ANALYSIS AND DESIGN OF GHANA HEALTH CARE CENTER USING THE NATIONAL IDENTIFICATION AUTHORITY

Sudhakar Murugesan
Department of Information Technology,
Valley View University
Techiman Campus,
P.Box.No: TM 183
Techiman, Ghana
E-mail: sudhakarmtech@gmail.com

ABSTRACT

The regular data access control system is to maintain the selective sharing of composite Personal Health Records (PHRs), cumulating from various healthcare providers in the cloud. This is one of the open researches in the current IT trend. A PHR service permit a patient to create, manage and control the personal health data in one place through the web, which makes the storage space, retrieval, and distribution of the medical information more efficient. Specifically, each patient secure the full control of medical records and can share the health data with a large range of users with healthcare contributors and family members. Due to the high cost of building and keeping up dedicated data centers, many PHR services are outsourced to be made available by third-party service providers. For decentralized data centers the emission of CO2 is high and the environment gets polluted. By designing reusable datacenters, information's or data can be shared through the PHR's. By this we can avoid the high emission of CO2 and enjoy flexibility; availability and compatibility (according to Moore's law). This paper propose and design an architecture which is to show that sharing data through a data centre assure reusability of resources and improve e-Health Care Service.

Keyword: - Green computing, Heath Care, Data Center

1. INTRODUCTION

In recent years, Personal Health Record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers (Boldvreva & Goy, 2008).

The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the other hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. Centre

The goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as personal and professional users, respectively. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. In addition, since those users' access requests are generally unpredictable. There has been a considerable increase in the average temperature of the earth in the past century. This rise in temperature is attributed to the effects of global warming brought about by the accumulation of greenhouse gases (GHG) in the atmosphere (Dong & Dulay, 2010).

The reason for increased GHG, mainly Carbon Dioxide (CO2), is because of the increased energy consumption which results in emission of pollutants. Natural calamities like typhoons, floods and changes in the sea levels are attributed to the CO2 fuelled greenhouse effect. It is estimated that during the last 30 years the CO2 emissions have gone up by 73%. India is ranked 5th amongst the countries in the list of global GHG emission, with USA and China contributing about 4 times emission than that of India. The Kyoto Protocol of 1997, which was signed by over 160 countries, including India, calls on all countries to reduce their emissions of greenhouse gasses by 5%, from the 1990 level, by the year 2012. Many governments around the world, including India have taken steps to reduce energy consumption and emissions. India is committed to reduce carbon intensity by 20-25% between 2005 and 2020. Currently, the ICT sector globally accounts for 0.9 metric gigatons of 0047HG emissions annually, or about 2% of total global emissions; which includes personal computers, servers, cooling equipment, fixed and mobile telephony, local area networks (LAN) and printers (Sadegbi & Winady, 2010).

Table I: Global CO2 Emissions

Global	**Gigatons CO2e 2012**	**Gigatons CO2e 2020**
Global CO2 emissions	40	51.9
Total ICT footprint	0.62	1.43
% of Global emissions	1.70%	2.80%

2. BACKGROUND

Health care IT sector spending in Ghana is currently localized according to user population; for example, more than 60 percent of spending on servers and software. However, many fossil fuel and material resources are located in rural areas, which have fewer than 20 percent of computing users and accounts for less than 25% of IT spending in Ghana. Building up Ghana's National cloud computing infrastructure over the next several decades. Because of recent advances in the health care infrastructure and network computing, moving the servers and datacenters to rural could be advantageous. There's not even a scientific answer to the question of how much energy a including energy used by the client device, network, and datacenter. Creating a clear segregation of data access between different users based on the nature of the users and attributes or relationship with the data owner is the end nature of output for this system. In this project, as usual segregation of users will be done and they didn't talk about the distribution of data among multiple databases. If the data is too complex, this system won't explain how the relativity of data is maintained between the tables and they didn't talk about the performance retrieval of massive data (Hur & Noh, 2010).

Privileged authorization nature given to the data owner which a serious flaw and it should not be case. The reason is, the data should be provided to provide to some of the government associated people to provide more secure nature for running the government institutions. In case of Emergency, the patients face will be detected through Fractal Segmentation concept to retrieve the relevant data of him and in turn an automatic SMS will be sent to the guardian indicating the user's data is accessed by the emergency team.
Building up Ghana's national cloud computing infrastructure over the next several decades. Because of recent advances in the health care infrastructure and network computing, moving the servers and datacenters to rural could be advantageous. There's not even a scientific answer to the question of how much energy a including energy used by the client device, network and datacenter.

Data centre's today typically offer power management and cooling features including fans that speed up or slow down as needed, as well as more-efficient power supplies. Blade servers are more efficient than regular rack servers because blades share a single chassis, as well as power and cooling. IT is a significant user of electricity, and is responsible for more than 2% of the world's carbon footprint – heavily on IT, such as banks and in many other white-collar industries, IT is often responsible for well over half of all electricity consumption for small and medium sized shopping centres. Express Shopping newsletter notifies the customers with recent promotions, and can provide convenience for shopping. Yet the newsletter imposes threat to resource and environment, for its colour ink printing paper (Ibraimi et al, 2009).

3. ARCHITECTURE

Currently The National Identification Authority database which eventually contains details of every Ghanaian and Non-Ghanaian citizen, an individual identity is defined in terms of demographic attributes is name, gender, age and address. But demographic data alone cannot guarantee uniqueness. Unique Identity is possible by linking demographic attributes with bio-metric attributes like fingerprint and iris patterns of the individual, so no need to create new users data's. The real time working of National Identification Authority (NIA). Following is the Operating model of NIA and real time flow of how the transactions take place in NIR model.

With recent advancement in technology, it is now possible to create a digital unique identity for an individual in a large population using bio-metric attributes (fingerprint and iris) which can be verified online. Each unique identity can be assigned multiple identity tokens of various kinds which can be used appropriately for authentication as her the business need of service rendered.

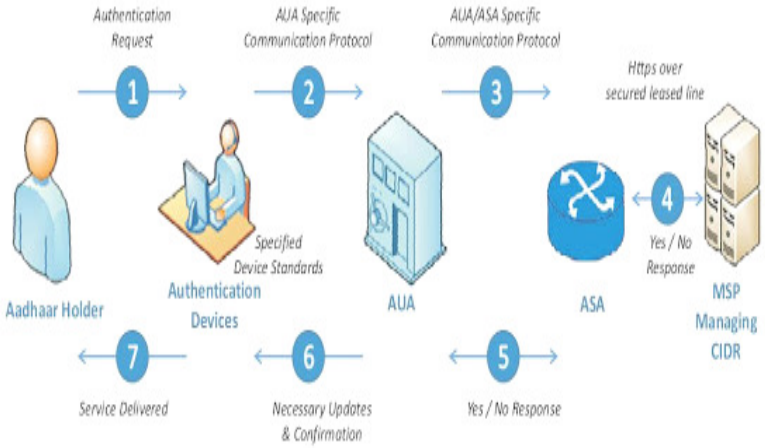

Fig 1: NIA Architecture

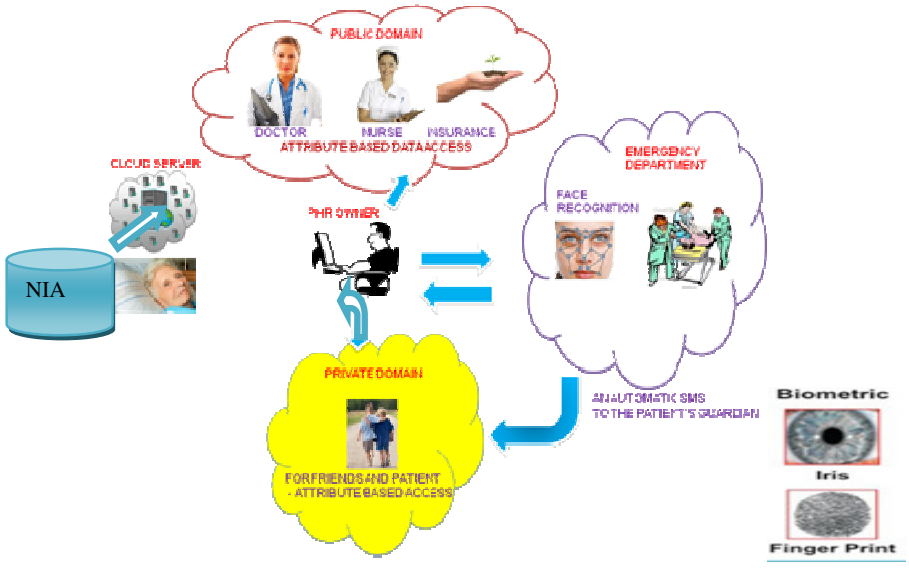

Fig. 2: NIA Data

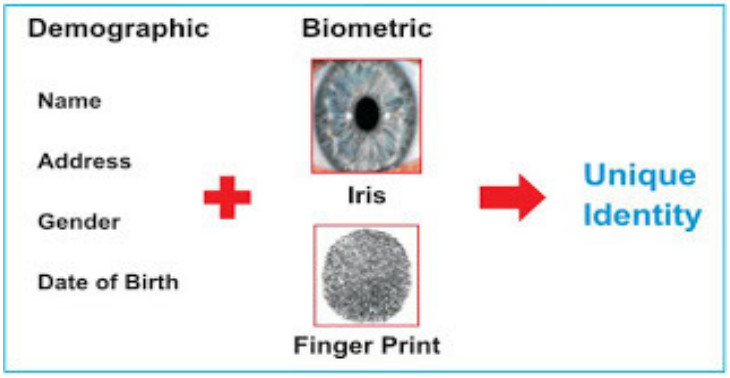

Fig 3: Demography and Identity Based Biometrics

3.1 System Architecture

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

We Endeavour to study the patient-centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In this way, our framework can simultaneously handle different types of PHR sharing applications' requirements, while incurring minimal key management overhead for both owners and users in the system. In addition, the framework enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios (Sadeghi & Winandy, 2010).

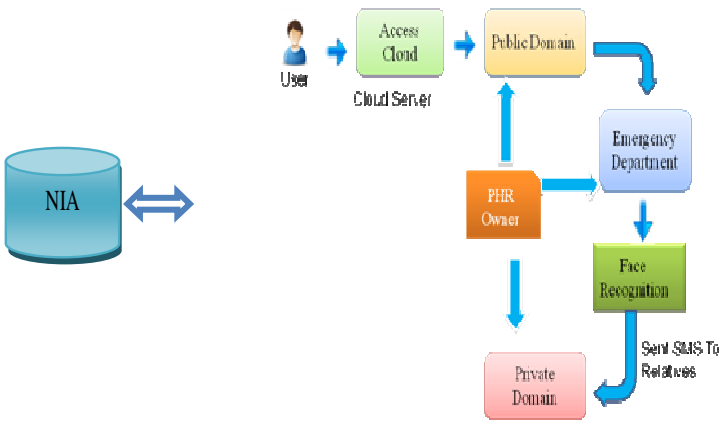

Fig. 4: Data flow Diagram

We demonstrate how our frame-work works using a concrete example. Suppose PHR owner Alice is a patient associated with hospital A. After she creates a PHR file F1 (labeled as "PHR; medical history; allergy; emergency"), she first encrypts it according to both F1's data labels, and a role-based file access policy. This policy can be decided based on recommended settings by the system, or Alice's own preference. It look like p1:= "(profession=physician) ∧ (specialty=internal medicine)∧(organization=hospital A)". She also sends the break-glass key to the ED. In addition, Alice determines the access rights of users in her PSD, which can be done either on-line or off-line. For example, she may approve her friend Bob's request to access files with labels {personal info}or{medical history}. Her client application will distribute a secret key with the access structure (personal info ∨ medical history) to Bob. When Bob wants to access another file F2 with labels "PHR - medical history - medications", he is able to decryptF2 due to the "medical history" attribute. For another user Charlie who is a physician specializing in internal medicine in hospital B in the PUD, he obtains his secret key from multiple AAs. But he cannot decryptF1, because his role attributes do not satisfyP1. Finally, an emergency room staff, Dorothy who temporarily obtains the break-glass key from ED, can gain access toF1 due to the emergency attribute in that key.

The separation of PSD/PUD and data/role attributes reflects the real-world situation. First, in the PSD, a patient usually only gives personal access of his/her sensitive PHR to selected users, such as family members and close friends, rather than all the friends in the social network. Different PSD users can be assigned different access privileges based on their relationships with the owner. In this way, patients can exert fine-control over the access for each user in their PSDs. Second, by our multi-domain and multi-authority frame-work, each public user only needs to contact AAs in its own PUD who collaboratively generates a secret key for the user, which reduces the workload per AA.

4. CONCLUSION

This highlights one of the key issues in Green IT – responsibility. Green IT is such a large topic that it extends far beyond the data center or the IT department. It also affects, and is the responsibility of, end users and lines of business within the organization, the procurement function, and middle and senior management. Sustainability, in all its aspects, is a key business driver in the 21st century. There is an increased realization across society that business practices and individual behavior needs to change. IT has a major role to play. As a major contributor to global carbon emissions its needs to get its own house in order, but more importantly the IT function needs to be more significantly involved in enabling the transition to a true low carbon economy. A novel framework of secure sharing of personal health records in cloud computing is proposed. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations.

REFERENCES

1. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," inACM CCS, ser. CCS '08, 2008, pp.417–426.
2. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010
3. H. L¨ ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," inProceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229
4. Hur and D. K. Noh, "Attribute-based access control with effi-cient revocation in data outsourcing systems,"IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.
5. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flex-ible delegation and revocation of user attributes," 2009.