iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60636

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Secure Cloud Services for the Healthcare Industry: Addressing Unique Challenges and Ensuring Compliance

Prajakta Sudhir Samant
Microsoft, USA

Abstract: ***The healthcare industry is increasingly adopting cloud computing to manage patient data, provide telehealth services, and support remote work. However, this adoption presents unique challenges due to stringent regulations governing the handling of personal health information (PHI), such as HIPAA in the United States and GDPR in the European Union. Non-compliance with these regulations can result in significant financial penalties, reputational damage, and loss of patient trust. This article explores the specific data security needs of the healthcare industry, the challenges in adopting cloud services, and the essential features of secure cloud services tailored for healthcare. It also discusses the integration of artificial intelligence (AI) and automation in cloud services to enhance data security and operational efficiency, as well as future trends in cloud computing for healthcare, such as the increasing adoption of AI and machine learning for predictive analytics and automated threat detection. By providing a comprehensive overview of the data security needs, challenges, and solutions in adopting cloud services for healthcare, this article aims to assist healthcare organizations in making informed decisions when considering the adoption of cloud services and to highlight the importance of prioritizing data security and compliance in the digital transformation of the healthcare industry.***

Keywords: ***Healthcare Cloud Computing, Data Security, HIPAA Compliance, Artificial Intelligence in Healthcare, Cloud Service Adoption***

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

I. INTRODUCTION

The healthcare industry has embraced cloud computing for managing patient data, enabling telehealth services, and facilitating remote work [1]. The global healthcare cloud computing market is expected to reach $64.7 billion by 2025 [2], driven by the adoption of electronic health records (EHRs) and the need for cost-effective, interoperable healthcare solutions [3]. A survey by the Healthcare Information and Management Systems Society (HIMSS) found that 83% of healthcare organizations are already using cloud services [4].

However, adopting cloud services in healthcare presents unique challenges due to stringent regulations like HIPAA in the U.S. and GDPR in the EU, which govern the handling of personal health information (PHI) [5, 6]. The $3 million fine levied against the University of Rochester Medical Center for HIPAA violations [7] is an example of how significant fines can result from non-compliance.

The average cost of a healthcare data breach in 2020 was $7.13 million [8], with the healthcare industry having the highest average time to identify and contain a breach at 329 days [8]. Data breaches can lead to reputational damage, loss of patient trust, and potential harm to patients' health and privacy [9].

To address these challenges, healthcare organizations must carefully evaluate cloud service providers, ensure they meet security and compliance requirements, implement strong access controls and encryption, and establish clear business associate agreements (BAAs) [10, 11, 12].

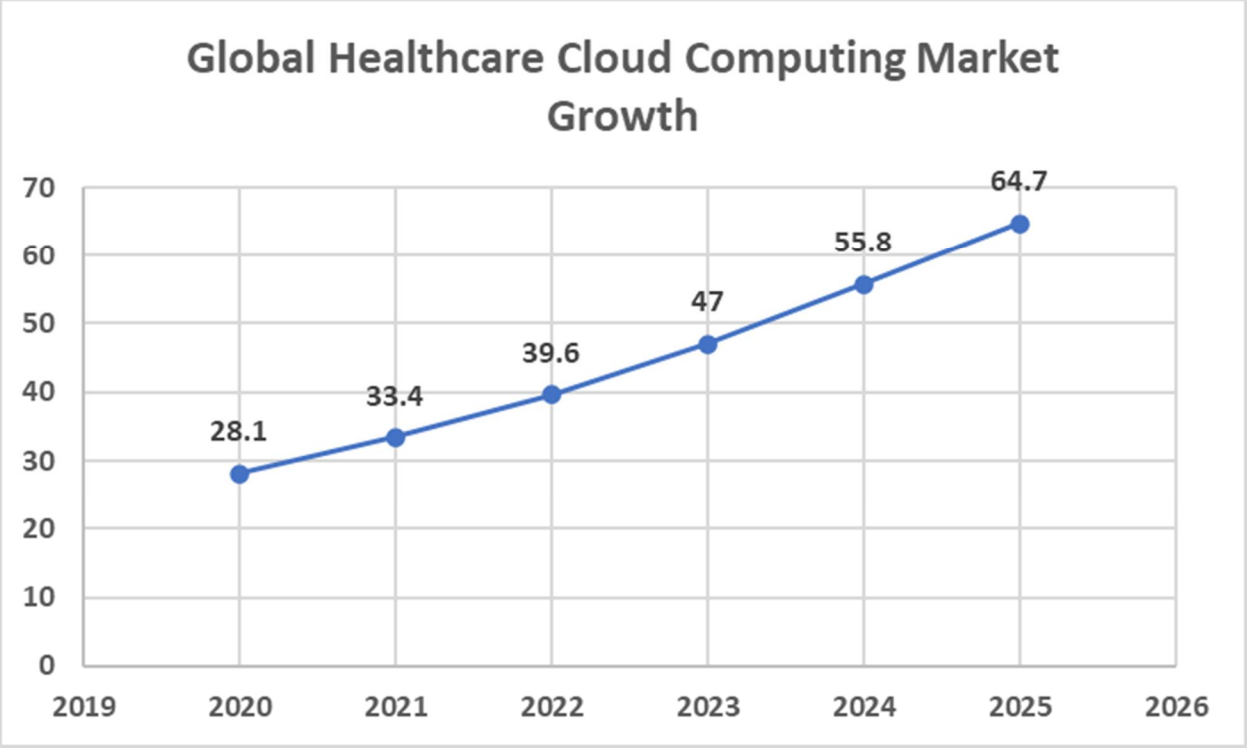


Fig. 1: Projected Growth of the Global Healthcare Cloud Computing Market (2020-2025)

II. THE UNIQUE DATA SECURITY NEEDS OF THE HEALTHCARE INDUSTRY

Healthcare providers must adhere to strict regulations like HIPAA in the U.S. and GDPR in the EU when handling, sharing, and protecting personal health information (PHI) [13, 18]. According to a survey by the Ponemon Institute, 54% of healthcare organizations have experienced a data breach involving PHI in the past two years [16]. This involves implementing robust security measures, conducting regular employee training, and ensuring compliance [14]. A HIMSS survey found that 82% of healthcare organizations provide regular security awareness training, with 79% conducting annual or more frequent training sessions [19].

PHI includes a wide range of sensitive data, such as patient identification information (e.g., name, address, social security number), medical records, billing information, and more [15]. A study by Verizon found that 58% of healthcare data breaches involved medical records, making it the most frequently compromised type of data in healthcare breaches [24]. Medical records are particularly valuable to cybercriminals, as they can be used for identity theft, fraud, and even blackmail [20].

Failing to protect PHI can result in severe consequences, including financial penalties, reputational damage, and potential harm to patients [16]. In 2020, the U.S. Department of Health and Human Services imposed $13.5 million in fines for HIPAA violations, with the largest single fine amounting to $6.85 million [21]. The average cost of a healthcare data breach in 2020 was $7.13 million, a 10% increase from the previous year [16]. The study also revealed that healthcare data breaches cost an average of $429 per compromised record, which is the highest among all industries [16].

Data protection regulations mandate encryption, access controls, audit trails, and breach notification protocols [17]. The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services, and, in some cases, the media, no later than 60 days following the discovery of a breach [22]. In contrast, the GDPR requires data controllers to notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach [23]. A survey by the Ponemon Institute found that 59% of healthcare organizations believe that compliance with data protection regulations is the most significant barrier to achieving a strong cybersecurity posture [25].

Barrier	Percentage of Organizations
Compliance with Data Protection Regulations	59%
Lack of Skilled Personnel	45%
Insufficient Budget	38%
Complexity of Security Solutions	27%

Table 1: Barriers to Achieving Strong Cybersecurity Posture in Healthcare

III. CHALLENGES IN ADOPTING CLOUD SERVICES FOR HEALTHCARE

1) *Data Security and Compliance:* Cloud service providers (CSPs) need to comply with healthcare regulations and address the need for end-to-end encryption, secure data storage, and controlled access [26]. According to a survey by the Cloud Security Alliance, 69% of healthcare organizations are concerned about data security and privacy when adopting cloud services [29]. CSPs must implement security measures such as encryption, access controls, and monitoring to protect PHI. For example, Amazon Web Services (AWS) offers a HIPAA-compliant cloud platform with built-in security features like encryption, access management, and auditing [30].
2) *Data Mobility and Portability:* Healthcare organizations must ensure the secure transfer of patient data across different jurisdictions, which may have varying data protection laws, while maintaining compliance [27]. A study by the European Union Agency for Cybersecurity (ENISA) found that 63% of healthcare organizations consider data portability a significant challenge when adopting cloud services [31]. CSPs should provide secure data migration tools and adhere to international data transfer agreements like the EU-US Privacy Shield and the Standard Contractual Clauses (SCCs) [32].
3) *Business Associate Agreements (BAAs):* BAAs between healthcare entities and CSPs delineate the responsibility for protecting PHI, ensuring both parties adhere to HIPAA and other regulations [28]. According to the U.S. Department of Health and Human Services, a BAA must include provisions for reporting breaches, ensuring the return or destruction of PHI upon termination of the agreement, and specifying the permitted uses and disclosures of PHI [33]. The $2.7 million settlement that Oregon Health & Science University paid in 2016 for not having a BAA with a cloud vendor serves as evidence that failing to establish a proper BAA can result in significant fines [34].

IV. SECURE CLOUD SERVICE FEATURES ESSENTIAL FOR HEALTHCARE

Cloud services provide suitable features for healthcare data, such as advanced encryption techniques, comprehensive access management systems, continuous security assessments, sophisticated threat detection mechanisms, and robust data backup and disaster recovery plans to ensure data integrity and availability [35]. A survey by the Cloud Security Alliance found that 91% of healthcare organizations reported using cloud services, with 65% stating that security is their top concern when adopting cloud technology [36]. For example, Microsoft Azure offers a HIPAA-compliant cloud platform with features like Azure Information Protection for data encryption, Azure Active Directory for access management, and Azure Security Center for continuous monitoring and threat detection [42].

The integration of AI and automation can help detect vulnerabilities and thwart runtime threats by proactively scanning for threats [37]. IBM Watson Health, for instance, leverages AI to analyze vast amounts of healthcare data and provide insights for improving patient care while ensuring data security and compliance [43]. A case study by IBM found that the use of Watson Health helped a large healthcare organization reduce security incidents by 60% and improve threat detection time by 50% [44]. Such enhanced data security and operational efficiency lead to improved patient care.

The shared responsibility model in cloud computing clarifies the security aspects managed by the CSP and those that fall under the healthcare provider's purview [38]. CSPs are typically responsible for securing the cloud infrastructure, while healthcare organizations are responsible for securing their applications, data, and access management [45]. A clear understanding of this model helps healthcare organizations allocate resources effectively and ensure a comprehensive security strategy.

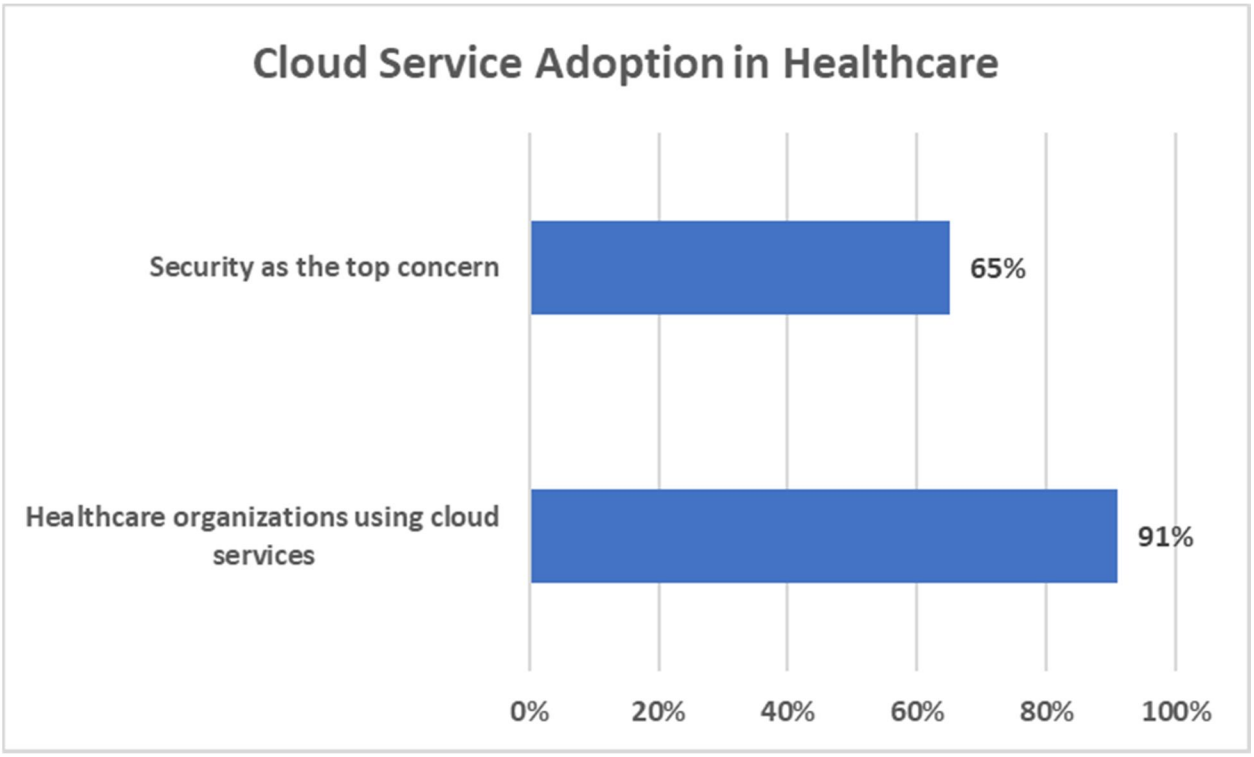


Fig. 2: Cloud Service Adoption and Security Concerns in Healthcare Organizations

V. FUTURE TRENDS IN CLOUD COMPUTING FOR HEALTHCARE

Emerging trends, such as the integration of AI and machine learning for predictive analytics and automated threat detection, will further help secure healthcare PHI [39]. A study by Frost & Sullivan estimates that the global market for AI in healthcare will reach $6.6 billion by 2021, growing at a CAGR of 40.7% from 2016 to 2021 [47]. The use of AI in healthcare has the potential to improve patient outcomes, reduce costs, and enhance data security by enabling real-time analysis of vast amounts of healthcare data and identifying potential security threats [50].

A report by MarketsandMarkets predicts that the healthcare cloud computing market will reach $64.7 billion by 2025, growing at a CAGR of 18.7% from 2020 to 2025 [40]. Big data analytics' rising popularity, the need for affordable healthcare solutions, and the rising demand for interoperable and collaborative healthcare systems are just a few of the factors that will drive this growth [46]. For instance, a case study by Amazon Web Services (AWS) demonstrated how a large healthcare provider in the United States leveraged AWS cloud services to process and analyze over 80 million patient records, resulting in a 60% reduction in data processing time and a 50% reduction in costs [51].

Technological advancements could further enhance data security and compliance in the cloud, revolutionizing the way healthcare organizations approach data protection [41]. The use of homomorphic encryption, for example, could enable healthcare providers to perform computations on encrypted data without decrypting it, thereby ensuring the privacy and security of sensitive healthcare information [52]. A proof-of-concept study by Microsoft Research demonstrated the feasibility of using homomorphic encryption to securely analyze genomic data in the cloud [53].

Another promising technology is blockchain, which could provide a secure and transparent way to manage PHI, enabling secure data sharing among healthcare providers and researchers [47]. A survey by IBM found that 56% of healthcare executives are actively exploring the use of blockchain in their organizations [54]. A pilot study by the MIT Media Lab and Beth Israel Deaconess Medical Center demonstrated the potential of using blockchain to securely store and manage patient consent for data sharing [48]. The study used the MedRec prototype, a decentralized record management system that leverages blockchain technology to manage authentication, confidentiality, accountability, and data sharing [55].

Year	Market Size (in billion $)	CAGR (2016-2021)
2016	0.6	40.7%
2017	0.9	40.7%
2018	1.3	40.7%
2019	1.9	40.7%
2020	2.8	40.7%
2021	6.6	40.7%

Table 2: Global Market for AI in Healthcare

VI. CONCLUSION

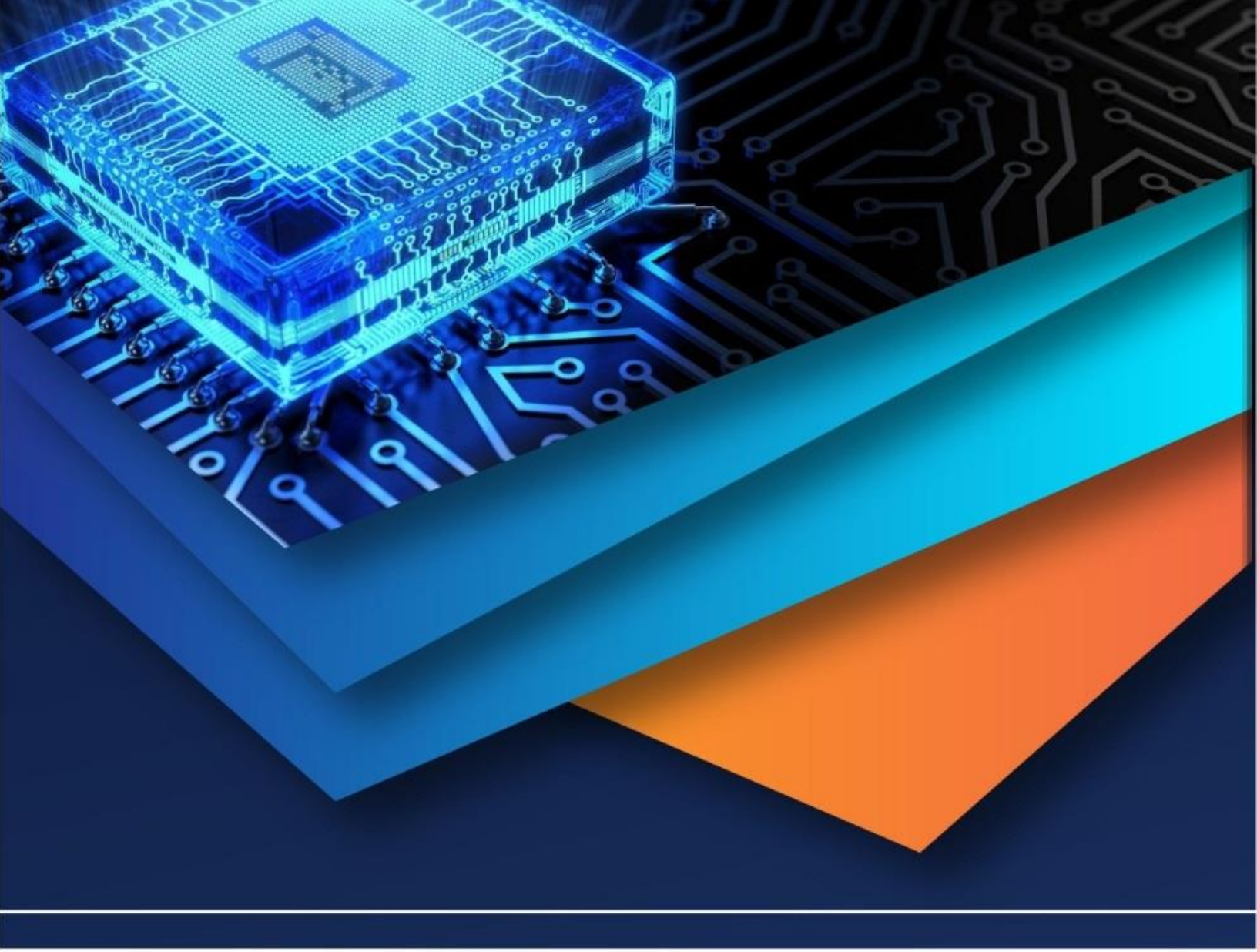
The adoption of secure cloud services is crucial for healthcare organizations to manage patient data, provide telehealth services, and support remote work effectively. To address the unique data security needs of the healthcare industry and ensure compliance with regulations such as HIPAA and GDPR, healthcare organizations must carefully evaluate cloud service providers and implement secure cloud services that offer advanced encryption, comprehensive access management, continuous security assessments, sophisticated threat detection, and robust data backup and disaster recovery plans. By leveraging the power of AI and automation in cloud services and staying informed about emerging trends, such as the increasing adoption of AI and machine learning for predictive analytics, the growing healthcare cloud computing market, and the potential of blockchain technology for secure data sharing, healthcare organizations can enhance data security, improve operational efficiency, and ultimately deliver high-quality patient care in the digital era.

REFERENCES

[1] Mathew and C. S. R. Prabhu, IEEE Access, vol. 8, pp. 150381-150400, 2020, doi: 10.1109/ACCESS.2020.3015957.
[2] MarketsandMarkets, "Healthcare Cloud Computing Market," 2020. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-computing-healthcare-market-347.html
[3] J. G. Anderson, Journal of Healthcare Engineering, vol. 2019, pp. 1-5, 2019, doi: 10.1155/2019/7983685.
[4] Healthcare Information and Management Systems Society (HIMSS), "2019 HIMSS U.S. Leadership and Workforce Survey," 2019. Available: https://www.himss.org/resources/himss-leadership-and-workforce-survey
[5] U.S. Department of Health & Human Services, "Summary of the HIPAA Security Rule," 2013. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[6] European Commission, "General Data Protection Regulation (GDPR)," 2018. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[7] U.S. Department of Health & Human Services, "University of Rochester Medical Center (URMC) Resolution Agreement," 2019. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html
[8] Ponemon Institute, "Cost of a Data Breach Report 2020," IBM Security, 2020. Available: https://www.ibm.com/security/data-breach
[9] M. A. Sahi et al., IEEE Access, vol. 6, pp. 464-478, 2018, doi: 10.1109/ACCESS.2017.2767561.
[10] S. Chenthara et al., IEEE Access, vol. 7, pp. 74361-74382, 2019, doi: 10.1109/ACCESS.2019.2919982.
[11] G. Manogaran et al., in Cybersecurity for Industry 4.0, 2017, pp. 103-126, doi: 10.1007/978-3-319-50660-9_5.
[12] K. Haufe et al., Scientific World Journal, vol. 2014, pp. 1-7, 2014, doi: 10.1155/2014/146970.
[13] C. S. Kruse et al., Technology and Health Care, vol. 25, no. 1, pp. 1-10, 2017, doi: 10.3233/THC-161263.
[14] D. Bogataj Jančič et al., Journal of Medical Systems, vol. 44, no. 1, 2020, doi: 10.1007/s10916-019-1485-0.
[15] M. A. Sahi et al., IEEE Access, vol. 6, pp. 464-478, 2018, doi: 10.1109/ACCESS.2017.2767561.
[16] Ponemon Institute, "Cost of a Data Breach Report 2020," IBM Security, 2020. Available: https://www.ibm.com/security/data-breach

[17] A. Youssef, International Journal of Computer Applications, vol. 159, no. 4, pp. 17-22, 2017, doi: 10.5120/ijca2017913188.
[18] European Commission, "General Data Protection Regulation (GDPR)," 2018. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[19] Healthcare Information and Management Systems Society (HIMSS), "2019 HIMSS Cybersecurity Survey," 2019. Available: https://www.himss.org/2019-himss-cybersecurity-survey
[20] Ponemon Institute, "2019 Cost of a Data Breach Report," IBM Security, 2019. Available: https://www.ibm.com/downloads/cas/ZBZLY7KL
[21] U.S. Department of Health & Human Services, "OCR Enforcement Highlights," 2021. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
[22] U.S. Department of Health & Human Services, "Breach Notification Rule," 2013. Available: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[23] European Commission, "Personal data breach notifications," 2021. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/personal-data-breach-notifications_en
[24] Verizon, "2020 Data Breach Investigations Report," Verizon, 2020. Available: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
[25] Ponemon Institute, "The State of Cybersecurity in Healthcare Organizations in 2020," Ponemon Institute, 2020. Available: https://www.ponemon.org/research/ponemon-library/security/the-state-of-cybersecurity-in-healthcare-organizations-in-2020.html
[26] S. Nepal, R. Ranjan, and K.-K. R. Choo, "Trustworthy Processing of Healthcare Big Data in Hybrid Clouds," IEEE Cloud Computing, vol. 2, no. 2, pp. 78-84, 2015, doi: 10.1109/MCC.2015.36.
[27] Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," Journal of Information Security and Applications, vol. 19, no. 1, pp. 45-60, 2014, doi: 10.1016/j.jisa.2014.04.003.
[28] K. Haufe, R. Dzombeta, and K. Brandis, "Proposal for a Security Management in Cloud Computing for Health Care," Scientific World Journal, vol. 2014, pp. 1-7, 2014, doi: 10.1155/2014/146970.
[29] Cloud Security Alliance, "Cloud Adoption in the Healthcare Sector," Cloud Security Alliance, 2021. Available: https://cloudsecurityalliance.org/artifacts/cloud-adoption-in-the-healthcare-sector/
[30] Amazon Web Services, "AWS HIPAA Compliance," AWS, 2021. Available: https://aws.amazon.com/compliance/hipaa-compliance/
[31] European Union Agency for Cybersecurity (ENISA), "Cloud Computing: Benefits, Risks and Recommendations for Information Security," ENISA, 2012. Available: https://www.enisa.europa.eu/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security
[32] European Commission, "EU-US Privacy Shield," European Commission, 2021. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en
[33] U.S. Department of Health & Human Services, "Business Associate Contracts," HHS.gov, 2017. Available: https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
[34] U.S. Department of Health & Human Services, "Oregon Health & Science University (OHSU) Resolution Agreement," HHS.gov, 2016. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ohsu/index.html
[35] 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.
[36] Cloud Security Alliance, "Cloud Adoption in the Healthcare Sector," Cloud Security Alliance, 2020. Available: https://cloudsecurityalliance.org/artifacts/cloud-adoption-in-the-healthcare-sector/
[37] G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, "Big Data Security Intelligence for Healthcare Industry 4.0," in Cybersecurity for Industry 4.0, 2017, pp. 103-126, doi: 10.1007/978-3-319-50660-9_5.
[38] A. A. Ali and R. Mohan, "Importance of Cloud Computing in Healthcare Industry," in Advances in Intelligent Systems and Computing, 2020, pp. 1097-1107, doi: 10.1007/978-3-030-32150-5_102.
[39] A. Esteva et al., "A guide to deep learning in healthcare," Nature Medicine, vol. 25, no. 1, pp. 24-29, 2019, doi: 10.1038/s41591-018-0316-z.
[40] MarketsandMarkets, "Healthcare Cloud Computing Market," MarketsandMarkets, 2020. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-computing-healthcare-market-347.html
[41] C. Wang, Y. Zhang, and X. Chen, "A Survey on Cloud-Assisted e-Health: From the Perspective of Security and Privacy Challenges," IEEE Access, vol. 7, pp. 181066-181082, 2019, doi: 10.1109/ACCESS.2019.2958956.
[42] Microsoft Azure, "HIPAA Compliance in Azure," Microsoft, 2021. Available: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/hipaa/
[43] IBM Watson Health, "IBM Watson Health," IBM, 2021. Available: https://www.ibm.com/watson-health
[44] IBM, "Advancing Healthcare with AI: Improving Patient Safety and Reducing Costs," IBM, 2019. Available: https://www.ibm.com/downloads/cas/WXBGNX8P
[45] Amazon Web Services, "Shared Responsibility Model," AWS, 2021. Available: https://aws.amazon.com/compliance/shared-responsibility-model/
[46] J. G. Anderson, "The Future of Cloud Computing in Healthcare," Journal of Healthcare Engineering, vol. 2019, pp. 1-5, 2019, doi: 10.1155/2019/7983685.
[47] M. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here," in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016, pp. 1-3, doi: 10.1109/HealthCom.2016.7749510.
[48] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.
[49] Frost & Sullivan, "Transforming Healthcare with Artificial Intelligence," Frost & Sullivan, 2018. Available: https://store.frost.com/transforming-healthcare-with-artificial-intelligence.html
[50] Y. Dai, S. Jia, and L. Luo, "A Survey on Artificial Intelligence in Healthcare," in 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 2969-2973, doi: 10.1109/BigData47090.2019.9006123.
[51] Amazon Web Services, "Large Healthcare Provider Uses AWS to Improve Patient Care," AWS, 2020. Available: https://aws.amazon.com/solutions/case-studies/large-healthcare-provider/

[52] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," ACM Computing Surveys, vol. 51, no. 4, pp. 1-35, 2018, doi: 10.1145/3214303.
[53] K. Lauter, A. López-Alt, and M. Naehrig, "Private Computation on Encrypted Genomic Data," in Progress in Cryptology - LATINCRYPT 2014, 2015, pp. 3-27, doi: 10.1007/978-3-319-16295-9_1.
[54] IBM Institute for Business Value, "Healthcare Rallies for Blockchain: Keeping Patients at the Center," IBM, 2016. Available: https://www.ibm.com/downloads/cas/BBRQK3WY
[55] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY