PROTECTING HEALTHCARE APPLICATIONS IN A CLOUD COMPUTING INFRASTRUCTURE

Oluwaseun Dare | ITCN4040 | 6th May 2018

PROTECTING HEALTHCARE APPLICATIONS IN A CLOUD COMPUTING INFRASTRUCTURE

INTRODUCTION

Digital health applications are critical to today's healthcare systems as it provides the ability for end users to access and use information at a rapid accelerated rate. Users for health information systems and data can include patients, doctors, nurses, primary car physicians, among other users. Sample data that can be accessed within a healthcare application can include patient data, demographics, critical patient records, imaging data, in addition to historical patient data for doctor / physician analysis. This data is critical to the daily functions that enables the healthcare environment function as an institution for providing better service to end users. With today's digital data cornered with big data analytics within the health care environmental systems, it is essential to create effective avenues for accessing and utilizing this generated data for ease of access and usage.

CLOUD COMPUTING INFRASTRUTURE

The quest to access data effectively and accurately has brought about the birth of cloud storage technologies. The numerous benefits provided by cloud infrastructures such as added security and transfer of risks has motivated leading industry technologies to adopt a cloud model for daily data access through cloud applications. The same benefits can also be applied to a health care system that incorporates some type of cloud applications within a cloud infrastructure. Cloud infrastructures can be accessed on site, as it can also be provided thorough numerous cloud service

providers. The definition of cloud computing spans across many variables to incorporate its associated benefits, models of offering, and methodology involved with deploying cloud computing infrastructures in a health care environment.

According to NIST's final definition of cloud computing, it envisions most of the characteristic properties offered through cloud deployment such as a "convenient, on-demand network access to a shared pool of configurable computing resources" ("Final Version of NIST Cloud Computing Definition Published," 2018). Some keywords that can be extracted with the accepted definition include access to data through convenient means in addition to an on-demand scalable architecture. This is an ideal data access medium for health care applications deployed in a cloud infrastructure with attached importance for data availability at any time at anywhere. With advancement in information technology and availability of information, electronic health care systems have replaced traditional paper-based medical systems (Liu et al., 2017, p. 1). This is due largely in part on the added and proven benefits of cloud flexibility such as universal accessibility coupled with the low cost of ownership and maintenance required to use the service.

The need for health care applications residing in the cloud comes with numerous added benefits coupled with compounded benefits being offered through a scalable cloud computing architecture. Taking an illustration, Mr. Smith, a patient at XYZ hospital has a monitoring device that transmit data to a server through his cell phone. This data is visible only by his physician, Dr John, which is used for analysis and health monitoring. With cloud computing, the data transmitted by Mr. Smith is closer to the patient as well as to the doctors, this data can be accessed at anytime as the applications are deployed "in the cloud". Mr. Smith and the physician is also making use of one of the available service models for cloud computing – software-as-a-service, or SaaS, which is a platform where software is available to end users for various data exchange and activities. In

addition, the underlying cloud infrastructures are managed by a third-party cloud service provider that often provides all the necessary maintenance and security required for operating the cloud infrastructure, a term known as transfer of risks. The illustration clearly depicts the essential characteristics of cloud infrastructures within a health care environment. With added flexibility, cloud service options are based on user demands and accessibility which relies heavily on organizational needs.

The infrastructure that offers the added benefits of flexibility for cloud computing is virtualization. According to Sgandurra & Lupu, 2016, p.4, "Virtualization is the key foundation for realizing cloud computing. This form of computing combines the physical power of computer, network, and storage to provide logical abstract of resources to be used "in the cloud" by end users, thereby providing the major service deployment models – software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). SaaS provides end users with applications that can be used to access the cloud infrastructure, while PaaS uses platform level access to deploy applications with various programming language. IaaS adds an additional access layer where cloud users have access to computing infrastructure to deploy and manage cloud application. The aforementioned cloud services cover various infrastructures within an organization ranging from size, management, and user population (Marinescu, 2013, p. 9). As such, service models include private, community, public, and hybrid clouds.

Private cloud is ideal for large organizations where such cloud delivery is maintained by the owning organization. Public cloud is a model whereby cloud service is generally available to the public through the sale of cloud services such as storage, computing power, and data access. Community clouds relies on shared infrastructure from various organizations supporting a

common cause and hybrid clouds is a composition of two or more clouds based on organizational needs.

Within a health care setting, all these forms of cloud service delivery options can be considered based on organizational needs and limitations. However, when considering cloud deployment for the health care industry, it is also important to note the underlying challenge that comes with cloud computing – security. Within a health care environment, access to customer data over the cloud can pose a security risk for cloud providers as well as data end users – patients and physicians. There are laws that safeguards the protection of user data within the health care industry, and as such, cloud service providers need to adhere to these laws in order to provide affordable and secured cloud environment for running health care applications.

According to Liu et al., 2017, p. 2, an average cloud server used by health care systems has access to all the data uploaded by users, thus posing an inherent security risk to such health care systems. Security risks can occur when such systems are hacked which exposes such critical patient data to the dark web and the internet. The security of such systems also spans to privacy concerns on where data is stored and used, mode of transmission, encryption capabilities, among other secured layer features that can be offered.

Although, these privacy and security concerns are major factors that hinder the effective deployment of cloud-based health care systems in hospitals and organizations, an approach to tacking security issues with cloud-based data transmission and retrieval is end to end encryption of user data. Encryption uses algorithms to decipher data by means of using hash and key functions. Only users with valid keys are able to decrypt and use such data. This means of data protection offers some insight into safeguarding personal and health records for users for data in motion, and data at rest for deploying health applications in a cloud environment. Data audition also introduces

another layer of security protection for data storage within a cloud computing infrastructure, and as such, some providers also offer remote data auditing service, using various protocols to effectively prove the reliability of data stored in the cloud (Sookhak et al., 2015, p. 2). An important feature of data auditing is the ability to cross-check a small portion of cloud data for integrity and tampering by using hash algorithms using the least possible computational requirements. This adds another layer of security for stored personal health data residing in the cloud, thereby increasing security considerations for such stored data.

Although, encryption and auditing services can add a layer of security to cloud components, the underlying infrastructure – virtualized systems, can also be attacked. As cloud computing resides on virtualized systems, any attack to a virtualized system also impacts the data stored on the resources being provided by the virtual machine, such as memory or storage attacks. To make an illustration, three virtual machines located at various geographical zones for high availability combine computing resources to form a cloud storage platform for health care applications. If one of the virtual machines gets attacked, it has a direct impact on the data stored on the cloud service platform. According to Sgandurra & Lupu, 2016, p.9, some common virtual machine vulnerabilities arise from it's detection. When an application is running from a virtual machine, its vulnerabilities are exploited to reveal holes for targeted attacks through exploitation of known vulnerabilities. Some proven methodology of circumventing such attacks is to hide the presence of a virtual machine, which can be achieved through the modification of configuration files to hide particular virtualized layer signatures for detection. Other common virtualized layer attacks include VM hopping and Cross-VM attacks, where attackers basically gain access to other virtual machines within the same cloud infrastructure, in addition to even gaining access to the underlying physical component of the virtual machine known as the hypervisor. When access is

gained, the attacker can use this means of exploit to steal information and data residing on the infrastructure, thereby compromising the integrity of the data stored on the cloud. Some of these threats can be minimized through the effective deployment of applications in a secured virtual machine with optimum security built into it's kernel. Examples include hypervisor hardening, which includes a set of tools for locking down hypervisor components, thus preventing them from external threats and attacks.

While security solutions can be limited to hardware and software defense for cloud-based systems, the protection of health care data also spans to the development of applications in a cloud environment. Application developers can safeguard access to applications by ensuring that it is only accessible as needed through users with authorized access to such cloud component.

CONCLUSION

Cloud-based health care systems takes advantage of cloud solutions to provide unmeasured benefits built into deployed applications, however, security considerations such as privacy concerns in addition to attacks from external bodies with the aim of stealing user data can often discourage organizations from offering cloud-based services. With a properly configured health system application and a security-hardened cloud infrastructure, health care organizations can also benefit from the numerous advantages of a cloud-based health care system such as the flexibility and scalability that comes with a cloud computing system.

REFERENCES

Final Version of NIST Cloud Computing Definition Published. (2018, January 8). Retrieved from https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

Liu, J., Ma, J., Wu, W., Chen, X., Huang, X., & Xu, L. (2017). Protecting Mobile Health Records in Cloud Computing. *ACM Transactions on Embedded Computing Systems*, *16*(2), 1-20. doi:10.1145/2983625 *

Marinescu, D. C. (2013). Cloud computing: Theory and practice. Available from https://ebookcentral.proquest.com/lib/eastcarolina/detail.action?docID=1213925#

Sgandurra, D., & Lupu, E. (2016). Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems. *ACM Computing Surveys*, *48*(3), 1-38. doi:10.1145/2856126 *

Sookhak, M., Gani, A., Talebian, H., Akhunzada, A., Khan, S. U., Buyya, R., & Zomaya, A. Y. (2015). Remote Data Auditing in Cloud Computing Environments. *ACM Computing Surveys*, *47*(4), 1-34. doi:10.1145/2764465 *