# Health Data in the Cloud

## *A Survey of Security and Privacy Concerns*

Oladipupo A. Popoola
MSc. Computer Security and Forensics
University of Bedfordshire
oladipupo.popoola@study.beds.ac.uk

*Abstract*: **One of the most sensitive sectors in any economy when it comes to information management is the Health sector. The healthcare sector majorly depends on large database of historical information acquired through various mediums which could include physical contact or digital mediums. As this historical information evolve into large datasets and the need for speedy accessibility is on demand, a modern technology paradigm becomes the new solution to this major evolution – Cloud Computing. To establish an environment which guarantees a reduction in time invested and cost incurred in the usage of health information, otherwise called data to facilitate efficient medical service delivery, the cloud – a seamless distribution of data warehouse over the network through several host of computers, has been a focus of adoption. Electronic health records (EHR), a Cloud services for the healthcare system are most beneficial when they are accessible at any place, and at any time. As relevant as Cloud computing is to health data, security is of a major concern especially when a long history of successful data breaches is evaluated.**

**This paper would be considering a survey of several concerns and the key factors that may discourage the migration of health data from the premise to the cloud.**

***KEYWORDS: Health data, Data Management, Security, Cloud Computing, Data Migration***

## I. INTRODUCTION

National Institute of Standard and Technology (NIST) [7] defines Cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal effort or service interaction. Cloud as a modern technology uses the internet to transmit data between distributed client computers and central remote servers to share and maintain data, applications and services [1]. This paradigm also is an abstraction that involves the coordination of various resources and making them available virtually. Interestingly, there has also been a growing academic and technological research into the subject of Cloud computing giving core insight into other crucial components such as Security and Auditing [3, 15], Access Control [13, 19], and Resource management [18, 19, 20].

As a surging demand for Cloud computing emerges due to the benefits of availability, lower overhead cost and flexibility it offers, organizations are now empowered with better efficiency at delivering their services maximally [14]. In Health informatics, it poses a concern as a term called *Trusted Computing*, that is Privacy. How can a cloud service provider (CSP) guarantee the protection of the data domicile with them either from breaches or illegal usage by the CSP itself? [13]. As a result, there has been vast discussions and arguments as to the various security and privacy issues that puts vital health information at major risk if lodged and distributed over the cloud [8].

## II. BACKGROUND

This section identifies and briefly describe the necessary preliminaries about Cloud Security. The Cloud itself is not solely dependent on its own security to remain trusted without the integrity of the Data being transmitted itself. Hence the need to understand how the terms Cloud, Data and Security works in their architecture.

### *A. Cloud Architecture*

The architecture of the Cloud comprises of a network of client computers accessing shared applications and services on a host of server computers. Essentially the architecture has also been classified into front-end and back-end [1]. The distributed client computers and the residual applications which are used to access the provisioned virtual resources are classified as front-end while the servers used to provision the virtual resources such as virtual servers, applications, databases, storages are regarded as back-end systems and these systems form the “cloud” of various accessible resources [14].

To ensure a concurrent and even distribution of resources to multiple end-users, high-level monitoring is implemented. Middleware and Protocols are two of the few embedded utilities used to manage the consistency required for smooth management of resources between all connected systems [14]. Deploying Cloud resources comes in variants depending on the scope of the organisations’ requirements. Popular deployments models are private, public, community and hybrid. Private deployments are operated within a specific organisation’s domain and is inaccessible from the external network. Public and Community deployments are openly available to the public but within the community area, accessibility is limited to the members of the public defined by a community. Hybrid deployments is a mesh of two or more types of deployment frameworks. [5]

### *B. Security & Privacy Architecture*

Now that we have a brief idea of how the cloud works, we would evaluate how they assure data security at a

more technical level. The most important focus of most popular CSPs is to ensure the Confidentiality, Integrity and Availability of the data entrusted to them [8]. To guarantee security, encryption is utilised. Some of the most commonly utilised encryptions are Searchable Symmetric Encryption, Identity-based Encryption, Threshold Secret Sharing, Attribute-based Encryption [21, 22].

## III. HACKERS, IN PURSUIT OF DATA

Cloud applications like EHR processes huge amount of health records from various health institutions who uses it to manage the consistency of their patients' records. EHRs hosted on security-deficient cloud platforms are likely to encounter one or more security threats which in record have been a problem or catastrophic to some health institutions [1]. Figure 1 below represents a statistic of what could be prone to threats in EHRs [4].

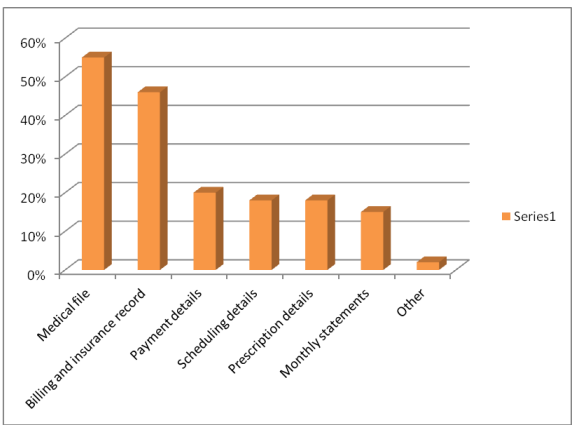


Figure 1. What Hackers want in any Health Data

A CSP, Skyhigh conducted a survey amongst healthcare organizations regarding Cloud service usage and security risks. The result of the research established 33% of the health organizations reported data leaks in 2014, while 79% stated that unauthorised data exposure was one of their prevalent challenges [8, 16].

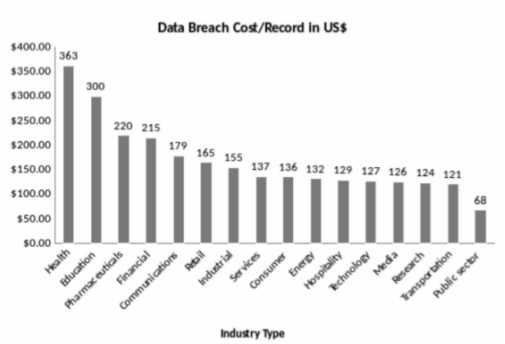


Figure 2. Data Breach Indicator

The figure 2 indicates that the health sector amongst others suffers more attacks resulting to high-cost data breaches [12]

## IV. KNOWN SECURITY & PRIVACY CONCERNS

Despite the surging demand for migrating to the Cloud, it is not without the concern for the risks associated with Cloud computing. A major concern around the distribution of sensitive health data over the cloud is the delegation, verification, and revocation of permissions and access rights with respect to an outside healthcare provider [9, 10]. The figure 3 below identifies the major classification of risks to take into consideration when moving health data to the cloud.

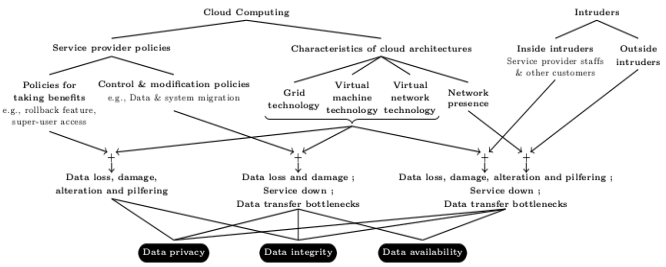


Figure 3. Classification of Risks associated with Moving into the Cloud

- Infringement of Data: This factor is one of the most popular reasons why health organisation are quite reluctant to have their health data moved to the cloud. As the figures above states, cloud computing seems to be the capital focus of many cyber-attacks. Cloud computing is emerging and so it is concerning its security. Sensitive health data can fall into the hands of unauthorised persons due to persistent attacks on the server holding the data. [14, 12, 7]. Internal or external threats can be the bane of the organizations access to cloud resources. Unauthorised access has been at the top of most internal threats. As such the prevalence of these data breaches is not accommodating to sensitive health data present on the cloud as it become the target to online cyber theft. [5].

- Loss of Data: Since data are stored on servers on physical locations, there is a probability of intentional or natural damages. Also, in the case where mismanagement is an issue, data could be deleted erroneously [14]. Data loss is at the core of the cloud computing security model. SaaS, IaaS and PaaS models for cloud computing implement applications to process business data and store customers' data in the data centres, developers use data to test software integrity during the system development life cycle and users create new drives on virtual machines and store data on those drives respectively. However, data is accessible within all three cloud models by unauthorized internal personnel, as well as hackers. [5]. This access may be detrimental to the lodged data.

- Service Hijacking: Also called Denial of Service (DoS) may involve a combination of several hacking techniques such as Phishing, and exploitation of

software vulnerabilities. Services such as EHRs is mostly the target of DoS attacks. By generating persistent and innumerable fake data calls to a certain cloud server pressures the server to utilize processor power, memory, disk space, and network bandwidth. The effect of this attack is that it makes the system intolerable, slow and keeps discourage the use of the service [14]. DoS can cause a catastrophic damage to the data which after a successful breach leaves the data to any manipulative control of the attackers [5].

- Security-deficient APIs: Application programming Interface (API) are the channels used by service users to access the various applications and services provisioned by the CSPs. Also between the third-party and the CSPs, API is used to make the service available on the cloud for users. EHRs, for instance, may come in various variants provisioned by different companies. The availability of HER on the cloud is empowered by API. It is therefore of major risk if the API by which users access the HER is insecure [14] thereby putting transmitted or stored data at risk. As much as it is the responsibility of both third-parties and the CSP to maintain the integrity of the API, regardless of the evolving models, it would take a lot more in terms of security for health organizations to confidently adopt cloud computing [5].

- Malware-injection attack: During the communication between the client and the server, when data are sent as packets, the meta-data are also sent to identify to both client and the server what the transmission is all about. This meta-data could be attacked with malicious codes resulting to eavesdropping or engaging a user with a service which was never initiated. Most data breaches also involve this form of attack especially for enumeration providing the attacker all information about a subsequent or pending data transfer. This type of attack is also known as a meta-data spoofing attack [6].

- Acquisition of CSP: It poses concern for health agencies using services such as EHRs when a CSP is acquired and the process of handing over may certainly disrupt service delivery. [17].

- Insufficient Due Diligence: Most health agencies do not have operational consultants before adopting modern technologies. Cloud computing is a very different technology that may have a negative impact if adequate consultation is not acquired before investing into it. [14].

- Shared Technology Vulnerabilities: All service, applications and compute resources on a cloud platform are shared. This means that there is no sole vulnerability pertinent to a service user. It is most likely to share the cost of a risk or vulnerability likely to be suffered by another service user.[14].

- Loss of Governance: Regardless of the cloud service model invested upon, the moment the power to manage, monitor and process applications and data on behalf of an organization such organization cease to have secured dominant authority of the resources. This is the case with cloud computing. Once the CSP takes over the storage, monitoring, service distribution or compute of resources owned by an organization, the CSP therefore has the authority over the management [5]. This is usually not a delighted option for most health organization.

- Lock-in Agreements: Due to the fact that most health organizations are not well informed on how cloud computing solutions works, most have been bounded to insufficient or unsatisfactory Service Level Agreements (SLAs). This has led many health organizations to wasteful investments especially at the first integration of service into the cloud [14, 17].

- Response to Incidence: Natural disasters and accidents are bound to happen. Health organizations feel safer with crude idea of premise storages as they seem to have physical mitigation ideas than an uncertainty that their data is safe regardless of an accident with a cloud service provider. [27].

- Availability Chain: It is usually common for CSPs to engage other CSPs to share compute capacity in order to deliver optimum service. The guarantee that the third-part CSP would be consistent and could be trusted with sensitive health data is questionable [14].

- Mismanagement of resources: This is often the case when the cloud service model is misunderstood or there is a misappropriation of resources allocated to diverse services and applications [14]. When this happens, health organizations may realize they are spending more on what is not needed.

## V. STANDARD SECURITY ISSUES DEFINED BY REGULATED BODIES RELATED TO THE CLOUD ENVIRONMENT

The table below is the provision security for standard security classification of issues surrounding cloud computing as defined by NIST and the Cloud Security Alliance (CSA) [2, 17]

| ***Security Issues*** | ***NIST*** | ***CSA*** |
|---|---|---|
| Governance and Enterprise Risk Management | Yes | Yes |
| Compliance and Audit | Yes | Yes |
| Information Management and Data Security | Yes | Yes |
| Portability and Interoperability | No | Yes |
| Identity and Access Management | Yes | Yes |
| Virtualization | Yes | Yes |
| Security as a Service | No | Yes |
| Traditional Security, Business Continuity and Disaster | Yes | Yes |

| *Security Issues* | *NIST* | *CSA* |
|---|---|---|
| Data Centre Operations | No | Yes |
| Incident Response, Notification And Remediation | Yes | Yes |
| Application Security | Yes | Yes |
| Availability | Yes | No |
| Encryption and Key Management | No | Yes |

## VI. CONCLUSION

With the ever-increasing adoption and provision of cloud services readily available and accessible to health organisations, security issues are like-wise becoming rampant and breaches actively crippling the smooth operation and distribution of cloud resources. In this survey, an effort has been made to broadly evaluate the various concerns which could deter any health organisation from taking advantage of the numerous benefits and advantages of moving their data, applications and services to the cloud. Perhaps, as recommendation, it would be best to incorporate a Trust Model or Trust Computing in order to suit the security needs of Health organisations.

## VII. REFERENCES


[1] G. Rathi, Abinaya. M, Deepika. M , Kavyasri. T: Healthcare Data Security in Cloud Computing, pp. 1808, 1811 (2015).

[2] A. Anusha Priya, R. Gunasundari: Securing Data on the Cloud Server by the User Authentication and Data Security Techniques. International Journal of Computer Applications, pp. 9-10 (2017)

[3] Kaiping Xue and Peilin Hong. A Dynamic Secure Group Sharing Framework in Public Cloud Computing. IEEE Transactions on Cloud Computing, 2(4):459–470, Oct.-Dec 2014.

[4] S.I. Khan, A. Sayed Md, L. Hoque: Privacy and Security Problems of National Health Data Warehouse: A Convenient Solution for Developing Countries, pp. 2-3 (2016),

[5] S. Dargan: Security Threats In Cloud Computing Environment. Journal of Information, Knowledge And Research In Computer Engineering pp. 619-620. (2015).

[6] G. Kulkarni, N. Chavan, R. Chandorkar, R. Palwe: Cloud Security Challenges. 2012 7th International Conference on Telecommunication Systems, Services, and Applications. pp. 89 (2012).

[7] P. Mell and T. Grance. The NIST Definition of Cloud Computing - Special Publication 800-145. National Institute of Standards and Technology, August 2011.

[8] Prasanna Balasooriya L.N., S. Wibowo, and M. Wells: Data Security and Privacy on the Cloud: Driving to the Next Era of Technology with Confidence, pp. 2-5 (2015).

[9] R. Aiswarya, R. Divya, D. Sangeetha, V. Vaidehi: Harnessing Healthcare Data Security in Cloud. 2013 International Conference on Recent Trends in Information Technology, pp. 483 (2013).

[10] V. Attasena, J. Darmont and N. Harbi: Secret Sharing for Cloud Data Security: A Survey, pp. 2.

[11] V.K. Saxena, S. Pushkar: Cloud Computing Challenges and Implementations. International Conference on Electrical, Electronics, and Optimization Techniques. pp. 2585-2586 (2016).

[12] S. I. Khan, A. Sayed Md, L. Hoque: Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some Recommendations. Computer Science Journal of Moldova, vol.24, no.2(71), pp 276-277 (2016).

[13] Heng He, Ruixuan Li, Xinhua Dong, and Zhao Zhang. Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud. IEEE Transactions on Cloud Computing, 2(4):471–484, Oct-Dec 2014.

[14] S. Zeadally, T. Islam and D. Manivannan: A Classification and Characterization of Security Threats in Cloud Computing, pp. 1,4-5 (2016).

[15] P. K. Tysowski and M. A. Hasan. Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds. IEEE Transactions on Cloud Computing, 1(2):172–186, July-December 2013.

[16] Will, M., Ko, R.: A guide to homomorphic encryption. The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues, pp. 1-34 (2015).

[17] A. Ghobadi, R. Karimi, F. Heidari, M. Samadi: Cloud computing, Reliability and Security Issue. ICACT 2014. pp. 507 (2014).

[18] A. S. Prasad and S. Rao. A Mechanism Design Approach to Resource Procurement in Cloud Computing. IEEE Transactions on Computers, 63(1):17–30, January 2014.

[19] J.M. Alcaraz Calero, N. Edwards, J. Kirschnick, L. Wilcock, and M. Wray. Toward a Multi-Tenancy Authorization System for Cloud Services . IEEE Security & Privacy, 8(6):48–55, Nov.-Dec. 2010.

[20] C. Papagianni, A. Leivadeas, S. Papavassiliou, V. Maglaris, and C. Cervello-Pastor A. Monje. On the Optimal Allocation of Virtual Resources in Cloud Computing Networks. IEEE Transactions on Computers, 62(6):1060–1071, June 2013.

[21] Y. Tong, J. Sun, S. M. Chow, and P. Li: Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability. IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 2, pp 420-421. March 2014.

[22] R. Shende, S. Kamble, S. Kakde: Health Data Access In Cloud-Assisted E-Healthcare System. International Conference and Workshop on Electronics & Telecommunication Engineering. pp. 170-171 2016