Development Healthcare Information Secure Cloud Implementation by RSA Cryptosystem

[1]Narayana Galla, [2]Sri M.Gnanavardhan
[1]M.Tech (CSE), [2]Assistant Professor
[1,2]K.I.Ts, Markapuram

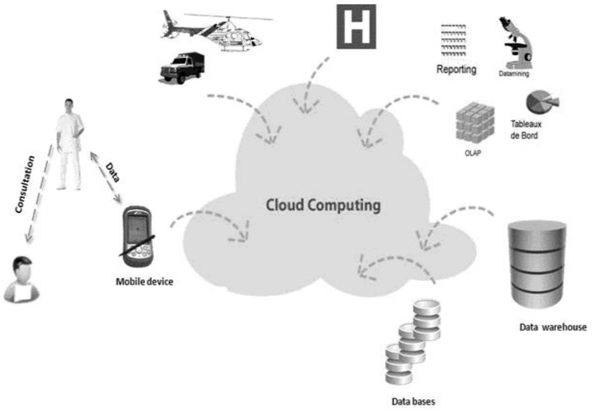
Abstract: Globally the healthcare sector is copious with data and hence using data recover techniques in this area seems shows potential. Healthcare sector collects huge amounts of data on a daily basis. Transferring data into secure electronic system of medical health can save lives and reduce the cost of healthcare services as well as early discovery of infectious diseases with advanced collection of medical data. In this study we have projected a best fit for data recover techniques in healthcare based on a case study. The proposed framework aims to provide self healthcare treatments where by several monitoring equipments using the cyberspace devices have been developed to help patients manage their medical conditions at home for example, diabetic patients can test their blood sugar level by using e-device. It's a better business strategy. Spend time working with your patients, not your patient healthcare software. When your software is installed in your office, you have to deal with potential interruptions such as power outages, software upgrades, hardware failures and human error. Cloud is a new technology used in different types of sectors to improve the effectiveness and efficiency of business model as well as solving problems in business world.

Keywords :* *Healthcare information, RSA Cryptosystem, Medical data, High level architecture of Health care.

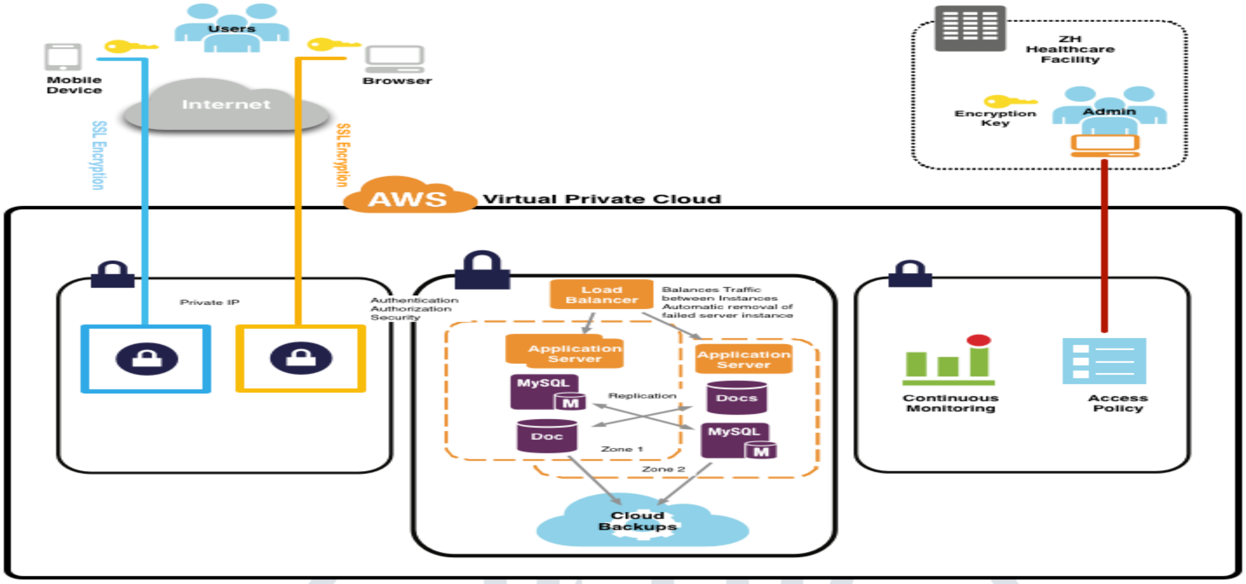
1. INTRODUCTION

Medical data are highly complex and difficult to analyze where as financial data are well organized but pose limited clinical value. Clinical data are very poor from the point of view of automated analysis systems that collect high quality data which will become part of routine clinical care, but are unlikely to have a large patient impact in 5-10 years. In most cases medical data is highly complex and difficult to analyze while financial data is well organized but has limited clinical value. Since the gap is between data gathering and comprehension, this paper proposes the way to fill the gap in Tanzanian context. The proposed framework can be used to predict future medical conditions for deadly diseases occurring in Tanzania. The framework makes predictions on what a patient has already experienced as well as the experience of other patients showing serious medical history. This provides physicians with insights on what might come next for a patient based on experiences of other patients. It also gives a prediction that is interpretable by patients.

The proposed framework can share information across patients who have similar health problems. This allows for better predictions when details of a patient's medical history are sparse. Cloud is an emerging technology used in different types of organizations to improve the efficiency and effectiveness of business processes. The application of cloud technologies would be of great benefit in assembling the required information, for example, in increasing operational efficiencies, fraud detection and enhance the overall decision making in organizations including public sectors. **Cloud** computing techniques analyze large data sets to discover new relationships between the stored data values. Healthcare is an information rich industry, warehousing large amount of medical data. The health-care industry finds it difficult to manage and properly utilize the huge medical data collected through different medical processes. Stored medical data collection is an asset for healthcare organizations if properly utilized. The healthcare industry can use cloud computing techniques to fully utilize the benefits of the stored medical datasets.



2. PROBLEM AND RELATED WORK



There is a lack of knowledge of the status of implementation of cloud computing technology within the healthcare system in Tanzania, the benefits of implementing such technologies and identification of best fit framework. Medical cloud computing is a key technique used to extract useful clinical knowledge from medical records. A number of scoring systems exist around the globe that uses medical knowledge for various conditions but we don't have any in Tanzania. We have number of examples which uses cloud computing for various reasons: Arkansas data network evaluates re-admission and resources utilization, compares the data against current scientific literature and then determines the best treatments to lower spending.

Group health co-operative sorts its patients by their demographic traits and medical conditions in order to discover which groups use the most resources. In this way, programs can be developed to help educate "problem" populations on how to better prevents or manage their conditions.

Investigation of the possible effects of multiple drug exposures at different stages of pregnancy on preterm birth, using Smart Rule, a cloud computing technique for generating associative rules. Framework for video mining in vivo microscopy images to track leukocytes in order to predict inflammatory response which allows researchers to capture images of the cellular and molecular processes in a living organism. Cloud computing based decision tools for evaluating treatment choices for uterine fibroids. The tool use cloud computing techniques to predict treatments choice for fibroids.

3. CLOUD COMPUTING

Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet. *Cloud computing exhibits the following key characteristics:*

Agility improves with users' ability to re-provision technological infrastructure resources.
Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks.
Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.
Multi tenancy enables sharing of resources and costs across a large pool of users.
Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
Utilization and efficiency improvements for systems that are often only 10–20% utilized.
Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford..
Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

4. PROPOSED FRAMEWORK

A proposed framework for Tanzania healthcare can be developed and grouped into four categories: infrastructure, administrative, financial and clinical applications. In the proposed framework two web portals can be developed: one for the clinician and the other one for patients. The framework can be beneficial for Tanzanian people and prove that hospitals can get better results and efficient care through an integrated and organized healthcare system. The figure below shows in detail how the framework should work. The common core component of the framework is an application suite, consisting of different operational application across Tanzania and integrated through a common operational database and this is important because it can ensure standard data and interfaces for clinicians and other users. In order to develop the proposed framework in Tanzania we introduced the following strategies.

Proposed **Fr**amework for Tanzania Healthcare System Clinical Data Exchange standards in Tanzania Healthcare System. *The goal of clinical data exchange standards* is to develop a comprehensive record of patients that will be available virtually anywhere in the country and accessible through any system. Once clinical data exchange have been implemented patients and drugs information should be available from one point to another. If this is not implemented, clinicians can face difficulties to exchange information with other clinicians across the country especially during disasters and emergency response situations. Also medical information cannot be readily available at the point of care.

Align proposed system with Clinical and Administrative Process The Tanzania Healthcare proposed system may not improve patient care if the system is not aligned with clinical and operational processes. Clinical processes refers to the interdependent and collaborative activities that are performed to provide effective and efficient patient care, while administrative process refers to the interdependent and collaborative activities related to operational and financial matter pertinent to patient

Protecting against loss of electronic health information Backups are used, in the very unlikely event, to recover data after loss or corruption. All electronic protected health information and transaction logs are automatically backed up on a schedule allowing the ability to restore the data back to the point of the retention period. Instead of having to maintain an expensive onsite backup system and deal with tapes, backups are automatically performed within the cloud.

These backups are periodically tested to ensure that they work. A backup solution that is not tested is no backup at all.

Protecting from outside threats There are security risks with cloud computing. However, in-house systems also come with risks. In the cloud-based solution the advantage is the technical platform and infrastructure is managed and updated by highly skilled technicians who understand the most current security measures to secure the technical components of the hardware and software to thwart intruders.

Healthcare systems are secured with password protection to prevent unauthorized. Audit logs of data access are available to ensure that data is available only with the appropriate security clearance. In addition we have included additional optional safeguards that may be implemented these include:
As the caretakers of your infrastructure, Healthcare enforces restrictive systems access policies with a stringent policy for passwords, and network access. We maintain system logs and monitoring as a part of our enforcement of these policies.

Keeping your electronic health information protected by using RSA - Cryptosystem

1. Choose two distinct prime numbers p and q.
2. Compute $n = pq$. .
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.
4. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

Encryption

A (party) transmits her public key *(n, e)* to B (Party) and keeps the private key secret. Bob then wishes to send message M to A.
He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c corresponding to

$$c \equiv m^e \pmod{n}$$

This can be done quickly using the method of exponentiation by squaring. B then transmits c to A.
Note that at least nine values of m will yield a cipher text c equal to m, but this is very unlikely to occur in practice for A and B.

Decryption

A can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \pmod{n}$$

Given m, she can recover the original message M by reversing the padding scheme.

Encryption is used to protect the health information while it is in transit. The encryption process encodes the information in a way that unauthorized parties or hackers cannot read it.
We use 2048 bit SSL encryption throughout the entire user session to better protect against security threats. In short, the larger the key size, the more computationally expensive it is for an attacker to use brute force to compromise the infrastructure. The US National Institute of Standards and Technology (NIST) recommends that organizations depreciate the use of 1024-bit keys by year-end 2013.

5. CONCLUSION

When a healthcare Information organization considers moving its service into the cloud, it needs strategic planning to examine environmental factors such as staffing, budget, technologies, organizational culture, and government regulations that may affect it, assess its capabilities to achieve the goal, and identify strategies designed to move forward. This paper provides useful strategic planning references for potential users to start cloud projects. Also proposed that could be applied by a healthcare Information organization to determine its direction, strategy, and resource allocation to move to the cloud paradigm. The model includes 4 stages: identification, evaluation, action, and follow-up. At the first stage, the organization analyzes the current status of the service process and identifies the fundamental service objective. Stage 2 is to evaluate the opportunities and challenges of adopting cloud computing. By using the SWOT analysis, the organization can determine the internal strength and weakness factors as well as the external opportunity and threat factors of adopting the new model. Some potential solutions to handle cloud issues have been also provided. Then, in stage 3, the organization draws up a cloud computing implementation plan. The author suggests that this should include at least the following: determine the cloud service and deployment model, compare different cloud providers, obtain assurance from the selected cloud provider, consider future data migration, and start a pilot implementation. The last stage is to deploy the cloud computing infrastructure and develop a follow-up plan to measure the health care service improvements.

6. REFERENCES

[1] Goldschmidt, P.G. HIT and MIS: Implications of health information technology and medical information systems. *Commun. ACM* **2005**, *48*, 69–74.

[2] Davidson, E.; Heslinga, D. Bridging the IT adoption gap for small physician practices: An action research study on electronic health records. *Inf. Syst. Manag.* **2006**, *24*, 15–28.

[3] Klein, R. An empirical examination of patient-physician portal acceptance. *Eur. J. Inf. Syst.* **2007**, *16*, 751–761.

[4] Young, H.M. Challenges and solutions for care of frail older adults. *Online J. Issues Nurs.* **2003**, *8*, 5.

[5] *HEALTHCAST 2020: Creating a Sustainable Future*. ricewaterhouseCoopers: London, UK, 2006.

[6] Singh, H.; Naik, A.D.; Rao, R.; Petersen, L.A. Reducing diagnostic errors through effective communication: Harnessing the power of information technology. *J. Gen. Internal Med.* **2008**, *23*, 489–494.

[7] Douglas, T.J.; Ryman, J.A. Understanding competitive advantage in the general hospital industry: Evaluating strategic competencies. *Strateg. Manag. J.* **2003**, *24*, 333–347.

[8] Lenz, R.; Reichert, M. IT support for healthcare processes—Premises, challenges, perspectives.*Data Knowl. Eng.* **2006**, *61*, 39–58