Personal Health Data Storage Protection on Cloud using MA-ABE

M.Rajeev Kumar,
Asst. Professor / IT
Veltech University,
Chennai, Tamilnadu, India.

M.Dhilsath Fathima,
Asst. Professor / IT
Veltech University,
Chennai, Tamilnadu, India.

M.Mahendran
Asst. Professor / IT
Veltech University,
Chennai, Tamilnadu, India.

ABSTRACT

Online personal health record (PHR) enables patients to handle their individual medical records in a centralized way, which really facilitates the storage, access and distribution of personal health data. With the appearance of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to like the flexible resources and diminish the operational cost, but by storing PHRs in the cloud, the patients be unable to find physical control to their personal health data, which makes it required for each patient to encrypt her PHR data prior to uploading to the cloud servers. Under encryption, it is difficult to achieve fine-grained access control to PHR data in a scalable and well-organized way. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. In this paper, we suggest a new patient-centric frame work and a suite of mechanism for data access control to PHRs stored in semi-trusted servers. To allow fine-grained and scalable access control for PHRs, we control attribute based encryption (ABE) techniques to encrypt every patient's PHR data. Different from earlier works in protected data outsourcing, we center on the multiple data owner scenario, and separate the user in the PHR system into multiple security domains that really decreases the key managing complexity for owners and users. In this way, a high degree of patient privacy is assured concurrently by developing multi-authority ABE and CC-MAABE.

Keywords

Cloud Computing, ABE, CC MA-ABE, MA-ABE, Personal Health Records.

1. INTRODUCTION

As Cloud Computing turn into prevalent, more and more susceptible information are being centralized interested in the cloud, such as emails, personal health records, government documents, etc. In recent years, personal health record (PHR) has appeared as a patient-centric model of health information swap over. It lets a patient to make, handle, and organize his/her personal health data in one place during the web, which has finished the storage space, retrieval, and distribution of the health information more efficient. Each patient has assured the full control of his/her medical records and can share their health data with broad range of users, as well as healthcare providers, family members or friends. To building and retaining specialized data centers many PHR services are outsourced to or supplied by third party service supplier. There are lots of security and time alone risks in PHR services broad adoption. Third party services providers of personal health information (PHI) obstruct main concern to the long-suffering as they cannot completely trust and third party storage server is regularly under attack by a variety of malicious behaviors which could guide to experience of PHI.

A possible and hopeful approach would be toward encrypting the data prior to outsourcing. PHR owners have to decide regarding encryption of files as well as access security to users. User with equivalent decryption key can access PHR file, while remain confidential to rest of users. Patient can award and cancel access rights when it is necessary. The authorized users could either need to access the PHR for personal use of specialized reason. Example of the previous is family members and friends while the later on can be medical doctors, pharmacists and researchers, etc. This paper can conclude to two categories individual and professional users' correspondingly. In order to keep personal heath data stored on semi trusted servers, this paper obtain on attribute based encryption (ABE) as the major encryption primitive. Using ABE, patient be able to selectively distribute his/her PHR among set of users by encrypting files under a set of attributes without knowing complete list of users. To integrate ABE into large scale PHR system, significant issues such as key management scalability, lively policy updates and efficient on demand revocation are nontrivial to resolve and remains largely up-to-date.

1.1 Personal Health Record

The Public health operational group explains PHR as: an electronic function through which individuals can access, handle and distribute their health information, and that of others for whom they are certified, in a private, secure, and confidential environment .The Personal Health Record (PHR) is an Internet-based set of tools that let people to contact and synchronize their lifetime health information and build suitable parts of it available to those who want it. PHRs present an integrated and complete view of health information, including information people make themselves such as warning signs and medicine use, information from doctors such as analysis and test results, and information from their pharmacies in addition to insurance companies. Individuals access their PHRs by means of the Internet, via state-of-the-art security and privacy controls, at some time as well as from every location. Family members, doctors or school nurses can observe parts of a PHR when essential and emergency room staff can retrieve vital information from it in an emergency. People are able to use their PHR as a communications hub: to send email to doctors, move information to experts, obtain test outcome and access online self-help tools. PHR connects each of us to the unbelievable possible of current health care and provides us control over our own information.

1.2 Novel on the Personal Health Record

The PHR is a single, person-centered system planned to track and support health activities across one's entire life experience; it is not restricted to a single organization or a single healthcare provider. The PHR be different from the electronic medical record (EMR) - a programmed platform designed for managing full medical information collected during a hospital stay or in a doctor's office. EMRs regularly contain a health record, doctors' explanation and laboratory and radiology consequences and are normally owned by and limited to the information collected by one doctor or hospital. The EMR not often contains information provided via the patient. Not all doctors use electronic medical records and many different systems exist, so when people change doctors or move to a new city their personal health information does not move with them. Health professionals are now approving new data principles that will formulate transfer of clinical data between doctors more common, but even connecting different doctors' medical record systems will not tie together all the important health information for each patient. An EMR might point out that a doctor wrote a prescription, but it would not show whether the patient filled the prescription, took the medication or if the treatment.

2. RELATED WORKS

In order to keep the personal health data stored on a semi-trusted server, we assume attribute-based encryption (ABE) as the key encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which permits a patient to selectively split her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a whole list of users. To recover upon the scalability of the above solutions, one-to-many encryption techniques such as ABE can be used. There has been a growing interest in applying ABE to protected electronic healthcare records (EHRs).

Key escrow (also known as a **"fair" cryptosystem**) is an agreement in which the keys required to decrypt encrypted data are held in escrow so that, under certain situation, a certified third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may desire to be capable to view the contents of encrypted communications.

Drawbacks

- Data's are saved in encrypted format by means of public key encryption.
- Providing a smaller amount security to data's.

2.1 Attribute Based Encryption (ABE)

By means of ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively distribute her PHR amongst a set of users by encrypting the file under a set of attributes, exclusive of the need to identify an absolute list of users. The difficulties per encryption, key making and decryption are simply linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, central issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date.

The Block Diagram for Existing system is given in Fig 1.

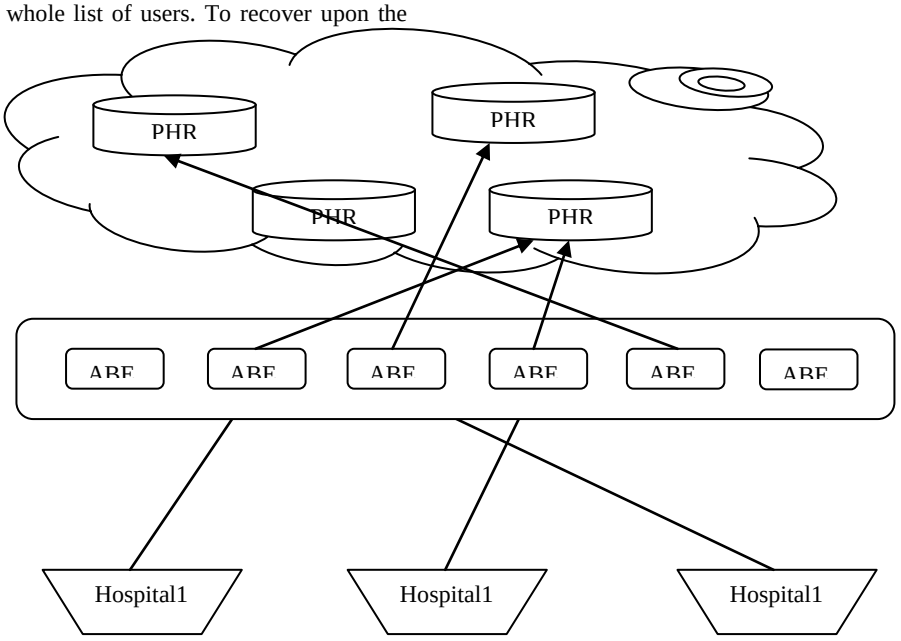

Fig 1: Existing System Diagram

EXISTING SINGLE AUTHORITY SYSTEM

2.2 Secure Attribute Based Structures

Attributes describe, categorize, or interpret the datum to which they are assigned. However, traditional attribute architectures and cryptosystems are unprepared to provide security in the face of various access requirements and environments. M.Pirretti [4] introduces a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives. A policy system that meets the requirements of complex policies is defined and demonstrates. Based on the needs of those policies, we offer cryptographic optimizations that greatly improve enforcement effectiveness.

2.3 New Testimony techniques intended for Attribute-Based Encryption: Accomplish Full Security through Selective Techniques

M.Li et at., [5] develop a new methodology for utilizing the prior techniques to prove selective security for functional encryption systems as a direct ingredient in devising proofs of full security. This deepens the relationship between the selective and full security models and provides a path for transferring the best qualities of selectively secure systems to fully secure systems. In particular, we present a Ciphertext-Policy Attribute-Based Encryption scheme that is proven fully secure while matching the efficiency of the state of the art selectively secure systems.

2.4 Expressive Key-Policy Attribute-Based Encryption by means of Constant-Size Ciphertexts

The key-policy attribute-based encryption (KP-ABE) systems tolerate for non-monotonic access configurations (i.e., that may contain negated attributes) and with invariable cipher-text size. Towards attains this goal, we show that a certain class of identity-based broadcast encryption schemes broadly yields monotonic KP-ABE [3] systems in the careful set model. We then illustrate a new well-organized identity-based revocation system that, when joint with a particular instantiation of our general monotonic structure, gives increase to the truly expressive KP-ABE understanding with constant-size ciphertexts. The downside of these new constructions is that private keys have quadratic size in the number of attributes. On the other hand, they diminish the number of pairing assessments to a constant, which come out to be an exclusive feature among communicative KP-ABE schemes.

2.4 Distributed Attribute-Based Encryption

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) allows encrypting data under an access policy, specified as a logical combination of characteristics. Such ciphertexts can be decrypted by anyone with a set of attributes that fits the policy. L.Ibraimi [6] commences the concept of Distributed Attribute-Based Encryption (DABE), where an arbitrary number of parties can be present to preserve attributes and their equivalent secret keys. This is in stark contrast to the classic CP-ABE schemes, where all secret keys are dispersed by one central trusted party. We provide the first construction of a DABE scheme; the construction is very efficient, as it needs only a constant number of pairing actions during encryption and decryption.

2.5 An Efficient Public-Key Attribute-Based Broadcast Encryption Scheme Allowing Arbitrary Access Policies

C.Dong et at., [7] explain a new public-key and provably protected attribute based transmit encryption system which chains composite access policies with AND, OR and NOT gates. Our idea, particularly targeting the execution of proficient Pay-TV systems, can handle combination of disjunctions by creation and disjunctions of conjunctions by concatenations, which are the mainly universal forms of Boolean expressions. It is based on an adjustment of the Boneh-Gentry- Waters broadcast encryption method in sort to achieve attribute collusion resistance and to maintain complex Boolean access policies. The safety of our scheme is established in the generic model of clusters with pairings. Finally, we evaluate our scheme to a number of other Attribute-based Broadcast Encryption designs, both in conditions of bandwidth necessities and accomplishment costs.

2.6 Protected the E-Health Cloud

M.Winandy et al., [8] point out a number of deficiencies of recent e-health resolutions and principles; mainly they do not address the client platform security, which is a critical aspect for the overall protection of e-health systems. To fill up this gap, we present security architecture for creating privacy domains in e-health infrastructures. Our result offers client platform security and suitably combines this through network security concepts. Additionally, we discuss more open problems and research challenges on protection, privacy and usability of e-health cloud schemes.

2.7 Attribute Based Data allocation through Attribute Revocation

S.Yu et al., [9] center on a key subject of attribute revocation which is awkward for CP-ABE plans. In particular, we re-solve this demanding issue by taking into account more realistic situations in which semi-trustable on-line alternate servers are available. As evaluated to existing schemes, our projected result enables the authority to cancel customer attributes with nominal effort. We accomplish this by exclusively combine the procedure of proxy re-encryption through CP-ABE, and facilitate the ability to hand over most of difficult tasks to proxy servers. Formal investigations illustrate that our proposed idea is provably secure adjacent to selected ciphertext attacks. In addition, we demonstrate that our procedure can also be related to the Key-Policy Attribute Based Encryption (KP-ABE) counterpart.

2.8 PEACE: An Efficient and Secure Patient-centric Access Control design in support of eHealth Care System

In order to declare the privacy of patient individual health information (PHI), we describe different access rights to data requesters according to their roles, and then assign different attribute sets to the data requesters. By use of these different sets of attribute, we make the patient-centric access strategies of patient PHI. The PEACE scheme [10] is able to promise PHI reliability and confidentiality by implementing digital

signature and pseudo-identity procedures. It includes identity based cryptography to aggregate distant patient PHI securely. Extensive security and performance investigation reveal that the PEACE plan is capable to reach preferred security necessities at the cost of a suitable communication delay.

2.9 Secure Organization of Personal Health Records by concerning Attribute-Based Encryption

A new technique which allows protected storage and restricted allocation of patient's health records in the abovementioned situations has projected by L.Ibraimi et al., [10] A novel alternative of a ciphertext-policy attribute-based encryption methods is planned to implement patient/organizational access control strategies such that everyone can download the encrypted data but only standard clients from the public area (e.g. family, friends, or fellow patients) or certified users from the specialized domain (e.g. doctors or nurses) are permitted to decrypt it.

2.10 Attribute-Based Access Control with well-organized Revocation in Data Outsourcing structures

An access control method by means of ciphertext-policy attribute-based encryption to implement access control guidelines with competent attribute and user revocation ability[11] has projected by J.Hur et al., The fine-grained access control can be realized by dual encryption methods which gets benefit of the attribute-based encryption and selective group key distribution in every attribute group. We show how to relate the planned mechanism to firmly handle the outsourced data. The investigation consequences point out that the projected scheme is well-organized and protected in the data outsourcing systems.

3. PROPOSED SYSTEM

3.1Problem Definition

These papers regard as a PHR system where there are several PHR owners and PHR consumers. The owners refer to patients who have complete control over their own PHR data, i.e., they can make, handle and terminate it. There is a central server belonging to the PHR service provider that supplies all the owners' PHRs. The users may approach from a range of features; for instance, a friend, a caregiver or a researcher. Users right of entry the PHR documents through the server in sort to read or write to someone's PHR, and a user be able to concurrently have access to numerous owners' data. A classic PHR system employs normal data formats. For example, continuity-of-care (CCR) (based on XML data structure), which is broadly utilized in representative PHR systems as well as Indivo, an open-source PHR system accepted by Boston Children's Hospital. Due to the nature of XML, the PHR files are reasonably prearranged by their types in a hierarchical way.

This paper recommends a narrative ABE-based skeleton for patient-centric secure distribution of PHRs in cloud computing surroundings, under the multi-owner backgrounds. To deal with the key management challenges, we abstractly separate the users in the system into two types of domains, namely public and personal domains. In the public domain, we make use of multi-authority ABE (MA-ABE) to get better the security and keep away from key escrow trouble. Projected a multiple-authority ABE (CC MAABE) explanation in which many TAs, MA-ABE scheme is utilized, somewhere each authority administers a disjoint set of attributes distributive. Suggest an improved MA-ABE plan In particular, an authority be able to cancel a user or user's attributes straight away by re-encrypting the cipher texts and report to users' secret keys.

Advantages

- The key advantage of our explanation is small re-keying message sizes.
- All user know how to obtain secret keys as of any subset of the TAs inside the system

Toward this end, we build the subsequent major contributions:

This paper suggests a fresh ABE-based framework intended for patient-centric protected distribution of PHRs in cloud computing backgrounds, under the multi-owner locations. To deal with the key organization challenges, we theoretically separate the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are directed distributive by attribute authorities within the previous, while everyone owner simply wants to administer the keys of a little number of users in her private domain. In this way, our structure can concurrently handle different kinds of PHR sharing applications' necessities, while acquiring minimum key management overhead for both owners and users in the system. In addition, the structure implement write access controls, handles active policy updates, and offers break-glass admission to PHRs under emergence situations.

During the public domain, we make use of multi-authority ABE (MA-ABE) and CC-MAABE to get better the security and keep away from key escrow difficulties. Every attribute authority (AA) in it administrates a disjoint subset of consumer role attributes, at the same time as none of them alone is capable to organize the security of the whole structure. We recommend method for key distribution and encryption as a result that PHR owners know how to identify personalized fine-grained role-based access guidelines at some stage in file encryption. In the personal domain, owners straightly allot access privileges intended for personal users and encrypt a PHR file under its data attributes. In addition, we improve MA-ABE via placing forward a proficient and on-demand user/attribute revocation scheme, and establish its security under standard security hypothesis. In this method, patients encompass full privacy control in excess of their PHRs.

This paper gives a systematic study of the difficulty and scalability of our planned secure PHR sharing solution, in conditions of several metrics in calculation, communication, storage space and key management. We as well contrast our scheme on the way to numerous preceding ones within complexity, scalability and security. Also, we exhibit the effectiveness of our method via employing it on a current workstation and performing experiments/models.

The Block Diagram for Existing system is given in Fig 2.

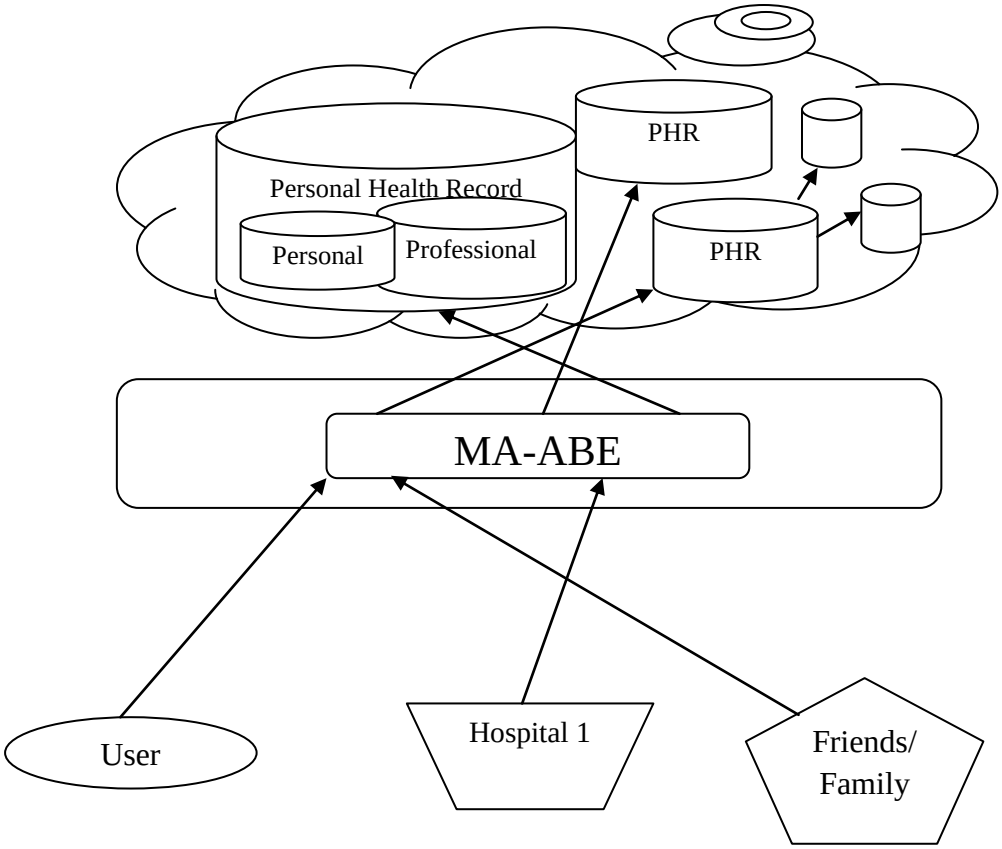

Fig 2: Proposed System Diagram

3.2Multi-Authority Attribute Based Encryption (MA-ABE)

Attribute based encryption (ABE) decides decryption capability supports on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities observe different set of attributes and subject matching decryption keys in the direction of users and encryptions are able to entail that a user get keys for suitable attributes from every authority prior to decrypting a message. Multi-authority ABE method by means of the thoughts of a trusted central authority (CA) and global identifiers (GID). On the other hand, the CA in that creation has the control to decrypt each ciphertext, which appears in some way conflicting to the unique objective of allocating control over lots of potentially untreated establishments. Furthermore, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which without need compromises the privacy of the user. In this paper, a suggestion for a answer which take away the trusted central authority, and keeps the users' privacy by avoiding the authorities as of grouping their information on particular users, therefore making ABE additional usable in practice.

Multi-authority ABE (MA-ABE) is to get better the security and avoid key escrow difficulty. Every attribute authority (AA) in it rules a disjoint separation of user role attributes, while not any of them alone is capable to manage the security of the complete system. We offer mechanism for key distribution and encryption consequently that PHR owners be able to identify personalized fine-grained role-based access strategies through file encryption. In the personal domain, owners straightly allocate access privileges designed for personal users and encrypt a PHR file under its data attributes. Additionally, we develop MA-ABE by setting forward a proficient and on-demand user/attribute revocations plans, and confirm its security under typical security statements. During this mode, patients encompass complete privacy be in charge of in excess of their PHRs.

4. CONCLUSION

Projected a new structure of protected allocation of individual health reports in cloud computing. Taking into account incompletely trustworthy cloud servers, we disagree that to completely understand the patient-centric theory, and a collection of methods for data access control to PHRs accumulated in semi-trusted servers by means of MA-ABE and CC-MAABE process that offers successful resolution to a quantity of the matters associated to on-demand user revocation and its security. However accomplishment and simulation, this paper shows that our clarification is together scalable and efficient. The results recommended that the projected design would afford reasonable performance and

also diminish the complication of key management at the same time as augment the privacy agreements evaluated with earlier mechanism.

5. FUTURE SCOPE

Upcoming effort will develop the security resolution (apply HIPAA requirements, by means of HTTPS) and will estimate the outcome through determines the interoperability degree accomplished by means of the presented solution.

6. REFERENCES

[1] Ming Li, Shucheng Yu, Yao Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption", IEEE Transactions on Parallel and Distributed System, pp. 131-143, 2013.

[2] Vida M, Lupse O, Stoicu-Tivadar L "Improving the interoperability of healthcare information system through HL7 CDA and CCD standards", IEEE International Symposium on Applied Computational Intelligence and Informatics, 2012.

[3] Oana Sorina Lupse, Mihaela Marcella Vida, Lacramioara Stoicu-Tivadar, "Cloud computing and Interoperability in healthcare information system", INTELLI 2012.

[4] 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.

[5] 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.

[6] 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.

[7] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[8] 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.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[10] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.

[11] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.

[12] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp and "Google, Microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.

[13] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

M.Rajeev Kumar born in the year October 1985, he received his Bachelor degree in 2006 in Information technology from Anna University Chennai, Master's degree in 2008 from the same University. He started his educational carrier in 2008 as lecturer in department of Information Technology, VelTech Dr.RR & Dr.SR Technical University, Chennai. Now he is working as an Asst. Prof. in the same University. His area of interest is Cloud and Networks.

M.Dhilsath Fathima born in the year September 1984, she received his Bachelor degree in 2005 in Computer science and Engineering from Anna University Chennai, Master's degree in 2011 from Sathyabama University. She started his educational carrier in 2005 as lecturer in department of CSE, Arignar Anna Institute of science and technology, Chennai. Now she is working as an Asst. Prof. in Veltech Dr.RR & Dr.SR Technical University. Her area of interest is cloud and Biometrics and Image processing.

M.Mahendran born in the year September 1983, he received his Bachelor degree in 2005 in Computer science and Engineering from Anna University Chennai, Master's degree in 2008 from Sathyabama University. He started his educational carrier in 2005 as lecturer in department of CSE, Veltech multitech Engineering College, Chennai. Now he is working as an Asst. Prof. in Veltech Dr.RR & Dr.SR Technical University. Her area of interest is cloud and Biometrics and Image processing.