International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Advanced Cloud Computing for Healthcare: Security Challenges and Solutions in Digital Transformation

Premkumar Ganesan

Technology Leader in Digital Transformation for Government and Public Sector ,Baltimore, Maryland

Abstract: ***Cloud computing has emerged as a pivotal solution for addressing complex digital challenges, yet it continues to face significant security concerns. This study provides a comprehensive analysis of the security challenges inherent in cloud computing and examines potential solutions to mitigate these risks. A systematic review was conducted using databases such as Scopus, PubMed, ScienceDirect, and Web of Science. Studies were meticulously selected based on rigorous inclusion and exclusion criteria, following an initial screening of titles and abstracts. The most relevant studies were then subjected to an in-depth analysis of their full texts to extract key findings. The review identifies critical security challenges, including issues related to data availability, integrity, confidentiality, and network security. Furthermore, it explores essential cloud infrastructure security measures, such as authentication, data classification, encryption, and the use of secure application programming interfaces (APIs). The findings underscore the importance of robust data encryption strategies for enhancing the security of cloud storage and retrieval processes. Additionally, the study addresses several fundamental concerns related to the cloud security engineering process, offering insights into best practices and emerging solutions.***

Keywords: Cloud Computing, Cloud Security, Data Encryption, Network Security, Cloud Infrastructure, Security Challenges

1. Introduction

The term "cloud computing" encompasses not only the apps themselves but also the hardware and software used by the datacenters that house these service-based Internet programs. Technological knowledge has never been more strong or dominant than it is now, thanks to the expansion of computing resources and the internet. As technology has grown more accessible and affordable, a new model for computing has emerged: cloud computing. The term "cloud" refers to large groups of interconnected virtualized resources, such as servers, databases, and software development kits, that can be adjusted on the fly to offer optimal resource utilization in terms of elasticity, scalability, and load balancing. The capacity to scale and distribute a service entity in its compressed form to multiple clients at a reasonable price is one of the main advantages of cloud computing over more traditional methods [1]. Many companies have built massive data centers all around the globe to function as their public clouds. These centers are there to meet the communication, storage, and processing demands of consumers. Some of these companies include Amazon, Google, and Microsoft. Cloud computing relies heavily on virtual storage to offer Internet-based, on-demand services [2]. One major perk of cloud computing is that it provides low-cost services while doing away with the requirement for customers to build up costly computer infrastructure. As cloud computing has grown more embedded in various parts of the business, scientists have been looking into new technologies that are tied to it. Businesses and individuals alike are moving their data, applications, and services to cloud storage servers due to the scalability and accessibility of these services. While there are many benefits to moving from on-premises to cloud computing, there are also many security concerns and difficulties that service providers and customers must face [3]. Now that even trustworthy third parties are offering cloud services, there are more security risks than ever before. The basic principle of cloud computing is to make all a company's resources—including software, IT infrastructure, and services—available to its clients through the internet. The term "cloud computing" refers to infrastructures that house numerous independent systems and a highly adaptable computer architecture. A growing number of companies are turning to this technology since it eliminates the need for in-house system maintenance and development staff [4]. A plethora of companies are working on effective cloud products and technologies, including Amazon Web Services (AWS), Google, IBM, Microsoft, and countless more [5]. With cloud computing, both the company and its consumers can access and share data through remote, virtualized data centers.

A widely used and widely adopted paradigm for service-oriented computing, cloud computing involves the delivery of computing infrastructure and solutions as a service. With its many appealing features (such as self-service on-demand, wide network access, resource pooling, etc.), the cloud has transformed the way computing infrastructure is abstracted and used [6]. While there are many exciting new innovations in cloud computing platforms, security remains a major problem and cloud computing worries persist [7]. Cloud services, software, and infrastructure are clearly becoming more popular in the post-COVID-19 environment, as they can be accessed whenever and wherever users need them. Several studies and innovations, like the one in [8], have been suggested to deal with security problems. But new ways to strengthen cloud security still have plenty of room to grow. Most current cloud security measures ignore potential threats to the cloud computing infrastructure from novel sources. Thereby, they are unable to identify security flaws or assaults that may originate from either the cloud provider or the customer. In addition, there is a dearth of literature that comprehensively surveys the many tiers of cloud architecture. Considering the critical nature of the subject, this article surveyed the challenges encountered by the cloud computing architecture on four distinct levels: the application, host,

Licensed Under Creative Commons Attribution CC BY

network, and data levels. It also details the current remedies that have been implemented to address these problems. Furthermore, this paper draws attention to several unresolved issues and provides recommendations for further research. To the best of our knowledge, this study is the initial attempt to systematically analyze the related security challenges and solutions at the application, host, network, and data layers of the cloud.

2. Literature Review

There has been a recent uptick in the need for technological healthcare services; solutions like cloud computing, telemedicine, AI, and electronic health can often deliver better services [9]. What we call "cloud computing" is actually the provisioning of various services via the Internet. Software, servers, databases, networking, and data storage are all examples of resources that fall under this category [10]. Cloud computing allows businesses and organizations to rent out resources, such as data storage and processing power, from third-party providers rather than owning their own infrastructure or data centers [11]. Cloud computing is widely used for shared resources, such as servers, networks, storage tools, and application software. In addition, with cloud computing, customers can access their data and programs through the Internet. Cloud computing has been increasingly popular across all sectors, including healthcare [12]. A great deal of information and data is produced by healthcare organizations. Improved storage and administration capabilities are essential for health-related big data. The accessibility of patient records is a top priority for the healthcare sector [8]. The availability of large datasets for scientific analysis is also crucial for health researchers. Mobile applications, patient portals, EMRs, IoT devices, and big data analytics are all examples of cloud technology used in healthcare [9–11]. Healthcare providers must significantly grow their data storage and network needs to meet service expectations. Additionally, patients have easy and widespread access to their health information using the cloud in electronic health records. Medical professionals, hospitals, and clinics are reshaping medical care using cloud computing [13]. Costs associated with operations and infrastructure, worries about the safety of real-time data exchange, and the need for reliable backup are all obstacles in the healthcare industry.

Among the many benefits of cloud computing are the following: decreased costs, improved speed, scalability, and flexibility; and fast and convenient user cooperation. Cloud computing makes the process of exchanging data easier. It may also help healthcare organizations cut expenditures on infrastructure and operations that are housed there [14]. Cloud computing revolutionizes data storage and handling processes, allowing industry stakeholders and patients to access information faster and removing obstacles. The many advantages of cloud computing aren't without their problems. Many healthcare organizations are wary of moving their data to the cloud because of privacy and security concerns, as well as the associated costs of the services [15].

Researchers and doctors should have access to the vast amounts of data created by healthcare organizations, but privacy issues must be considered [16–18]. Given the rapid expansion, realization, and implementation of cloud computing in healthcare organizations, it is crucial to detect healthcare difficulties and security risks as they arise. Cloud computing has many advantages, but it has also introduced new security risks that healthcare organizations must investigate. Not only does this study aim to uncover security concerns in cloud technology, but it also reviews present security solutions and provides new ones. Cloud computing has many potential benefits to the healthcare business, but there are also many obstacles, problems, and security concerns that need to be addressed.

3. Cloud Computing in the Healthcare Sector: Benefits and challenges

Technological innovations have become essential in the ever-changing healthcare industry, making a positive impact on patient care, operational efficiency, and medical research. Cloud computing is one of these innovations that has become a game-changer, with many advantages and some disadvantages. This blog delves at the benefits and challenges that healthcare organizations have when trying to implement cloud computing, as well as the many ways in which cloud computing has affected the healthcare sector.

Understanding Cloud Computing in Healthcare:

To facilitate quicker innovation, more adaptable resources, and economies of scale, computing services such as servers, storage, databases, networking, software, analytics, and intelligence are being delivered through the internet, or the cloud. By using distant servers instead of on-premises data centers, cloud computing allows for the storing and access of massive volumes of data in the healthcare industry. This data includes patient information, medical imaging, and research data.

Benefits of Cloud Computing in Healthcare

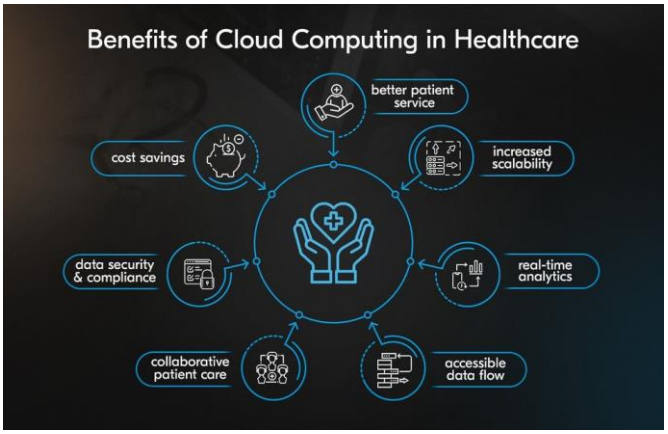

Figure 1: Benefits of Cloud Computing in Healthcare

By reducing costs and increasing quality of care, cloud computing affects providers and patients alike. Although the advantages of cloud computing are often difficult to differentiate from those of other technologies it enables, we have selected the six advantages that our clients mention most frequently.

1) Cost savings

The resources you use using cloud computing services are charged on an as-used basis. Instead of worrying about setup

Licensed Under Creative Commons Attribution CC BY

and hardware management, your healthcare organization can focus on patient care because cloud service providers take complete responsibility for administration, maintenance, and availability. Truthfully, not all medical centers have dedicated information technology (IT) teams. The technology used by cloud service providers is of the highest quality. In addition, they safeguard your data from cyberattacks and the resulting financial loss by adhering to flawless security practices. With the cost of a single data breach surpassing $10.93 million yearly in the highly regulated and competitive healthcare industry, this is clearly an advantage. Indirectly, cloud computing helps healthcare providers save money, which means patients pay less for treatment. This is due to infrastructure efficiency, workflow optimization, improved patient management, and other advantages.

2) Better customer service

A patient-centric approach is expected by 81% of patients, indicating an increasing demand for more personalized care. Cloud computing is frequently necessary to handle the high volume of personalized patient care that modern healthcare providers are expected to give. From the initial consultation to insurance processing and record retrieval, the usage of cloud computing in healthcare improves transparency throughout the patient journey. Many cloud-based technologies have emerged to improve patient interaction and management, such as telemedicine, chatbots, and automated appointment booking in mobile apps. Treatment results and patient satisfaction are both enhanced by more precise disease prediction and diagnosis.

3) Increased scalability

Scalability has always been a major obstacle to overcome in the healthcare industry. High availability and uptime are essential characteristics of healthcare software that processes massive amounts of data in multiple formats. Meanwhile, healthcare isn't exactly a rock-solid business. Rapid application scaling may be necessary in the event of even a small epidemic, whereas rapid application scaling may be necessary to optimize costs during calmer periods. The agility and scalability of cloud computing services, in contrast to on-premises computers, will allow your clinic to respond quickly to changing conditions, such as a pandemic or flu season.

4) Real-time analytics

With cloud computing, massive amounts of data can be stored, and millions of requests can be processed in a matter of seconds. When combined with AI, it opens new possibilities for real-time data analytics, which in turn opens new possibilities for better, more tailored diagnoses and treatments. However, real-time analytics have many more applications beyond just healthcare. Clinical trials, medication discovery, and medical research are all powered by analytics. Genomic research and teamwork, for instance, have a home in the cloud. The study's authors assert that cloud computing will most certainly continue to serve as the backbone of widespread genetic cooperation.

5) Accessible data flow

Electronic health records (EHR) replaced paper records in 2014 due to a federal mandate. Cloud computing has revolutionized healthcare by providing accessible and scalable storage for massive amounts of data. Properly secured data stored in the cloud can be readily accessed by authorized individuals from any internet-connected device. All records are kept consistent and up to date with the help of real-time updates. In addition, healthcare data can be integrated across systems thanks to cloud computing's enhancement of data interoperability. Your data is readily accessible for sharing and always use.

6) Collaborative patient care

Healthcare organizations and experts are now able to interact on shared data in real-time thanks to cloud computing. Doctors can access their patients' medical information and even consult with other experts in the field by sharing them with them. Clinicians get immediate access to vital records when patients use kiosks to input their information into medical databases. All a patient's medical records, including test results and magnetic resonance imaging (MRA) scans, can be instantly accessible to doctors and nurses as the laboratory uploads them. Now doctors and chemists can collaborate on improved treatment strategies by sharing data. The use of cloud computing can also streamline the process of patient care coordination among various healthcare providers, insurance companies, and clinics. Everyone involved may immediately access the medical records of other professionals, rather than placing the burden of care management on the patient, a problem that 63% of patients express dissatisfaction with. These advantages make it very evident why cloud computing is becoming an integral part of healthcare organizations. Even so, moving to the cloud isn't always easy.

7) Data security and compliance

Protecting sensitive patient information and keeping it in line with regulatory standards like HIPAA (Health Insurance Portability and Accountability Act) in the US are two of the many benefits of cloud computing for healthcare organizations. Health records stored in the cloud are protected from hackers, data breaches, and other cyber dangers by means of robust encryption, access limits, and routine security audits. To further reassure healthcare organizations that their data management processes adhere to industry-specific requirements, cloud platforms provide built-in compliance capabilities and certifications.

Challenges of adopting cloud computing in healthcare:

Cloud computing has many advantages, but there are also several problems that must be solved before it can be used successfully in healthcare.

1) Data Security and Privacy Concerns

Healthcare organizations still have valid worries about data security and privacy, even though cloud service providers have strong security safeguards in place. The potential for data breaches, illegal access, and cyberattacks is ever-present, and the ramifications of compromising patient data are substantial. Cloud service providers in the healthcare industry must be subject to rigorous security standards and subject to frequent audits to detect and address any flaws. They should also train employees on how to properly safeguard company data and establish stringent internal security rules.

Licensed Under Creative Commons Attribution CC BY

2) Compliance with Regulations

Adopting cloud computing is a significant problem for the healthcare industry due to the high level of regulation in this sector. Healthcare organizations should check that their cloud solutions are legal in all jurisdictions because regulations vary by area. Take the United States as an example. Healthcare organizations are obligated to adhere to HIPAA standards, which outline the proper storage, access, and sharing of patient information. When it comes to privacy and data protection in Europe, GDPR is the law to follow. It can be challenging to navigate various regulatory frameworks, and there are substantial fines and reputational harm that can come from not complying.

3) Data Interoperability

Information in healthcare is frequently stored in separate systems and formats, making data interoperability a major obstacle. Since data must be seamlessly integrated from many sources, cloud computing, if not applied properly, might make this problem worse. To overcome obstacles related to interoperability, healthcare organizations should use standardized protocols and data formats that allow for the flow of data between various systems. Healthcare providers can make better clinical decisions when interoperability guarantees that they have access to complete and accurate patient records.

4) Latency and Downtime

In the healthcare industry, where quick access to information can literally mean life or death, latency and downtime are major concerns. Because of how dependent cloud-based systems are on constant internet connectivity, any outage can compromise the availability of vital information and programs. Collaboration between healthcare organizations and cloud providers is essential for establishing stable internet connections and reducing the likelihood of downtime. They should also be prepared to deal with service interruptions if they occur.

5) Resistance to Change

Staff may be resistant to the adoption of cloud computing due to the substantial adjustments it requires to workflows and processes. Many in the medical field are wary of embracing new technology for fear that it would interfere with their daily work or put patients at risk. Investing in thorough training and support for personnel is crucial for healthcare organizations to overcome resistance to change. Building trust and encouraging adoption of the new technology can be achieved by showing personnel the advantages of cloud computing and involving them in the decision-making process.

6) Vendor Lock-In

An issue with cloud computing is vendor lock-in, which occurs when users find it difficult to transfer data or switch providers after a specific cloud solution has been set up. Having to rely on just one vendor can reduce your options and wind up costing you more in the long run. Careful evaluation of cloud service providers and consideration of solutions offering interoperability and data portability can help healthcare organizations avoid the danger of vendor lock-in. To be able to move providers easily, they should also make sure the conditions of their contracts are crystal clear.

4. Future Trends in Cloud Computing for Healthcare

The future of cloud computing in healthcare is likely to be influenced by several factors as the technology develops further.

1) Increased Adoption of Artificial Intelligence and Machine Learning

The future of healthcare cloud computing is looking bright, thanks to artificial intelligence (AI) and machine learning (ML). Clinical decision-making can be aided by cloud-based AI and ML systems that can sift through mountains of data in search of patterns and outcomes. When fully implemented, these technologies might completely alter the landscape of personalized medicine, treatment planning, and diagnostics.

2) Expansion of Telehealth Services

The widespread use of telehealth services has been expedited because to the COVID-19 epidemic and is anticipated to persist. Telehealth technologies, which allow for remote consultations, virtual visits, and remote patient monitoring, rely on cloud computing for its infrastructure. With the increasing popularity of telehealth, cloud solutions are crucial for providing safe and smooth access to healthcare.

3) Enhanced Data Interoperability

There will be persistent focus on enhancing healthcare data interoperability. With the help of cloud computing, data can be easily integrated from many sources, giving healthcare providers access to accurate and full patient records. Achieving genuine interoperability and improving care coordination will require standardized data formats and protocols.

4) Focus on Cybersecurity

Cybersecurity will always be an important concern for healthcare organizations that use the cloud, especially because cyber threats are always changing. To safeguard customer information from hacks and other forms of cybercrime, cloud providers will implement stringent security protocols. To reduce cybersecurity risks, healthcare organizations should make cybersecurity awareness and training a top priority for their employees.

5) Personalized Medicine

The field of personalized medicine, which considers a patient's unique genetic composition, lifestyle choices, and other variables when developing a treatment plan, would greatly benefit from cloud computing. Cloud computing can store and analyze massive datasets, including genetic data, which can lead to the development of more targeted treatments and better health outcomes for patients.

Licensed Under Creative Commons Attribution CC BY

5. Cloud Computing Architecture

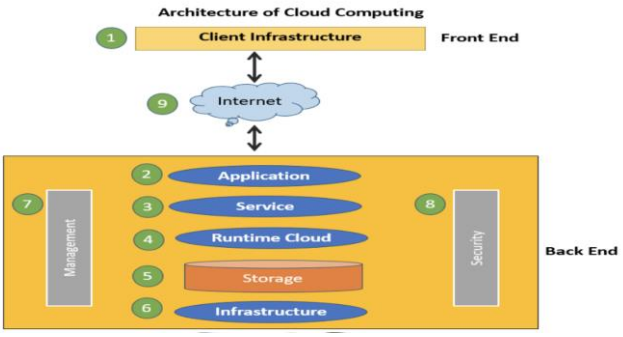

Figure 2: Cloud Computing Architecture

Cloud computing's architecture allows tenant organizations to process massive amounts of data with ease. Cloud architectures may be enhanced by certain features such as resource sharing, self-service, measurement services, and extensive network access. Cloud computing design combines Service Orientated design (SOA) with Enterprise Data Architecture (EDA), also known as Event Driven Architecture. Client infrastructure and applications are just two parts of the cloud computing architecture, which also includes runtime, storage, management, and security. The architecture that the client or user can see is called the frontend. Included are the client-side interfaces and applications that are required to use cloud computing platforms. It is possible for the frontend and backend to communicate via a network, such as the Internet. The front end can also communicate with the back end by means of the middleware. Web servers, tablets, cellphones, and clients of varying sizes are all examples.

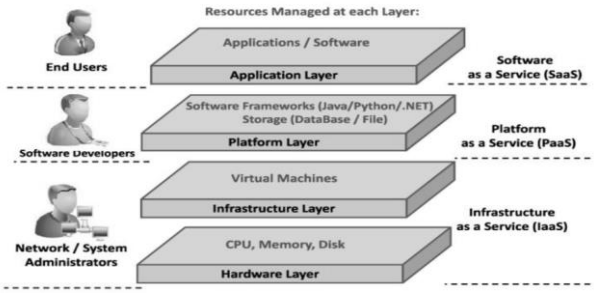

Figure 3: Components of Cloud Architecture

Frontend of Cloud Computing Architecture: The front end of the cloud computing architecture displays all user interface interactions. One cannot function without the other parts that comprise a user interface. The frontend primarily consists of the user interface, software, client infrastructure, and network.

Backend of Cloud Computing Architecture: The backend is responsible for making the frontend work. Its components include hardware and storage. An organization that offers cloud computing services has complete command of the infrastructure supporting cloud computing. The cloud architecture's backend relies on reliability to keep everything together. The key components of the backend architecture include the application, storage, infrastructure, runtime cloud, management software, and security.

Types of Cloud Computing in Healthcare

Two perspectives allow us to categories the various forms of healthcare cloud computing: deployment and distribution.

*1) **Distribution Model***

- **SaaS (Software as a Service):** Removes the requirement for software installs on-premises by delivering programs over the internet.
- **IaaS (Infrastructure as a Service):** Provisions servers, storage, and networking as virtualized resources accessible over the internet.
- **PaaS (Platform as a Service):** Rather than worrying about the underlying infrastructure, developers may use this platform to create, deploy, and manage apps.

*2) **Deployment Model***

- **Community:** Healthcare providers in a certain area or network are only one example of an organisation that can benefit from utilising a community cloud.
- **Private:** Private clouds, whether hosted in-house or by an outside vendor, are exclusively available to a single enterprise. They provide an enhanced degree of command and safety.
- **Public:** Examples of third-party providers that run public clouds are Google Cloud, Microsoft Azure, and Amazon Web Services (AWS). Through the internet, these platforms provide resources and services that may be scaled up or down.
- **Hybrid:** Hybrid clouds enable data and application sharing by combining public and private cloud environments.

What Are the Risks of Cloud Computing In Healthcare?

There are several data and privacy-related implementation concerns that organizations should be aware of when using cloud computing for healthcare applications, despite the many advantages, such as easier data accessibility and reduced costs. A summary of the possible dangers of healthcare cloud computing is as follows:

*1) **Healthcare Data Security and Privacy Risks***

Data privacy and security are major issues when storing sensitive patient information on the cloud. Patient data is vulnerable to cyberattacks, data breaches, and unauthorized access. Loss of patient confidence, legal trouble, and monetary fines are just some of the dire outcomes that can result from data breaches. Between 2009 and 2023, there have been over 5,887 data breaches documented in the healthcare sector alone. At present, there have been 387 incidents of data breaches in 2024, and more reports are continually pouring in. As a result, companies need to find cloud security specialists that can advise them on how to avoid data breaches on the cloud.

*2) **Restricted Ecosystem***

The healthcare business cannot be made more efficient and productive just by accepting cloud technologies. For healthcare organizations to fully utilize this technology, they must implement solutions using data science, the internet of things, and artificial intelligence.

Licensed Under Creative Commons Attribution CC BY

3) Security Challenges

The main reason to use cloud technology is to store healthcare data. Nevertheless, there are security concerns as well. Data that is shared on a server with other firms might not be adequately isolated because of how the main cloud is configured. The remote technologies that were supposed to personalize them could also end up failing. Healthcare agencies are unable to implement cloud solutions because of this.

4) Issues in Adopting Technologies

The entire task management process needs to be transformed to transition from a legacy framework to cloud technology. Make sure your staff at healthcare agencies fully grasp how these new tools will improve their day-to-day operations. To ensure that clients can make the most of the new system, they might enquire about or select cloud-based healthcare solution providers that offer training during the handover. Customers and their teams are always trained by Mind Inventory before a project is handed off, so they can make the most of the software solutions.

5) Compliance Challenges

Data management regulations, such as HIPAA in the US and GDPR in Europe, impose stringent obligations on healthcare organizations. On your own, you can struggle to meet all of the compliance requirements; however, with the assistance of cloud specialists who are familiar with these regulations, you can complete the deployment without a hitch.

6) Vendor Lock-In

The inability to easily switch to other platforms or interact with other systems could result from becoming dependent on cloud services provided by a single vendor. Therein lies the danger of vendor lock-in for enterprises. Limitations on flexibility and the ability to transfer providers in an emergency can be caused by vendor lock-in. Cloud methods that facilitate data portability and interoperability should be seriously considered by organizations seeking to lessen their reliance on any one provider.

7) Cloud Cost Management Issues

Although there are certain hidden expenses associated with cloud computing, such as unpredictable charges and unpredictable consumption patterns, it can be difficult to manage and foresee these costs. Disruptions to budgets and financial plans might occur due to unforeseen expenses. Therefore, companies should consult cloud professionals to learn how to optimize their cloud costs so that they can make the most of cloud services without breaking the bank.

How to Mitigate Associated Risks When Building Cloud-based Healthcare Solutions?

There are several potential dangers when developing healthcare solutions for the cloud, but they can be mitigated by following established procedures and strategies. If you're concerned about the potential dangers of healthcare cloud computing, here's what you can do:

1) Decide Your Objectives

Get a feel for the needs, such as the kind of cloud systems your healthcare company is looking for. Please explain why your healthcare company has decided to use a cloud ecosystem. Popular justifications for migrating workloads to the cloud include:

- Saving expenses
- Healthcare compliance management
- Security improvement
- Data protection and better backups
- Portability
- Easy accessibility

Communicating with your cloud service provider becomes much easier once you have a firm grasp of the primary goals. And they can adapt their cloud computing services to meet the specific needs of your company.

2) List out the Things to Switch to the Cloud

Even though you have a lot of processes that could benefit from moving to the cloud, you should know which ones are most in need of this upgrade. As a result, take a look at your healthcare organization's present pipeline and identify the things that are slowing down your healthcare team's operations or inhibiting high-quality medical delivery. Priorities the quick transition to the cloud after evaluating your company's procedures to achieve the maximum benefits. In addition, it will aid in measuring the exact time required for the technical delivery and improving communication with the technology vendor.

3) Ensure Cloud Data Security and Privacy

Whether data is in transit or at rest, it is susceptible to compromise. Cloud security best practices recommend encrypting sensitive data to prevent breaches and unauthorized access due to the data's vital nature. Ensuring that only authorized workers can access sensitive data also necessitates the use of effective authentication and authorization systems. To find and fix vulnerabilities in cloud-based healthcare solutions, frequent audits and security assessments are necessary once all installations are complete.

4) Maintain Compliance with Regulations

Make that the cloud provider you choose abides by all applicable data protection rules and regulations, including HIPAA, GDPR, and any local ones. You should make sure that your healthcare cloud solutions are compliant by checking and staying current with new compliance clauses and needs. Furthermore, establish a compliance audit team to aid in keeping meticulous records of compliance activities and doing routine checks to guarantee continuous conformity.

5) Ensure to Have an Effective Backup and Recovery Strategies

To avoid data loss due to corruption or inadvertent deletion, have your cloud services provider and the team managing your cloud-based healthcare solution set up automatic backups of all important files on a regular basis. To swiftly restore data and services in the event of a malfunction or outage, make sure you have a thorough disaster recovery plan. In order to ensure that healthcare data is immediately available in the event of an outage, it is essential to have data backup across numerous locations, as well as distinct cloud regions and availability zones. This is a best practice in cloud management.

Licensed Under Creative Commons Attribution CC BY

6) Employee Multi-Cloud Strategy

When you deploy your healthcare application to just one cloud platform, you run the risk of being unable to take use of features offered by other cloud providers. To increase adaptability and decrease reliance on any one provider, a multi-cloud approach is a good bet.

6. Real-World Examples of Cloud Computing in HealthCare

Innovative solutions that improve patient care, expedite operations, and assist medical research have been made possible by cloud computing, which has become a cornerstone in the healthcare industry. The healthcare business is already making use of cloud computing in the following ways:

1) AZ Delta – Equips EMR With Cloud and ML Abilities

As it prepared to provide better healthcare services, the massive regional hospital in Belgium, AZ Delta, faced the problem of managing its massive amounts of medical data. Although it had previously digitized its healthcare data, it was in a dispersed format. Its data includes complicated and diverse kinds of information, such as the hundreds of data points found in a single patient's electronic medical record. More than 650,000 people use this facility annually for consultations.

- It used cloud services to safely store sensitive medical data in a Virtual Private Cloud with 3-factor authentication and cloud identity, considering its need for centralized and powerful data processing.
- Big Query is used by that cloud to quickly organize and analyze data points numbering in the hundreds of millions.
- Data will also be handled using ML algorithms to meet the specific healthcare requirements of various patterns.

Now, AZ Delta can execute a query in 15 seconds instead of the 15 minutes it used to take with older systems, all because it strategically implemented cloud computing into its healthcare software solution and chose Google Cloud Provider as its cloud service provider. In addition, it has quickly and easily cleansed data from 50,000 patients, using around 500,000 data points.

2) Pfizer – Utilizes Cloud Computing Capacity For COVID-19 Vaccine Development

One of the world's foremost pharmaceutical and biotech companies, Pfizer, was interested in creating its own scientific data cloud (SDC). Rapid access to biotech data, which used to take weeks or months, was a demand that led to its partnership with AWS cloud.

Over time, Pfizer and AWS worked together to migrate Pfizer's server infrastructure and applications to the AWS cloud. Considered one of the quickest cloud migrations for a firm of Pfizer's scale, it relocated over 8,000 servers and 1,000 apps to the cloud in just 42 weeks.

This resulted in a large reduction of carbon blueprints (around 4,700) and $37 million.

Pfizer also benefited from this cloud adoption step during COVID-19, when the company required powerful cloud computing capabilities to conduct analysis for the vaccine development process.

3) Teladoc – Useas Cloud Infrastructure to Offer Real-time Doctor-Patient Video Conferencing

Among the many telemedicine providers, Teladoc Health stands out for its innovative use of cloud computing to facilitate virtual consultations between patients and medical experts. Healthcare is becoming more accessible, particularly in underprivileged areas, thanks to the cloud architecture, which enables real-time video conferencing, secure data transmission, and remote monitoring. It can provide its customers with 100% network availability because it is built on a strong cloud architecture. Because of this, it is also compatible with a wide range of electronic medical record systems. Several Blue Cross Blue Shield plans around the country, Aetna, and UnitedHealthcare are among the more than fifty U.S. health insurers that employ Teladoc Health Services to improve patient experiences. Furthermore, Teladoc virtual care services are offered to employees by more than 40% of Fortune 500 companies, as well as by small enterprises, labor unions, and public-sector employers.

7. Conclusion

The healthcare industry stands to benefit greatly from cloud computing's capacity to facilitate sophisticated analytics, improve data storage and administration, foster better cooperation, and lower costs. Problems with data interoperability, privacy and security, and regulatory compliance are some of the obstacles to cloud computing adoption. Healthcare organizations may improve patient care, organize operations more efficiently, and fuel innovation in medical research by tackling these problems and utilizing cloud computing. With the rapid advancement of technology, cloud computing is poised to revolutionize healthcare by facilitating better, more tailored treatment for individuals all over the globe. This paper provides an overview of the major security concerns with cloud computing and the proposed solutions to these problems. But there are still some unanswered questions that may cause concern and even danger to certain die-hard CC supporters. In the end, we believe that cloud computing provides a great foundation for businesses to grow and thrive. But you must exercise extreme caution when bringing one into your home. When choosing a supplier, be sure to consider their compliance standards and whether they have a strategy to address risks and weaknesses. While cloud computing has great promise for both academics and businesses, several challenging challenges remain, such as virtualization, security, performance, dependability, scalability, and interoperability. This paper introduces the concept of cloud computing and discusses some of the problems that must be fixed before this technology can be widely used and become an integral part of our daily lives. In a private setting, cloud computing is tackling many problems. Regardless, cloud benefits are now well-understood, especially when considering companies. But there are several security holes in this functionality that make it problematic to use in the cloud. The use of cloud computing is on the rise, but with it come new security risks as more and more businesses adopt this model. Every company uses a safe infrastructure for transferring data to off-site servers.

Licensed Under Creative Commons Attribution CC BY

References

[1] Saravanan, N.; Umamakeswari, A. Lattice based access control for protecting user data in cloud environments with hybrid security. *Comput. Secur.* **2021**, *100*, 102074.
[2] Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. *J. Supercomput.* **2020**, *76*, 9493–9532.
[3] Abdurachman, E.; Gaol, F.L.; Soewito, B. Survey on Threats and Risks in the Cloud Computing Environment. *Procedia Comput. Sci.* **2019**, *161*, 1325–1332. [**Google Scholar**] [**CrossRef**]
[4] Dong, S.; Abbas, K.; Jain, R. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access* **2019**, *7*, 80813–80828. [**Google Scholar**] [**CrossRef**]
[5] Alhenaki, L.; Alwatban, A.; Alamri, B.; Alarifi, N. A Survey on the Security of Cloud Computing. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019. [**Google Scholar**]
[6] Domingo-Ferrer, J.; Farràs, O.; Ribes-González, J.; Sánchez, D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Comput. Commun.* **2019**, *140*, 38–60. [**Google Scholar**] [**CrossRef**]
[7] Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Comput. Sci. Rev.* **2019**, *33*, 1–48. [**Google Scholar**] [**CrossRef**]
[8] Ibrahim, F.A.M.; Hemayed, E.E. Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. *Comput. Secur.* **2019**, *82*, 196–226. [**Google Scholar**] [**CrossRef**]
[9] Qureshi, A.; Dashti, W.; Jahangeer, A.; Zafar, A. Security Challenges over Cloud Environment from Service Provider Prospective. *Cloud Comput. Data Sci.* **2020**, *1*, 1–48.
[10] Farsi, M.; Ali, M.; Shah, R.A.; Wagan, A.A.; Kharabsheh, R. Cloud computing and data security threats taxonomy: A review. *J. Intell. Fuzzy Syst.* **2020**, *38*, 2517–2527
[11] Devipriya, K.; Lingamgunta, S. Multi Factor Two-way Hash-Based Authentication in Cloud Computing. *Int. J. Cloud Appl. Comput.* **2020**, *10*, 56–76. [**Google Scholar**] [**CrossRef**]
[12] Deebak, B.; Al-Turjman, F.; Mostarda, L. Seamless secure anonymous authentication for cloud-based mobile edge computing. *Comput. Electr. Eng.* **2020**, *87*, 106782. [**Google Scholar**] [**CrossRef**]
[13] Irshad, Azeem & Chaudhry, Shehzad & Alomari, Osama & Yahya, Khalid & Kumar, Neeraj. (2020). A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework. IEEE Systems Journal. PP. 1-9. 10.1109/JSYST.2020.2998721.
[14] Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y.; Yu, K. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. *IEEE Access* **2020**, *8*, 70604–70615.
[15] Zimba, A.; Chen, H.; Wang, Z. Bayesian network based weighted APT attack paths modeling in cloud computing. *Future Gener. Comput. Syst.* **2019**, *96*, 525–537. [**Google Scholar**] [**CrossRef**]
[16] Patil, R.; Dudeja, H.; Modi, C. Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. *Comput. Secur.* **2019**, *85*, 402–422. [**Google Scholar**] [**CrossRef**]
[17] Sarveshwaran, Velliangiri & .P, Karthikeyan & Kumar, V Vinoth. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. Journal of Experimental & Theoretical Artificial Intelligence. 33. 10.1080/0952813X.2020.1744196.
[18] Aldribi, A.; Traoré, I.; Moa, B.; Nwamuo, O. Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. *Comput. Secur.* **2020**, *88*, 101646

Licensed Under Creative Commons Attribution CC BY