Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

Assessing the Risks and Security Implications of Integrating Cloud Computing in Healthcare

[1]Neha Gupta ,[2]Payal Baghel, [3]Priya Gupta ,[4]Ashwini Rai

[1]School of Computer Applications Manav Rachna International Institute of Research and Studies, Faridabad

[2]School of Computer Applications Manav Rachna International Institute of Research and Studies, Faridabad

[3]School of Computer Applications Manav Rachna International Institute of Research and Studies, Faridabad

[4]School of Computer Applications Manav Rachna International Institute of Research and Studies, Faridabad

Abstract:- Cloud computing in healthcare has streamlined data management, ensuring secure storage and accessibility of patient records. It has facilitated seamless collaboration among healthcare professionals, enabling timely consultations and enhancing patient care. Additionally, cloud-based analytics have empowered medical research, leading to faster insights, innovative treatments, and improved overall healthcare outcomes. The chapter focuses on how cloud computing technology has revolutionized the healthcare sector. The healthcare industry, which has historically been defined by paper-based systems and data fragmentation, is facing rising demand brought on by population expansion and aging demographics. As a response to these issues, cloud computing is predicted to be able to handle an increase in healthcare demand of 11–17% by 2025. Cloud computing enables patient empowerment, interoperability amongst healthcare organizations, and significant cost savings by leveraging IT-enabled fitness gadgets, electronic health data, and collaborative platforms. The chapter explains the financial benefits and motivations for adopting cloud-based solutions in an era where healthcare costs have reached unaffordable levels and emphasizes the necessity of effective deployment and validation procedures.

Keywords*: Cloud security, Healthcare sector, Data security, Cloud service providers, HIPAA, GDPR, Vendor lock-in*

1. Introduction

Cloud computing is a groundbreaking technology with continuously expanding uses, and its impact extends into the healthcare industry. The adoption of cloud computing in healthcare has experienced rapid growth, especially accelerated by the COVID-19 pandemic. This trend indicates that a substantial portion of healthcare services is poised to transition to cloud platforms, with a strong focus on providing cost-effective and highly efficient healthcare services globally. [1].

The healthcare industry's adoption of cloud computing has gained momentum, especially in response to the challenges posed by the pandemic. As reported on www.businesswire.com, the worldwide healthcare cloud computing market is forecasted to achieve approximately $25.54 billion by 2024 and is anticipated to surge to $89 billion by 2027, highlighting its significant significance. Cloud computing has become a necessity for delivering patient-centred care effectively. Infrastructure as a Service (IaaS), a cloud computing architecture, is experiencing the most significant growth, with an anticipated 32% increase by 2027 [2]. Interestingly, healthcare providers currently allocate only about 10% of their revenue to IT, a notably lower investment compared to other industries, which typically allocate 25%.

Throughout the COVID-19 pandemic, virtually every facet of healthcare relied heavily on cloud computing. This technology played a pivotal role in sharing medical records securely, streamlining backend processes, and facilitating the development and maintenance of health applications. Furthermore, it harnessed the natural language processing capabilities of machine learning to sift through and analyse vast volumes of unstructured data, including doctor and lab notes. Cloud computing also came into play for the interpretation of radiologists' readings [3]. The synergy between cloud computing and healthcare holds immense potential for enhancing various healthcare functions, such as telehealth and virtual care, medication adherence monitoring, combating drug theft and counterfeiting, optimizing resource allocation, and ensuring consistency in medical records, as per insights from the healthcare division of Renesas Electronics Corporation, a Tokyo-based company.

In a clinical scenario where a patient presents with chest symptoms and a headache, cloud-based analysis proves invaluable in uncovering concealed patient information. Leveraging their expertise, healthcare providers can make diagnoses and document critical information. The patient's chat interface would display the primary diagnosis, while the cloud system provides additional patient details, including past visits and treatments.

Nevertheless, as healthcare stakeholders ponder the adoption of cloud computing, it becomes imperative to gain a comprehensive understanding of the unique advantages and challenges specific to their medical practices and healthcare delivery objectives. This entails optimizing patient outcomes, ensuring patient safety, and bolstering cost-efficiency, productivity, and the overall effectiveness of care and treatment. A crucial aspect of this process involves establishing robust contractual relationships with Cloud Service Providers (CSPs) via cloud service agreements and service level agreements (SLAs) [4]. Furthermore, it's essential to carefully deliberate over the diverse service delivery models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), as each model carries distinct requirements and obligations. The selection of a cloud deployment model, whether it's private, public, or hybrid, also has strategic implications and necessitates thorough assessment.

Cloud computing in healthcare builds upon two foundational technologies: grid computing and virtualization. Grid computing involves a network of geographically dispersed computers with significant computational power, facilitating virtual simulations. Virtualization, on the other hand, allows for the visualization of systems and interactions between different systems. Cloud computing services, exemplified by Software-as-a-Service (SaaS), enable users to remotely manage applications and resources. This includes the availability of virtualized computers in the cloud, accessible via the internet, with features like storage bandwidth and guaranteed processing power [5]. For instance, Amazon EC2 is an illustrative example of IaaS, allowing rapid setup and configuration of virtual servers through web-based interfaces. Similarly, Platform-as-a-Service (PaaS) offers operating systems and services for applications, exemplified by the Google search engine. Lastly, Data Storage-as-a-Service (dSaaS) fulfills storage and bandwidth requirements for user needs.

In conclusion, cloud computing's integration into healthcare is revolutionizing the industry by improving efficiency, data accessibility, and the quality of patient care. Nevertheless, healthcare organizations must meticulously plan their cloud adoption strategies to ensure optimal outcomes for both patients and healthcare providers.

2. Current State Of Healthcare Industry

The healthcare sector has conventionally been slow to embrace technology for enhancing patient care, often relying on paper records and handwritten notes, which results in data fragmentation and unnecessary costs due to duplication.

The ongoing fluctuations in supply and demand within the healthcare industry are driving the adoption of cloud computing. Growing demand for healthcare services is driven by factors such as population growth, aging, and increased consumer interest in wellness. These factors are expected to shape the role of IT and, consequently, cloud computing in healthcare [6]. Projections estimate an 11-17% increase in healthcare demand between 2014 and 2025.

The use of IT-enabled fitness trackers and mobile applications empowers individuals to take control of their health metrics, making them more informed and capable of making healthcare decisions. As electronic health records, Picture Archiving and Communication Systems (PACS), and advanced clinical systems continue to evolve, there is increasing pressure on existing storage capacities. The implementation of digital pathology systems, for instance, can place significant demands on infrastructure and often divert attention away from clinical aspects.

According to a study by CDW, 37% of healthcare providers have included cloud adoption in their strategic plans, with 22% currently in the planning stages and 25% in the process of implementation [7]. Among those who have already embraced cloud computing, there is an average cost reduction of 20% for the applications that have been implemented.

Healthcare reform and regulations are reshaping the industry, leading to market consolidation and driving faster growth in consumer wellness-oriented mobile health applications. This shift underscores the need for native cloud applications that align with changing consumer requirements and regulatory compliance.

The healthcare industry is moving toward an information-centric care model, underpinned by open standards that promote collaboration, cooperative workflows, and the sharing of information. Figure 1 illustrates a market summary of cloud-based healthcare systems. Cloud computing offers an IT infrastructure that enables various healthcare entities to leverage enhanced computing capabilities at reduced initial costs, fostering innovation and modernization. Additionally, cloud environments promote collaboration and information sharing across the healthcare ecosystem, facilitating cross-industry services.

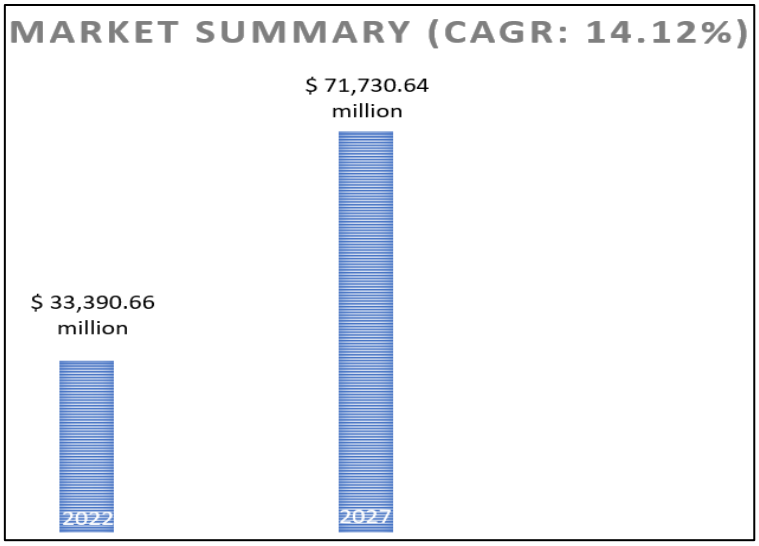

Figure 1: Market share summary of healthcare systems

The decentralization of healthcare delivery is providing patients with more choices in where they receive care, ranging from hospitals to retail clinics and telemedicine options [8]. Patients are increasingly becoming more proactive in managing their health, using smartphones and wearables to monitor their well-being and access healthcare services. Cloud computing allows individuals to access a range of healthcare services from various providers, including the option to consult with some providers remotely through mobile e-visits. The shift in healthcare incentives from volume to value-based care encourages medical professionals to promote healthier behaviours and choices. Several developed nations are setting up healthcare data clearinghouses and data centers to enhance data mobility and enhance patient care. [9].

3. Benefits Of Adopting Cloud In Healthcare

Cloud computing introduces an innovative business model that brings forth numerous advantages for the healthcare industry. The integration of cloud technology into medical services offers significant benefits for both

patients and healthcare organizations. It elevates the quality of patient care, fosters collaboration among healthcare institutions, and greatly reduces IT costs for healthcare companies.

This collaborative approach promotes the interoperability of healthcare services, leading to quicker and more efficient responses to patient needs. The advantages extend to various stakeholders in the healthcare sector, including hospitals, clinics, imaging centers, pharmacies, and insurance companies [10]. This encompasses the secure exchange of patient medical records, prescription details, X-rays, test results, referrals to physicians, and physician availability. This information can be accessed from anywhere by authorized entities.The economic benefits of cloud computing in healthcare are substantial, offering cost flexibility and the potential for reduced expenses. It eliminates the need for heavy capital expenditures since IT resources are acquired on-demand and billed as operational expenses. Furthermore, the expenses associated with the staffing needed to deploy and manage IT resources are incorporated into the costs of cloud computing. Consequently, the necessity for additional skilled IT staff in healthcare organizations and related expenses can be significantly reduced, particularly when utilizing Software as a Service (SaaS) solutions.

Healthcare IT systems hosted in the cloud have the potential to enhance healthcare capabilities by enabling extensive interoperability and integration. These services, being Internet-based and using standard protocols, easily connect with other systems and applications. While challenges related to Electronic Health Record (EHR) and Electronic Medical Record (EMR) vendor contracts and technical compatibility persist, cloud services excel in secure information sharing [11]. Additionally, they facilitate rapid development and innovation, especially for mobile and Internet of Things (IoT) devices, effectively addressing the requirements of evolving healthcare technologies. Some of the prominent benefits of Cloud in Healthcare are:

A. Clinical Benefits:

One of the most significant clinical advantages of cloud technology is access to previously unattainable applications. For instance, digital pathology managed through cloud services has a profound clinical impact by making expensive services more accessible. Access to remote pathologists enables facilities in remote areas to offer new services and rely on experts for diagnoses.

B. Business Benefits:

Healthcare providers, primarily focused on patient care, often allocate less to IT investments compared to other industries. In many cases, stretched IT staff relies on non-technical staff for support. Cloud technology allows providers to access specific experts for system management and maintenance. Cloud providers typically have specialists in block storage, network security, and data archiving, simplifying system management. Cloud technology transforms healthcare delivery, providing consistent IT services and scalable infrastructure on a pay-as-you-go model [12]. This shift allows healthcare providers to concentrate on their core mission: delivering effective patient care.

C. E-health and Telemedicine:

Cloud technology facilitates collaboration among medical specialists, enabling remote clinical care for patients worldwide. Patients benefit from timely consultations and expert advice, transcending geographical boundaries. This streamlined approach revolutionizes healthcare accessibility and ensures patients receive the best possible care, regardless of their location.

D. Drug Discovery:

Cloud computing provides essential computational power for drug discovery from extensive chemical databases. Researchers can efficiently analyze complex data, accelerating the process of identifying potential therapeutic compounds. This efficiency not only expedites drug development but also holds the promise of discovering innovative treatments for various diseases, ultimately saving lives.

E. Healthcare Information Systems:

Cloud computing strengthens healthcare management systems, enhancing patient care, HR management, and financial operations. It enables seamless querying services, leading to improved efficiency in healthcare operations. With real-time data access and streamlined processes, healthcare organizations can optimize resources and focus on delivering high-quality patient care, leading to a more efficient and patient-centric healthcare ecosystem [13].

F. Personal Health Records (PHR):

PHR cloud-based programs facilitate effortless data sharing and access, empowering users to manage their health records conveniently. This secure and accessible platform encourages active participation in personal healthcare management. By enabling individuals to take charge of their health information, PHR systems promote a proactive approach to healthcare, leading to better-informed decisions and improved overall well-being.

G. Clinical Decision Support System (CDSS):

CDSS, based on expert medical knowledge, offers vital recommendations for diagnosing illnesses and suggesting treatments. Additionally, integration with mobile devices and fitness trackers allows continuous monitoring of patients' vital signs, ensuring proactive healthcare interventions. This integration of technology not only enhances diagnostic accuracy but also promotes preventive healthcare, ultimately improving patient outcomes and reducing the burden on healthcare systems [14].

H. Cloud-based Digital Libraries:

Medical practitioners and students can access current research and information via cloud-based libraries.

4. Drivers For Cloud Adoption In Healthcare

The adoption of new technologies in healthcare has historically been slow due to the absence of key drivers. However, recent developments, including increased investments and greater attention to healthcare on national agendas, have amplified the motivations for adopting cloud-based solutions.

The escalating cost of healthcare delivery has reached unsustainable levels in some countries, accounting for as much as 35% of the gross domestic product. To address this issue, governments are compelled to seek cost-effective solutions. The imperative to lower healthcare costs has become a central focus in society, influencing political agendas and leading to the exploration of alternative models that promise cost savings and operational efficiencies [15].

For healthcare organizations to embrace these new solutions and prove their return on investment (ROI) without significant upfront expenses, mechanisms must be in place to deploy, test, and validate their effectiveness.

Clinical innovation, which ultimately enhances patient care and outcomes, remains a primary objective for hospitals. Enabling healthcare facilities to adopt new technologies cost-effectively becomes a compelling driver for cloud adoption.

Recent data analysis has confirmed that cost savings are a fundamental driver of cloud adoption, aligning with previous research highlighting the importance of cost savings in the decision to adopt cloud computing [16].

Potential Cloud Drivers and Use Cases:

In addition to the typical costs associated with transitioning to a cloud-based solution, organizations may encounter technical and organizational challenges, as well as a learning curve. Nonetheless, the benefits can go beyond merely reducing long-term IT and healthcare expenditures, encompassing increased revenue from innovative services and enhanced patient satisfaction achieved by seamlessly integrating healthcare into daily life.

IT Cost Reduction: Cloud technology has the potential to significantly reduce costs associated with delivering services across diverse domains within the healthcare enterprise, including finance, administration, IT management, application development and support, data networking, service desk, end-user computing, and data centers.

Connected Healthcare: This model leverages technology to provide seamless healthcare across multiple providers, offering patients opportunities to engage with medical staff and receive care beyond physical healthcare facilities through mobile and wearable devices connected to cloud-based systems [17].

Big Data Analytics: The advanced adoption of healthcare IT enables the harnessing of "Big Data" to collect, extract, and analyze extensive medical data, promoting insights into processes, treatments, effectiveness, costs, and conditions. Cloud-based solutions facilitate the secure sharing of essential medical information among authorized healthcare organizations, expediting research and development.

Telemedicine: Telemedicine technology brings specialized medical advice to remote areas and underserved regions, making healthcare more accessible. Cloud computing plays a vital role in providing the necessary connectivity channels for telemedicine.

IoT Enabled Healthcare: Internet of Things (IoT) devices and wearable technologies provide real-time patient data, enabling remote monitoring and flexibility in patient lifestyles. Cloud systems simplify the management of IoT device connectivity requirements.

Diagnostic Support: Cloud-based systems assist medical practitioners in diagnosis, offering access to the latest research and information from colleagues worldwide, reducing time spent on diagnosis and improving productivity.

Application Development and DevOps: Cloud computing services support DevOps practices, enabling rapid application development and reliable delivery of healthcare services.

Disaster Recovery as a Service (DRaaS): Healthcare systems are critical, necessitating continuous availability even in the face of IT failures. DRaaS eliminates the need for organizations to invest in and uphold their disaster recovery setups, providing flexibility to adjust to evolving business requirements.

In conclusion, the healthcare sector is increasingly recognizing the importance of cloud adoption due to factors such as rising healthcare costs and the drive for cost savings, improved patient care, and innovative solutions. Cloud technology is poised to play a pivotal role in transforming healthcare delivery.

5. Impact Of Cloud Computing In Indian Healthcare Firms

The healthcare industry in India has been particularly impacted, experiencing significant improvements in efficiency, accessibility, and patient care due to the adoption of cloud technologies.

A. Enhanced Efficiency and Resource Optimization:

Cloud computing has enabled Indian healthcare firms to optimize their resources effectively. By moving their data and applications to cloud-based platforms, these firms have reduced the burden of maintaining extensive IT infrastructures. This shift allows them to focus more on core healthcare services, streamline administrative processes, and allocate resources efficiently, ultimately leading to cost savings and improved operational efficiency [4].

B. Improved Patient Care and Accessibility:

One of the most remarkable impacts of cloud computing in Indian healthcare is the enhancement of patient care. Cloud-based electronic health record (EHR) systems have facilitated seamless access to patient data, enabling healthcare professionals to make informed decisions quickly. Patients, too, benefit from this accessibility as they can view their health records, schedule appointments, and consult with healthcare providers remotely through telemedicine services [7]. This increased accessibility has been especially valuable in rural areas, where quality healthcare services were previously limited.

C. Strengthening Telemedicine Services:

India, with its vast geographical expanse and diverse population, faces challenges in providing healthcare services to remote and underserved areas. Cloud computing has played a pivotal role in strengthening telemedicine services

[12]. Through secure cloud platforms, doctors can conduct virtual consultations, share medical records, and even perform diagnostic analyses remotely. This advancement has not only improved healthcare accessibility but also has been crucial during emergencies and pandemics, ensuring continuity of care while minimizing physical contact.

D. Data Security and Compliance:

Concerns about data security and privacy have always been paramount in healthcare. Cloud service providers have responded by implementing stringent security measures, often exceeding industry standards. In India, where data security regulations are becoming increasingly stringent, cloud computing offers healthcare firms the opportunity to store and manage patient data securely while ensuring compliance with legal requirements such as the Personal Data Protection Bill [16]. This secure environment fosters trust among patients and healthcare providers alike.

E. Facilitating Medical Research and Innovation:

Cloud computing has accelerated medical research and innovation in Indian healthcare firms. Researchers can leverage cloud-based platforms to process and analyze vast datasets efficiently, leading to advancements in disease understanding, drug discovery, and treatment methodologies. Collaborative research efforts, both nationally and internationally, have been facilitated by cloud technology, enabling Indian healthcare professionals to contribute significantly to the global scientific community.

6. Security Issues Of Cloud Computing In Healthcare

The primary cloud security challenges within the healthcare sector, as identified by experts, center around data security, privacy, and trust concerns. These challenges encompass:

Lack of Trust in Cloud Solutions: Within the healthcare ecosystem, stakeholders including patients, physicians, medical staff, and healthcare management express reservations about relying on cloud solutions [1]. Patients are particularly concerned about the security of their medical data when entrusted to cloud service providers. Building trust within the doctor-patient relationship can help alleviate these concerns. Medical staff often lack awareness of cybersecurity and data protection, necessitating awareness campaigns and training to mitigate mistakes made by individuals and social engineering attacks.

Lack of Security and Technology Expertise: Transitioning from on-site IT infrastructure to cloud-based systems requires personnel with a profound understanding of cloud technologies and their associated security and data protection aspects [3]. This shift sometimes necessitates different knowledge and skills than those possessed by existing on-site IT personnel, potentially resulting in job losses. Moreover, the high demand for cloud security experts in the healthcare sector exceeds the available supply, hindering the progress of cloud computing adoption.

Cybersecurity Investment Prioritization: Many healthcare organizations face financial constraints and limited public funding support, restricting the allocation of financial resources to advance digitalization, cybersecurity, and data protection maturity [15].

Proving Regulatory Compliance of Cloud Service Providers (CSPs): Healthcare clients often struggle to determine which CSPs align with their specific legal requirements, limiting their choices for collaboration. Evaluating a CSP's compliance can be complex and costly. However, some CSPs publicly disclose their compliance status on their websites, often backed by third-party assessments or government certification programs [12]. Nonetheless, the intricate regulatory requirements concerning healthcare-related data may lead some CSPs to exclude this market segment from their business model.

Integration of Cloud with Legacy Systems Challenges: Integrating cloud solutions into existing healthcare organization infrastructure, including outdated legacy systems, poses substantial challenges. These legacy systems may lack support from their providers, making integration and interoperability with new technology complex [14]. This also exposes these systems to cybersecurity threats. Although hybrid deployment models offer flexibility by

combining on-premises and cloud solutions, they entail significant deployment costs, especially when adding extra security features or integrating security elements with on-premises security perimeters.

Loss of Governance: The transition to cloud services can raise concerns about relinquishing control and governance over data. Healthcare organizations may worry about their ability to maintain control over sensitive patient information.

Risk Management: Effective risk management is critical to mitigate potential security threats and breaches, ensuring data protection and privacy [8].

Indefinite Provider Compliance: The degree of adherence to security and privacy requirements by cloud service providers varies, making it challenging to ensure consistent compliance.

Organizational Inertia: Resistance to change within healthcare organizations can impede the implementation of security measures and the adoption of cloud solutions.

Network Security Challenges: The proliferation of wireless sensor networks has led to increased network security challenges in cloud infrastructure. Common network attacks, such as IP spoofing, port scanning, and DoS attacks, pose a threat to cloud resource availability. No specific security standard exists for wireless networks, but potential solutions like APIs, data classification, and security management protocols can enhance security in cloud computing networks 13].

Integrity and Availability Challenges: Implementing cloud-based services introduces challenges related to data integrity and service availability. Loss or leakage of information in the cloud can have severe legal and business repercussions. The Confidentiality, Integrity, and Availability (CIA) triad are central factors in cloud system security [5].

DoS Attacks: Denial of Service (DoS) attacks aimed at disrupting cloud resource availability pose a significant threat. Protecting resource availability becomes crucial in mitigating such attacks.

Lack of Specific Security Standards for Wireless Networks: The absence of tailored security standards for wireless networks complicates cloud network security efforts.

Addressing these challenges necessitates a comprehensive approach that encompasses policies, technology solutions, training programs, and ongoing vigilance. Protecting the confidentiality and integrity of healthcare data is imperative from legal and ethical perspectives [7]. Additionally, the virtual infrastructure of web-based networks presents vulnerabilities that must be addressed to counter ongoing cyber threats and hacking attempts, underscoring the need for robust security measures.

7. Associated Risks Of Cloud

In the healthcare sector, the adoption of cloud computing has become increasingly prevalent due to its potential to deliver scalability, cost-efficiency, and accessibility to critical medical data and services. However, alongside these benefits, there are associated risks that demand meticulous consideration in the context of healthcare operations [2]. One of the primary concerns revolves around data security, as incorrect cloud configuration or insufficient security measures can result in data breaches and unauthorized entry to confidential patient data. These breaches have the potential to jeopardize patient confidentiality and the accuracy of medical records, emphasizing the need for rigorous security protocols.

Another crucial aspect of cloud computing in healthcare pertains to compliance and legal matters. In the United States, healthcare entities are obligated to adhere to the Health Insurance Portability and Accountability Act (HIPAA), which imposes stringent regulations concerning the safeguarding of patient data. Cloud service providers must also comply with these regulations, making it essential for healthcare organizations to make careful choices and effectively manage their cloud services [4]. Similarly, in Europe, the General Data Protection Regulation (GDPR) imposes rigorous data protection regulations, adding complexity to cloud implementations and emphasizing the legal hurdles that healthcare organizations encounter.

Data loss and recovery present substantial concerns in healthcare cloud computing. Despite the robust infrastructure of cloud data centers, incidents of data loss can occur due to technical failures or human errors. Ensuring rapid data recovery in healthcare settings is critical for patient care continuity and maintaining data integrity.

Moreover, the risk of vendor lock-in is a strategic consideration. Healthcare organizations that become overly dependent on a specific cloud provider may find it challenging to migrate to alternative solutions, leading to potential inflexibility and cost escalation [6].

Interoperability issues persist as well, as healthcare systems must seamlessly integrate with cloud-based solutions and on-premises infrastructure to provide comprehensive patient care. Downtime and availability problems during cloud outages can disrupt healthcare services, causing patient care interruptions and financial losses, further emphasizing the need for a robust cloud strategy.

Data portability remains a complex issue, as transferring patient data between different cloud providers can introduce risks of data loss or corruption. Ethical concerns regarding the use of patient data in cloud-based research and analytics, such as ensuring informed consent and data ownership, add additional layers of complexity [8].

Furthermore, managing cloud costs effectively is a constant challenge, and healthcare organizations must deploy monitoring and cost management strategies to prevent unexpected financial burdens. Vulnerabilities in cloud infrastructure can expose healthcare operations to cyberattacks and other threats, jeopardizing the availability of critical healthcare services [10].

The dearth of IT expertise within healthcare organizations may hinder the effective management of cloud environments, necessitating collaboration with skilled cloud service providers. Regulatory changes in the healthcare sector can pose challenges in maintaining compliance within the cloud. Relying on third-party vendors for cloud services introduces risks associated with their security practices and business continuity. Finally, data silos, arising from disparate cloud systems and providers, can impede comprehensive patient care by fragmenting critical medical data [11].

To mitigate these multifaceted risks, healthcare organizations must undertake thorough risk assessments, employ robust security measures, ensure compliance with applicable regulations, and craft comprehensive data governance and disaster recovery plans. Furthermore, staying abreast of evolving cloud technologies and best practices is imperative for effectively managing these risks in the dynamic and ever-evolving landscape of healthcare cloud computing [13].

In this section, we examine the primary data protection challenges associated with Cloud services in the healthcare sector:

1. Privacy by Design: Healthcare providers must ascertain whether Cloud services have adhered to privacy-by-design principles, encompassing policies and measures. This includes minimizing the processing of personal data, early pseudonymization, transparent data processing, enabling data subject oversight, and enhancing security features. Achieving these objectives can involve specific technologies and policies such as authentication, attribute-based credentials, and privacy-preserving computations [12].

2. Data Management: Healthcare organizations, acting as authorized entities with consent, collect, organize, and manage patient data. Sometimes, this data is automatically transmitted to the Cloud (e.g., from medical devices) or input by delegated individuals (e.g., medical practitioners). Depending on the Cloud service type, data input may originate from different sources, posing accuracy challenges. Measures for ensuring data accuracy should be in place, even when third parties are involved [14]. Organizations must establish their data governance models/frameworks to identify the most sensitive data types and apply the necessary controls. Interoperability, especially in healthcare, is crucial, given the versatile range of services offered by Cloud computing.

3. Data Deletion: Ensuring the ability to erase data promptly after the expiration of retention periods or upon a data subject's request is of utmost importance. Data subjects can substantiate their deletion requests based on GDPR grounds, such as data no longer being necessary for the initial purpose or data subject consent withdrawal.

Cloud providers have made partial progress in identifying data storage areas through data tagging. However, effectively deleting data remains a technical challenge [16].

4. Data Portability: The challenge of data portability is closely linked to the risk of vendor lock-in, a common concern in Cloud Computing. Data portability involves the smooth transfer of one's data from one provider to another without any loss. In healthcare, specific standards are in place to ensure interoperability and, by extension, data portability.

5. Encryption: Implementing encryption is one of the most crucial yet challenging measures. It is essential to safeguard data secrecy and integrity, but it must be applied across various data transfer and storage channels. Encryption measures should be implemented at both the client and server levels, as well as in the connecting channels [17]. The responsibility for encryption extends to both the cloud customer and the cloud provider, and this responsibility carries substantial technical and legal ramifications.. It's worth noting that some Cloud Service Providers (CSPs) retain full control of encryption keys, which has implications for data security and control.

These challenges emphasize the necessity of robust data protection strategies, encompassing technical solutions and compliance with regulatory frameworks like GDPR. In the healthcare sector, where sensitive patient data is involved, addressing these challenges is critical for securely leveraging Cloud services.

8. Possible Solutions Of Security Issues And Risks

Security and data protection are of paramount importance in the adoption of healthcare solutions that rely on cloud technology. This in-depth discussion explores crucial facets of protecting healthcare data in the cloud. It emphasizes the shared responsibility model, regulatory compliance, and various security controls:

Shared Responsibility Model: A fundamental distinction between traditional IT and cloud services lies in the shared responsibility model. While most obligations in traditional IT setups fall on the organisation, with cloud computing, they are split between the cloud service provider and the healthcare organisation as the customer. Clarity in defining and understanding these roles and responsibilities is crucial for effective security and data protection.

Compliance with Regulations: Healthcare data is subject to rigorous regulations in numerous countries, such as HIPAA in the USA and GDPR in the EU. These regulations impose obligations on entities handling healthcare data, often referred to as electronic Protected Health Information (ePHI). Compliance with these regulations is imperative and involves both cloud service providers and customers.

Requirements Breakdown: To ensure security and privacy, requirements are categorized into three main areas: physical, administrative, and technical safeguards.

a. **Physical Safeguards:** Cloud providers generally maintain robust facility access controls, but healthcare organizations must verify these controls. This encompasses ensuring the security of workstations and device media, particularly for mobile devices, including IoT devices and those used by medical professionals.
b. **Administrative Controls:** Both cloud customers and providers share responsibilities in meeting administrative requirements, which are similar in both cloud and traditional environments. Healthcare organizations may need to enhance their systems to align with cloud security and privacy requirements.
c. **Technical Controls:** Cloud providers must encrypt protected health information (PHI) during both transmission and storage. Effective encryption key management is crucial, using standardized, not custom, implementations of secure algorithms. Technical controls also encompass authentication and authorization, which can be intricate in hybrid cloud solutions spanning multiple systems. For accessing ePHI across unsafe networks, it is advised to use third-party authentication through a central Identity and Access Management system, with a focus on two-factor authentication.

Authentication and Authorization: Authentication is pivotal in healthcare systems to prevent unauthorized access. In hybrid cloud environments, where multiple systems require authentication, the complexity is heightened. Third-party authentication anchored in a central Identity and Access Management system is advisable

and strong advocacy exists for two-factor authentication, especially when accessing ePHI over unsecured networks like the Internet.

Logical and Physical Security: Organizations must vigilantly manage both logical and physical security facets throughout the ePHI lifecycle. The HIPAA HITECH Act serves as a framework supporting secure ePHI exchange. To prevent ePHI data loss, a key strategy is minimizing its collection and storage, ensuring data is retained only when absolutely necessary.

Patient Access: Regulations often grant patients the right to access their ePHI, creating a challenge for healthcare IT systems. Providing a user-friendly interface for patients to access their data across multiple applications and systems is essential. Equally crucial is ensuring robust authentication mechanisms to guarantee that only the authorized patient can access their data.

Data Encryption: Protected health information (PHI) should be encrypted by cloud service providers both in transit and at rest. The usage of standardised encryption techniques and proper key management are essential. Data can become illegible by encryption if the customer gets access to the keys.

Data Minimization: To reduce the risk of data loss, organizations should avoid collecting and storing ePHI unless absolutely necessary. Minimizing data collection and securely disposing of unnecessary data are important practices.

Secure Access to the Facility:

Physical Security Measures: At their data centres, cloud providers must put strong physical security measures in place, such as controlled access, surveillance, and security guards, to prevent unauthorised physical access.

Network Security:

a) Encryption: All data transmitted between healthcare organizations and the cloud must be encrypted using strong encryption protocols to ensure data security even if intercepted.

b) Intrusion Detection and Prevention Systems (IDPS): Use IDPS to find and stop unauthorised network breaches or access attempts.

c) Firewalls and Access Controls: Employ access controls and firewalls to limit network access to approved users and devices.

d) Regular Network Monitoring: Continuously monitor network traffic for anomalies or suspicious activities that may indicate a security breach.

Data Security:

a) Data Encryption at Rest: Ensure data stored in the cloud is encrypted at rest to protect patient information even if unauthorized access occurs within the cloud infrastructure.

b) Access Control and Authentication: Implement strict access controls and authentication mechanisms to ensure only authorized personnel can access and modify patient data.

c) Data Backup and Disaster Recovery: Have reliable disaster recovery procedures in place and regularly back up patient data to avoid data loss in the event of unplanned incidents.

Staff Training and Regulatory Compliance Awareness:

a) Training: Provide comprehensive training to staff members with access to patient data, emphasizing security best practices and compliance requirements.

b) Regulatory Compliance: Stay informed and adhere strictly to healthcare data privacy and security regulations, such as HIPAA or GDPR.

c) Regular Audits and Assessments: Perform regular security audits and evaluations to detect potential weaknesses and guarantee alignment with industry norms and regulatory requirements.

Incident Response Plan:

Create a strong incident response strategy to promptly and efficiently manage security breaches or data breaches, which includes notifying affected parties as mandated by regulations.

Vendor Risk Assessment:

Before selecting a cloud provider, conduct a thorough risk assessment of the vendor's security practices, infrastructure, and compliance certifications.

Regular Security Updates:

Ensure all software and systems used in the cloud environment are regularly updated with security patches to address known vulnerabilities.

Data Ownership and Portability:

Clarify data ownership and portability rights in contracts with cloud providers to ensure smooth transition or retrieval of data when necessary.

Security is paramount in healthcare data management, and when contemplating cloud migration, strict confidentiality, privacy, and security are essential. Ensuring adherence to regulations like HIPAA is a fundamental necessity when shifting medical records to the cloud. The process of transferring sensitive healthcare data to a third-party entity is intricate, necessitating strong security measures to protect access controls, audit controls, authentication, authorization, transmission security, and storage security. Effectively addressing these concerns holds significant importance in establishing confidence in cloud systems and encouraging their adoption within the healthcare sector. Prominent cloud service providers such as Microsoft, Google, and Amazon are actively dedicated to crafting and enacting stringent policies and protocols to guarantee the security and privacy of customer data. In summary, ensuring security and data protection in healthcare cloud solutions necessitates a thorough understanding of shared responsibilities, strict compliance with regulations, and implementation of various safeguards, robust encryption practices, and provision of secure patient access to their information. These practices are vital for maintaining the confidentiality and integrity of healthcare data. Securing the storage and management of personal health information in the cloud is paramount to maintain trust and regulatory compliance.

10. Conclusion

In conclusion, the integration of cloud computing into the healthcare sector represents a transformative shift, accelerated by the COVID-19 pandemic, offering cost-effective and efficient services. While cloud technology offers immense potential for telehealth, data analysis, and innovation, it comes with data security and privacy challenges. To navigate this landscape successfully, healthcare organizations must establish strong relationships with providers, adapt to changing demands, and prioritize patient-centric care. Addressing security challenges requires a multifaceted approach, including compliance, encryption, access controls, and risk assessments. Ultimately, embracing best practices ensures optimal patient care while upholding data security and privacy standards in the evolving healthcare environment.

Refrences

[1] AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012), ―e-Health cloud: opportunities and challenges‖. Future internet, 4(3), pp. 621-645.

[2] Alharbi, F., Atkins, A., & Stanier, C. (2017), ―Cloud Computing Adoption in Healthcare Organisations: A Qualitative Study in Saudi Arabia‖, In Transactions on Large-Scale Data-and Knowledge-Centered Systems XXXV (pp. 96-131). Springer, Berlin, Heidelberg.

[3] Alharbi, F., Atkins, A., & Stanier, C. (2017, February), ―Decision makers views of factors affecting cloud computing adoption in saudi healthcare organisations‖. In Informatics, Health & Technology (ICIHT), International Conference on (pp. 1-8). IEEE.

[4] Rostrom T, Teng CC. Secure communications for PACS in a cloud environment. Conf Proc IEEE Eng Med Biol Soc. 2011;2011:8219–22.

[5] Mell P, Grance T. The NIST definition of cloud computing (draft). NIST Spec Publ. 2011;800(145):7.

[6] Rosenthal A, Mork P, Li MH, Stanford J, Koester D, Reynolds P. Cloud computing: a new business paradigm for biomedical information sharing. J Biomed Inform. 2010;43(2):342–53.

[7] IHS 2016 Update: The Complexities of Physician Supply and Demand: Projections from 2014 to 2025 https://www.aamc.org/download/458082/data/2016_complexities_of_supply_and_ demand_projections.pdf

[8] Mckinsey & Company (August, 2016): How tech-enabled consumers are reordering the healthcare landscape. http://healthcare.mckinsey.com/how-tech-enabled-consumers-are-reordering-healthcarelandscape

[9] Search Health IT: HITECH Act http://searchhealthit.techtarget.com/definition/HITECH-Act

[10] HIPAA http://www.hhs.gov/hipaa/ [10] Cloud Standards Customer Council 2015, Practical Guide to Cloud Service Level Agreements, Version 2.0. http://www.cloud-council.org/deliverables/practical-guide-to-cloud-service-agreements.htm

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council (2016): EU General Data Protection Regulation. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[12] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.

[13] Rath, M. (2019). Security challenges and resolution in cloud computing and cloud of things. In Applying Integration Techniques and Methods in Distributed Systems and Technologies (pp. 79-102). IGI Global.

[14] Kaur, C., Mourad, H. M., & Banu, S. S. (2019). Security and Challenges using Clouds Computing in Healthcare Management System.

[15] Kamoona, M. A., & Altamimi, A. M. (2018, July). Cloud Ehealth Systems: A Survey on Security Challenges and Solutions. In 2018 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 189-194). IEEE.

[16] Dang, L. M., Piran, M., Han, D., Min, K., & Moon, H. (2019). A survey on Internet of things and cloud computing for healthcare. Electronics, 8(7), 768.

[17] Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access, 9, 8820-8834.