ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

Classification of Cloud Services and Security Analysis in Healthcare Sector

K. Divya Tejaswini[1], Shaik Kaneez Fathima[2], Shaik Maseera[3], Shaik Pasupula Shahista[4], Vadla Anjali[5], IndlaSuneela[6]

[1,2,3,4,5]Chaitanya Bharathi Institute of Technology, Proddatur, A.P, India.

divyasunny.k23@gmail.com[1], kaneezshaik16@gmail.com[2], shaikmaseera44@gmail.com[3], spshahista@gmail.com[4], anjalivadla03@gmail.com[5], suneelaindla534@gmail.com[6]

ABSTRACT

Cloud computing has become an essential technology in the healthcare industry, offering scalable, cost-effective, and flexible solutions for managing vast amounts of data, improving patient care, and enhancing operational efficiency. The three primary types of cloud services—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—each play a unique role in healthcare organizations, supporting everything from data storage and management to software applications and platform development. Despite the many benefits, the adoption of cloud services in healthcare also introduces significant security and privacy challenges, particularly with regard to safeguarding sensitive patient information. This paper explores the classification of cloud services in the healthcare sector, examining how each model is applied to meet the diverse needs of healthcare providers. It also analyzes the security implications associated with cloud computing, focusing on critical issues such as data encryption, access controls, regulatory compliance (e.g., HIPAA and GDPR), and third-party risk management. A comprehensive understanding of these cloud service models and security concerns is essential for healthcare organizations to ensure the protection of patient data, meet legal and ethical standards, and fully leverage the advantages of cloud technologies. Ultimately, this study provides insights into how healthcare organizations can effectively balance the benefits of cloud computing with the need for robust data security measures to optimize patient care and organizational performance.

Keywords: Cloud Services , Risk Assessment , Healthcare Security

I. INTRODUCTION

The healthcare industry is undergoing a significant transformation driven by advancements in technology, with cloud computing playing a pivotal role in this evolution. Cloud services offer healthcare organizations a wide range of tools and infrastructure that enable them to store, manage, and process vast amounts of data more efficiently and cost-effectively. These services include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which provide scalable, flexible, and accessible solutions for healthcare operations.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org





Cloud computing in healthcare allows for greater collaboration, improved patient care, and more streamlined operations. It facilitates real-time access to critical patient information, supports telemedicine, and enables efficient management of electronic health records (EHRs), among other applications. The integration of cloud-based systems also provides healthcare organizations with the ability to scale their IT infrastructure in response to fluctuating demands, without the need for significant capital investment in physical hardware.

However, as with any technology that handles sensitive data, especially in sectors such as healthcare, cloud computing comes with significant security concerns. Patient data is highly sensitive and protected by stringent regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States and GDPR (General Data Protection Regulation) in Europe. Ensuring the security and privacy of this data while leveraging the benefits of cloud technology requires robust security measures, including encryption, access controls, data backup, and disaster recovery protocols.

II. LITERATURE SURVEY

Sinhasane,S.(2019).“Revolutionary Impact of Cloud Solutions on Healthcare.”Discusses the significant changes and challenges in digitizing healthcare services due to legacy systems and the sensitivity of personal information, emphasizing the global struggle in healthcare digitization.

Abrar H., Hussain S. J., Chaudhry J., Saleem K., Orgun M. A., Muhtadi J. A., Valli C (2018). “Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry.”Analyzes the risks associated with cloud sourcing in healthcare, emphasizing the need for comprehensive security measures in cloud computing models within the industry.

III. EXISTING SYSTEM

Compared to security and privacy issues in e-health cloud-based system, it doesn't provide reliable and accurate access control requirements. Patient may not access privileges to their confidential information without following HIPAA regulations. There is a problem to receive threats to the security and privacy of patients' health data, and a widely held belief that these cannot be adequately addressed.

Advantages In Existing Method

- **Cloud Storage**: Allows easy access to patient records from anywhere.
- **Cost-Effective**: Reduces the need for physical infrastructure in hospitals.
- **Data Backup**: Ensures recovery of medical data in case of system failure.
- **Scalability**: Can handle large amounts of healthcare data efficiently.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

Disadvantages

- **Patient's data can be shared** – Increased accessibility raises risks of unauthorized access and misuse.
- **Not secured** – Weak encryption and controls make data vulnerable to breaches and cyberattacks.
- **Chance of privacy disclosure** – Poor data protection may expose sensitive patient information to third parties.

IV. PROPOSED SYSTEM

The proposed scheme offers an eye-catching categorization of cloud benefits and threats in the healthcare sector providing many important tools and applications. In this way, the information exchange and management are boosted because less time is consumed. Adopting cloud services in health sector demands that security issues be taken into consideration. This is made clearer below where some major web-based dangers are analyzed. Cyber-attacks and the fact that authorized users (doctors, nurses and patients) lack knowledge of technical issues are the two most important challenges**.**

Advantages:

No chance of data loss – Cloud storage keeps patient data safe with backups and recovery options.
Highly secured and trustable – Strong security measures protect data from hacking and breaches. **Access authentication with strong passwords and authorization** – Only authorized users can access data using secure login methods.

Architecture/Project Flow:

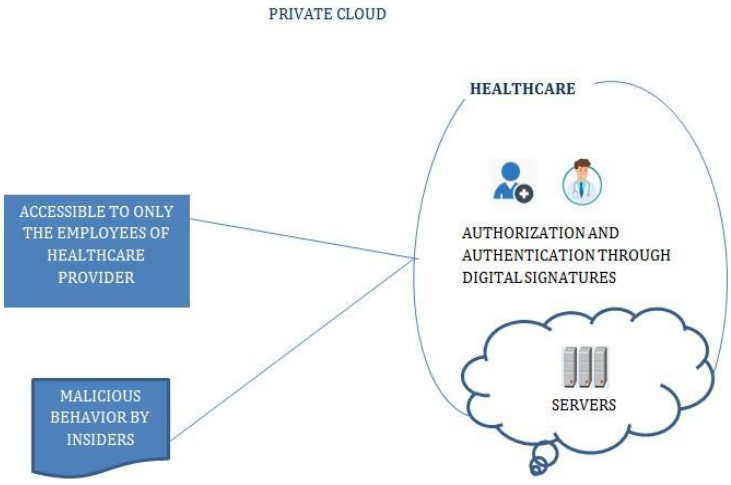


Figure 1 : Shows the Architecture Flow

MODULE:

Doctor:
- Doctor can initially register with their details.
- Then login with valid email id and password and Captcha value.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

- The Doctor can view the patient's details and Appointments.
- The doctor checks the health of the patients and sends reports to the patients.

Patient:

- Patient can initially register with their details
- Then login with valid email id and password and Captcha value.
- Patient can view the doctors and book the appointment.
- Patientscan view the doctors and then book a slot for checkup and view their health reports.

V. CONCLUSION

The existing systems for the classification of cloud services and security analysis in healthcare focus on leveraging a range of cloud service models (IaaS, PaaS, and SaaS) to meet healthcare organizations' diverse needs while ensuring security and compliance. The primary focus is on ensuring patient data privacy, meeting regulatory standards such as HIPAA, and implementing robust security measures such as data encryption, IAM, and continuous compliance monitoring. With cloud services becoming integral to healthcare, ongoing security analysis and the adoption of best practices will be essential to protect sensitive health data from emerging threats.

REFERENCES:

[1] nhasane, S. (2019). Revolutionary Impact of Cloud Solutions on Healthcare. [Online] artner, Inc., https://gtnr.it/2PAcf79, Accessed on 27th February 2020

[2] Spok (2019) "Infographic: How Healthcare Deploys Software as a Service (SaaS)", https://bit.ly/38uLcR4, Accessed on 6th March 2020

[3] Thriveni T. K. and Dr Prashanth C S R (2015) "Real-time threat prediction for cloud-based assets using big-data analytics", https://bit.ly/2YgTbQ6, Accessed on 20th June 2020

[4] Abrar H., Hussain S. J., Chaudhry J., Saleem K.,Orgun M. A., Muhtadi J. A. and Valli C. (2018) "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry", https://bit.ly/38fEEWr, Accessed on 24th February 2020

[5] Zola A. (2018) "How Healthcare Can Benefit from Data Integration",Intersog, https://bit.ly/3aAOtA3, Accessed on 6th March 2020

[6] King T. (2018) "Healthcare Data Integration: 5 Software Tools to Consider", Solutions Review, https://bit.ly/2TvLbZb, Accessed on 6th March 2020

[7] Victoria S. (2018) "3 Types of Collaboration Software Tools to Improve Your Workflow", RubyGarage, https://bit.ly/2Irl7b3, Accessed on 6th March 2020

[8] LaPointe J. (2017) "Top 10 Enterprise Resource Planning (ERP) Vendors By Hospital Use", Revcycle Intelligence, xtelligent Healthcare Media, https://bit.ly/2VTS5ck, Accessed on 7th March 2020

[9] Servercloud Canada (2017) "Reliable, Secure & Compliant Disaster Recovery", https://bit.ly/2Qf88hh, Accessed on 9th March 2020