid foundation is established for a thorough and enlightening examination of next-generation security in the healthcare industry.

2. Literature review

Amidst the convergence of technological progress and the complexities of healthcare systems, it is crucial to prioritize enhancing the security of social medical public healthcare. This literature review explores a collection of academic works, each providing distinct perspectives on the incorporation of advanced technologies for enhancing security in healthcare. The chosen papers collectively explore the intricacies of safeguarding healthcare ecosystems in an increasingly digitalized landscape, covering topics such as artificial intelligence (AI), blockchain, the Internet of Things (IoT), and cognitive computing.

The healthcare industry, propelled by the swift implementation of digital solutions, confronts unparalleled difficulties in protecting patient data, guaranteeing confidentiality, and reducing cyber risks. In this context, the literature analyzed here provides insights into novel methods and solutions that utilize the potential

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

of cutting-edge technologies. These studies encompass a wide range of strategies to strengthen healthcare security, including detecting cybersecurity attacks in IoT and exploring the synergy between AI and blockchain.

M. Abdullahi et al.[14] investigates the utilization of artificial intelligence (AI) techniques for identifying cybersecurity attacks in the Internet of Things (IoT). Abdullahi and his team conduct a thorough analysis of current research in this field, offering valuable observations on the changing state of IoT security. The review highlights the significance of AI in improving the ability to identify and respond to threats in IoT ecosystems, thereby adding to our understanding of how to strengthen cybersecurity in this interconnected model.

H. Abie[15] explores the convergence of cognitive cybersecurity and healthcare ecosystems facilitated by Cyber-Physical Systems (CPS) and Internet of Things (IoT). The paper discusses the specific difficulties presented by the combination of CPS-IoT in healthcare, with a focus on the necessity of implementing cognitive cybersecurity measures. The findings enhance our comprehension of safeguarding healthcare systems amidst advancing technologies, thereby facilitating the development of robust and intelligent cybersecurity strategies.

Alabdulatif et al.[16] specifically examine the security consequences that arise from the integration of blockchain and AI in smart healthcare applications. The paper assesses the efficacy of these technologies in strengthening healthcare security through an application-based analysis. The findings provide valuable insights into the practical implementation of blockchain and AI for improved security in the ever-changing field of smart healthcare.

Alshehri[17] focuses on the collaboration between blockchain and AI to enhance cybersecurity in medical IoT (Internet of Things) settings. The study investigates how these technologies can collectively improve the security stance of internet-connected medical devices. The study offers a thorough analysis of the possible uses and advantages, elucidating the practical integration of blockchain technology in enhancing cybersecurity.

Chakraborty et al.[18] presents a sophisticated AI-driven healthcare cybersecurity system that utilizes multi-source transfer learning techniques. The paper explores the intricacies of using transfer learning to improve the efficiency of AI in healthcare cybersecurity. The research enhances the advancement of intelligent systems that can adapt and learn from various data sources to reinforce cybersecurity in healthcare.

Ghazal's[19] investigation centers on the interdependence of Internet of Things (IoT) and Artificial Intelligence (AI) in the domain of healthcare security. The study explores how the combination of these technologies can be utilized to tackle security challenges that are specific to the healthcare field. The study offers valuable insights into securing healthcare ecosystems in the era of digital transformation by highlighting the interdependence of IoT devices and the intelligence of AI.

Gopalan et al.[20] perform an extensive examination of the security of Internet of Things (IoT) in the healthcare sector, specifically emphasizing the involvement of Artificial Intelligence (AI). The survey consolidates current knowledge, emphasizing significant patterns, difficulties, and resolutions in safeguarding healthcare IoT environments through the utilization of AI technologies. The findings provide a valuable resource for comprehending the present situation and identifying potential paths for future research and development.

Muheidat et al.[21] investigate the utilization of artificial intelligence and blockchain

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

technology in the field of cybersecurity. The paper thoroughly investigates the potential for these technologies to combine and strengthen cyber defenses in different applications. The research enhances the comprehension of how the combined influence of AI and blockchain strengthens cybersecurity measures by offering a comprehensive overview.

Prawiyogi et al.[22] explore the field of Cyber-Physical Systems (CPS) and IoT-enabled healthcare ecosystems, emphasizing the importance of incorporating cognitive cybersecurity measures. The paper highlights the significance of integrating cognitive elements into cybersecurity strategies to tackle the complexities of CPS-IoT in the healthcare sector. The discoveries establish a basis for implementing comprehensive cybersecurity strategies that consider the cognitive elements of emerging technologies.

Rajawat et al.[23] examine the convergence of artificial intelligence (AI) and blockchain technology to enhance the security of healthcare data in smart cities. The paper explores how these technologies can collectively tackle the distinct challenges presented by healthcare data security in urban settings. The findings enhance the ongoing discussion on safeguarding healthcare data in the context of smart city infrastructure.

The literature review conducted by Sreedevi et al.[24] offers a thorough examination of how cognitive computing is applied in various domains such as healthcare, cybersecurity, big data, and IoT. The paper provides a comprehensive overview of the latest advancements, challenges, and potential future directions in the integration of cognitive computing in these domains, based on a synthesis of existing literature. The review is an invaluable resource for researchers and practitioners who are seeking a comprehensive understanding of the various applications of cognitive computing.

Thomasian et al.[25] explore the cybersecurity obstacles that are unique to the Internet of Medical Things (IoMT). The paper examines the distinct factors involved in ensuring the security of internet-connected medical devices, highlighting the significance of strong cybersecurity measures in the healthcare sector. The findings enhance the ongoing discussion regarding the security of medical devices and patient data in the era of the Internet of Medical Things (IoMT).

Wylde et al.[26] provide a thorough analysis that specifically examines the interaction among cybersecurity, data privacy, and blockchain technology. The paper rigorously analyzes the potential benefits and obstacles of utilizing blockchain technology to improve cybersecurity and safeguard data privacy. The review offers valuable insights into the changing landscape of secure and privacy-preserving technologies by providing a comprehensive viewpoint.

The literature surveyed offers valuable insights and highlights the ever-changing nature of the healthcare security landscape. Continual innovation and adaptation are necessary due to ongoing challenges such as data breaches, ransomware threats, and ethical considerations. As the healthcare industry progresses, it is imperative for its security strategies to adapt accordingly. The amalgamation of these academic publications propels us towards a future in which healthcare security is not just a defensive measure, but a vital part of a robust and patient-focused healthcare system. The interdisciplinary nature of these studies, which encompass computer science, healthcare, and policy, emphasizes the need for collaborative endeavors to navigate the complex terrain of healthcare security in the digital era. The insights derived from this literature review provide guidance for researchers, practitioners, and policymakers as they navigate the intricate challenges of social medical public healthcare

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

security. These insights point towards a future where advanced technologies are used wisely to guarantee the trust, confidentiality, and resilience of healthcare systems..

3. Security Challenges in Social Medical Public Healthcare

3.1.Cybersecurity Threats

- **Data Breaches and Cyber Attacks:** The persistent threat of data breaches and cyber-attacks poses a significant challenge to the security of social medical public healthcare systems. The vast repositories of sensitive patient information make healthcare organizations lucrative targets for cybercriminals. Data breaches not only compromise the confidentiality of patient records but also expose individuals to identity theft, financial fraud, and other malicious activities. The healthcare sector's reliance on interconnected networks and digital platforms amplifies the risk, demanding robust cybersecurity measures to thwart unauthorized access and protect the integrity of healthcare data.
- **Ransomware Threats in Healthcare:** Ransomware poses a particularly insidious threat to social medical public healthcare systems. These malicious attacks involve encrypting critical healthcare data, rendering it inaccessible until a ransom is paid. The potential consequences of ransomware attacks in healthcare are severe, ranging from disrupted patient care and compromised medical records to financial losses and damage to the reputation of healthcare institutions. The sophisticated nature of ransomware requires continuous vigilance, proactive cybersecurity measures, and resilient backup systems to mitigate the impact of potential attacks.

3.2.Privacy Concerns

- **Patient Data Confidentiality**: Ensuring the confidentiality of patient data is a paramount concern in social medical public healthcare. The sensitive nature of health information demands stringent privacy safeguards to protect individuals' rights and maintain trust in healthcare systems. Unauthorized access to patient records, whether intentional or accidental, can have far-reaching consequences, including breaches of doctor-patient confidentiality, identity theft, and compromised healthcare decisions. The challenge lies in balancing the need for accessibility to patient data for medical purposes with robust security measures that safeguard against unauthorized disclosures.
- **Ethical Considerations in Healthcare Security**: The ethical considerations surrounding healthcare security further complicate the landscape. Striking the right balance between protecting patient privacy and enabling necessary data access for medical professionals requires careful navigation. Ethical challenges may arise in the deployment of advanced technologies, such as AI and biometric security, raising questions about consent, transparency, and potential biases. Balancing the ethical dimensions of healthcare security involves continuous scrutiny of practices, policies, and technologies to ensure that patient rights are upheld while also meeting the evolving needs of healthcare delivery.

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

Table 1 Summarized description with potential impact and Mitigation strategies

Category	Subcategory	Specific Challenge	Potential Impact	Mitigation Strategies
Cybersecurity Threats	Data breaches and cyber attacks	Unauthorized access, theft, or manipulation of sensitive health data	Loss of patient privacy, financial losses, operational disruptions, reputational damage	- Implement robust cybersecurity measures (firewalls, intrusion detection, data encryption) - Regularly update software and systems
	Ransomware threats in healthcare	Encryption of critical healthcare systems and data, demanding ransom payments to restore access	Patient care delays, potential loss of life, financial losses, data corruption	- Implement secure backups and disaster recovery plans - Regularly test backups and recovery procedures
Privacy Concerns	Patient data confidentiality	Unauthorized access, sharing, or use of patient data	Violation of patient privacy rights, discrimination, identity theft, reputational damage	- Implement privacy-by-design principles in all healthcare systems - Implement de-identification and anonymization techniques - Utilize privacy-preserving technologies like blockchain
	Ethical considerations in healthcare security	Balancing the need for secure data storage and accessibility with patient privacy and autonomy	Potential ethical dilemmas involving data sharing, use for research or other purposes, profiling, and discrimination	- Develop clear ethical guidelines for healthcare data management and use - Foster open communication and transparency with patients about their data

In conclusion, the security challenges in social medical public healthcare are multifaceted and dynamic. The threat landscape is characterized by persistent cybersecurity risks, including data breaches and ransomware attacks, which demand continuous vigilance and adaptive security measures. Privacy concerns, particularly regarding patient data confidentiality and ethical considerations, add complexity to the security discourse. Addressing these challenges requires a holistic approach that integrates robust cybersecurity protocols, ethical frameworks, and privacy-enhancing technologies to fortify the resilience of social medical public healthcare systems against the evolving threats in the digital era.

4. Leveraging Advanced Technologies for Healthcare Resilience

4.1. Artificial Intelligence and Machine Learning

- Predictive Analytics for Healthcare Security: Artificial Intelligence (AI) and Machine Learning (ML) are crucial in predictive analytics for healthcare security. These technologies utilize

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

algorithms to examine past data, detect patterns, and forecast potential security risks. Within the realm of healthcare resilience, the utilization of predictive analytics can forecast potential risks, allowing for proactive actions to protect patient data and maintain the reliability of healthcare systems. Through analyzing past cyber incidents, artificial intelligence (AI) enables the development of predictive models that improve the overall security of healthcare environments.

- AI-Driven Threat Detection and Response : Artificial Intelligence-Powered Detection and Response to Security Threats. The implementation of AI-powered threat detection and response mechanisms greatly enhances the resilience of healthcare security. Machine learning algorithms have the capability to consistently observe network activities and detect any abnormalities that could potentially signify a security breach. The implementation of this real-time threat detection system enables prompt response measures, thereby reducing the consequences of potential security incidents. Moreover, AI facilitates the implementation of automated reactions to familiar dangers, diminishing the need for human involvement and improving the effectiveness of healthcare security operations.

Table 2 Major work related in the field of AI and healthcare

Author	Key Focus	Methodology	Key Findings	Limitations
Assiri[27]	Facial emotion recognition using thermal images and machine learning	Proposed a novel method using active regions, CNNs, and parallelism to achieve 96.87% accuracy in facial emotion recognition on thermal images.	Limited dataset; lack of comparison with other approaches using thermal images.	Explore the use of thermal images for emotion recognition in other domains.
Xia et al.[28]	Diagnosis of Alzheimer's disease using EEG signals and deep learning	Developed a deep pyramid CNN model to achieve 92.12% accuracy in classifying Alzheimer's disease patients from healthy controls using EEG signals.	Requires large datasets and high-quality EEG recordings; real-world implementation challenges.	Investigate the use of EEG for monitoring disease progression and treatment response.
Elhoseny et al.[29]	Medical image security in the Internet of Things	Proposed a hybrid optimization algorithm with cryptography to protect medical images during transmission in IoT environments.	Improved security and reduced computational cost compared to existing methods.	Explore the integration of AI with blockchain technology for enhanced security in healthcare data sharing.

Khan et al.[30]	Breast cancer detection and classification using deep learning and transfer learning	Developed a deep learning framework using transfer learning to achieve 94.5% accuracy in detecting and classifying breast cancer from mammograms.	Requires large datasets and access to specialized medical equipment.	Investigate the use of deep learning for early detection and personalized treatment of breast cancer.
Akter et al.[31]	Chronic kidney disease (CKD) prediction using deep learning	Developed a hybrid deep learning model for accurate and real-time prediction of CKD stages from clinical data.	Achieved high accuracy and computational efficiency, but requires further validation on large clinical datasets.	Develop clinical decision support systems for personalized CKD management and early intervention.
Reddy et al.[32]	Diabetic retinopathy and diabetic macular edema (DR-DME) classification using deep learning	Proposed a modified grey-wolf optimizer with deep learning CNNs to achieve 95.23% accuracy in DR-DME classification from retinal images.	Improved accuracy compared to existing methods, but requires further validation on diverse datasets.	Develop AI-powered tools for automated screening and early detection of DR-DME to prevent vision loss.
Pattanayak et al.[33]	Machine learning algorithm optimization	Explored the use of GridSearchCV, cross-validation, and stacking for optimizing machine learning algorithms in various healthcare applications.	Demonstrated the effectiveness of different optimization techniques for improving model performance.	Investigate the application of advanced optimization methods like evolutionary algorithms for healthcare AI models.
Jayasudha et al.[34]	Heart disease detection using deep learning and hybrid optimization	Proposed a hybrid optimization-based ensemble classifier using deep learning to achieve 98.2% accuracy in heart disease detection from ECG signals.	Improved accuracy compared to existing methods, but requires further validation on large and diverse datasets.	Develop AI-powered tools for personalized risk assessment and early intervention for cardiovascular diseases.
Joudar et al.[35]	Autism spectrum disorder (ASD) diagnosis and management using AI	Reviewed the use of AI-based approaches for improving ASD diagnosis, triage, and prioritization.	Identified promising opportunities for AI in ASD care, but highlighted challenges related to data privacy, bias, and interpretability.	Develop responsible and ethical AI frameworks for ASD diagnosis and intervention, while addressing data privacy concerns.

4.2.Blockchain technology

- Ensuring the safety and protection of healthcare transactions and records: The utilization of blockchain technology brings forth a distributed and unalterable ledger, which is especially advantageous in safeguarding healthcare transactions and records. Every transaction is securely connected to the preceding one, forming an unchangeable chain. Within the healthcare sector, this guarantees the authenticity and reliability of patient records, prescriptions, and billing transactions. The transparency of blockchain technology reduces the possibility of unauthorized modifications to medical data, thereby promoting trust among stakeholders and patients.

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

- Enhancing Data Integrity and Transparency: In addition to ensuring the security of transactions, blockchain technology improves the reliability and openness of data in healthcare systems. The decentralized nature of blockchain guarantees that all authorized participants possess equal access to a consistent collection of immutable records. Patients have the ability to track the source and any changes made to their medical data, allowing for a clear and open understanding of their health information. This level of transparency not only cultivates confidence but also guarantees the precision and dependability of healthcare data.

Table 3 Major work related in the field of Blockchain and healthcare

Author(s)	Key Focus	Methodology	Key Findings
A. A. Siyal et al.[8]	Exploring potential applications of blockchain in healthcare	Literature review and analysis	- Secure data storage and patient record management - Supply chain tracking for pharmaceuticals - Improved data access and sharing
L. Ismail et al.[36]	Proposing a lightweight blockchain architecture for healthcare	Design and simulation of a new blockchain architecture	- Improved scalability and transaction processing speed compared to traditional blockchain - Reduced resource consumption and energy footprint
T. Kumar et al.[37]	Identifying key requirements and challenges for using blockchain in healthcare	Literature review and analysis of existing blockchain applications in healthcare	- Secure and efficient data management - Patient privacy and data protection - Regulatory compliance and interoperability
H. M. Hussien et al.[38]	Reviewing current trends and opportunities for using blockchain in healthcare	Literature review and analysis of recent research and development in blockchain healthcare applications	- Improved data security and transparency - Enhanced medication traceability and supply chain management - Increased efficiency and automation of healthcare processes
A. Farouk et al.[39]	Proposing a blockchain platform for industrial healthcare with a focus on data sharing and collaboration	Design and conceptualization of a new blockchain platform	- Improved security and transparency of data sharing between healthcare providers and manufacturers
P. Zhang et al.[40]	Overview of potential use cases for blockchain technology in healthcare	Literature review and analysis of existing and proposed applications	- Secure medical record management - Personalized medicine and precision healthcare - Supply chain tracking and counterfeit prevention

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

4.3.Internet of Things (IoT) in Healthcare

- Devices for Monitoring Healthcare Connectivity: The Internet of Things (IoT) enables the integration of numerous interconnected devices in healthcare to monitor patients in real-time. Wearable devices, intelligent sensors, and medical Internet of Things (IoT) devices gather valuable health data, facilitating proactive healthcare interventions. Continuous monitoring improves patient care and enhances healthcare resilience by facilitating early detection of health issues. Utilizing IoT devices for remote patient monitoring enhances the ability to promptly address emerging health issues.
- Security implications for Internet of Things (IoT) in the healthcare sector: The incorporation of IoT in healthcare presents security challenges that require careful attention. Healthcare Internet of Things (IoT) devices serve as vulnerable gateways for cyber threats. To ensure the resilience of healthcare systems, it is necessary to establish strong security measures for IoT devices, which include implementing encryption, secure communication channels, and regular software updates. Healthcare organizations can optimize the advantages of IoT technology while minimizing security vulnerabilities by taking into account these factors.

Table 4 Major work related in the field of IOT and healthcare

Author(s)	Key Focus	Methodology	Key Findings
J. Mishra et al.[41]	Predicting heart disease using ECG data collected through IoMT devices	Three-layer deep learning model with a meta-heuristic approach for feature selection	The proposed model achieved an accuracy of 95.2% in heart disease prediction.
M. M. Yaqoob et al.[42]	Heart disease diagnosis using federated learning on EHR data	Modified artificial bee colony algorithm for feature selection combined with federated learning	The proposed approach achieved an accuracy of 92.7% in heart disease diagnosis.
S. Bebortta et al.[43]	Predicting heart disease using EHR data collected through IoMT devices	Federated learning approach for privacy-preserving analysis of EHR data	The proposed model achieved an accuracy of 89.5% in heart disease prediction.
L. Rachakonda et al.[44]	Detecting stress levels using physiological data collected through IoMT devices	Deep neural network (DNN) integrated into an edge device for real-time stress detection	The proposed system achieved an accuracy of 87.2% in stress level detection.
K. Rezaee et al.[45]	Stress recognition in smart homes using data from multiple sensors	Fusion-based learning approach that combines data from various sensors in the smart home environment	The proposed framework achieved an accuracy of 93.1% in stress recognition.

4.4.Cloud Computing for Healthcare Data Security

- Secure Storage and Processing of Healthcare Data: Cloud computing offers scalable and secure solutions for storing and processing large quantities of healthcare data. Cloud platforms provide encryption mechanisms, access controls, and audit trails to protect sensitive patient information. Healthcare organizations can enhance data management resilience by utilizing cloud storage, which guarantees data availability, scalability, and redundancy.
- Cloud-Based Security Measures for Healthcare Systems: Cloud-based

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

security measures in healthcare encompass more than just data storage. Cloud service providers provide sophisticated security capabilities, including threat detection, intrusion prevention, and real-time monitoring. These measures improve the security of healthcare systems by implementing a centralized and proactive strategy to identify and address potential security threats. Furthermore, cloud solutions frequently incorporate inherent compliance features that cater to regulatory demands in healthcare data management.

Table 5 Major work related in the field of Cloud computing and healthcare

Author(s)	Key Focus	Methodology	Key Findings	Limitations
Casola et al.[46]	Challenges and opportunities of cloud computing for healthcare data	Review of existing literature	Cloud computing offers scalability, cost-effectiveness, and accessibility for healthcare data, but raises concerns about privacy, security, and regulatory compliance.	Lack of empirical research
Marwan et al.[12]	Improving security in healthcare clouds using machine learning	Proposed ML-based intrusion detection system for healthcare cloud environments	ML can enhance anomaly detection and threat prediction in healthcare clouds, but requires high-quality data and continuous model training.	Limited practical implementation and validation
Minh Dang et al.[47]	Integration of IoT and cloud computing for healthcare applications	Review of existing literature and case studies	IoT and cloud computing enable remote monitoring, real-time data analysis, and improved patient care, but raise concerns about interoperability, security vulnerabilities, and resource limitations.	Theoretical focus, limited empirical data
Altowaijri[48]	Secure architecture for healthcare cloud data storage and processing	Proposed architecture with multi-layered security mechanisms and access control protocols	Multi-layered approach provides robust security, but implementation complexity and potential performance overhead need further consideration.	Prototype implementation and performance evaluation
Daman et al.[49]	Security concerns associated with healthcare cloud adoption	Review of existing literature and case studies	Healthcare cloud environments face risks related to data breaches, unauthorized access, malware, and insider threats.	Emphasis on general security issues, not specific solutions

Conclusively, incorporating sophisticated technologies into healthcare resilience is a complex undertaking. The integration of Artificial Intelligence, Blockchain, Internet of Things, Biometric Security Solutions, and Cloud Computing strengthens the security measures in the healthcare industry. These technologies not only mitigate current vulnerabilities but also enable proactive and adaptable responses to emerging threats,

Submitted: 27-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

thereby ensuring the ongoing trust and safety of patients in the evolving healthcare system.

5. Conclusion

The incorporation of cutting-edge technologies represents a significant change in how security challenges are approached in the constantly changing field of social medical public healthcare. With the growing digitization of healthcare systems, it is crucial to strengthen their resilience against cyber threats and guarantee the confidentiality of patient information. This paper has examined the complex network of healthcare security, delving into its historical background, current strategies, and the transformative capabilities of advanced technologies.

The literature review has revealed the complex and diverse aspects of healthcare security, recognizing the shortcomings of conventional methods and emphasizing the importance of a proactive and flexible approach. The integration of Artificial Intelligence (AI), Blockchain, Internet of Things (IoT), Biometric Security Solutions, and Cloud Computing presents a potential opportunity to enhance the robustness of social medical public healthcare systems.

- Artificial Intelligence and Machine Learning revolutionize predictive analytics and threat detection. Through the utilization of algorithms to analyze extensive datasets, artificial intelligence (AI) improves the capacity to anticipate potential security risks, enabling proactive measures and swift responses to emerging challenges.
- Blockchain Technology provides a decentralized and tamper-resistant framework, ensuring the security of healthcare transactions and records. The inherent transparency of blockchain technology not only ensures the integrity of data, but also promotes trust among stakeholders, establishing a strong basis for the resilience of healthcare systems.
- The implementation of Internet of Things (IoT) in Healthcare involves the integration of interconnected devices that enable real-time monitoring, thereby transforming the delivery of patient care. Although the advantages are significant, it is crucial to carefully assess security measures in order to minimize potential risks and weaknesses related to the widespread use of IoT devices.
- Cloud Computing for Healthcare Data Security offers scalable and secure solutions for the storage and processing of data. Strategic implementation of cloud-based security measures enhances the overall resilience of healthcare systems by providing advanced threat detection and compliance features.

Nevertheless, these technological progressions are not devoid of obstacles. The paper has explored the complex network of security obstacles, encompassing cybersecurity risks like data breaches and ransomware attacks, as well as urgent privacy issues related to the confidentiality of patient data and the ethical considerations inherent in healthcare security.

When dealing with the intricate landscape of advanced security, it is essential to highlight the comprehensive aspect of resilience. In addition to the technological aspects, policy implications, legal considerations, and ethical dimensions are crucial factors that influence the effectiveness of advanced technologies in healthcare security. In order to ensure the responsible and fair implementation of these technologies, it is imperative for stakeholders to work together to establish regulatory frameworks, ethical guidelines, and comprehensive security protocols.

As we wrap up this investigation, it is clear that incorporating advanced technologies has great

potential for strengthening the resilience of social medical public healthcare. The path ahead entails a harmonious and cooperative strategy, where technology is in accordance with ethical standards, and innovation coexists with strong security protocols. This research provides guidance for healthcare stakeholders, policymakers, and technologists as they navigate the intricate field of healthcare security in the age of advanced technologies. It aims to lead them towards a future where cutting-edge security is synonymous with the ability of healthcare systems to withstand challenges.

References

[1] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, no. January, p. 103164, 2021, doi: 10.1016/j.jnca.2021.103164.

[2] M. M. Islam, S. Nooruddin, F. Karray, and G. Muhammad, "Multi-level feature fusion for multimodal human activity recognition in Internet of Healthcare Things," *Inf. Fusion*, vol. 94, no. August 2022, pp. 17–31, 2023, doi: 10.1016/j.inffus.2023.01.015.

[3] B. Kapoor, B. Nagpal, and M. Alharbi, "Secured healthcare monitoring for remote patient using energy-efficient IoT sensors," *Comput. Electr. Eng.*, vol. 106, no. October 2022, p. 108585, 2023, doi: 10.1016/j.compeleceng.2023.108585.

[4] A. Rejeb *et al.*, "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," *Internet of Things (Netherlands)*, vol. 22, no. February, p. 100721, 2023, doi: 10.1016/j.iot.2023.100721.

[5] 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.

[6] 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.

[7] A. I. Taloba *et al.*, "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare," *Alexandria Eng. J.*, vol. 65, pp. 263–274, 2023, doi: https://doi.org/10.1016/j.aej.2022.09.031.

[8] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, pp. 1–16, 2019, doi: 10.3390/cryptography3010003.

[9] A. Ukil, S. Bandyoapdhyay, C. Puri, and A. Pal, "IoT healthcare analytics: The importance of anomaly detection," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2016-May, pp. 994–997, 2016, doi: 10.1109/AINA.2016.158.

[10] S. A. Haque, M. Rahman, and S. M. Aziz, "Sensor anomaly detection in wireless sensor networks for healthcare," *Sensors (Switzerland)*, vol. 15, no. 4, pp. 8764–8786, 2015, doi: 10.3390/s150408764.

[11] M. Fahim and A. Sillitti, "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," *IEEE Access*, vol. 7, pp. 81664–81681, 2019, doi: 10.1109/ACCESS.2019.2921912.

[12] M. Marwan, A. Kartit, and H. Ouahmane, "Security Enhancement in Healthcare Cloud using Machine Learning," *Procedia Comput. Sci.*, vol. 127, pp. 388–397, 2018, doi: https://doi.org/10.1016/j.procs.2018.01.136.

[13] S. Bhattacharya and M. Pandey, "Issues and Challenges in Incorporating the Internet of Things with the Healthcare Sector," 2021, pp. 639–651.

[14] M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electron.*, vol. 11, no. 2, pp. 1–27, 2022, doi: 10.3390/electronics11020198.

[15] H. Abie, "Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, 2019, pp. 1–6, doi: 10.1109/ISMICT.2019.8743670.

[16] A. Alabdulatif, I. Khalil, and M. Saidur Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis," *Appl. Sci.*, vol. 12, no. 21, 2022, doi: 10.3390/app122111039.

[17] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," *Electron. Res. Arch.*, vol. 31, no. 2, pp. 708–728, 2023, doi: 10.3934/era.2023035.

[18] C. Chakraborty, S. M. Nagarajan, G. G. Devarajan, T. V Ramana, and R. Mohanty, "Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method," *ACM Trans. Sens. Networks*, 2023, doi: 10.1145/3597210.

[19] T. M. Ghazal, "Internet of Things with Artificial Intelligence for Health Care Security," *Arab. J. Sci. Eng.*, no. November, 2021, doi: 10.1007/s13369-021-06083-8.

[20] S. S. Gopalan, A. Raza, and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey," in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2021, pp. 1–6, doi: 10.1109/ICCSPA49915.2021.9385711.

[21] F. Muheidat and L. Tawalbeh, *Artificial Intelligence and Blockchain for Cybersecurity Applications*. Springer International Publishing, 2021.

[22] A. G. Prawiyogi and L. Meria, "For a CPS-IoT Enabled Healthcare Ecosystem Consider Cognitive Cybersecurity," vol. 2, no. 1, pp. 24–32, 2023.

[23] A. S. Rajawat, P. Bedi, S. B. Goyal, R. N. Shaw, A. Ghosh, and S. Aggarwal, *AI and Blockchain for Healthcare Data Security in Smart Cities*, vol. 1002. Springer Singapore, 2022.

[24] A. G. Sreedevi, T. Nitya Harshitha, V. Sugumaran, and P. Shankar, "Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review," *Inf. Process. Manag.*, vol. 59, no. 2, p. 102888, 2022, doi: https://doi.org/10.1016/j.ipm.2022.102888.

[25] N. M. Thomasian and E. Y. Adashi, "Cybersecurity in the Internet of Medical Things," *Heal. Policy Technol.*, vol. 10, no. 3, p. 100549, 2021, doi: https://doi.org/10.1016/j.hlpt.2021.100549.

[26] V. Wylde *et al.*, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Comput. Sci.*, vol. 3, no. 2, pp. 1–12, 2022, doi: 10.1007/s42979-022-01020-4.

[27] B. Assiri and M. A. Hossain, "Face emotion recognition based on infrared thermal imagery by applying machine learning and parallelism," *Math. Biosci. Eng.*, vol. 20, no. 1, pp. 913–929, 2023, doi: 10.3934/mbe.2023042.

[28] W. Xia, R. Zhang, X. Zhang, and M. Usman, "A novel method for diagnosing Alzheimer's disease using deep pyramid CNN based on EEG signals," *Heliyon*, vol. 9, no. 4, p. e14858, 2023, doi: 10.1016/j.heliyon.2023.e14858.

[29] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 10979–10993, 2020, doi: 10.1007/s00521-018-3801-x.

[30] S. U. Khan, N. Islam, Z. Jan, I. Ud Din, and J. J. P. C. Rodrigues, "A novel deep learning based framework for the detection and classification of breast cancer using transfer learning," *Pattern Recognit. Lett.*, vol. 125, pp. 1–6, 2019, doi: 10.1016/j.patrec.2019.03.022.

[31] S. Akter *et al.*, "CKD.Net: A novel deep learning hybrid model for effective, real-time, automated screening tool towards prediction of multi stages of CKD along with eGFR and creatinine," *Expert Syst. Appl.*, vol. 223, no. April 2022, p. 119851, 2023, doi: 10.1016/j.eswa.2023.119851.

[32] V. Purna Chandra Reddy and K. K. Gurrala, "Joint DR-DME classification using deep learning-CNN based modified grey-wolf optimizer with variable weights," *Biomed. Signal Process. Control*, vol. 73, no. July 2021, p. 103439, 2022, doi: 10.1016/j.bspc.2021.103439.

[33] S. Pattanayak and T. S. B, *on Machine Learning Algorithms Using GridSearchCV , Cross Validation and Stacked*. Springer International Publishing, 2022.

[34] R. Jayasudha, C. Suragali, J. T. Thirukrishna, and B. Santhosh Kumar, "Hybrid optimization enabled deep learning-based ensemble classification for heart disease detection,"

Signal, Image Video Process., vol. 17, no. 8, pp. 4235–4244, 2023, doi: 10.1007/s11760-023-02656-2.

[35] S. S. Joudar *et al.*, *Artificial intelligence-based approaches for improving the diagnosis, triage, and prioritization of autism spectrum disorder: a systematic review of current trends and open issues*, vol. 56, no. s1. Springer Netherlands, 2023.

[36] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight Blockchain for Healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019, doi: 10.1109/ACCESS.2019.2947613.

[37] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2018, pp. 1–7, doi: 10.1109/HealthCom.2018.8531136.

[38] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: Trends and opportunities," *J. Ind. Inf. Integr.*, vol. 22, p. 100217, 2021, doi: https://doi.org/10.1016/j.jii.2021.100217.

[39] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: Vision and future opportunities," *Comput. Commun.*, vol. 154, pp. 223–235, 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.058.

[40] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Chapter One - Blockchain Technology Use Cases in Healthcare," in *Blockchain Technology: Platforms, Tools and Use Cases*, vol. 111, P. Raj and G. C. B. T.-A. in C. Deka, Eds. Elsevier, 2018, pp. 1–41.

[41] J. Mishra and M. Tiwari, "IoT-enabled ECG-based heart disease prediction using three-layer deep learning and meta-heuristic approach," *Signal, Image Video Process.*, 2023, doi: 10.1007/s11760-023-02743-4.

[42] M. M. Yaqoob *et al.*, "Modified Artificial Bee Colony Based Feature Optimized Federated Learning for Heart Disease Diagnosis in Healthcare," *Appl. Sci.*, vol. 12, no. 23, 2022, doi: 10.3390/app122312080.

[43] S. Bebortta, S. S. Tripathy, S. Basheer, and C. L. Chowdhary, "FedEHR: A Federated Learning Approach towards the Prediction of Heart Diseases in IoT-Based Electronic Health Records," *Diagnostics*, vol. 13, no. 20, 2023, doi: 10.3390/diagnostics13203166.

[44] L. Rachakonda, S. P. Mohanty, E. Kougianos, and P. Sundaravadivel, "Stress-Lysis: A DNN-Integrated Edge Device for Stress Level Detection in the IoMT," *IEEE Trans. Consum. Electron.*, vol. 65, no. 4, pp. 474–483, 2019, doi: 10.1109/TCE.2019.2940472.

[45] K. Rezaee, X. Yang, M. R. Khosravi, R. Zhang, W. Lin, and G. Jeon, "Fusion-based learning for stress recognition in smart home: An IoMT framework," *Build. Environ.*, vol. 216, no. March, p. 108988, 2022, doi: 10.1016/j.buildenv.2022.108988.

[46] V. Casola, A. Castiglione, K.-K. R. Choo, and C. Esposito, "Healthcare-Related Data in the Cloud: Challenges and Opportunities," *IEEE Cloud Comput.*, vol. 3, no. 6, pp. 10–14, 2016, doi: 10.1109/MCC.2016.139.

[47] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electron.*, vol. 8, no. 7, pp. 1–49, 2019, doi: 10.3390/electronics8070768.

[48] S. M. Altowaijri, "An architecture to improve the security of cloud computing in the healthcare sector," *EAI/Springer Innov. Commun. Comput.*, pp. 249–266, 2020, doi: 10.1007/978-3-030-13705-2_10.

[49] R. Daman, M. M. Tripathi, and S. K. Mishra, "Security issues in cloud computing for healthcare," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 1231–1236.