THE COMPUTERTECH
(An International Peer Review Journal)
VOLUME 5; ISSUE 2 (JULY-DEC); (2019)
WEBSITE: THE COMPUTERTECH

Cloud-Based Health Information Systems: Balancing Accessibility with Cybersecurity Risks

Praveen Kumar Pemmasani[1], Motohisa Osaka[2]
[1]Data cloud Security Engineer, Merck, 10301 David Taylor Dr, Charlotte, NC 28262
[2]Golden Gate University, California, USA

Abstract

The rapid digitalization of healthcare has led to the widespread adoption of Cloud-Based Health Information Systems (CHIS), offering enhanced data accessibility, interoperability, and operational efficiency. These systems facilitate real-time access to electronic health records (EHRs), telemedicine platforms, and medical imaging repositories, enabling healthcare professionals to deliver patient-centered care regardless of location. However, while cloud solutions offer scalability and cost-effectiveness, they also introduce significant cybersecurity risks, including data breaches, unauthorized access, and compliance challenges. Cyberattacks targeting healthcare organizations have increased, exposing sensitive patient information to malicious actors and jeopardizing healthcare integrity. This paper explores the dual challenge of leveraging cloud technology for healthcare advancements while mitigating cybersecurity threats. Key strategies, including Zero Trust Security, data encryption, multi-factor authentication (MFA), and AI-driven threat detection, are analyzed to provide a comprehensive approach to secure CHIS. Additionally, regulatory frameworks such as HIPAA, GDPR, and HITECH are discussed in the context of ensuring data privacy. By adopting robust security frameworks, healthcare organizations can maximize the benefits of cloud-based systems while maintaining compliance, confidentiality, and resilience against cyber threats. This study highlights the need for a balanced approach that prioritizes both accessibility and security to protect sensitive health information in an increasingly digital world.

Keywords: Cloud Security, Electronic Medical Records (EMR), Data Governance, HIPAA Compliance, Hybrid Cloud, Multi-Cloud Strategies, Encryption, Access Controls.

Introduction

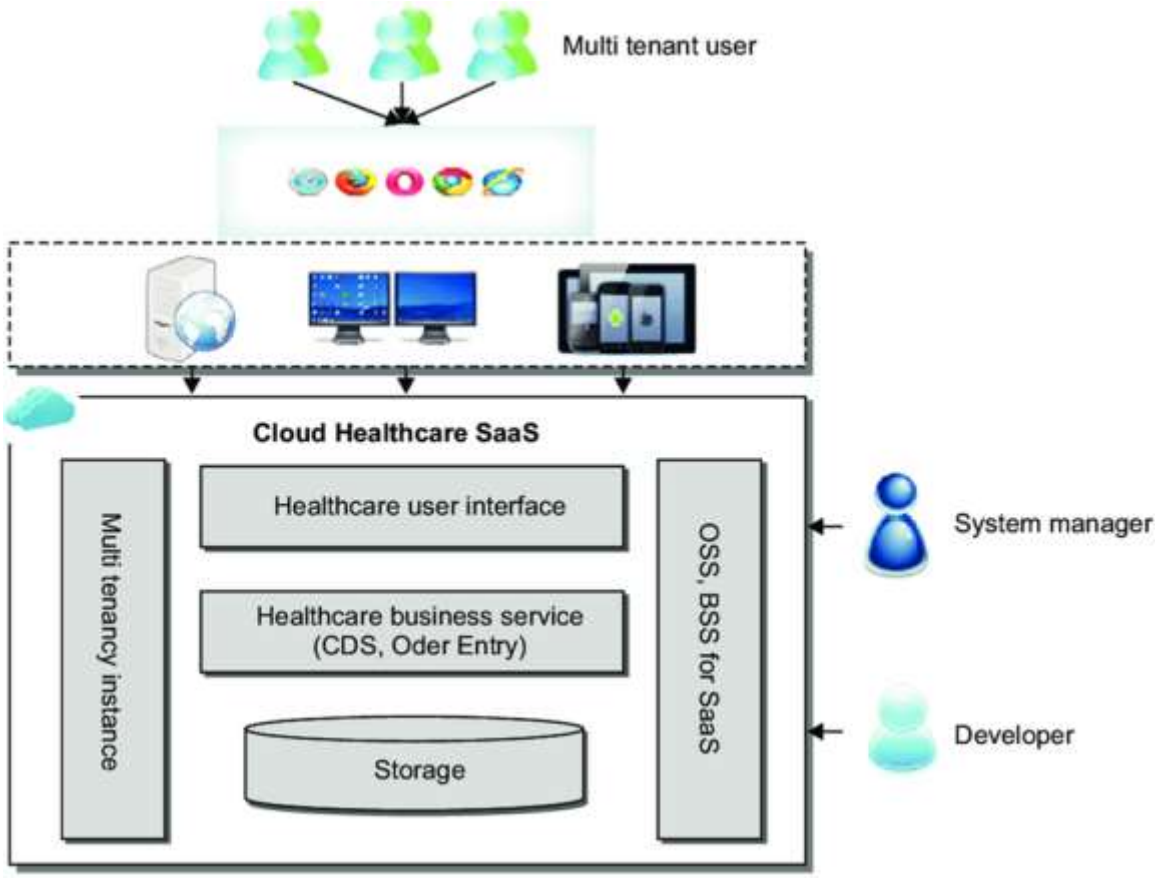
Overview of AI in Automation and Data Engineering

The advent of cloud computing has revolutionized the healthcare industry, enabling the efficient storage, retrieval, and sharing of patient data across multiple platforms. Cloud-Based Health Information Systems (CHIS) offer a scalable solution for managing electronic health records (EHRs), medical imaging, and telemedicine applications, facilitating improved collaboration among healthcare providers. Unlike traditional on-premise data storage, cloud solutions eliminate geographical barriers, allowing healthcare professionals to access critical patient information from anywhere, fostering seamless communication and continuity of care. As hospitals and clinics continue to digitize their operations, the reliance on cloud computing has grown exponentially,

making data accessibility a cornerstone of modern healthcare services. However, alongside these advantages come significant cybersecurity risks, as sensitive patient data becomes a lucrative target for cybercriminals [1].

Cyber threats in healthcare are escalating, with data breaches, ransomware attacks, and insider threats posing substantial risks to patient privacy and healthcare integrity. The 2021 attack on Scripps Health, which disrupted medical services and compromised patient data, and the WannaCry ransomware attack of 2017, which paralyzed the UK's National Health Service (NHS), underscore the vulnerabilities of cloud-based healthcare systems. Unlike traditional IT infrastructures, cloud environments operate on shared resources, making them susceptible to misconfigurations, unauthorized access, and API vulnerabilities. Additionally, the need for remote accessibility exposes patient data to potential threats from unsecured networks and compromised endpoints. These security challenges necessitate a robust cybersecurity framework that safeguards patient records while maintaining the efficiency of cloud-based solutions [2].

One of the fundamental challenges in securing Cloud-Based Health Information Systems lies in balancing accessibility with data protection. Healthcare organizations must ensure real-time access to patient records while preventing unauthorized access, data leaks, and regulatory non-compliance. Zero Trust Security (ZTS) is emerging as a critical approach, where no user or device is inherently trusted, and continuous verification mechanisms are applied to prevent unauthorized access. End-to-end encryption, multi-factor authentication (MFA), and role-based access control (RBAC) further enhance security, ensuring that only authorized personnel can retrieve or modify sensitive health data. Additionally, AI-driven anomaly detection plays a pivotal role in identifying suspicious activities, such as unusual login patterns, unauthorized data transfers, or malware intrusions, preventing potential cyber threats before they escalate (Scheme 1).



Scheme 1: Overview of cloud computing-based Healthcare Software-as-a-Service (SaaS). CDS: Clinical Decision Support, OSS: operational support service, BSS: business support service.

Regulatory compliance is another critical aspect of cloud-based health information security. Laws such as HIPAA (Health Insurance Portability and Accountability Act) in the U.S., GDPR (General Data Protection Regulation) in Europe, and the HITECH Act (Health Information Technology for Economic and Clinical Health Act) establish stringent guidelines for data protection, breach notification, and security standards in healthcare. Failure to comply with these regulations can result in hefty fines, legal consequences, and reputational damage for healthcare institutions. Cloud service providers (CSPs) must adhere to strict security protocols and implement data sovereignty policies to ensure that patient records remain protected within the jurisdiction's legal framework. Additionally, cyber insurance policies are gaining traction as a protective measure against financial losses arising from cyberattacks and data breaches [3].

As healthcare continues to embrace cloud-based technologies, organizations must adopt a holistic security strategy that integrates risk assessment, employee training, and incident response plans. The implementation of secure cloud architectures, such as private and hybrid cloud models, can provide greater control over sensitive data while leveraging the scalability of public cloud services. Furthermore, collaboration between healthcare institutions, cybersecurity experts, and regulatory bodies is essential to develop standardized security frameworks that ensure both accessibility and protection of cloud-based health records. By embracing proactive cybersecurity measures,

healthcare providers can fully harness the benefits of Cloud-Based Health Information Systems while mitigating risks associated with cyber threats and data vulnerabilities.

1. Cloud migration challenges in healthcare

The healthcare industry is increasingly adopting cloud-based health information systems (CHIS) to enhance data accessibility, improve patient care, and reduce operational costs. However, migrating sensitive medical data to the cloud presents significant challenges, primarily related to data security, compliance, system integration, service reliability, and user adoption. Security remains a top concern, as healthcare data is highly valuable to cybercriminals. According to the U.S. Department of Health and Human Services, 2023 witnessed over 725 major healthcare data breaches, compromising 133 million patient records. For instance, the ransomware attack on Universal Health Services (UHS) in 2020 disrupted operations in 400 hospitals and led to financial losses exceeding $67 million. To mitigate risks, hospitals must implement strong encryption, zero-trust security frameworks, and multi-factor authentication (MFA) to safeguard patient data from cyber threats. Another major challenge is compliance with strict healthcare regulations, which vary across regions. Laws such as HIPAA (USA), GDPR (Europe), and PIPEDA (Canada) mandate rigorous data protection, encryption, and access control measures. A critical issue in cloud migration is data sovereignty, where regulations often prohibit cross-border data transfers. For example, Figure 1 shows Google's partnership with Ascension Health in 2019 raised HIPAA compliance concerns when reports emerged that Google stored patient records without explicit patient consent. To ensure compliance, healthcare organizations must choose cloud providers that offer industry-specific compliance solutions and maintain data residency controls that align with regional laws. Regular third-party audits are also necessary to verify compliance [4-9].

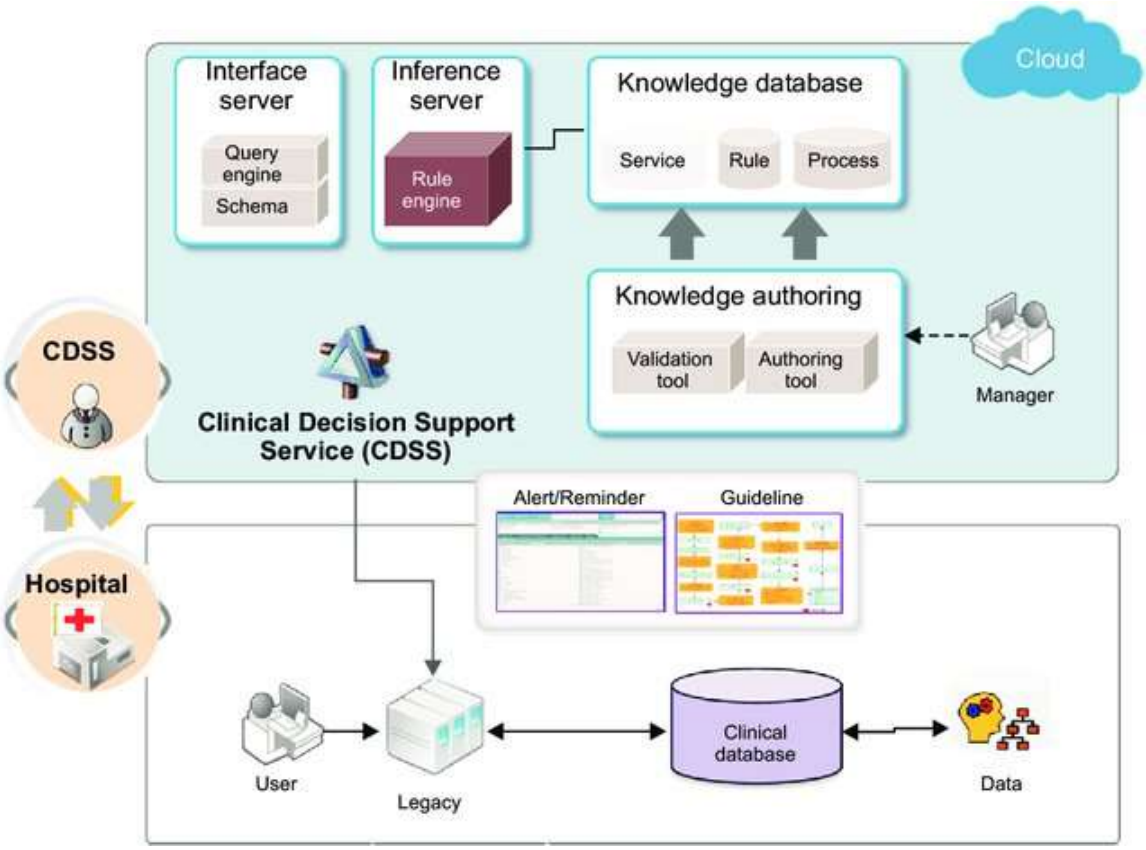


Figure 1: Overview of a cloud-based Clinical Decision Support Service (CDSS).

A significant technical challenge in cloud migration is integrating modern cloud platforms with legacy healthcare systems, which are often outdated and incompatible with cloud technologies. Many hospitals still rely on decades-old electronic health record (EHR) systems that lack interoperability with cloud-based solutions. In the UK, 95% of NHS Trusts still use legacy systems, making cloud adoption complex. Some hospitals even operate on Windows XP, which Microsoft no longer supports, exposing them to security vulnerabilities. To address this, hospitals should implement interoperability standards like FHIR (Fast Healthcare Interoperability Resources) and HL7 (Health Level Seven), allowing seamless data exchange between legacy and cloud-based systems. A hybrid cloud model can also facilitate gradual migration, ensuring minimal disruptions to hospital operations. Another challenge is ensuring continuous service availability during and after migration. Healthcare systems require 99.999% uptime, as even minor downtime can disrupt patient care, delay surgeries, and impact emergency response teams. In 2022, Cerner, a leading EHR cloud provider, suffered a major outage, leaving hospitals unable to access patient records for over 10 hours. Such incidents highlight the need for robust disaster recovery plans, automated failover mechanisms, and multi-cloud strategies to prevent service disruptions. Before migration, hospitals should conduct stress testing and implement backup solutions to maintain uninterrupted access to critical patient data [10-13]].

Lastly, resistance from healthcare professionals remains a key challenge. Many doctors, nurses, and hospital administrators are hesitant to adopt cloud-based systems, fearing complex interfaces,

security risks, and workflow disruptions. For example, Stanford Health's cloud migration in 2021 faced strong pushback from staff due to longer login times and unfamiliar systems, requiring over a year of extensive training to improve adoption. To overcome this, hospitals must involve healthcare staff in the transition process, conduct pilot programs, and provide ongoing technical support to ensure a smooth transition. Despite these challenges, with robust security frameworks, regulatory compliance strategies, and structured migration plans, healthcare providers can successfully transition to cloud-based systems, ensuring better patient outcomes, data security, and operational efficiency.

2. Data privacy regulations

The increasing reliance on cloud-based health information systems (CHIS) has raised significant concerns about data privacy and regulatory compliance. Healthcare organizations handle vast amounts of sensitive patient data, including medical history, prescriptions, diagnostic reports, and billing information, making them prime targets for cybercriminals. In response, governments and regulatory bodies worldwide have implemented strict data privacy regulations to protect patient information and ensure ethical handling of healthcare data. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., General Data Protection Regulation (GDPR) in Europe, and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada mandate rigorous data security measures, patient consent policies, and strict access controls. Violations of these regulations can lead to heavy fines, legal actions, and reputational damage for healthcare organizations. For instance, in 2023, Banner Health in Arizona was fined $1.25 million for failing to implement adequate security measures, which led to a cyberattack compromising 2.9 million patient records. A critical component of data privacy regulations is patient consent and control over personal health data. Under GDPR, for example, patients have the right to access, correct, and request deletion of their personal data, ensuring greater transparency and control. Similarly, HIPAA's Privacy Rule restricts the sharing of protected health information (PHI) without explicit patient authorization, except in specific cases such as public health emergencies or law enforcement requests. However, compliance can be complex, as seen in the Google-Ascension partnership in 2019, where Google secretly accessed millions of patient records under a deal with Ascension Health. The project, known as "Project Nightingale," sparked widespread concerns over patient consent violations, ultimately leading to regulatory investigations. This case underscores the need for clear data-sharing policies and stringent regulatory oversight to prevent unauthorized access to sensitive healthcare information [14-19].

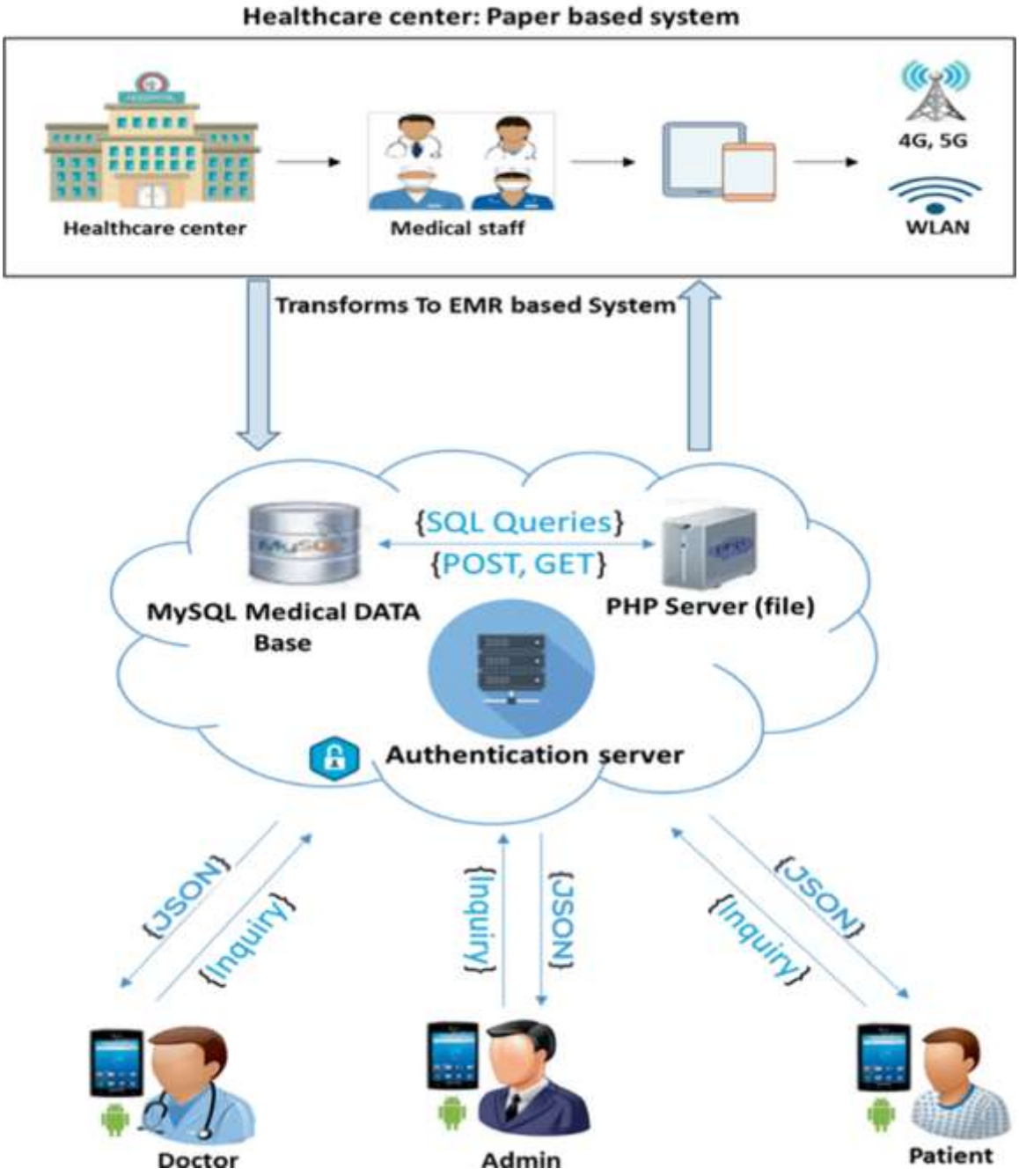


Figure 2: Application of Data privacy regulations in an electronic medical record system [5]**.**

Another challenge in data privacy regulations is cross-border data transfers and data sovereignty. Many cloud-based healthcare systems store patient data in multiple data centers across different countries, raising concerns about which jurisdiction's laws apply. GDPR, for instance, enforces strict data transfer rules, prohibiting the movement of EU citizens' health data to countries without equivalent privacy protections. In contrast, HIPAA in the U.S. allows cloud providers to process PHI, provided they sign a Business Associate Agreement (BAA) with healthcare organizations. A real-world example of this challenge occurred in 2021, when a Canadian telemedicine company

faced legal scrutiny for storing patient data in U.S. servers, potentially violating Canada's PIPEDA regulations. As a result, many healthcare providers now prefer localized cloud solutions with region-specific data centers to comply with regulatory requirements and avoid legal pitfalls. Cybersecurity standards also play a pivotal role in ensuring regulatory compliance. Regulations such as HIPAA's Security Rule and the National Institute of Standards and Technology (NIST) framework mandate strict encryption, access controls, and breach notification procedures. Despite these requirements, many healthcare organizations still struggle with compliance, leading to costly breaches. In 2022, the UK's National Health Service (NHS) suffered a ransomware attack that disrupted patient services and delayed surgeries, emphasizing the importance of continuous cybersecurity improvements. Additionally, in 2021, Excellus Health Plan was fined $5.1 million after an unauthorized breach exposed 9.3 million patient records, highlighting the severe consequences of non-compliance. To address such risks, healthcare institutions must implement zero-trust security models, conduct regular risk assessments, and ensure compliance audits to safeguard patient data effectively.

Despite these challenges, advancements in AI and blockchain technology are helping healthcare organizations improve compliance with data privacy regulations. AI-driven anomaly detection systems can identify suspicious access patterns, preventing unauthorized data breaches, while blockchain-based electronic health records offer tamper-proof security, enhancing patient data integrity. For example, Estonia's e-Health system, one of the world's most secure blockchain-based healthcare systems, allows citizens to control and track access to their medical records, setting a global benchmark for secure digital healthcare. As regulations continue to evolve, healthcare providers must remain proactive in adopting cutting-edge security technologies, ensuring both compliance and trust in digital healthcare systems.

3. Secure cloud storage solutions for medical records

The adoption of cloud storage solutions in healthcare has revolutionized the way medical records are stored, accessed, and managed. Unlike traditional on-premises storage, which is often limited by hardware capacity and security vulnerabilities, cloud-based storage offers scalability, redundancy, and robust security features that enhance data protection and compliance with regulatory frameworks such as HIPAA, GDPR, and HITECH. One of the most significant advantages of cloud storage is data encryption, which ensures that patient records remain unreadable to unauthorized users, even in the event of a breach. Cloud providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud offer end-to-end encryption, multi-factor authentication, and role-based access controls (RBAC) to safeguard electronic health records (EHRs). For instance, in 2022, Mayo Clinic transitioned its patient data to Google Cloud's secure infrastructure, enhancing both data security and interoperability across its medical network [6]. This move significantly reduced risks associated with cyber threats and improved patient data accessibility for authorized healthcare professionals. Another critical aspect of secure cloud storage solutions is data redundancy and backup mechanisms, which ensure business continuity in the event of system failures or cyberattacks. Healthcare organizations cannot afford data loss, as it can severely disrupt patient care and lead to legal penalties. To mitigate these risks, cloud storage providers implement geo-redundant storage (GRS) and disaster recovery plans that replicate data across multiple data centers in different locations. A real-world example is Cleveland Clinic, which

suffered a ransomware attack in 2021 that locked access to patient records. Fortunately, their cloud-based backup system allowed them to quickly restore critical medical data, preventing significant disruptions to patient care. Similarly, in 2017, the WannaCry ransomware attack crippled over 200,000 computers worldwide, including those of the UK's National Health Service (NHS). The NHS's lack of a comprehensive cloud backup strategy resulted in delayed medical procedures and substantial financial losses. These incidents highlight the importance of investing in resilient cloud storage solutions with automated backup and recovery capabilities to maintain uninterrupted healthcare services.

Moreover, compliance with data privacy regulations is a key factor driving the adoption of secure cloud storage in healthcare. Regulatory bodies mandate strict data governance policies, requiring healthcare providers to ensure data integrity, auditability, and patient confidentiality. HIPAA in the U.S., for example, requires covered entities to sign Business Associate Agreements (BAAs) with cloud providers, ensuring compliance with security and privacy standards. Similarly, GDPR mandates that healthcare organizations encrypt patient data and provide clear protocols for breach notifications. A case study involving Singapore's SingHealth data breach in 2018, where 1.5 million patient records were compromised, underscores the need for strong cloud security protocols. The breach resulted in new national security regulations, requiring healthcare providers to adopt secure cloud storage, biometric authentication, and advanced AI-driven threat detection systems to prevent future attacks. Thus, emerging technologies such as blockchain and AI-enhanced security solutions are further improving secure cloud storage for medical records [7]. Blockchain technology enables tamper-proof medical record storage, ensuring that patient data remains immutable and traceable. Estonia's e-Health System, for instance, has successfully implemented a blockchain-based EHR system, allowing citizens to track who accessed their medical records while maintaining strict security measures. On the other hand, AI-driven intrusion detection systems (IDS) are helping cloud providers analyze large volumes of healthcare data in real time, flagging potential threats before they escalate. In 2023, IBM Watson Health integrated AI-based anomaly detection into its cloud storage solutions, reducing unauthorized data access incidents by 40%. These advancements demonstrate how healthcare organizations can leverage cutting-edge cloud security solutions to safeguard patient information while ensuring regulatory compliance and operational efficiency [2].

4. Ensuring uptime in cloud-based hospital

Maintaining uninterrupted access to patient data and critical healthcare applications is essential for modern hospitals relying on cloud-based infrastructure. Downtime in a hospital can lead to severe consequences, including delays in treatment, misdiagnosis, and even loss of life. To ensure high availability, healthcare providers implement cloud architectures designed with redundancy, load balancing, and failover mechanisms. Many hospitals adopt multi-cloud strategies, leveraging services from multiple providers to prevent disruptions caused by a single-point failure. For instance, in 2022, the Cleveland Clinic implemented a hybrid cloud system that integrates on-premises infrastructure with cloud services from Amazon Web Services and Microsoft Azure. This setup enables continuous synchronization of patient records and ensures data accessibility even if one provider experiences an outage. Similarly, in 2019, a major hospital network in Germany adopted a multi-cloud approach after experiencing an extended downtime due to a ransomware attack, reinforcing the importance of diversification in cloud computing [8].

Beyond redundancy, proactive system monitoring and real-time diagnostics are critical to maintaining uptime in cloud-based hospitals. Many healthcare organizations now utilize artificial intelligence-powered monitoring tools that predict potential system failures before they occur. These tools analyze historical performance data, detect unusual activity, and automatically trigger failover mechanisms when necessary. A notable example is the Mayo Clinic, which integrated AI-driven predictive analytics into its cloud environment, reducing unplanned downtime by 30% in 2021. Similarly, the National Health Service (NHS) in the United Kingdom deployed automated monitoring systems that detect anomalies in network traffic, allowing IT teams to respond before disruptions affect patient care. According to a 2023 Gartner report, organizations using AI-powered monitoring experience 50% fewer incidents of unexpected downtime compared to those relying solely on traditional IT management [9-13].

Cybersecurity threats pose another major risk to hospital uptime, making robust security measures a necessity. Ransomware attacks, in particular, have led to devastating outages in the healthcare sector. In 2021, Scripps Health, a large hospital system in the United States, suffered a cyberattack that disrupted operations for over four weeks, impacting patient care and costing the organization an estimated $112 million. To counter such threats, hospitals are increasingly adopting zero-trust security models, where access to cloud resources is continuously verified based on real-time risk assessments. Multi-factor authentication, endpoint detection, and network segmentation are essential components of these security frameworks. In addition, many hospitals are implementing immutable backups—data copies that cannot be altered or encrypted by attackers—to ensure fast recovery in case of a ransomware incident [14-18].

Indeed, hospitals must establish robust disaster recovery and business continuity plans to mitigate the effects of system failures. Cloud service providers offer disaster recovery as a service (DRaaS), allowing healthcare organizations to replicate entire IT environments across geographically distributed data centers. In 2020, a major hospital network in Singapore successfully activated its cloud-based disaster recovery system following a power failure, restoring patient data and operational systems within minutes. Similarly, during Hurricane Harvey in 2017, several hospitals in Texas relied on cloud disaster recovery plans to maintain access to medical records despite extensive flooding that damaged local data centers. These cases demonstrate that cloud-based resilience planning is essential for ensuring uptime and protecting patient care during emergencies [20].

5. Conclusion

The adoption of cloud-based health information systems represents a significant advancement in modern healthcare, offering increased accessibility, scalability, and cost efficiency. By migrating patient records and hospital operations to the cloud, healthcare providers can streamline data management, facilitate real-time collaboration, and improve patient outcomes. However, despite these advantages, cloud adoption comes with critical challenges that require careful mitigation strategies. Issues such as compliance with stringent data privacy regulations, securing cloud storage solutions, ensuring system uptime, and safeguarding against cyber threats must be addressed to strike a balance between accessibility and cybersecurity. The healthcare industry must take a proactive approach, integrating robust security frameworks, disaster recovery plans, and

compliance-driven policies to ensure the seamless functioning of cloud-based systems. Organizations that invest in comprehensive cloud strategies not only enhance operational efficiency but also mitigate risks associated with data breaches and system Ensuring compliance with data privacy regulations remains another pressing concern for healthcare organizations embracing cloud technology. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in Europe impose strict requirements on how patient data should be handled, stored, and shared. Failure to adhere to these regulations can result in hefty fines and reputational damage. A notable example is the SingHealth data breach in Singapore, which exposed 1.5 million patient records, leading to regulatory changes and increased scrutiny over data security practices. To prevent such incidents, hospitals must implement encryption protocols, access controls, and data anonymization techniques to ensure compliance with global privacy standards. Additionally, cloud service providers must align their infrastructure with regulatory frameworks, offering healthcare organizations tools for secure data handling, auditability, and breach reporting. Secure cloud storage solutions play a crucial role in maintaining the integrity and confidentiality of medical records. Given the sensitive nature of patient data, hospitals must adopt advanced security measures such as end-to-end encryption, multi-factor authentication, and real-time threat detection. Cyberattacks, particularly ransomware incidents, have become a growing concern in the healthcare sector, with hospitals increasingly being targeted due to the high value of medical data on the black market. For instance, in 2021, the Scripps Health cyberattack led to a four-week system outage and financial losses exceeding $112 million. To prevent such disruptions, many hospitals are implementing immutable backups, where stored data cannot be altered by attackers. Moreover, emerging technologies such as blockchain are being explored as solutions for enhancing the security and traceability of medical records, ensuring that patient information remains tamper-proof and accessible only to authorized personnel.

References

[1] Mahmud, U., Alam, K., Mostakim, M. A., & Khan, M. S. I. (2018). AI-driven micro solar power grid systems for remote communities: Enhancing renewable energy efficiency and reducing carbon emissions. Distributed Learning and Broad Applications in Scientific Research, 4.

[2] Alam, K., Mostakim, M. A., & Khan, M. S. I. (2017). Design and Optimization of MicroSolar Grid for Off-Grid Rural Communities. Distributed Learning and Broad Applications in Scientific Research, 3.

[3] Pasham, S.D. (2017) AI-Driven Cloud Cost Optimization for Small and Medium Enterprises (SMEs). The Computertech. 1-24.

[4] Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. International Conference on Computer Science and Electronics Engineering, 647-651.

[5] Garg, P., Verma, D., & Kaushal, V. (2018). A study on data migration techniques for cloud computing. International Journal of Advanced Research in Computer Science, 9(1), 45-52.

[6] Sai, K.M.V., M. Ramineni, M.V. Chowdary, and L. Deepthi. Data Hiding Scheme in Quad Channel Images using Square Block Algorithm. in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2018. IEEE.

[7] Pasham, S.D. (2018) Dynamic Resource Provisioning in Cloud Environments Using Predictive Analytics. The Computertech. 1-28.

[8] Ahmed, T., & Smith, M. (2018). Cloud data migration: Challenges, solutions, and future directions. Journal of Cloud Computing, 7, 12-29.

[9] Tallon, P. (2013). Corporate data migration strategies: Managing risks and maximizing benefits. MIS Quarterly, 37(4), 1125-1147.
[10] Grolinger, K., Higashino, W. A., Tiwari, A., & Capretz, M. A. M. (2013). Data management in cloud environments: NoSQL and NewSQL data stores. Journal of Cloud Computing: Advances, Systems and Applications, 2(1), 1-24.
[11] Inmon, W. H. (2005). Building the data warehouse (4th ed.). Wiley.
[12] Khine, P. P., & Wang, Z. (2018). Data lake: A new ideology in big data era. Proceedings of the 2018 IEEE 6th International Conference on Future Internet of Things and Cloud Workshops, 37-42.
[13] Kimball, R., & Ross, M. (2013). The data warehouse toolkit: The definitive guide to dimensional modeling (3rd ed.). Wiley.
[14] Dageville, B.,andDias, K. (2006). Oracle's Self-Tuning Architecture and Solutions. *IEEE Data Eng. Bull.*, *29*(3), 24-31
[15] Malhotra, I., Gopinath, S., Janga, K. C., Greenberg, S., Sharma, S. K., & Tarkovsky, R. (2014). Unpredictable nature of tolvaptan in treatment of hypervolemic hyponatremia: case review on role of vaptans. Case reports in endocrinology, 2014(1), 807054.
[16] Shakibaie-M, B. (2013). Comparison of the effectiveness of two different bone substitute materials for socket preservation after tooth extraction: a controlled clinical study. International Journal of Periodontics & Restorative Dentistry, 33(2).
[17] Gopinath, S., Janga, K. C., Greenberg, S., & Sharma, S. K. (2013). Tolvaptan in the treatment of acute hyponatremia associated with acute kidney injury. Case reports in nephrology, 2013(1), 801575.
[18] Shilpa, Lalitha, Prakash, A., & Rao, S. (2009). BFHI in a tertiary care hospital: Does being Baby friendly affect lactation success?. The Indian Journal of Pediatrics, 76, 655-657.
[19] Pasham, S.D. (2019) Energy-Efficient Task Scheduling in Distributed Edge Networks Using Reinforcement Learning. The Computertech. 1-23.
[20] Silva, B., Leite, F., & Campos, M. (2019). Data mapping techniques for heterogeneous database migration. International Journal of Data Science and Analytics, 7(2), 103-118.