eHealth: A Case Study on the Application of Cloud Technology for Managed Dissemination of Medical and Health related information

Davian R. Chin

The University of East London

u2204075@uel.ac.uk

Abstract: Cloud computing has revolutionised the IT industry, making high performing and high-capacity IT infrastructure accessible to businesses and other industries in an efficient, flexible, and cost-effective way. The healthcare industry is one of the major adopters of cloud technology driven by the need to offer healthcare service to larger geographical locations, and to share medical knowledge and healthcare data among healthcare professionals on a much wider scale. This paper explores the most fundamental concepts in cloud computing and presents a case study that highlight critical issues to consider when designing the architecture for an eHealth cloud computing system which aims to optimise the dissemination of healthcare data among healthcare professionals and patients.

Keywords: cloud, technology, virtualisation, healthcare, hybrid, security, deployment, architecture

1. Introduction

1.1. A brief historical perspective and conceptualisation of cloud computing

The idea of "cloud computing" dates to the 1960s when computer scientists, John McCarthy and chief scientist of ARPANET, Leonard Kleinrock predicted that there will come a time when computing will be packaged as kind of public "utility" which will be the basis of a new type of technology (Erl, Puttini and Mahmood, 2013, p. 25). Today, the rapid developments in IT hardware and software have driven advances in medical technology, critical diagnostics, and health data analytics (Chang et al., 2021) which are significantly improving the way life-changing decisions are made improving patients' access to medical knowledge and enabling the effective sharing of resources and technical knowledge among health professionals global (Sahi, Lai and Li, 2016, p.1).

1.2. Motivation for cloud computing and drivers of cloud migration

The fundamental characteristics of the cloud computing paradigm that are driving the transformation from onsite computing systems to cloud-based computing systems are the significantly lower costs, high efficiency, and flexibility associated with cloud solutions in contrast to onsite systems (Sahi, Lai and Li, 2016, p.1). Furthermore, the high scalability and the reduced need for human intervention in resource management and administration provides further incentive for migration (Molo et al., 2021, p. 1).

1.3. Looking ahead: opportunities and challenges of cloud computing

The future of the healthcare industry is towards sustainable development which will require a more data-centric approach to design and architecture. Additionally, further advances in cloud computing will drive the healthcare industry to become more digitised and location independent. However, this transformation is not without challenges (Chang et al., 2021). According to Sahi, Lai and Li (2016, p.1-2), cloud computing distributes data across the internet which introduces risks to the security and privacy of the data. The authors claim that healthcare personnel are "distrustful" (Chang et al., 2021, p. 3) of the technology as

potentially potent risk to data security and privacy are associated with cloud-based systems (Molo et al., 2021, p. 9). This is particularly nontrivial when the data is sensitive. Additionally, Other risks such as unexpected financial costs and the emergence of security vulnerabilities associated with improper implementation are possible (Chang et al., 2021, Sahi, Lai and Li, 2016).

1.4. Overview of paper

This paper aims to identify and understand the impact of critical factors that impact the overall success of developing and implementing a cloud computing system and to suggest and evaluate a design for an eHealth cloud system. In the first part of this paper, we will discuss important concepts and terminologies that arise when discussing cloud computing systems and architectural design considerations. Next, we will discuss the challenges of migrating to cloud-based systems and how to overcome them. Next, we will discuss, considering previous discussions, considerations that can increase the likelihood of success and reduce the risks associated with cloud system migration for a specific case study for an eHealth system. Lastly, we will summarise important lessons learnt about cloud system migration and discuss critical factors that can affect the likelihood of success of such systems.

2. Literature Review

2.1. Cloud mechanisms, architectures, deployment, and delivery

When discussing cloud computing, we normally talk about its *computing mechanisms*, *architecture*, *deployment*, and *delivery*. Cloud computing mechanisms speaks to aspects of its infrastructure delivery models, resource management and monitoring, and access control and security mechanisms (Erl, Mahmood and Puttini, 2013). Cloud computing architecture refers to models for combining the various cloud computing mechanisms to flexibly deliver cloud computing services and resources to cloud customers (Erl, Mahmood and Puttini, 2013). Figure 2.1 shows a graphical description of a general cloud system architecture.

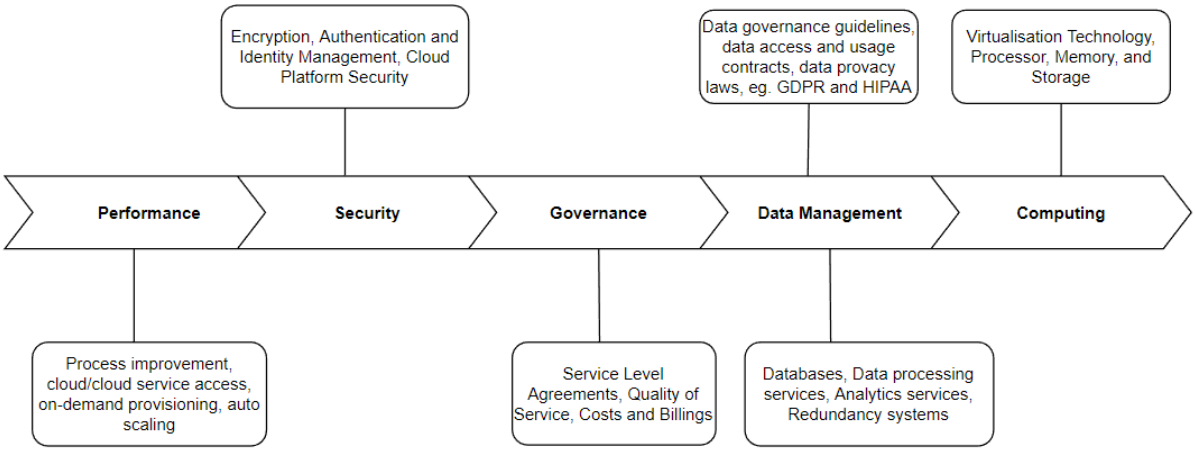


Figure 2.1. Schematic diagram of a typical cloud system architecture. It shows the various layers involved in the design and implementation of a cloud-based system, and some of the components that are considered in each layer.

All cloud computing solutions offer *pay-as-you-go*, and *on-demand* resource provisioning technology to their customers, enabling them to flexible manage rented cloud resources and scale their business to meet their needs (Molo et al., 2021). However, every business is

different and may require that cloud computing systems that are customised to meet their business needs. (Molo et al., 2021, p. 3).

2.2. Cloud deployment and delivery models

Cloud consumers are vast and varied and they require cloud solutions that can flexibly meet their business needs. Cloud providers can deploy cloud solutions to cloud consumers in diverse ways each with different configurations (of cloud mechanisms) depending on the use case. There are three popular deployment models used by cloud providers today (Ramesh, Delen and Turban, 2021, p. 599): *private clouds*, *public clouds*, and *hybrid clouds*. *Community clouds* are also popular within certain groups (Molo et al., 2021, p.3).

Public clouds belong to external cloud providers, who are responsible for providing and maintaining the underlying IT infrastructure and computing resources (Erl, Mahmood and Puttini, 2013). Public clouds tend to be the cheaper cloud options for companies as it requires very little time and financial overheads to get started (Ramesh, Delen and Turban, 2021), however, they are the least secure as the physical IT resources provisioned are shared by other cloud users and cloud owners (Erl, Mahmood and Puttini, 2013, p. 44 and Molo et al., 2021, p. 9)

Private clouds allow the cloud user to occupy the role of cloud consumer and cloud owner as the same time clouds (Erl, Mahmood and Puttini, 2013). Private clouds belong to the organisations that uses them, and its IT resources reside within the organisation's perimeter, making it more secure than public clouds (Ramesh, Delen and Turban, 2021, p. 599). Private clouds, however, can incur significant costs as the cloud owner is fully responsible for the management and maintenance of the underlying IT infrastructure and resources clouds (Ramesh, Delen and Turban, 2021, p. 599).

Hybrid clouds uses a combination of public and private cloud technology to flexibility handle data of different sensitivity level (Erl, Mahmood and Puttini, 2013, p. 76).

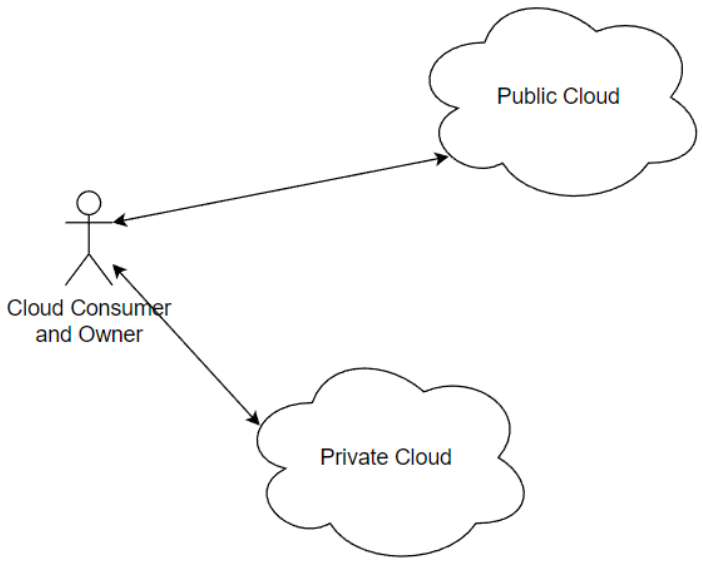


Figure 2.2 shows a simplified schema for a hybrid cloud

Hybrid clouds can be complex and present difficulties in management and maintenance as the private cloud will require some effort (as mentioned in the previous section) and there is now the issue of ensuring network connectivity and interoperability (Ramesh, Delen and Turban, 2021, p. 599) between the two separate clouds which could be from different cloud providers (Erl, Mahmood and Puttini, 2013).

A community cloud is a public cloud that restricted to a specific group of individuals who has the responsibility to manage and maintain the cloud (Erl, Mahmood and Puttini, 2013).

Cloud customers access cloud services in three major configurations:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

The major difference the configurations lies in the amount of control that the cloud customer will have over the IT resources provisioned.

IaaS provides virtualised network infrastructure, cloud storage and servers to the cloud customer with administrative privileges to use them and to build their own applications. The cloud customer pays for the underlying infrastructure (Ramesh, Delen and Turban, 2021, p. 595).

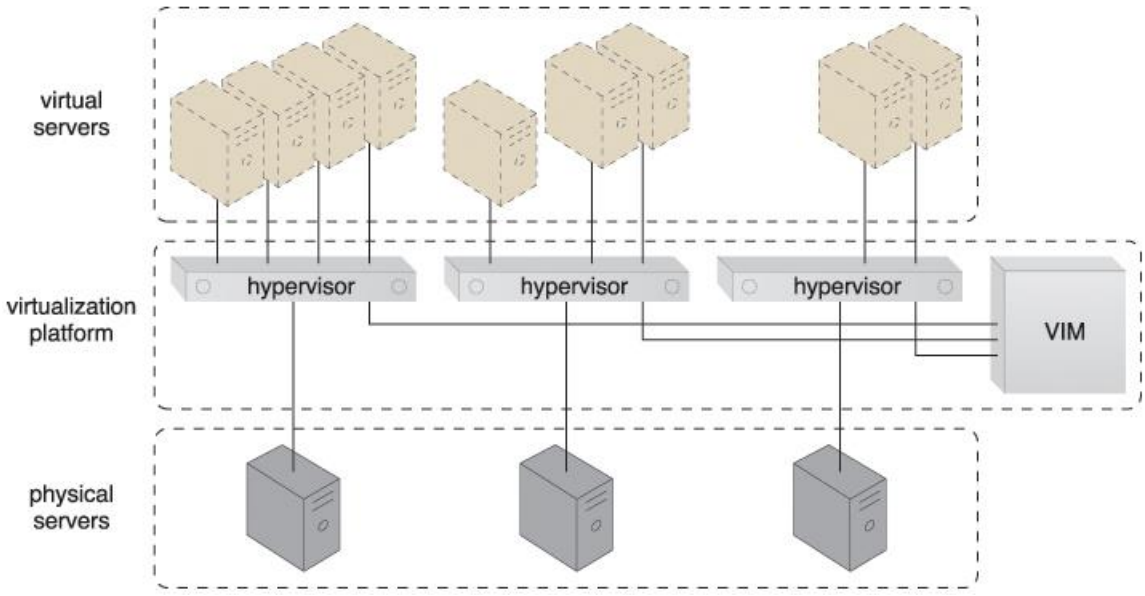
PaaS provides cloud customers with a pre-built environment with a pre-installed set of tools and IT resources to support application development and deployment. The cloud customer has less administrative rights in this model and less control over the underlying IT resources that support the pre-built environment (Erl, Mahmood and Puttini, 2013).

In SaaS, cloud customers pay for and use pre-built software without any rights to the underlying cloud resources and infrastructure. The cloud customer pays for the use of the software (Ramesh, Delen and Turban, 2021, p. 595).

2.3. Cloud infrastructure mechanisms

2.3.1. Virtualisation and virtual servers

Virtualisation is the process of creating virtual versions of a physical resource. Physical infrastructures such as networks, computer storage, servers (Ramesh, Delen and Turban, 2021, p. 596) and computer processors can be virtualised and provisioned as on-demand and pay-per-use services (Erl, Mahmood and Puttini, 2013, p. 145). The diagram below shows how a physical server can be virtualised to create multiple virtual server images.



Adapted from (Erl, Mahmood and Puttini, 2013, p. 200)

The hypervisor, sometimes called the *virtual machine manager* (VMM), shown in the diagram is a software interface between the *virtual infrastructure manager* (VIM) and the virtual servers. The hypervisor provides mechanisms to manage the distribution of IT resources among the virtual servers that are associated with a given physical server. The VIM provides tools for distributing multiple hypervisors across a pool of physical servers (Erl, Mahmood and Puttini, 2013, p. 200). Virtualisation is the building block for developing cloud systems (Erl, Mahmood and Puttini, 2013, p. 200). Virtualisation technology allows cloud providers to create virtualised resource pools of physical and virtual resources to provision cloud solutions specific certain business needs on-demand.

2.3.2. *Cloud storage*

Cloud storage mechanisms provide logical storage units for cloud customers as on-demand and pay-per-use services accessed via cloud storage services. Cloud storage are available in three basic types: *block*, *object*, and *file*.

Block storage stores discrete chunks of data in blocks (like how physical hard drives store data). This type of storage is suitable for structured data (fixed format) (Erl, Mahmood and Puttini, 2013, p. 200).

Object storage is a more flexible storage model that can manage high volumes of unstructured data. It is therefore good for storing immutable data such as sound files, photographs, dataset, and other data varieties.

File store makes use of the standard file systems for storing data. It consists of a collection of data grouped into folders (Erl, Mahmood and Puttini, 2013, p. 147). File storage sits on top of the block and object storage infrastructure, so a file will use block or object storage. For example, a file folder may contain a combination of text, picture, and music files. Figure 2.3 shows the interoperability of the three basic cloud storage models in a typical cloud-based system.

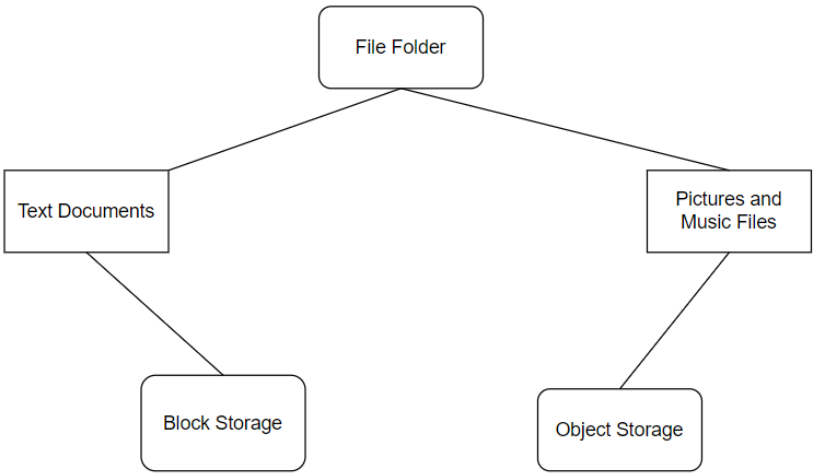


Figure 2.3 shows the interoperability of file systems with the other type of cloud storage in a typical cloud system.

2.3.3. Cloud compute

Cloud compute deals with the provisioning of virtual processors for the cloud computing system. Typically, cloud compute covers memory, storage, CPU, and an operating system such as LINUX. Since computational operations works on input to create an output, CPUs will require an attached memory system as well as storage, and an operating system to manage job scheduling and resource management.

Figure 2.4 below shows the compute layer for a typical cloud computing system.

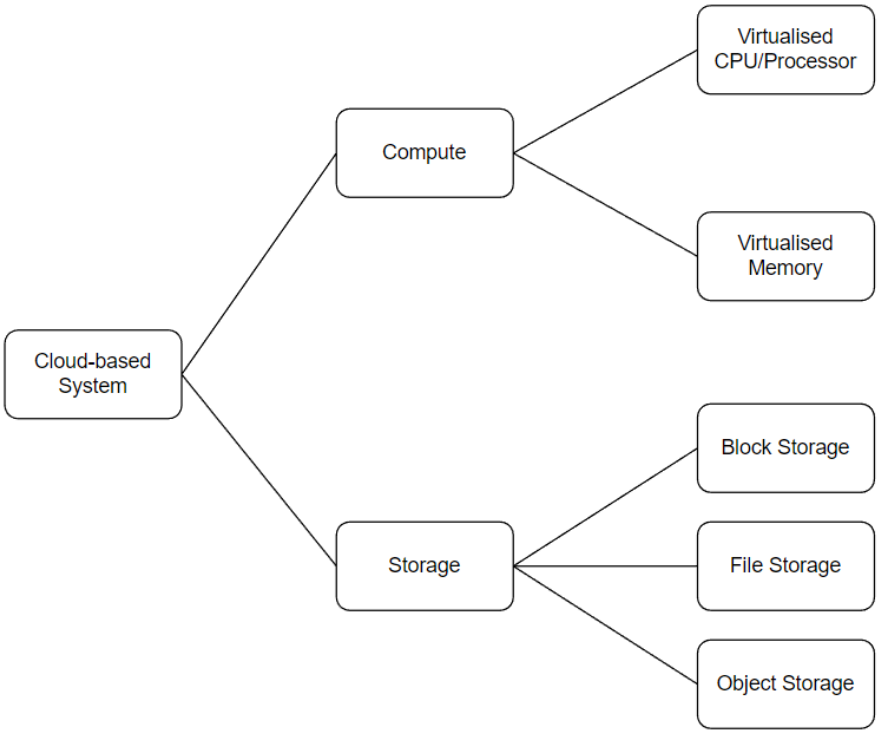


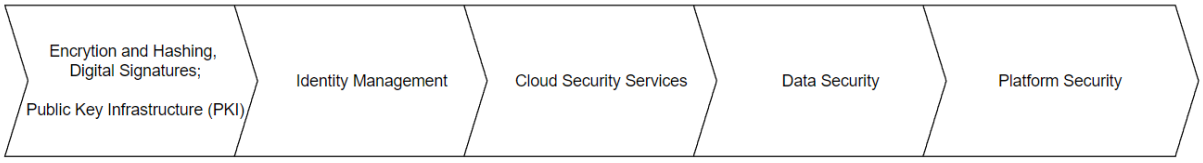
Figure 2.4 shows a typical compute layers for a cloud-based system.

2.3.4. Cloud databases

Database systems sit on top of the cloud storage system offer a structured way for cloud users to interact with data residing in the cloud storage. Most cloud providers will provide database application to cloud users which can either be a cloud-native database, for example Microsoft Azure Cloud SQL Database, or other third-party non-native databases such as Oracle.

2.3.5. Cloud security

A good cloud security model is fundamental to any cloud-based system. The diagram below gives a brief overview of the layers of security mechanisms used to secure a cloud-based system.



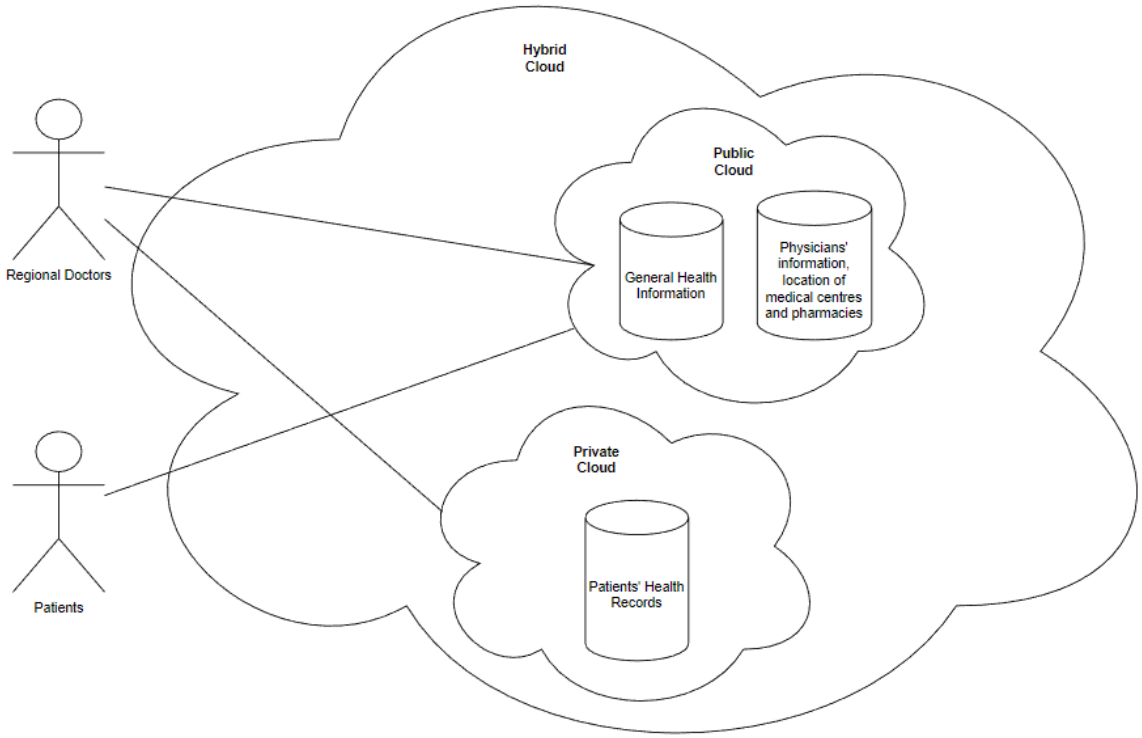
Encryption is a network security mechanism used to protect data transmitted over a network from eavesdropping threats, thereby preserving the privacy of transmitted data. Hashing secures the integrity of the data as across a network. There are two types of encryptions: symmetric and asymmetric encryption. Symmetric encryption uses a single shared key to encrypt and decrypt a message, while asymmetric encryption uses a public (available to the public) and a private key (unknown only by the intended recipient) for encryption and decryption. A message that is public key encrypted is only accessible to a recipient with the associated private key. This makes the decryption exceedingly difficult for an unauthorised recipient. A hash function computes a hash for a fixed length message, locking it. The intended recipient will use the same hash function to compute the message hash to verify its integrity. Encryption and hashing technologies play important roles in the digital signature security mechanisms to preserve the privacy and integrity of data sent across a network. A digitally signed message consists of digital signature (small message encrypted by a private key) attached to data sent across the network. The intended recipient verifies this digital signature to ensure that the message's integrity is intact (Erl, Mahmood and Puttini, 2013, p. 229 - 236).

Identity and access management mechanisms monitors and controls access to cloud systems and cloud services based on predefined access policies. IAM mechanism comprises of four major components: authentication, authorisation, user management and credential management. The main purpose for IAM systems is function as a countermeasure against security threats such as DDoS attacks, insufficient authorisation, virtualisation attacks and containerisation attacks (Erl, Mahmood and Puttini, 2013, p. 242).

IAM is an example of a cloud security service. Other are Zero Trust protocols, Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) are modern options that defend against the latest security threats to cloud-based systems (Microsoft Security, n.d.).

2.4. The eHealth Use Case

eHealth is a proposed non-commercial and scalable cloud-based solution geared towards optimising dissemination of health-related data for general-purpose consumption, improving patient care, and for improving collaboration and information sharing among healthcare professionals in the region. The use case diagram below gives an overview of how doctors and patients will interact with the cloud-based system.



The use case diagram shows a hybrid cloud consisting of a public cloud and private cloud.

Regional doctors can access sensitive patient information stored in the private cloud for research and information sharing purposes. They can also access the public cloud to update general health information knowledge base.

Patients can access the public cloud to obtain general healthcare information from the general health knowledge based, as well and get information about the regional physicians, location of the regional medical centres and pharmacies.

By migrating to a cloud-based system, the eHealth system can leverage the benefits of cloud computing systems discussed the previous sections of this paper and reserve the option of scaling the solution to a much wide perimeter in the future which is a long-term goal of this use case.

3. Discussion and Analysis

3.1. Risks and Challenges of Cloud Migration

Migrating heath-related data to the cloud comes with various security and data privacy risks since transmitting data over the internet raises the risk of data theft or loss of integrity and privacy (Molo et al., 2021, p. 9 and Chang et al., 2021). Also, data hosted on public clouds is now residing in a third-party domain and so there is loss of control over the data which raise

questions over continuous compliance with data handling standards (data governance guidelines) and other data privacy regulations (Molo et al., 2021, p. 9).

Improper implementation of a cloud solution can cause massive financial overruns that could derail the entire project. It can also cause the emergence of security vulnerabilities that could put sensitive data (e.g., patient health records) at risk (Erl, Mahmood and Puttini, 2013). Improper implementation can lead to breakdown in reliability and interoperability in hybrid clouds which will degrade performance of the cloud solution (Molo et al., 2021, p. 8, 10). In the healthcare industry, information integration and sharing mechanisms, and proper cost management are important considerations that must carefully managed to increase the likelihood of success for cloud-based solutions and reduce the security risks that could emerge based on the previous discussion (Chang et al., 2021, p. 4). Additionally, eHealth cloud systems require high reliability with little tolerance for errors in data. It is therefore important to safeguard the confidentiality and integrity of the data as data leaks can put patients at risk (Chang et al., 2021, p. 5).

3.2. Proposed Cloud System Architecture

In this section we will describe a proposed architecture for the use case described in section 2.4 above. We will start by describing the requirements for the cloud solution.

3.2.1. Requirements

Requirement	Description
Processes	1. Regional doctors should be able to query/search the database containing patients' health records. 2. Regional doctors should be able to update the general health information database with new health-related information. 3. Patients should be able to search the general health information database based on general healthcare topics. 4. Patients should be able to search information on regional doctors, medical centres, and pharmacies.
Data	1. General health information 2. Patients' health records 3. Geographic data of medical centres and pharmacies 4. Doctors' information
Security	1. Access to the patients' health records should require authentication and authorisation. 2. Only doctors from the specified region should have access to the cloud.
Governance	1. Patients' health records should not be accessible to the public 2. Regional doctors should have access to the patients' health records.

	3. Data governance guidelines must be adhered to whe handling the patients' health records. 4. Data security and privacy regulations must be adhered to when managing the patient's health records.

3.2.2. Desired System Characteristics

Characteristics	Description
Security	1. Cloud system should be accessible via a VPN connection. 2. Patients' health records should be accessible via a separate authentication portal.
Governance	1. Patients' health records should reside on a private cloud. 2. Doctors should require authentication for access to the patients' health records. 3. Data must be store, disseminated and discarded in accordance with the data governance guidelines and data privacy and security regulations.
Operation	1. Regional doctors access the cloud system via a VPN which grants access to the cloud system. 2. Regional doctors can use a database API to search physicians' details, medical centres, and pharmacies information. 3. Regional doctors can access a separate login portal that conducts an additional authentication that provides access to the patients' health records. 4. Patients can login to the system via a VPN. 5. Patients can use a database API to search physicians' details, medical centres, and pharmacies information.

3.2.3. Final System Architecture

The eHealth Cloud System will use a hybrid community cloud model with a public cloud and a private cloud component. Access to the cloud system will be via a VPN. Cloud security services IAM and Service Governance will manage user authentication and monitor compliance of data security and privacy regulations. A separate access portal will provide to authenticated access to the private cloud. Cloud governance service will ensure that patients' health records adhere to data governance policies and data privacy and security regulations (Imperva, n.d.).

The use of a community cloud in the solution makes sense since it is only to serve a small group of individuals (regional doctors and patients). The use of a hybrid cloud is valid given that

patients' health records is sensitive data and should only be accessible by a smaller group of individuals and require additional security guarantees. As such a public cloud will not meet this requirement.

The general health information, physicians' details and location details of medical centres and pharmacies are all public data and will reside in a public cloud. A relational database management system is a viable choice for managing this public data is structured data. Additionally, search and retrieve transactions will be conducted on this data and this make relational databases a viable choice.

Patients' health records will reside in a NoSQL database. The rationale behind this is that patients' data make contain photographic data such as X-ray scans or ultrasound images which are not structure data and therefore not suitable for storage in relational databases (Erl, Khattak, and Buhler, 2016).

5. Conclusion and Recommendation

In conclusion, we learnt that cloud computing is an emerging and disruptive technology that is increasing in popularity due to its ability to bring compute and IT infrastructure to industry on-demand and in a cost-effective way. It enables the development of flexible solutions allowing cloud providers to be responsive to the diverse and complex needs and requirements of businesses and industry and make scaling of resources easy with little administrative intervention. The advantages of cloud computing have driven fast adoption of cloud technology in the healthcare industry. However, despite the benefits of cloud computing, there remain challenges and obstacles to cloud migration in healthcare. The emergence of security threats and risks to data privacy and integrity have cause a lack of trust in cloud-based systems in the healthcare industry as well as the risk of poor performing and unreliable cloud solutions due to improper implementation.

In designing an eHealth cloud system, it is critical to gain and clear understanding of the use case and requirement before beginning to design the architecture of the cloud system so we do not end up with a wrong solution to the problem we set out to solve, and so will end up with an unreliable cloud solution.

It is also important to avoid intrinsic bias in determining the cloud, database, or applications to use to build the solution. This bias could be due to familiarity with a particular cloud provider, technology, or application. This will naturally lead to a poorly optimised cloud solution. We can avoid this bias by first developing a logical architecture for the system without giving any thought to any cloud provider. Also, when designing the physical architecture, consider all viable options before settling on a final architecture.

Security and data privacy must be a principal component in every phase of the design process if we are to safeguard our data and system comprehensively. Data governance is a key step to safely manage and disseminate data resources and can help to ensure that the cloud solution remain in compliance with data privacy regulations (IBM, n.d.).

Overall, adopting a systems approach to designing cloud-based systems can help to ensure that we design the correct solution for a use case, and a solution that is optimal, dependable, scalable, and cost-effective.

References

1. Chang, S.-C., Lu, M.-T., Pan, T.-H. and Chen, C.-S. (2021). Evaluating the E-Health Cloud Computing Systems Adoption in Taiwan's Healthcare Industry. Life, 11(4), p.310. doi:10.3390/life11040310.
2. Erl, T., Mahmood, Z. and Puttini, R. (2013). Cloud Computing: Concepts, Technology & Architecture. United States: Pearson.
3. Erl, T., Khattak, W. and Buhler, P. (2016). Big Data Fundamentals: Concepts, Drivers & Techniques. Boston: Prentice Hall.
4. IBM. (n.d.). *What is data governance? | IBM*. [online] Available at: https://www.ibm.com/topics/data-governance [Accessed 4 Sep. 2022].
5. Imperva. (n.d.). *Cloud Governance | Framework & Model Principles | Imperva*. [online] Available at: https://www.imperva.com/learn/data-security/cloud-governance/.
6. Microsoft Security. (n.d.). *Comprehensive Security for Business | Microsoft Security*. [online] Available at: https://www.microsoft.com/en-gb/security/business.
7. Molo, M.J., Badejo, J.A., Adetiba, E., Nzanzu, V.P., Noma-Osaghae, E., Oguntosin, V., Baraka, M.O., Takenga, C., Suraju, S. and Adebiyi, E.F. (2021). A Review of Evolutionary Trends in Cloud Computing and Applications to the Healthcare Ecosystem. Applied Computational Intelligence and Soft Computing, 2021, pp.1–16. doi:10.1155/2021/1843671.
8. Ramesh, S., Delen, D. and Turban, E. (2021). *Systems for Analytics, Data Science, & Artificial Intelligence: Systems for Decision Support*. 11th ed. United Kingdom: Pearson Education.
9. Sahi, A., Lai, D. and Li, Y. (2016). Security and Privacy Preserving Approaches in the eHealth Clouds with Disaster Recovery Plan. Computers in Biology and Medicine, 78, pp.1–8. doi:10.1016/j.compbiomed.2016.09.003.