Journal of Science and Technology

ISSN: 2456-5660 Volume 5, Issue 06 (December -2020)

www.jst.org.in *DOI: https://doi.org/10.46243/jst.2020.v5.i06.pp178-189*

Improving Security Control in Cloud Computing for Healthcare Environments

Mohanarangan Veerappermal Devarajan

Ernst & Young (EY), Sacramento, USA

Email ID: gc4mohan@gmail.com

ABSTRACT

Cloud computing has transformed a variety of businesses by providing scalable and cost-effective data storage and management options. However, sensitive sectors such as healthcare face major security issues due to the extremely sensitive nature of patient data and stringent regulatory regulations. The purpose of this study is to solve security concerns in cloud computing for healthcare contexts by presenting a comprehensive security management system. The framework includes risk assessment, security implementation, continuous monitoring, compliance management, and the integration of modern security technologies. Potential threats and weaknesses in the cloud environment are discovered through a thorough risk assessment, enabling the adoption of appropriate security measures like as authentication, encryption, and intrusion detection and prevention systems. Continuous monitoring ensures early detection of questionable actions and adherence to regulatory norms. Furthermore, the use of modern technologies such as blockchain and multi-factor authentication improves the security posture of cloud-based healthcare systems. Case studies from healthcare organizations such as the Mayo Clinic and Cleveland Clinic demonstrate how cloud computing solutions may be successfully implemented while ensuring data security and compliance. By implementing the proposed framework, healthcare companies can effectively mitigate security risks and reap the benefits of cloud computing to improve patient care and operational efficiency while protecting the integrity, availability, and privacy of sensitive healthcare data.

Keywords: Security Management, Risk Assessment, Blockchain, Risk Mitigation, Continuous Monitoring Authentication, Encryption, HIPAA, GDPR, Data Integrity, Confidentiality.

1. INTRODUCTION

Cloud computing has greatly altered several industries by providing scalable, adaptable, and cost-effective solutions for data storage and management. However, with these advantages come significant security issues, particularly in sensitive industries like healthcare. Security management in cloud computing for healthcare is crucial due to the highly sensitive nature of medical data and the stringent regulatory regulations that regulate its usage and protection.

Security management in cloud computing is putting in place methods, rules, and technology to protect cloud-stored data from unauthorized access, breaches, and other threats. In the healthcare industry, this includes safeguarding patient records, preserving data privacy, and ensuring the quality and availability of healthcare services. The goal is to reduce risks connected with cloud computing while maximizing its benefits to improve healthcare delivery.

Cloud computing originated in the 1960s with the concept of time-sharing and virtual machines. However, it wasn't until the late 1990s and early 2000s that cloud computing took on its present shape, with the introduction of services like Amazon Web Services (AWS). The healthcare industry, which has generally been conservative about embracing new technology due to privacy concerns, has increasingly adopted cloud computing, pushed by the need for better data management, cost savings, and improved patient care.

Cloud computing in healthcare is implemented using a variety of tools and platforms. Leading cloud service providers are:

Amazon Web Services (AWS) provides a portfolio of cloud services specifically designed for healthcare, such as data storage, analytics, and compliance tools.

Microsoft Azure offers a variety of cloud-based solutions for healthcare, with a focus on data security, interoperability, and regulatory compliance.

Google Cloud Platform (GCP): Provides comprehensive data storage and machine learning capabilities, with an emphasis on security and compliance.

IBM Cloud: Known for its emphasis on security, IBM Cloud offers a variety of healthcare-specific solutions, such as data analytics and AI-powered insights.

These systems provide the infrastructure and technologies required to handle, analyze, and protect healthcare data in the cloud.

Several healthcare businesses have successfully deployed cloud computing solutions. For example, Mayo Clinic and Cleveland Clinic have collaborated with cloud providers such as Google Cloud and Microsoft Azure to improve data management capabilities. These collaborations allow these institutions to use modern analytics, improve patient care, and maintain strict security measures.

Protection of patient data, preservation of data integrity, availability, regulatory compliance, and trust-building are security management's core goals in healthcare cloud computing. Assuring correctness and consistency throughout the data's lifecycle, safeguarding accessibility without compromising performance, and preventing breaches and illegal access are all necessary to achieve this. To remain in compliance, adherence to laws like GDPR and HIPAA is essential. The integrity of healthcare data and the dependability of cloud-based services can be strengthened by healthcare providers by putting strong data protection mechanisms in place and building and maintaining trust among patients, providers, and stakeholders.

Although cloud computing has come a long way, there are still research gaps about how to integrate security measures in an efficient manner. The existing body of literature emphasizes the need for more thorough frameworks specifically designed to handle the unique security issues associated with cloud computing in the healthcare industry. In particular, there are few thorough studies that concentrate on the application of cutting-edge security measures. Furthermore, not much research has been done on how new technologies like blockchain and artificial intelligence affect cloud security in healthcare environments. Furthermore, there is a conspicuous lack of efficacious risk mitigation tactics that are particularly customized to the distinct complexities of healthcare settings. In order to preserve patient data and promote confidence in cloud-based healthcare services, it is critical to fill up these research gaps and guarantee the ongoing development and effectiveness of security measures in healthcare cloud computing.

The adoption of cloud computing by healthcare enterprises presents unique security challenges, mostly due to the sensitive nature of patient data and strict legal requirements. The main difficulty is coming up with and putting into practice strong security management plans that successfully reduce risks such as illegal access, data breaches, and compliance infractions while utilizing cloud computing's benefits to improve healthcare services. This calls for the creation of customized security measures, a thorough examination of the risks unique to clouds, constant monitoring, and adjustment in response to new threats and developments in technology. Healthcare companies may safeguard patient information, maintain regulatory compliance, and maximize cloud computing's advantages for better healthcare delivery by proactively tackling these issues.

Cloud computing security is still a recurring problem in healthcare that calls for constant innovation and attention to detail. Healthcare businesses can safely use cloud computing to improve patient care and operational efficiency by using comprehensive security procedures and having a complete understanding of unique dangers. Effective navigation of the changing security landscape and protection of sensitive healthcare data in the cloud require additional study and cooperation amongst parties. Healthcare institutions may strengthen their security posture and build confidence in the use of cloud technology to advance healthcare services by placing a high priority on collaboration and continuous improvement.

2. LITERATURE SURVEY

Griebel et al. (2015) explore the potential applications and drawbacks of cloud computing in healthcare in their scoping review. In addition to examining current developments, applications, and research needs, they evaluate the possible effects on patient care, data security, and operational effectiveness. They also assess tactics and best practices for integrating cloud solutions into healthcare environments successfully.

Sultan (2014) perform a thorough examination of the advantages of cloud computing for healthcare delivery, emphasizing its affordability, scalability, and accessibility. They also cover the difficulties and roadblocks that arise when putting cloud solutions into practice, like data security and legal compliance. By analyzing effective case studies and creative applications, they demonstrate how cloud computing enhances operational effectiveness and patient care. They also go over ways to reduce risks and take advantage of cloud computing prospects in the healthcare industry. Finally, they discuss potential future developments and paths for using cloud computing technology into healthcare delivery networks.

Abdelaziz et al. (2018) present a cloud computing infrastructure-specific machine learning framework intended for use in healthcare applications. They show how resource allocation, patient outcomes, and service quality can all be improved by using machine learning algorithms to analyze healthcare data. The writers talk about how cloud-based technologies and machine learning models can be integrated to provide real-time analytics and decision assistance. The effectiveness of machine learning in enhancing many facets of healthcare delivery in cloud environments is illustrated through case studies. In addition, they discuss issues like model interpretability, interoperability, and data protection and offer techniques to get over them when using cloud-based machine learning systems for healthcare.

Mehraeen et al. (2017) do a comprehensive analysis of security risks associated with cloud computing implementations in the healthcare industry. They discuss particular issues that healthcare companies deal with, such as risks to the integrity, confidentiality, and privacy of data. Cloud security is examined in relation to regulatory compliance standards like GDPR and HIPAA. Along with cutting-edge technology like encryption and threat detection systems targeted at fortifying security in healthcare cloud settings, best practices and methods for reducing risks and boosting resilience are examined.

Ali et al. (2018) provide an extensive analysis of cloud computing's potential in healthcare. They explore opportunities for improving healthcare delivery, emphasizing scalability, accessibility, and cost-effectiveness. Challenges like data security, regulatory compliance, and interoperability are identified and examined. The authors overview various applications of cloud computing in healthcare, including telemedicine, electronic health records (EHR), and predictive analytics. Real-world case studies highlight transformative impacts of cloud-enabled healthcare solutions. Future directions and advancements are considered, along with recommendations for addressing challenges and maximizing opportunities in leveraging cloud computing for enhancing healthcare services.

Ermakova et al. (2013) provide a thorough analysis of the body of literature in order to clarify the state of the field research on cloud computing in the healthcare industry. They include implementation obstacles, benefits, and applications in their evaluation of recent studies and publications. Analysis is done on trends and new themes in cloud computing research that are relevant to healthcare, like patient-centered care and data security. The writers provide a thorough grasp of the topic by synthesizing empirical research, case studies, and theoretical frameworks. In order to progress the topic of cloud computing in healthcare, they point out gaps in the literature and potential areas for further investigation. In an effort to support decision-making and innovation in this field, they also address the implications of current study findings for healthcare professionals, legislators, and technology developers.

Critical security and privacy issues are examined by Gavrilov and Trajkovik (2012) while deploying cloud computing systems in healthcare settings. Their investigation dives into particular problems including regulatory compliance issues and data breaches and illegal access. Cloud environments in the healthcare industry are subject to certain regulations and standards, including GDPR, HITECH, and HIPAA. In order to protect sensitive healthcare data, the authors examine security precautions and best practices, such as encryption and access limits. Third-party cloud service provider risks are assessed, and methods for guaranteeing security management accountability and transparency are suggested. In order to handle changing threats and preserve data integrity and confidentiality in the cloud, they stress the significance of ongoing monitoring, auditing, and incident response procedures.

A methodical approach to protecting privacy in cloud computing infrastructures for processing and storing healthcare data is presented by Kundalwal et al. (2018). Their thorough privacy framework takes care of cloud-based healthcare data availability, confidentiality, and integrity. They recognize and evaluate privacy issues and healthcare-specific regulations, including GDPR, HIPAA, and local data protection laws. To reduce privacy threats, privacy-enhancing technologies are described, such as data encryption and access controls. To make sure privacy regulations are followed, the writers assess the capabilities of cloud service providers and the terms of their contracts. We talk about governance, risk management, and audit procedures to ensure accountability and privacy assurance over the whole cloud data lifecycle.

Cloud computing security is examined by Ali et al. (2015); advantages, difficulties, important precautions, new tactics, and legal issues are all covered. Centralized administration, automatic upgrades, and scalable security mechanisms are some advantages that lead to improved security. Difficulties include shared responsibility models, data breaches, and regulatory complications. Critical safety precautions include strong encryption, restricted access, and ongoing surveillance. It is explored how to solve changing difficulties with emerging technologies like cloud-native security tools and zero-trust architecture. Building confidence between providers and users is facilitated by adherence to industry standards and regulatory frameworks, which also encourage best practices in security.

3. METHODOLOGY

This technique describes an all-encompassing approach to risk assessment, security measure deployment, ongoing monitoring, and compliance management for cloud computing in the healthcare industry. The approach is divided into multiple essential parts, each of which focuses on a different facet of cloud security management.

3.1. Risk Assessment

The first step in locating potential security threats and weaknesses in the cloud environment is risk assessment. This procedure includes:

Identifying Assets: This entails locating and comprehending the crucial cloud infrastructure assets, such as databases, apps, and patient records. Identifying the assets in the area is essential to creating suitable security protocols.

Threat Modeling: This involves locating possible risks that can jeopardize the cloud environment's security. These dangers could be virus assaults, illegal access attempts, or data breaches. It is possible to plan for proactive security by being aware of these hazards.

Vulnerability Analysis: It's critical to assess cloud infrastructure vulnerabilities. Weaknesses or holes in security that could be used by attackers are known as vulnerabilities. Finding potential security flaws can be aided by carrying out a thorough vulnerability study.

Risk Evaluation: After threats and vulnerabilities have been identified, it's critical to evaluate the possibility that these threats would exploit the vulnerabilities and the possible consequences of doing so. By ranking hazards according to their seriousness, this risk rating helps allocate resources for risk reduction initiatives.

$$Risk = Likelihood\ of\ Threat \times Impact\ of\ Threat$$

Likelihood of Threat: This is the likelihood or chance that a threat or possible risk event will materialize. It evaluates the likelihood that a specific danger will manifest as a real issue or incident.

Impact of Threat: This is a reference to the extent or gravity of the repercussions in the event that the threat materializes. It assesses the potential injury or damage in the event that the danger materializes.

The total risk associated with a danger can be calculated by multiplying the likelihood of the threat by its impact. In essence, it measures the degree of risk or anxiety that a particular threat scenario poses.

This formula is frequently used to prioritize risks and distribute resources efficiently in a variety of industries, including project management, insurance, and cybersecurity. Organizations can reduce the negative effects on their operations or objectives by allocating resources and choosing risk mitigation techniques based on an assessment of the likelihood and impact of prospective threats.

3.2. Implementation of Security Measures

The risk assessment must be used to determine which security measures are necessary to apply. Among these actions are:

By limiting unwanted access and data breaches, authentication and access control make sure that only people with permission can access critical resources. Data encryption is essential for safeguarding information because it prevents illegal access or alteration by rendering data unintelligible during transmission and storage.

Systems for detecting and preventing intrusions (IDPS) act as proactive barriers against malicious activity by continuously scanning the cloud environment for unusual activity and swiftly addressing any dangers that may arise.

By combining and analyzing security data from several sources, Security Information and Event Management (SIEM) systems are essential for real-time security incident monitoring and management. This allows for the prompt identification and remediation of security risks and breaches.

Combining these steps strengthens cloud-based systems' security posture by reducing risks and guaranteeing the availability, confidentiality, and integrity of critical information and resources.

3.3. Continuous Monitoring

Sustaining the cloud environment's security requires ongoing monitoring. Constant observation of the cloud environment identifies questionable activity early on, strengthening security against possible intrusions. Frequent security audits maintain compliance by ensuring that security policies and laws are followed. To enable the quick discovery and handling of security issues, log management entails gathering and examining data logs from many sources. When combined, these procedures strengthen cloud-based systems' security posture, allowing for proactive threat mitigation and guaranteeing data integrity and confidentiality.

3.4. Compliance Management

Adherence to regulatory requirements is crucial in the healthcare industry. Respecting particular healthcare laws such as GDPR in the EU and HIPAA in the US is part of this. It is imperative to establish and implement security policies that conform to industry best practices and these standards. Staff members are guaranteed to be knowledgeable about security measures and processes by holding periodic training sessions. Healthcare businesses may maintain data security standards, safeguard patient confidentiality, and reduce the likelihood of regulatory infractions by giving regulatory compliance, policy development, and employee training first priority.

3.5. Advanced Security Technologies

Cloud environments in the healthcare industry can greatly improve their security posture by implementing state-of-the-art security technology. In order to improve overall defensive systems, artificial intelligence (AI) is essential for seeing threats, recognizing anomalies, and reacting quickly to security problems. Because blockchain technology is decentralized and immutable, it plays a critical role in protecting patient records and maintaining data integrity. Furthermore, by requiring several verification elements, Multi-Factor Authentication (MFA) fortifies authentication methods and increases security against unwanted access. Healthcare companies may strengthen their cloud infrastructures, reduce risks, and maintain the security and confidentiality of critical patient data by utilizing these cutting-edge solutions.

3.6. Framework for Security Management

All of the aforementioned elements are included in the suggested framework to create a unified framework for handling security in cloud computing for healthcare.

Table 1: Security Measures and their Impact.

Security Measure	**Impact on Security**
Authentication and Access Control	stops unwanted access to private information
Encryption	prevents access to data while it is in transit
IDPS	detects and stops harmful activity
SIEM	permits quick reaction to security incidents in real time
Continuous Monitoring	guarantees constant watchfulness against security risks
Compliance Management	Guarantees compliance with legal mandates.
AI and Blockchain	Improves security with modern technology.

The table 1 lists different security measures along with how they improve security. While encryption protects data in transit, authentication and access control stop unwanted access. IDPS stops malicious activity by detecting it. SIEM makes incident response in real time possible. Vigilant danger detection is ensured by ongoing monitoring. Adherence to legal regulations is ensured by compliance management. Blockchain and AI use cutting-edge technologies to provide better protection, which improves security.

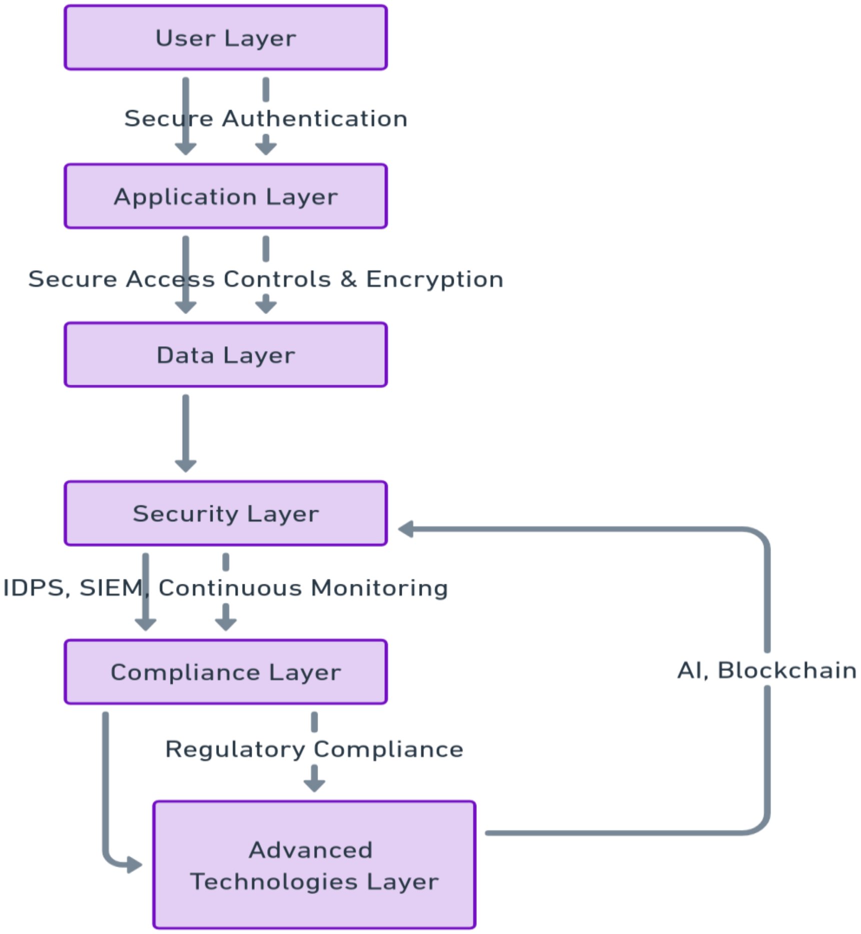

Figure 1: Security management in cloud computing for healthcare.

The Figure 1 design consists of numerous levels, each addressing a different area of security management.

- ***User Layer:*** Users gain access to healthcare services through secure authentication techniques.
- ***Application Layer:*** Applications communicate securely with data storage and processing services using encryption and access controls.
- ***Data Layer:*** Data is stored in encrypted formats and accessible via secure means.
- ***Security Layer:*** Security techniques such as IDPS, SIEM, and continuous monitoring technologies are used to safeguard the cloud environment.
- ***Compliance Layer:*** Ensures compliance with regulatory standards and policies.
- ***Advanced Technologies Layer:*** Uses AI and blockchain to improve security and data integrity.

3.8. Case Studies

Case Study 1: Mayo Clinic

Mayo Clinic has used Google Cloud for data analytics and patient care. Mayo Clinic protects patient data and complies with HIPAA rules by employing Google's security capabilities.

Case Study 2: Cleveland Clinic

Cleveland Clinic relies on Microsoft Azure for its cloud computing needs. Cleveland Clinic can effectively and securely handle patient data using Azure's sophisticated security and compliance solutions.

The technique for security management in cloud computing for healthcare includes a systematic approach to risk identification, security implementation, and continual monitoring and compliance. Healthcare firms can reduce security risks and improve their cloud computing infrastructure by implementing sophisticated technologies and following best practices. This complete strategy is critical to ensuring the integrity, availability, and privacy of sensitive healthcare data.

4. RESULT AND DISCUSSION

The approach described offers a thorough foundation for handling security in cloud computing for medical purposes. Healthcare businesses can effectively manage security threats by carrying out comprehensive risk assessments, putting in place suitable security measures, keeping a close eye on the environment, and making sure that regulatory standards are being followed. By identifying risks and preserving data integrity, integrating cutting-edge technology like blockchain and artificial intelligence (AI) improves security. The architecture diagram, which covers user access, application communication, data storage, security methods, compliance, and cutting-edge technologies, demonstrates the multi-layered approach to security management. Mayo Clinic and Cleveland Clinic case studies show how to successfully deploy cloud computing technologies while following stringent regulatory guidelines. All things considered, this methodology offers healthcare organizations an organized way to strengthen security protocols, protecting patient information and guaranteeing the accuracy and accessibility of cloud-based healthcare services.

5. CONCLUSION

In summary, strong protection of sensitive patient data is urgently needed, and this is addressed by the security management framework described for cloud computing in healthcare settings. Healthcare companies can reduce dangers and take advantage of cloud technology by methodically evaluating risks, putting in place suitable security measures, and guaranteeing continued monitoring and compliance. The efficacy of these tactics in practical implementations is illustrated through case studies such as Cleveland Clinic and Mayo Clinic. In order to protect data integrity, availability, and privacy and to build confidence in cloud-based healthcare services, it is imperative that modern technology and best practices be embraced.

6. FUTURE ENHANCEMENT

The integration of cutting-edge technologies like homomorphic encryption to guarantee privacy-preserving data analysis, decentralized identity management systems utilizing blockchain for secure authentication, and the creation of AI-driven anomaly detection systems for proactive threat identification and response are some of the future improvements for security management in cloud computing for healthcare.

REFERENCES

1. Gribel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., ... & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. BMC medical informatics and decision making, 15(1), 1-16.
2. Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management, 34(2), 177-184.
3. Abdelaziz, A., Elhoseny, M., Salama, A. S., & Riad, A. M. (2018). A machine learning model for improving healthcare services on cloud computing environment. Measurement, 119, 117-128.
4. Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: a systematic. Global journal of health science, 9(3), 157-168.
5. Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, 146-158.
6. Ermakova, T., Huenges, J., Erek, K., & Zarnekow, R. (2013). Cloud computing in healthcare–a literature review on current state of research.
7. Gavrilov, G., & Trajkovik, V. (2012). Security and privacy issues and requirements for healthcare cloud computing. ICT Innovations.
8. Kundalwal, M. K., Singh, A., & Chatterjee, K. (2018, October). A privacy framework in cloud computing for healthcare data. In 2018 International conference on advances in computing, communication control and networking (ICACCCN) (pp. 58-63). IEEE.
9. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information sciences, 305, 357-383.