A Secured Cloud based Health Care Data Management System

Md. Fakhrul Alam Onik
Islamic University of Technology

Syed Sabir Salman-Al-Musawi
Islamic University of Technology

Khairul Anam*
Islamic University of Technology

Nafiul Rashid
Islamic University of Technology

ABSTRACT
With the advent of Information Technology many research works are going on medical data collection. But most of the works are facing shortcomings in management of data. A huge amount of data that is generated by different sensors and uploaded into the server through Wireless Sensor Network (WSN) faces a several types of security, privacy, flexibility, scalability and confidentiality challenges. Existing architectures for patient's health data collection lack of different types of security issues. In this paper, we have proposed a secured *Health cloud* architecture for patient's health data collection. Our work is based on WSN integrated with Cloud computing technology. We have proposed to have Cypher text Policy-ABE within our cloud infrastructure to guarantee data security, privacy and fine grained access control of data. We have also give constraint on attributes of different types of patients to reduce unnecessary data storage. Thus our proposal makes the whole data collection and management technique unique.

General Terms
Cloud Computing, Medical Cloud, Health Cloud.

Keywords
Cloud Computing, Wireless Sensor Network, H-cloud, CP-ABE, Data Encryption, Decryption

1. INTRODUCTION
Over the past three decades, computer systems are used extensively in medical and healthcare systems. For the documentation, storage, processing, analysis and presentation of patient's information storage devices and server systems are used in developed countries today. Yet, most healthcare systems are built on the basis that consists of paper medical records, handwritten test results, non-digitized images, handwritten notes and fragmented IT systems. Sharing of information across providers is inefficient and insecure and portability of data is very rare. Doctors and physician depend on the medical staffs for patient's data, coordinating their care schedules and other administrative systems activities[1]. All these processes are cumbersome and time consuming. So, there exists many more challenges in this sort of systems where a large number of records are stored and data requirements are scalable, flexible, easy to create, update, manage and access etc. but security has topmost priority.

It is found by a research on Healthcare systems in 2009 in USA that half of $2.2 billion that is used in medical and healthcare systems is wasted. So, for improving Healthcare Information Technology (HIT) a Health Information Technology for Economic and Clinical Health (HITECH) Act has been passed. An amount of $18 billion are included for medical records so that records are kept in a format known as Electronic Medical Record(EMR)[2].

Our main focus is the patient's data collection, storage, access, analysis, and presentation etc. We have suggested the current patient data collection techniques are time consuming, inefficient, laborious for the staffs. It is also obvious that currents technique is violating the real time data access for diagnostics or monitoring the patients.

Our proposed solution is based on the concept of "*Cloud Computing"* a distributed computing system where a pool of virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered. We have proposed a "*Health Cloud*" model which is based on Cloud Computing and wireless sensor networks (WSN) concept. Electronic apparatus and machines that are attached to the patient's body containing "Sensor" will send the patient's data to the cloud. Doctors, physicians and medical staffs access the cloud and use those data for further analysis. The patients themselves can also see their personal information , medication etc. We have also followed the *Right Management* Technique [3] which ensures when, by whom and how data are accessed, even after it has been distributed through arbitrary communication channels. *Right management technique* ensures that only authorized users can access the cloud with the unique valid username and password (secret key) and it also ensures the data privacy, security with no intrusion of outsiders in the whole systems. Previously most of the security mechanisms for data are implemented outside the cloud system. Our proposed model security is based on the Attribute Based Encryption (ABE) algorithm that has to be set up within our cloud architecture that will guarantee the security, privacy and confidentiality of the sensed data of the patients. We have also included different access structure policy for different users in the system for the flexibility and dynamicity of the system.

The rest of the paper is organized as follows: section 2 contains related works, section 3 contains cloud computing, section 4 Health Cloud, section 5 contains our proposed Health cloud architecture, section 6 contains Background: Attribute Based Encryption, section 7 contains security and technical challenges, section 8 Simulation and performance analysis and last section contains conclusion and future work.

2. RELATED WORK
Several works have been done using the concept of ubiquitous and distributed computing in medical sector . UbiMon [4] proposed wearable and implantable sensors for distributed mobile monitoring of the patients. Patient's will carry sensors and they relay the vital data of the patients to some nodes for further analysis and processing. But this does not fulfill the requirement of the scalable, securable, and flexible data transfer.

Telemedicine [5] an adaptive communication middleware for home monitoring for heart-patients is being developed. This helps remote monitoring and diagnosis of the patients. There are also some challenges in this kind of systems like-scalable, heterogeneity of the devices, protocols , database management, configuration of server, data security etc.

MobiHealth project, Knostantas *et al.* [6] proposed an Body Area Sensor Network (BASN) prototype and tested that in nine preliminary cases in healthcare . For internal BAN communication they have used Bluetooth and Zigbee. And for communicating with external technologies they have used General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UMTS). But after integration of the total system they did not get the expected result in the end. The exceptions were security, integrity and privacy of the data transmission.

A group of researchers [7] have recently introduced a multitier telemedicine system that can perform real-time analysis on medical data and it also provides feedback to the users and uploads data to the server. It also suffers from the same problems with data integration, privacy and security.

ESPAC [8] collects the data from the patients then at first it sends it to the hospital server and from there it is uploaded into the cloud. There is lack of flexibility and dynamicity of this kind of system. If the Hospital server fails to send the data or the server itself crash for some reasons then the whole data will not be sent. So, this kind of systems lack security and privacy of the data.

Liang et al. [9] proposed a self-controllable access policy for the patients so that they can have easily access to their PHI (Personal Health Information). But this sometimes causes the whole system unsecured. Yu et al. [10] well defined access structure policy based on KP-ABE for managing and storing data in the cloud. Privacy and confidentiality of patient's information and use of secret key for accessing data from the cloud are guaranteed in this kind of system. Besides, many of research works have shown that use of fragmentation after encryption on data makes the data more reliable and improves the system's overall performance as potential intruders always try to compromise more data file to access.

All of the above works they have implemented the security policy outside the cloud which is controlled by Administrator. In reality, this consumes more time for the user requested service and data sometimes becomes unreliable. For that purpose, we have proposed to have the security policy and access structure within the cloud so that the overall system performance regarding with security issues becomes more flexible. We have proposed to implement CP-ABE algorithm in our infrastructure to make the system more reliable.

3. WHAT IS CLOUD COMPUTING

There has been much discussion about what cloud computing actually means. The term cloud computing seems to originate from computer network diagrams that represent the internet as a cloud. Most of the IT companies and research teams such as IBM [11], Gartner [12] and Forrester research [13] have produced white papers to define the meaning of this term. The US National Institute of Standards and Technology (NIST) has developed a definition considering all aspects of it- "*a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction* [14] ".

Cloud computing is becoming one of the most expanding technologies in the computing industry today. It enables its' users migrate their data and computation to the remote place with minimal impact of system performance [15]. It typically provides several benefits that cannot be realized otherwise. The benefits are-

- *Scalable*: Cloud computing provides as much computing power as any user wants. Though the underlying structure is not infinite it mitigates the developer's dependence on any specific hardware.
- *Quality of Service (QoS)*: Unlike the other datacenter and distributed systems, Cloud provides much higher QoS than typically possible. This is due to the lack of the dependence on specific hardware. If one machine fails, other machines can provide the required QoS without hampering system performance.
- *Specialized Environment*: Users use custom interfaces, tools and services to meet their needs. This helps the users to use a new infrastructure with the latest legacy code.
- *Cost Effective*: Users pay as they get the requested service from the cloud providers, thus cloud is referred to as *Payment as a Service* (PaaS). This greatly reduces the risk for institutions which may be looking to build a scalable system.
- *Simplified Interface* - Whether using a specific application, a set of tools or Web services, Clouds provide access to a potentially vast amount of computing resources in an easy and user-centric way. We have investigated such an interface within Grid systems through the use of the Cyberaide project [16, 17].

3.1 Role of Cloud computing in Medical Sector

In today's world most of the healthcare organizations need to modernize their IT infrastructure so that they can be able to provide safer, faster and more efficient healthcare delivery. But this requires a massive upgradation and development of their existing IT infrastructure. But constructing this kind of infrastructures involves huge amount of capital expenditure and sizeable operating and management expenses. But "Cloud technology" mitigates that need to invest in IT infrastructure, by providing access to hardware, computing resources, applications, and services on a 'per use' model. And thus it dramatically brings down the cost and eases the adoption of technology. Several EMR vendors and patrons are offering their cloud-based solutions and providing an alternative approach to help hospitals better manage the overall data management system which formerly needed massive capital IT investments to support EMR implementations.

Health Information Exchanges (HIEs) are established in USA and other developed countries which are cloud-based information repository where information can be more easily shared between hospitals, health systems, physicians, and clinics. Many technology vendors and service providers are emerging today who are already building cloud-based HIEs, many of which are already functioning very efficiently and providing awesome service to patients, administrative authorities, and providers. To improve their research many pharmaceutical companies are adopting cloud and drug development to discover newer, cheaper, and more effective treatment protocols and medicines. Hospitals and physicians have started to use cloud-based medical records and medical image archiving services. The objective is to mitigate the burdensome task from hospital IT departments and allow them to focus on supporting other imperatives such as EMR adoption and improved clinical support systems [18].

4. HEALTH CLOUD (h-Cloud)

Cloud computing actually offers multiple benefits for enterprise computing environments, similarly h-Cloud provides an infrastructure that allows hospitals, medical practices, insurance companies, and research facilities to improve their work capacity in a great extent and computing resources at lower initial capital outlays. Additionally, h-Cloud environments will lower the barriers for innovation and modernization of HIT systems and applications and make the overall health data management system more flexible and scalable.

Besides, information contained within h-Cloud can also be better analyzed and tracked (with the proper information governance) so that health and treatments data, costs, performance, and effectiveness studies can be analyzed and acted upon accordingly. With the help of h-Clouds, patient information can be shared easily and more securely among authorized physicians and hospitals. Thus it provides more timely access to life-saving information and reduces the need for duplicate testing. Besides, in early years cloud-based solutions such as *remote video conference physician visits* is tested where physician checks patients through video conference remotely. Developing this kind of cloud based healthcare solution for rural health and at the event of disasters is fruitful and praiseworthy. Besides, Hospitals and physicians are starting to see cloud-based medical records and medical image archiving services. Objective of this kind of solution is to reduce the burdensome task of the doctors, medical staffs etc. with improved medical systems.

5. PROPOSED h-Cloud ARCHITECTURE

"Figure 1" shows our proposed h-cloud architecture where Wireless Sensor Network (WSN) is integrated with cloud computing for storing patient's health data in the cloud . Our proposed architecture is scalable and able to store a large amount of data generated by sensors. As Patient's healthcare data are very sensitive we propose to have the security mechanism inside the cloud to guarantee data confidentiality, integrity, security, and fine grained access control. Previously security policies are implemented outside the cloud. Unlike existing patient healthcare DB management systems, security enforcement and key management in our solution are totally transparent to users (patients and doctors) and do not require their interventions.

For our model, we have considered two categories of users, healthcare professionals (doctors, nurses, medical staffs) and patients, and is composed of the following modules:

Security manager: It checks user authentication request for logging into the system through *right management* technique where *license key* (user name, password) is used. It also identifies which kind of access request is wanted- *read* or *write* using CP-ABE algorithm. Actually this is the main security part of our total system. We have proposed to implement CP-ABE algorithm here for the security of the data. In shortly, CP-ABE will generate private key and public key to encrypt set of attributes using access structure policy for the health data. The users (doctors, medical staffs and patients) use private key to decrypt and access the files.

Service manager: It is responsible for taking user request and delivers the necessary services according to the request.

Cloud Database: It is actually the cloud storage of the data that are uploaded from the WSN. It contains all up-to-date health data of the patients that are transmitted to it periodically. Health data contains patient's heart beat, blood pressure etc.

Based on the operation our proposed scheme can be classified as follows:

Step 1: Patient's Health Data collection

At the patient's side there is a sensor node which collects patient's health data (heart beat, blood pressure, motion and physiological) from the biomedical equipment that uses electric signal and transmits it to the secured WSN from where data is uploaded to the cloud using a fast and scalable Sensor Data Dissemination mechanism [19] [20].

Step 2: Data Encryption

In this step, CP-ABE algorithm is used to encrypt data. For encryption at first CP-ABE generates a public key and a master key. After that based on the attributes of the users on the system `cpabe-keygen` generates a private key for a set of attributes. Then `cpabe-enc` is used to generate a public key and encrypt the data based on the access structure policy.

Step 3: Access to the cloud and Decryption of Data

To access data from the cloud the users should authenticate and granted access permission. Using *right management* technique this authentication is ensured. From the users (doctors, nurses, medical staffs) side user logs onto the system from their handheld devices or PCs through the WEB 2.0 application using his unique name and password (secret key). User then can decrypt data (cyphertext) if and only corresponding access policy structure supports him and he has the private key of the attributes . We have also proposed an image-based authentication and activity-based access control to enhance security and flexibility of user's access [21].

To achieve fine-grained access control, we have proposed to use Attribute Based Encryption (ABE) technique to encrypt data before storing them on the cloud. Establishing ABE in medical cloud computing is a real challenge. Data are represented by logical expression and encrypted with an access structure in ABE. If the user has the secret key that satisfies access policy then they can easily decrypt those encrypted data. Though ABE consumes much more processing power than symmetric cryptography it is very useful for data encryption. Besides, another advantage of using ABE is that authorization information can be embedded in the encrypted data so unauthorized users cannot have access to the data without secret key. But the situation becomes cumbersome when the data changes access policy [22]. So,when the data changes it's access policy the corresponding data is re-encrypted with the new changed access structure and upload it to the cloud. Another challenge is that who will construct the access structure and given policy and also the secret keys to access those data from the cloud.

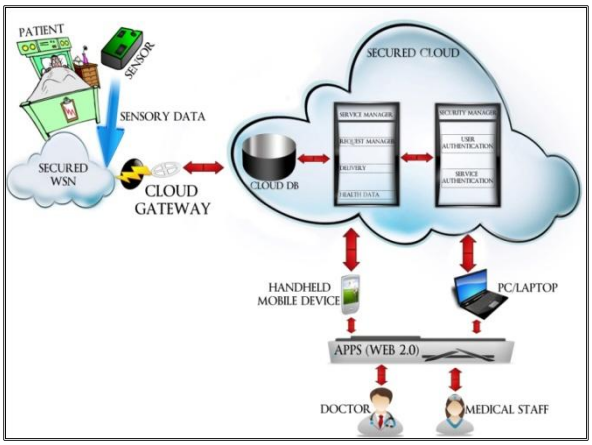


Fig 1 : Proposed H-Cloud Architecture.

For solving the first challenge we have proposed to use both randomly generated symmetric key (**RSK**) and ABE to encrypt data. So, all files are encrypted using a randomly generated symmetric key (RSK) and encrypt the RSK by ABE. Then the encrypted files are uploaded to the cloud DB for user authorized users. Each authorized user has a secret key, if it satisfies the access structure policy then the user can easily decrypt the RSK and hence decrypt the file. If the data changes it's access policy the corresponding data is re-encrypted with the new changed access structure using RSK and upload it to the cloud. Thus the overhead sing ABE is reduced here.

To solve the second challenge we have proposed a new module *Security Manager* which specifies and enforces the security policies of the healthcare institution. It is used by the administrators of the healthcare institutions to define rules as "who can access to what" but it is embedded within cloud.

Based on these administrator specified rules, security manager generates ABE security parameters *access structure* and *secret key*.

The secret key is used for the user privileges on a specific file in the cloud. Since the users have to decrypt data secret key is used for this purpose. Access structure refers to the access policy of the users on the file. Not all users in the system are given the same privileges on all files. For example, only doctors has both the *write* and *read access* policy on the patient records while the nurses have only the *read access*. Thus our proposed system will ensure to improve system usability since a patient has no action to do to secure his data.

Several advantages related to our proposal are-

- It removes the time consuming burdensome task of collecting patient's data manually and possibility of typing errors
- Patient's health data is uploaded in the real time so always up-to-date information is found.
- It ensures the data security and privacy.
- It also provides the way of distant medical healthcare.
- As *Security Manager* is within the cloud so if we implement our CP-ABE security policy within our cloud so there will be some more time can be saved in key generation, encryption and decryption.
- We are defining some fixed attributes for each type of different patients so that unnecessary information about patients cannot be saved in the cloud database. Thus we are proposing to have more flexibility in data management system.

5.1 Policy Enforcement on Access Permission

The security policy of each fragment of data is embedded within the respective fragment using a *sticky policy* method [23]. This policy is cryptographically developed within the fragment so that other policy will not work within the fragment.

Read access of the data fragment is maintained and protected by symmetrically encrypt every single data fragment with a symmetric key. This symmetric fragment key is in turn encrypted with the license key of the user. When any user makes a request it is matched with the user's license key for decrypting the fragment key corresponding rights in the policy.

Write access to a data fragment is maintained by cloud DB. The cloud DB checks users access policy for any fragment that is to be written and granted write privileges (update and delete) to that.

6. BASICS OF CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION(CP-ABE)

Attribute-based encryption (ABE) [24], one of most preferable identity-based cryptographic systems where attributes are taken as input and cryptographic operations are done on those attributes based on defined policies. In shortly, In Attribute-Based Encryption a user's identity is composed of a set, S, of strings which serve as descriptive attributes of the user. For our case the patient's attributes are contact information, disease, medicines, medical tests etc. There is an another set of attributes S_1 that helps a use to decrypt a message if his identity S has at least k attributes matched with the set S_1, where k is a parameter set by the administrator of the system. The Attribute-Based Encryption system only needs to know the description of the user for determining his *secret key*.

The ABE consists of four algorithms:

- Setup (*k*): This algorithm takes security parameter and attribute value as input, k and outputs a master key *MK* to generate secret keys in the Key generation algorithms and a set of public parameters *PK* .
- Key-Gen (*S,MK*): The authority executes the Key-Gen algorithm for generating a new secret key *SK*. The algorithm takes as input a set of user's attributes, *S*, and the master-key MK and outputs a secret key *SK* corresponding to *S*.
- Encryption (M,S_1,PK): This Encryption algorithm takes input a message *M*, with a set of attributes S_1 (access structures) , and the public parameters *PK*. It outputs a ciphertext, *CT*.
- Decryption (CT, S_1, S, SK): The Decryption algorithm is run by a user with identity *S* and secret key *SK* to decrypt a ciphertext *C* that has been encrypted with S_1. With the help of identity attributes *S* and secret key *SK*, this decryption algorithm is used to decrypt a ciphertext *CT* that has been encrypted by *S*. If the set $|S \text{ union } S_1|$ is greater than or equal to k this algorithm shows the decrypted message *M*.

7. SECURITY AND TECHNICAL CHALLENGES

We describe some of the core challenges [25] in designing wireless sensor networks based cloud computing for healthcare applications.

7.1 User Authentication Management

Users can easily access their personal information y through cloud services and make it available to various services across the Internet. An identity management (IDM) mechanism can help authenticate users in the cloud and to do log onto the cloud system. Existing authentication mechanism based on password has some inherent limitation and poses significant risks. For this reason, IDM system should always be able to protect private and confidential information of the users and processes. While users interact with a service provided by the cloud, this service might need to guarantee that their identity is protected from other services with which it interacts. Besides, cloud providers must differentiate customer identity and authentication information from other shared services in the cloud environments.

7.2 Privacy and Protection of Data

Privacy of the data in the cloud computing environment is one of the top most priority challenges. As cloud provides their users as a shared infrastructure so user's personal information are often susceptible unauthorized access and exposure. So, cloud service providers must assure high degree of privacy-

protection mechanisms to guarantee user submitted personal information as well as the stored data in the cloud. As sensed data are sent using Wireless Sensor Network (WSN) so information such as- who created the data, who has the access priority of using these data, what kind of access policy does one have, who modified it and so on are important and they should be kept with maximum level of security protection so that intruders cannot access it.

7.3 SLA and QoS

SLA refers to the part of the service contract where the level of service is defined. The service integrator provides the platform for each individual service provider that helps them to guarantee the QoS as well as SLA. Many cloud service providers use traditional Web Services Description Languages (WSDL) to describe the services such as- bandwidth, delay time, power efficiency etc. Besides, automatic infrastructures that uses different types of wireless devices often lack of QoS and SLAs.

7.4 Access Policy Collaboration

As cloud environment consists of heterogeneous server and each server may have different types of access policy structures and security approaches so synchronization among these should be ensured for the overall performance of the cloud. But for synchronization purpose the QoS and security approaches are sometimes hampered. So, cloud providers should manage and collaborate the access policy among the servers in a way so that no security breaches are occurred.

```
[root@localhost ~]# time cpabe-keygen -o doctor_priv_key pub_key master_key 'employee_category <
3  experience > 5 and 2 of (cardiac_profile,medicinal_profile,surgical_profile) '

real    0m0.067s
user    0m0.060s
sys     0m0.000s

[root@localhost ~]# time cpabe-enc pub_key doctor1.pdf 'employee_category = 3 and experience = 9
and 2 of (cardiac_profile,surgical_profile,medicinal_profile)'

real    0m0.154s
user    0m0.140s
sys     0m0.008s

[root@localhost ~]# time cpabe-dec pub_key hasnat_priv_key medicaldata.cpabe

real    0m0.056s
user    0m0.036s
sys     0m0.016s
```

Fig 2: Example of the usage of Cpabe toolkit.

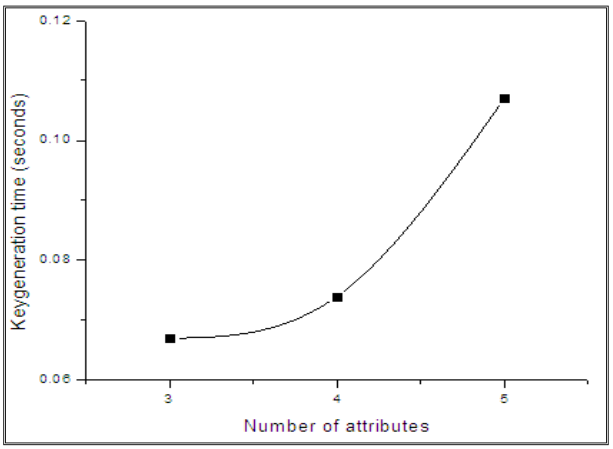
8. SIMULATION AND PERFORMANCE ANALYSIS

For the simulation purpose we have used *cpabe* toolkit [26]. It is an open source package for cryptography used in LINUX environment. It is composed of four algorithms that we have described earlier. We have done our simulation in Red Hat Linux 5.0 using VMware 7.0. All the experiments are carried out in VM ware which provides default 1.66 GHz single-processor with 1 GB RAM. As our proposed architecture and implementation of the ABE algorithm in our system will provide the maximum security and confidentiality of the data, for this we have simulated the ABE algorithm many times with data having different number and types of attributes to clarify the result.

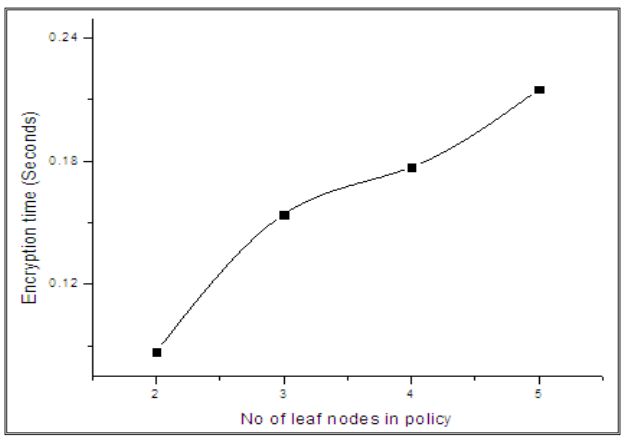
"Figure 2" provides a sample usage of ABE in our simulation. Cpabe-keygen command generates a private key for the set of attributes- cardiac_profile, medicinal _profile and surgical_ profile for a doctor. We have changed the attributes number different times and tested each time. Cpabe-enc tool is then used for encryption of data. It generates a public key which encrypts a file under a defined access structure policy. This policy allows doctors and other medical staffs to decrypt the file. Cpabe-dec tool allows the users to use a private key to access the encrypted files. As each user has different access structure policy for accessing data from the cloud our proposed module "*security Manager"* automatically defines the access policy for the user identifying user category. Thus our system provides fine grained access structure and which enhances our overall system security.

8.1 Performance Measurement

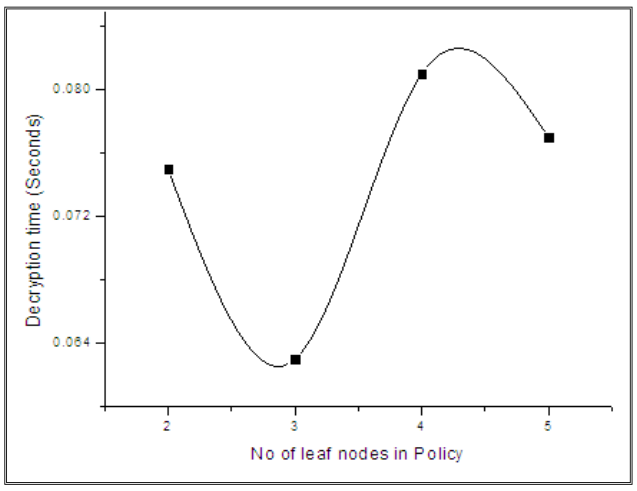
We have provided some simulation results that we have found using cpabe toolkit. We have calculated total time for generating key, encryption and decryption. "Figure 3" shows our simulation result based on private key generation time, encryption time and decryption time. We have found the time running *cpabe-keygen, cpabe-enc and cpabe-dec* by using different number of attributes thus changing access tree size.



(a) Key generation time



(b) Encryption tim



(c) Decryption time

Fig 3: Performance analysis using Cpabe toolkit.

cpabe-keygen should have run linearly with the increasing number of attributes. As we have tested key generation time with less attributes so it is found at first it becomes curve (actually graph with many attributes does not show any curve) and then increases linearly with number of attributes. Our assumption is that patients do not have more than a predefined number of attributes according to his/her disease types. We have assumed it for the flexibility of the data. Similarly, with the increasing number of leaf nodes in policy the running time of *cpabe-enc* at first increase linearly and then creating a curve shape it again becomes linear with time. But for measuring the running time of *cpabe-dec* we have faced difficulties as it depends on the access tree and number of attributes. For the variation on the decryption time, we ran *cpabe-dec* two times on a series of randomly generated attributes and found the curve that is in "Figure 3(c)".

From the figure it is easy to see that decryption time randomly increases with the amount of leaf nodes in the access policy. Our simulation should be optimal as we are implementing CP-ABE within the cloud in *Security Manager*. Previously it is implemented on *Healthcare Administration* or others administrative parts of the system which is actually supervised by human experts. But our proposed solution will have it in cloud architecture so that the overall time for key generation, encryption and decryption should be less compared to the other implementation. Besides, it also reduces the overhead to generate private keys for unwanted attributes of the patient as we have proposed to define a fixed number of attributes for the flexibility of the system. Thus our proposed solution will provide topmost security and confidentiality of the patient's health data.

9. CONCLUSION

In this paper, we have demonstrated the challenges of storing data using cloud computing technology. Accordingly, we have proposed a *Health Cloud* architecture for secured data management of the patients. To implement a fine grained privacy and security policy, We have proposed to implement Cipher text-Policy Attribute Based Encryption **(**CP-ABE**)** algorithm within our proposed *Security Manager* module in our system. Our system allows the users to have a fine grained access control using private keys to decrypt the encrypted files. Through performance evaluation we have measured the time needed for key generation, encryption and decryption. We are claiming that if we implement the CP-ABE algorithm in the cloud then there will be less performance overhead for the security and confidentiality of the data. Because it does not need to check whether a user in the cloud is doctor or other medical staff or patient. As at the time of authorization in the cloud, the user always defines his/her category or type in the system. So, there is no need for an administrative person to do the same and we have proposed to have an automotive system. It would be more efficient if we can implement the whole "Health Cloud" architecture and find out the limitations. In our upcoming research, we are planning to implement the whole system and to go through more to performance evaluation of key generation time, encryption time and decryption time.

10. REFERENCES

[1]http://www.cloudbook.net/downloads/index.php?file=cloudbook-magazine-aug- 2010.pdf

[2] http://www.dynamicglobalstaffing.com/news

[3] Milan Petkovi´c, "Rights Management Technologies: A Good Choice for Securing Electronic Health Records?". In ISSE/SECURE 2007: securing electronic business processes: highlights of the Information Security Solutions Europe/SECURE 2007 Conference, page 178. Springer, 2007

[4] Ng, J., Lo, B., Wells, O., and Sloman, M. (2004). Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon). In Proceedings of the International Conference on Ubiquitous Computing (Ubicomp).

[5] Singh, G., O'Donoghue, J., and Soon, C. K. (2002), "Telemedicine: Issues and Implications". Technology Health Care,10(1):1–10

[6] D. Konstantas et al., "Mobile Patient Monitoring: The MobiHealth System". Proc. Int'l. Cong. Med. and Care Compunetics, Hague, The Netherlands, 2–4 June 2004

[7] E. Jovanov et al., "A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation". J. NeuroEng. and Rehab., vol. 2, no. 11, Mar. 2005, p. 6.

[8] Mrinmoy Barua*, Xiaohui Liang, Rongxing Lu and Xuemin Shen. "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud Computing", International Journal of Security and Networks, 2011

[9] X. Liang, R. Lu, X. Lin, and X. Shen. "Patient self-controllable access policy on phi in healthcare systems", AHIC 2010, Kitchener, Ontario, Canada, pp.1–5

[10] S. Yu, C. Wang, K. Ren and W. Lou, (2010), "Achieving secure, scalable, And fine-grained data access control in cloud computing", INFOCOM, 2010 Proceedings IEEE, San Diego, CA, USA, pp.1–9.

[11] IBM, Staying aloft in tough times, 2009

[12] C.D. Plummer, T.J. Bittman, T. Austin, D.W. Cearley and D.M. Smith. Cloud Computing: Defining and Describing an Emerging. Phenomenon, 2008

[13] Staten, J., Is Cloud Computing Ready For The Enterprise? 2008.

[14] Mell, P. and GRANCE, T. 2009. Draft NIST Working Definition of Cloud Computing.

[15] L. Wang, G. von Laszewski, A. Younge, X. He, M. Kunze, and J. Tao. Cloud computing: a perspective study. New Generation Computing, to appear in 2010.

[16] G. von Laszewski, A. Younge, X. He, K. Mahinthakumar, and L. Wang. "Experiment and Workflow Management Using Cyberaide Shell", 4th International Workshop on Workflow Systems in e-Science (WSES 09) in conjunction with 9th IEEE International Symposium on Cluster Computing and the Grid. IEEE, 2009

[17] G. von Laszewski, F. Wang, A. Younge, X. He, Z. Guo, and M. Pierce, "Cyberaide JavaScript: A JavaScript Commodity GridKit". GCE08 at SC'08. Austin, TX: IEEE, Nov. 16 2008.

[18] http://csrc.nist.gov/ publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[19] L. Vinh, X.H. Le, S. Lee. "Semi Markov Conditional Random Fields for Accelerometer Based Activity Recognition (submitted)".

[20] M. Hassan, E. Huh, " A Framework of Sensor-Cloud Integration:Opportunities and Challenges". International Conference on Ubiquitous , Information Management and Communication.

[21] H. Jameel, R.A. Shaikh, H. Lee and S. Lee. Human Identification through Image Evaluation Using Secret Predicates. Topics in Cryptology - CT-RSA 07, LNCS 4377 (2007) 67–84.

[22] Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah and Yacine Challal "Secure and Scalable Cloud-based Architecture for e-Health Wireless sensor networks"

[23] M.C. Mont, S. Pearson, and P. Bramhall. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. In Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on, pages 377–382. IEEE, 2003

[24] A. Sahai and B. Waters, "Fuzzy Identity-Based encryption," in LectureNotes in Computer Science, vol. 3494, 2005, pp. 457–473

[25] Hassan Takabi and James B.D. Joshi, Gail-Joon Ahn", Security and Privacy Challenges in Cloud Computing Environments", IEEE computer society,

[26] CP-ABE toolkit : http://acsc.cs.utexas.edu/cpabe.