International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 4 (April '2016)

PATIENT CENTRIC FRAMEWORK FOR HEALTH CARE SECTOR

A.Pavithra,
UG Scholar,
Student of Information Technology,
VelTech University,
Chennai, India.

A.Maria Sharmila,
UG Scholar,
Student of Information Technology,
VelTech University,
Chennai, India.

M.Uvaneshwari,
Assistant Professor/IT,
VelTech University,
Chennai, India

Abstract: In health care, a basic requirement for attaining persistence of care is the unlined access to circulated patient health records in an incorporated and merged manner, directly at the point of care. However, Health care Sector holds an important amount of sensible information, and permitting data to be accessible at many various sources increases concern associate to patient privacy and data theft. Access control results must ensure that only clearance for users have access to such critical records for licit purposes, and access control policies from disseminate Health care Sector must be correctly reverberated and implemented consequently in the incorporated Health care Sectors. In this paper, we propose an incorporated access control scheme that subscribe patient centric framework of virtual composite Health care Sectors using various levels of coarseness, conciliating data aggregation and privacy protection essentials. We also enunciate and address problem and mechanisms on policy anomalousness that occur in the composition of distinct access control policies from various data sources.

Keywords: *Attribute Based Encryption, Cloud Computing, Health Care Record, Multi-Authority Attribute Based Encryption, Cipher Text-Policy Attribute Based Encryption, Personal Health Record.*

I.INTRODUCTION

In the developed world, healthcare has acquired to a point where patients can have lot of providers containing primary care physicians, specialists and even alternative medicine practitioners to address their various medical needs. It is not rare for patients to visit supplier who are physically detached from one another; some are situated across town, while others are across the country. As an outcome, medical records can be found disconnected end-to-end full health sector. From the clinical view, delivering proper patient care necessitate access to merged and integrated patient data that is often gathered in real-time to control the freshness of time-sensitive data.

Yet the information dissemination in current healthcare settings typically results in scrupulous, time-consuming endeavor to prevail a patient's complete medical account, or not necessary duplication of tests and other probe. A practical and predicting approach would be to encrypt the information before outsourcing. Personal Health Record owners have to resolve about encryption of files and access security to users. User with representing decryption key can access personal health record file, while continue confidential to rest of users. Patient can grant and revoke access privileges when it is mandatory. The authorized users may either necessitate accessing the Personal Health Record for private purpose of professional use.

We resolved to two categories personal and professional user's resp. in order to protect personal health information lay on semi trusted servers, we follow attribute based encryption as the main encryption primitive. Using attribute based encryption, in a selective manner patient can share his/her personal health record among set of users by encrypting files under a set of attributes without acknowledge complete list of users. To incorporate attribute based encryption into huge scale personal health record system significant problem such as key management scalability, dynamic policy updates and efficient on require revocation are nontrivial to resolve and remains mostly up-to date.

2. BACKGROUND RESEARCH

Attributes define, sort out, or comment the data point to which they are specified. However, traditional attribute architectures and cryptosystems are poorly supplied to provide security in the face of various access prerequisite and environments.
In this paper, we introduce emerging attribute-based encryption primitives, based on this primitives introduce a

novel secure information management architecture. A policy system that fulfills the needs of complex policies is well formed and instance.

Based on the prerequisite of those policies, we present cryptographic optimizations that immensely betterment enforcement efficiency [1]. We develop a new methodology for applying the anterior techniques to prove selective security for working encryption systems as a direct component in formulating proofs of full security.

This intensifies the relationship between the selective and full security models and allows a path for changing the best qualities of selectively secure systems to fully secure systems. In particular, we exhibit a Cipher text-Policy Attribute-Based Encryption scheme that is turn out fully secure while equalizing the efficiency of the state of the art selectively secure systems [2].

Cipher-text policy Attribute-Based Encryption permit to encrypt data under an access policy, specified as a logical compounding of attributes. Such cipher texts can be decrypted by anyone with a set of attributes that fits the policy. We acquaint the concept of Distributed Attribute-Based Encryption, where an arbitrary number of parties can be present to observe attributes and their representing secret keys.

This is in crude contrast to the classic CP-ABE schemes, where all secret keys are distributed by one central trusted party. We render the first construction of a DABE scheme; the construction is very effective, as it necessitates only a invariant number of pairing performance during encryption and decryption [3]. Complex access policies with AND,OR and NOT gates supports a new public- key and provably secure attribute based broadcast encryption scheme. This scheme, for pay-TV system especially pointing the implementation efficiently, can manage conjunctions of disjunctions by construction and disjunctions of conjunctions by concatenations, which are the most normal forms of Boolean expressions.

It is based on an alteration of the Boneh-Gentry- Waters broadcast encryption scheme in order to attain attribute collusion resistance and to subscribe composite Boolean access policies. The security of our scheme is demonstrated in the generic model of groups with pairings. In conclusion, we compared our scheme to various other schemes, both in terms of bandwidth prerequisite and implementation costs [4].

A new approach which enables secure storage and operated sharing of patient's health records in previously mentioned scenarios. A new form of the cipher text-policy attribute-based encryption scheme is suggested to implement patient/ organizational access control policies such that everyone can download the encrypted data, but authorized users from the professional domain are allowed to decrypt it or only authorized users from the social domain [5].

3. MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION (MA-ABE)

Attribute based encryption specifies decryption ability based on a user's attributes. In a multi-authority Attribute based encryption strategy, multiple attribute-Authorities scanned various sets of attributes and problem proportionate decryption keys to users and encryptions can involve that a user obtain keys for suitable attributes from each authority before decrypting a message. Multi-authority attribute Based Encryption scheme using the concepts of a trusted central authority and global identifiers. However, the CA has the power to decrypt every cipher text, which seems for some reason mutually exclusive to the original aim of distributing control over many potential un-trusted authorities.

Moreover, in that construction, the use of an ordered GID allowed the dominance to aggregate their data to build a full profile with all of a user's attributes which without any necessity compromises the secrecy of the user. In this paper, we suggest a solution which transfers the trusted central authority, and protects the user's privacy by precluding the authorities from pooling their data on special users, thus making attribute based encryption more usable in exercise.

Multi-authority attribute based encryption is to better the security and keep off key escrow issue. Each attribute authority in it regularizes a disjoint subset of user role attributes, while none of them entirely is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized close-grained role-based access policies during file encryption.

In the personal domain, owners instantly assign access prerogative for private users and encrypt a PHR file under its data property. Furthermore, we raise MA-ABE by assigning forward an efficient and on-demand user annulment scheme, and prove its security under standard security suppositions. In this way, patients have full private control over their personal Health records.

4. MODULES EXPLANATION

Registration Module

This module is used to store all data about the patient, doctor and patient relations information and also hospital details.This model is common for all the hospitals each hospitals should register their id and necessary details then they will get the username and password. The admin from the particular hospital will gather all the necessary data about the patient i.e. name, age, phone no, and mail id, address etc. The admin will register the data in the hospital database then he will render a user name and password to the patient mail id and also to mobile. Over here the sub modules are patient, doctor, and patient relations data. This module helps the management to

store the data about patient chronicle from the first with personal information's.

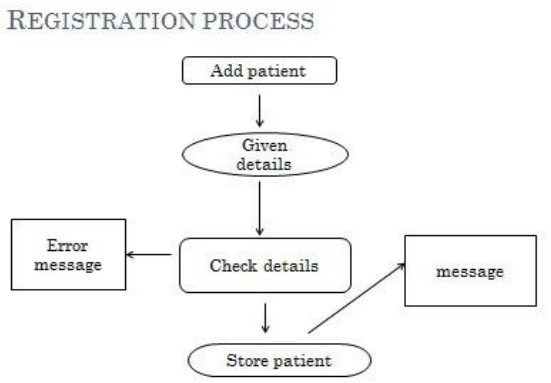

Figure 1: Registration Module

Authentication and Verification Module

The user will be logged in by enter the login details, after receiving the username and password from the registration module.

Over here this module will execute the authentication and confirmation process in the database, if the id is consist of new user he will be getting the new registration or else the user will get their home page screen. Else he will get the error message like check your user and password.

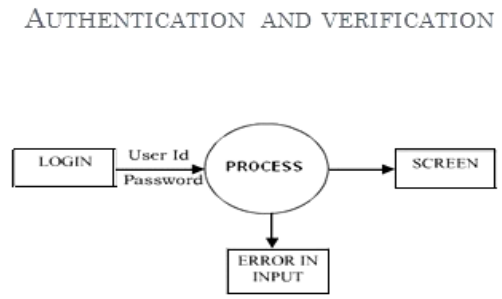

Figure 2: Authentication and Verification Module

Transaction Module

In this module, regular updating the patient test report and their status will be observed. The sub modules are blood test, x-ray test, master health check up, patient's relative comments and doctor's comment about patient. This module will give brief idea about the status of the patient like prescription details, medicine list, in case the patient is admitted into other hospital they will be easily discovered the patient status in the transaction module information's.

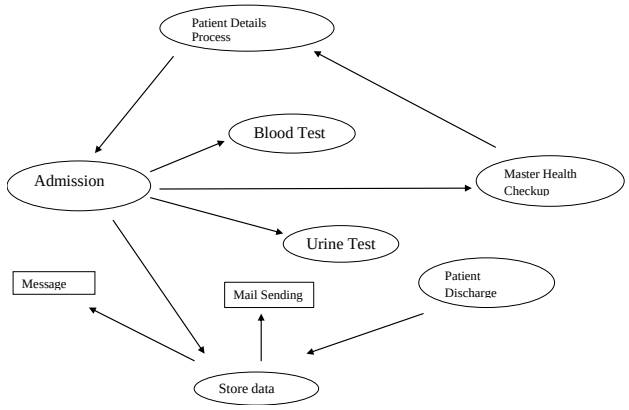

Figure 3: Transaction Module

Encryption Module

In this module, patient id is encrypted by using hmac md-5 algorithm and it is mailed to the cloud database. So the unauthorized person cannot track the patient id in the database. If another hospital need to access the particular patient record database they want to click the view other hospital information in this module by submitting their Id, name of the patient Id and also the hospital name, then they will get OTP to their email id.

By using that they can able to view the patient personal record for the particular instance. To improve the security I have added the three features in my module one is OTP, image is updated in the DB, assigning the patient ids in random way then that id will be decrypted.

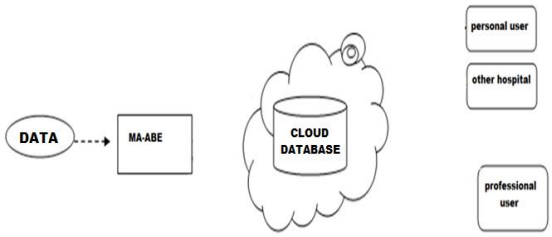

Figure 4: Encryption Module

Sample Snapshot

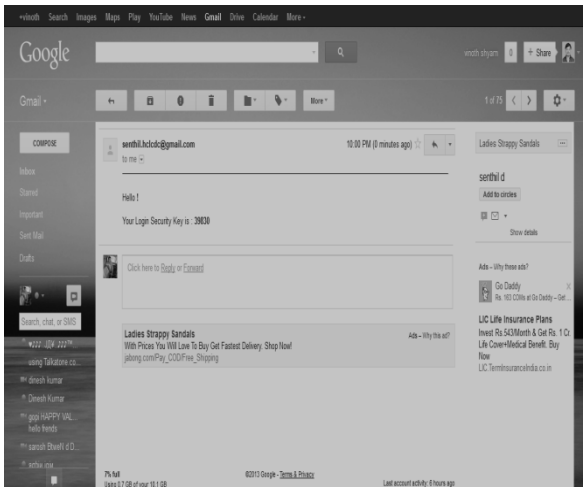

Figure 5: OTP is delivered to corresponding hospital admins mail id

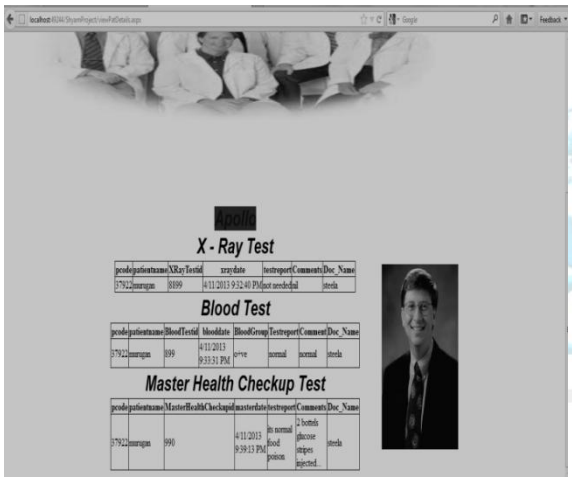

Figure 6: Summarised Personal Health Record

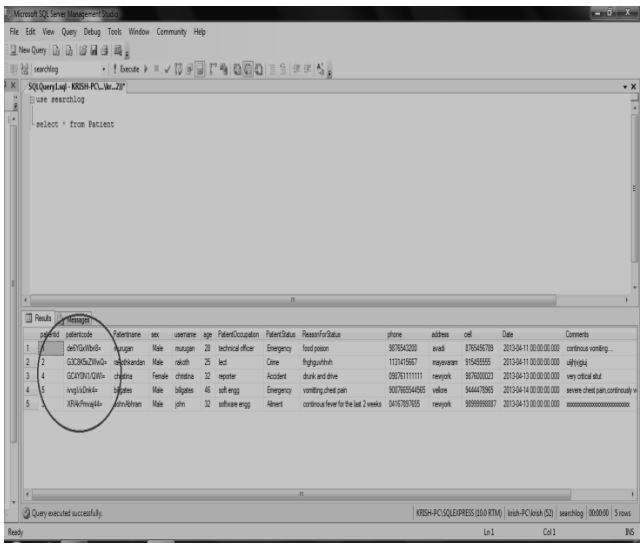

Figure 7: By using MA-ABE, patient unique user id is encrypted in the data base.

5. CONCLUSION

In this Proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers using MA-ABE and CC-MAABE method that provides effective solution to some of the issues related to on-demand user revocation and its security. Though implementation and simulation, we show that our solution is both scalable and efficient.

The results suggested that the proposed design would provide reasonable performance and also reduce the Complexity of key management while enhance the privacy guarantees compared with previous works. Future work will improve the security solution implement HIPAA requirements, using HTTPS and will evaluate the results through measuring the interoperability degree achieved by the presented solution.

REFERENCE

[1] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," Journal of Computer Security, vol. 18, no. 5, pp. 799-837, 2010.
[2] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.
[3] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.
[4] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.
[5] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.
[6] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm'10, Sept. 2010, pp. 89–106.
[7] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.
[8] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," BMJ, vol. 322, no. 7281, p. 283, Feb. 2001.