OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Review Article

Healthcare Usage of Cloud Computing and Resources

Christopher M Hannock*

Department of Computer Science, University of California, Berkeley, USA

ABSTRACT

Cloud computing has been an ever-growing field within information technology. As most businesses are finding ways to utilize cloud service providers, there is one industry that has not been as willing to make the shift. This paper will cover the different models of cloud computing, hesitation in making the shift, why the shift should be made, and discuss the overall benefits of cloud computing. With the current Coronavirus pandemic, the need for increased budgets, bandwidth, and access has increased drastically. Cloud computing is a computing model which takes place over the internet and provides scalability, reliability, availability and low cost of computer reassures. This paper also discusses the concerns that healthcare providers have in switching from legacy systems to a new cloud-based solution.

Keywords: Cloud computing; Information technology; Network; Healthcare

INTRODUCTION

Cloud computing has proved to be a new way of networking. Examples of cloud computing can be seen from using Apple's I Cloud to the network that all your patient data is stored in a hospital. Origins of cloud computing can date back to the 1960s but the first mention of cloud computing in writing was in a document in 1996. In 2006, the type of cloud that was most known was Infrastructure-as a-Service also known as IaaS. This allowed the client to use the cloud service provider's infrastructure without the need for having their own data center and equipment. As the cloud grew and the benefits became more well known, the healthcare industry started to see how cloud computing could help them. Through research presented within this paper, it will be seen how healthcare can benefit from cloud computing and why it should have already happened [1]. Cloud computing is a very promising trend of computing which left the attention in the academic researches and as well as in the software industry. Cloud computing is a computing environment which provides availability, scalability, and flexibility of computer reassures at a deferent level of abstraction with low running cost [2]. Cloud Computing refers to the applications, the hardware and software delivered as services over the Internet. The cloud computing services provided in four models, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Integration Platform as a Service (iPaaS) [3]. Cloud computing can be defined as a computing method to provide computing as the utility to meet the everyday needs of the general business community.

LITERATURE REVIEW

There are three distinct service models in cloud computing. These models are Infrastructure-as-a-Service (IaaS) like mentioned previously, Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). In a PaaS model, the client can use the platform provided by their cloud service provider to develop applications and design what they need on that platform. A SaaS setup is a complete software package in the cloud that included services from an IaaS or PaaS model. The IaaS model gives the client infrastructure for storage on equipment that belongs to the cloud service provider that they have in secure data centers. What some groups may be concerned about in their switch to cloud computing from their local network is the loss of control. In the IaaS model, the client has no control over the storage, hypervisor security, or environmental security. Instead, they have control over their local machines for the operating systems and applications running on them. The bigger our business gets and the more advanced our software solutions become, the more likely it is that inconsistent data and clunky workarounds will become part of our day-to-day business. Software integration is critical in reducing the potential for inefficient workflows through its centralization of information. It also often leads to

Correspondence to: Christopher M Hannock, Department of Computer Science, University of California, Berkeley, USA, E-mail: hannock19@students.ecu.edu

Received: April 22, 2021; **Accepted:** May 7, 2021; **Published:** May 14, 2021

Citation: Hannock CM (2021) Healthcare Usage of Cloud Computing and Resources. J Inform Tech Softw Eng.S4:002.

increased collaboration among various stakeholders and improved transparency [4].

Cloud computing benefits

Since the Coronavirus pandemic has affected the world, the importance of information technology and cloud computing has grown. Some people visit their doctors virtually with telehealth conferencing and having to share Personally Identifiable Information (PII) over that video conference. The importance of information security could not be stressed more. With the exchange of this type of information, the hospitals need to have the technology available to protect that video conference call and still be able to give the same quality service as if the patient were in the office. With this greater impact of information technology happening in the hospital, the hospitals need to protect themselves against attacks and increase their budget for the networking team [5].

Healthcare seems to be one of the last industries to start making the move to cloud computing veering away from locally-owned networking. This is not without hesitation from the new health customers in the cloud. With patient confidentiality and the policies on patient information, health organizations were uncertain about the transformation to a cloud-based solution. In an article from Perry Price, Price mentions that through a survey, 52% of the responses to why the company was hesitant to move to the cloud were because of data security and compliance with federal regulations.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 were designed to ensure the protection of patients and their personal data. Although this act was passed before cloud computing took off, the rules and regulations of the act can still be extended to cloud service providers from healthcare companies. The HIPAA has both privacy and a security rule. The privacy rule is to ensure that the patient data can be used and distributed when needed to better the patient, The security rule is to ensure that the data of the patient is secure and is protected. The government has taken measures to ensure the responsibilities of both parties involved. In 2016, the Office of Civil Rights (OCR) started to become more involved by issuing guidance. “OCR recognizes the value of a "shared security model. It says each party should confirm their responsibilities in writing and acknowledges that cloud service providers may not be responsible for compliance failures caused by their customer's actions or inactions”. This is important as this provides protection both ways to ensure neither party can blame the other. Like Miliard stated, the roles and responsibilities should be outlined and agreed upon to ensure that the business relationship will stand the test of time. This quote also shows the separate entities of the businesses. If the healthcare provider chooses an IaaS model, the cloud service provider cannot be held responsible for what their client does with their equipment [6].

Before many healthcare companies were shifting to cloud computing, they were making up most of the cyber-attacks. Ransomware was the choice of attack against the healthcare companies and “data shows that data exfiltration and data extortion was the reason behind 70 percent of the ransomware attacks”. “In 2017, the total number of healthcare breaches mounted to 477, affecting 5.6 million patient records”. Ransomware attacks like WannaCry and Ryuk have affected and exploited these health systems also. With these kinds of staggering figures, it becomes clear that these companies need newer solutions. If these companies do choose to move to a cloud computing operation, they still must take precautions to ensure the network is still secure on their end.

DISCUSSION

Now that there have been the findings of why healthcare companies should at least consider switching to cloud computing, these are benefits of why cloud computing will prove too beneficial to these companies. Cloud computing offers a cheaper alternative while also having others manage the network. This reduces the number of employees that the organization must hire and ensures that the network is running smoothly. An example of a cloud service provider is Virtustream, a Dell Technologies Business. In a published article from that business, Virtustream states that companies like healthcare companies are typically running on legacy systems and information. This is what has led to the focus on companies like these healthcare companies because they pose an easy target to get information from. The article contains a graphic to show the benefits that their clients have experienced. For their testimonials, the companies are using a program named Epic. The clients noticed that the return on investment was near 350% in three years and there was 43% lower operations cost in three years. The performance of the application also works faster and more efficiently. This shows empirical data of how cloud computing can be beneficial to healthcare companies and that information security should no longer be what holds companies back from shifting to a cloud-based solution [2].

Not to distract away from the importance of having a cloud-based solution but, the local network to the clients still needs to enact policies to ensure that the network is secure. There should be policies in place to discuss remote access to information. With some employees trying to work from home, this adds to the potential of information being leaked or exposed. Although the cloud provider manages the network and secures data flows from the business to the cloud provider, the cloud provider does not have control of the end-user devices that are connected to their clients' network. Mobile devices on the network can also open vulnerabilities to the network that have to be closed. By simplifying technical complexity to deliver change through an integrated hybrid platform, organizations mitigate risk. Following consistent processes and knowing the status of integrations are eased with an integrated hybrid platform (also known as PaaS – Platform as a Service).

In continuing to combat the hesitation of moving to cloud-based operations, the numbers do not lie. In a 2019 article on healthcare cloud doubts, the author mentions that only 7% of security incidents were because of the cloud-based, 65% were not cloud-related, and 28% are uncertain. Although these numbers were based on data from two years ago, it can be inferred that cloud service providers are working hard to keep the number of security events on their network to a minimum.

The competition between these providers will continue to benefit the businesses that choose the cloud as they are constantly trying to improve. It is also seen through Patterson's data that, in 2019, that 7% of those surveyed trusted the cloud, 55% trusted it on a limited basis, and 18% did not trust it. With the Coronavirus pandemic only a year after Patterson published his findings, the push to cloud-based solutions grew stronger. A theoretical of the likeness of an attack to happen on the legacy systems that these businesses use is far greater than being on a cloud-based solution. It is inevitable that these companies make the shift, but it will be in time as these organizations work through their doubts and see testimonials. For successful cloud data integration, we need to bring a developer who is an expert in this field. He should help us in application development and its integration with the cloud systems. In order to optimize our business operations, we need the right development team, which will streamline our process and will help us in data security as well.

It has been shown how beneficial it is for companies to have cloud-based solutions. This is true for most businesses, not just healthcare businesses although this was more focused on the latter. Davis states that "reliable, offline, air-gapped backups of critical data is one of the most important elements healthcare providers need". This also brings the idea of redundancy throughout the network to ensure that data is backed up and there is limited impact to the healthcare providers during changes and configurations. Some healthcare providers like hospitals do not stop and the network needs to account for that. In a different work by Davis, there was an interesting statistic based on a survey. Of the companies surveyed, 80% of them said they would be likely to reach out to a cloud provider and 44% of them said they would be highly likely to reach out to a cloud provider.

CONCLUSION

Once companies see how beneficial cloud computing is for their business, most companies will make the shift. Security is important not only to the healthcare providers but also to the cloud service providers who will undertake the responsibilities of handling secure data. it should consider the types of tools that we wish to include in our solution along with the kind of integration that would work best for our company. After all, in today's technology industry, all the choices are up to us. With shared responsibility that the two businesses can establish, the security measures can be delegated and regulated to ensure compliance for health and patients related data to traverse from the healthcare site to secure data centers.

REFERENCES

1. Kakkar P. Revolutionizing supply chain with cloud based applications. American Jour of Com Arch. 2021;8(1):1-5.
2. Kakkar P. Business Transfomation with Cloud ERP. IJMTE. 2021;11(3):27-31.
3. Sakoda HS. SaaS and integration best practices. Fujitsu Sci & Tech J. 2009;45(3):257-264.
4. Alauthman M, Almomani A, Alweshah M, Omoushd W, Alieyane K. Machine learning for phishing detection and mitigation. CRC Press. 2019;48-74.
5. Ayoubi S, Limam N, Salahuddin MA, Shahriar N, Boutaba R, Estrada-Solano F, et al. Machine learning for cognitive network management. IEEE Communications Magazine. 2018;56(1):158-165.
6. Giliberto A. RightScale 2019 State of the Cloud Report from Flexera Identifies Cloud Adoption Trends. 2019.