ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

CBPPP: Cloud Based Patient Centric Privacy Preserving System

Nishant Kumar, Nitish Kumar, C.Anuradha

UG Student, Dept. of C.S.E., Bharath University, Chennai, India

UG Student, Dept. of C.S.E., Bharath University, Chennai, India

Assistant Professor, Dept. of C.S.E., Bharath University, Chennai, India

ABSTRACT: Management of personal health records has found way to distributed computing resources from traditional ones. While the advancement in technology has facilitated confidential storage of data, the concern over privacy and authenticated access still hovers around. The work in this paper addresses the present concerns of health care providers over privacy and security breach and at the same time excels in scalability and maintenance from existing systems through a yawning gap. The work presented here propounds a countenance based access mechanism for encrypting as well as decrypting the patient data. The basic principle is to evade any unauthorized ingress by enabling the patient with such efficient mechanism. It constructs a dynamic and flexible environment between patient and health care providers through attribute relying access that can even resist botnets and Distributed Denial of Service Attacks.

KEYWORDS: attribute relying access; authentication; botnets; decrypting; distributed computing; health records; scalability.

I. INTRODUCTION

The digitization of medical facilities with customized and day by day more secure framework has taken place by leaps and bounds across the world with notable mechanism like the PCEHR incorporated by the Australian government and the HIPAA by the American ministry of health. The existing systems allow the patients more discreetness and control over their data. Conventionally patient's details were considered the property of healthcare provider with the most important entity in the process having no say in how the details were handled but with technological advent and awareness the practices and ethics have drastically changed. While the existing mechanism greatly enhances patient coordination with similar ailments and virtually provides a support system, the health care provider cannot always be relied on the privacy aspect. Although cloud resources provides easier and on the go solutions, it is also a murkier place to be trusted upon. The issues regarding patient details are not simplistic as it involves their crucial health statistics like mental stability, reproductive health, contagious infections and related history which if disclosed to unreliable personnel can hamper their job prospects, relationships, and societal involvement and in totality undermine their future life. So, an efficient mechanism must be there to allow the patient to decide how much and with whom they want to disclose their confidentiality. In this paper, by extending the techniques of attribute relying ingress control and authorized authenticated signatures on de-identified health information we realize two levels of patient centric privacy preserving, only the physicians directly authenticated by the patient can access the patients' personal health information and authenticate their identities at the same time; the physicians and third party not directly authorized by patients cannot authenticate the patients' identities but recover the non-relevant health information; while the unauthorized persons are not allowed such access obtain . The main contributions of this paper are summarized as follows.

(1) A countenance based model is proposed and extended and for the privacy of secured authenticated details attribute based framework is established to allow the patients to authorize the corresponding physicians by setting an access tree supporting patient centric mechanism.

(2) Based on this model, cloud based framework for patient centric privacy-preserving healthcare scheme (CBPPP) in the distributed multi healthcare system is proposed.

As to the lacunas of traditional system, an operator may declassify patients' information for vengeance, spite, profit, or

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

other reckless purposes. Hazards from inadvertent or on purpose release of contagious, mental health, chronic ailment diagnoses and genetic information are all well in light on both web and mass media. In the traditional privacy preserving techniques, the trust of system operators goes without saying as is conventionally presumed. But it is well known fact that such presumptions have resulted in malicious consequences; therefore, we need to construct such a system to eradicate any above assumption. In addition, a healthcare system needs to be able to deal effectively with a very great amount of patients' confidential data along with ensuring user trust, patient centric ingress control, and patients' authentication. Thus, a multi-level security system is required to protect the privacy of such systems. To maintain the solution of all such concerns and see to it that they are taken care of, in this paper, we propose a framework to secure patients' details. This patient centric mechanism has advanced security technique at its heart for storing and maintaining the health information. The framework allows control over confidential details and thus eliminates the dependency on trusted third parties or system operators. In this framework, the encrypted details residing in the cloud server are accessed from different locations. The rest of this paper is organized as follows. We discuss similar work in the subsequent section. In Section III, the proposed model of the healthcare system is illustrated. We provide existing work and experimental setup with some prerequisites required throughout the paper together with the result in Section IV ,Section V and Section VI simultaneously. Here, we provide the underlying of our mechanism through the algorithms and technologies used for our privacy model. Based on it, we propose a patient centric privacy preserving cloud based system (CBPPP) in the distributed healthcare system. In Section VII we give some basic description of our modules that we propose in our work. The culmination of the paper is brought by the Section VIII which presents the conclusion.

II. RELATED WORK

Apart from the existence of mechanism for access control of Patients' personal health details we present above, there exist many authentication mechanism by pseudonyms and other privacy preserving techniques. Lin and group presented SAGE [1] which is not only the content oriented privacy but also the contextual privacy. Sun [2] presented a solution to privacy and emergency issues based on anonymous confidential, pseudorandom number generator and proof of knowledge. Lu proposed privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof [3]. However, the heavy computational overhead of Zero Knowledge Proof means it cannot be directly applied to the distributed multi healthcare systems where the computational resource for both patients and doctors is bound. Riedl presented a new architecture pseudonymization of information for privacy in E-health (PIPE) [4].The concept of patient centered health information systems was for the first time introduced by Szolovits et al., in 1994[5]. In their work, the authors proposed an entity (patient) based health information system which integrates all health-related information about an individual. Following their work, a patient-centric health record management system named Indivo [6] was proposed. This web-based system enables a patient to assemble, maintain and arrange his or her personal medical data as a secure copy. The security of the health record is based on policies set by the users, and using encryption where the data is encrypted such that only the trusted Indivo server which has access to the private keys can decrypt the data before sending it to the users. Recently, Microsoft [7] and Google [8] introduced their patient-centric web-based electronic health record system. These systems allow patients to maintain a copy of their health record, access the health data whenever needed, and share the data with other users based on the access policies set by the patient. Digitization of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclosure attacks and statistical analysis in [9] and suggested secure mechanism guaranteeing anonymity and privacy in both the personal health information transferring and storage at a healthcare provider [10] have always been in existence. Schechter [11] proposed an anonymous authentication of membership in dynamic groups. However since the anonymous authentication mentioned above are established based on public key structure (PK), the need of an certificate authority (CA) and unique public key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore SPOC [12] system come very close to the work sought here but fails when threat from hacks and similar issues crop up.

III. PROPOSED WORK

In this paper, we consider achieving our proposed goals with greater efficiency. In distributed multi healthcare systems, all the entities can be classified into three main classes: the directly authorized physicians who are authorized by the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

patients, the indirectly authorized personnel who are authorized by the authorized physicians for medical consultant or research and the unauthorized persons. The patient's identity can only be verified by the patient directly authorized physicians who happen to have a key required in the access structure ingress. When patients 'personal health information tends to be transferred by authorized physicians and shared among distributed healthcare centers or research institutions for medical consultation or scientific research, the identity of the patients should be well protected since only the personal health information is required for these tasks. In this paper, by extending the techniques of attribute relying access control and designated verifier key mechanism on confidential health information, we realize different levels of patient centric requirement: only the physicians directly possessing the key from centre and matching the access requirement structure of the patients' symptoms can access the patients' personal health information and authenticate their identities simultaneously; the physicians and research staff not having access to the verifier signature the indirectly cannot declassify or authenticate the patients' identities but recover the personal health information if the patient is willing; while any other person can obtain neither. The main contributions soughted by this paper are summarized as follows.

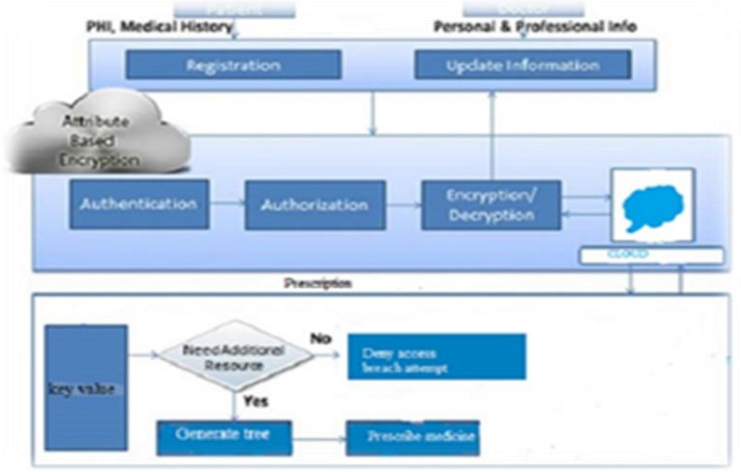
(1) A patient centric attribute relying privacy framework to allow the patients to authorize the corresponding physicians by setting an access tree supporting flexible requirements.
(2) Based on above model, a cloud based patient centric privacy preserving system (CBPPP) in the distributed multi healthcare system is proposed, providing different levels of security and privacy mechanism for the patients.
Information is maintained and accessed using attribute relying access control which identifies medical practitioners according to their skills. For e.g. the doctor gets a different store keeping of details and a verifying scheme by the medical centre while a third party like Insurer gets what the patient agrees upon. The proposed mechanism can aid a medical user in emergency to identify other medical users, and can further control only those patients who have similar symptoms to participate in the opportunistic computing while concealing users' details. As more confidential information is exchanged and stored by the medical users in the traditional systems through the web, there is a need to secure data stored in such systems. Major vulnerability of encrypting data is that it can be selectively exchanged only at levels which require giving unauthenticated users the private key to be accessed against a public key. We develop an enhanced version of fine-grained sharing of encrypted data that relies on access structure of Attribute-Based Encryption (ABE). In this system, encrypted details are labelled with sets of attributes and keys are associated with access structures that control which information a user is able to decrypt. In our construction each user's key is associated with a tree-access structure where the leaves are associated with attributes. A user is able to decrypt a text if he has sufficient privileges. For instance, if a user U1 has the key associated with the access structure "P AND Q", and M2 has the key associated with the access structure "Q AND R", we would not want them to be able to decode encrypted information whose only attribute is Q by probability. To achieve this, we adapt and generalize the techniques introduced to deal with more complex settings. We will show that this system gives us a strong method for encryption with access control for applications such as exchanging log information. In addition to this, we provide a delegation mechanism for our construction. Basically, it allows any user that has a key for access structure P to access a key for access structure Q, if and only if Q is more restrictive than P. Somewhat bewildering, we observe that our construction with the delegation property subsumes attribute relying access encryption. Hence, implementing the attribute based algorithm in the healthcare system leads to maximum privacy concealment which eliminates the major issues of insecure digitized information on the web. At the same time the framework aims at the security and confidentiality issues, and develops a patient centric privacy access control of cloud computing in distributed healthcare. Review of the detrimental effects of the current scenario of the medical healthcare platform particularly in the security module proves that identify mitigation alternatives may reduce the privacy disclosure issues which illustrate the differences between the existing and the proposed framework. Evaluation of the relationship between the different medical users effectively testimonies that such a mechanism is dire need together with the restrictive effectiveness of third party intervention .Thus to sum up the model greatly enhances the current trend and practices followed in medical world as well as is presented as an intellectual discovery that can significantly be incorporated in similar systems with required customizations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015



IV. EXISTING WORK

In the present healthcare facilities, the personal health information is exchanged among the patients residing in respective communities suffering from the common ailment for mutual support, and across d healthcare providers equipped with their own dedicated databases servers for improving the quality of treatment, it also brings about a series of concerns, especially how to ascertain the security and privacy of the patients' personal health details from various threats in the wireless transmission media such as eavesdropping and unwanted access. One of the prime issues is access control of patients' personal health data, as most patients are apprehensive about the confidentiality of health information since it is likely to make them in peril for unauthorized collection and reveal. So, in distributed healthcare systems, which detail of the patients' personal information should be sharable and with which person their personal health information should be shared with have become two main problems requiring concrete solutions. There have emerged various research works on the same issues. A fine-grained distributed data access control method is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control method is there for access privilege if and only if the patient and the physician meet in person. Recently, fine-grained data access control in multi-owner establishment is also proposed for securing confidential health records in cloud environment. However, it mainly concerns the cloud computing system which is not sufficient given the increasing volume records in cloud computing system. Moreover, it is not just to only provide the data control and security of the patient's health information in the curious and creepy cloud server model.

V. EXPERIMENTAL SETUP

The work detailed in this framework is built around presented algorithms and mechanisms. The implementation of the work detailed above was performed by MIRACLE Library for simulated encrypted patient health record operations along with GCC compilers. The technology used for a simulated behaviour of coding was JAVA.

V.I SIGN

The signing algorithm outputs a signature of message m which can only be verified by the directly authorized physicians whose set of attributes satisfies the access tree T . The patient firstly chooses a polynomial $qx(\cdot)$ for each node x including the leaf nodes in the access tree T . These polynomials are chosen in the way of a top-down approach, starting from the root node P. For each node x in the tree, let dx be the threshold value of node x and set the degree of the polynomial $qx(\cdot)$ to be $Dx = dx - 1$.Starting with the root node P, the algorithm chooses a random $y \in Zr$ and sets $qP(0) = y$. Then, it chooses dx other points in the polynomial qP randomly to define it completely deterministic algorithm that uses the patient's private key, the uniform public key of the healthcare provider where the physicians work and a message m to generate a signature σ. That is, $\sigma \leftarrow Sign(skR , rkD,m)$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

V.II **KEY GENERATION**

This is a randomized algorithm that takes as input an access structure say *A*, the master key *MK* and the defined public parameters *PK*. It outputs a decryption key D.Assume that the healthcare provider holds a uniform ephemeral private key *sk(D) = hc* shared by each physician working in it and the corresponding public key is *pk*

V.III **KEY EXTRACTION**

Key phrase extraction selects the phrases from a controlled vocabulary that best describe an access mechanism. The training data is matched with a set of predefined structure with each phrase in the vocabulary, and builds a classifier for each phrase. A new structure is processed by each classifier, and assigned the key phrase of any existing model that matches positively. The key phrases that can be assigned are ones that already exists in the training data. Key phrases are usually chosen based on the access sought and level of discreetness required. In many contexts, key phrases to documents are assigned for which they have allowed the access to. Professional indexers often choose phrases from a predefined "controlled vocabulary" relevant to the domain at hand. However, assigning key phrases manually is cumbersome. So, we provide automatic extraction techniques which are of great benefit. There are two fundamentally different approaches to this, but the best one with Kea is to provide useful metadata where none existed before.

V.IV **BILINEAR PAIRING**

Let *n* be a prime number. Let *G1 = hpi* be an additively-written group of order *n* with identity ∞, and let *GT* be a multiplicatively-written group of order *n*
with identity *1*.
A bilinear pairing on (*G1*, *GT*) is a map *ˆe: G1 × G1 → GT* that satisfies the following conditions:
(1) *(Bilinearity) for all R, S, T ∈ G1*,
ˆe(R + S, T) = ˆe(R, T)ˆe(S, T) and
ˆe(R, S + T) = ˆe(R, S) ˆe(R, T).
(2) *(Non-degeneracy) ˆe (P, P) 6= 1*.
(3) *(Computability) ˆe* can be efficiently computed.

V.V **ENCRYPTION**

This randomized algorithm accepts an input a message m, a set of attributes γ, and the public parameters *PK*. It outputs the cipher text e for this scheme. $K_{encp} = e\ (g1, g2)\ b$

V.VI **DECRYPTION**

This algorithm accepts as input – the encrypted details *E* that was encrypted under the set γ of attributes, the decryption key D_k for access structure and the public parameters *PK*. It outputs the message say *M* if γ ∈ *A*.

V.VII **ACCESS STRUCTURE**

We propose an attribute relying access tree that accounts for a perfect match between patient details and physician's specialty thereby ensuring a discreet mechanism of anonymity of the patient's personal health information. Let *T* be a tree representing an access structure. The non-leaf nodes of the tree designate an optimal gate, represented by its children and an optimal value. If *number x* is the number of children of a node *x* and *kx* is its threshold value, then $0 < kx \leq number\ x$. When *kx* = 1, it is an OR gate and when *kx* = *x*, the represented gate is AND. The aforesaid mechanism ensures that the patient in need of a medical specialist is directed through such a mechanism discreetly without even system operators or any third party for that matter able to sneak a peek into his/her health details and once the patient access structure direct to such a physician whose skills match the generated tree behaviour together with the key verification scheme can further anonymity be granted otherwise at any stage it rejects any such breach attempts.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

VI. RESULT

We now consider the efficiency of CBPPP in terms of storage overhead, complexity and communication cost. So far the overhead is concerned; the size of public parameters in our scheme is linear to the number of attributes one provides. The private key consists of two group elements in cyclic group G for every leaf node in the key's corresponding access tree. That is the number of group elements in private keys equals to the number of attributes in the union of ω D and an existing set of attributes ψ_x. Assuming ω_x to be one of the public parameters, the sign scheme consists of a group element in cyclic group corresponding to each attribute in ω_x and ψ_x. In case of computational overhead, the mechanism is in good stead fro ones existing. In algorithm described, the provision of automated key generation is an efficient one and linear to the number of nodes in the access tree. However, to guarantee the confidentiality, the work outperform than the traditional ones. At the same time, the construction clearly is at a bay from fine-grained encryption and conventional system supporting flexible predicates, since in our construction the partial verifying key $e(g1, g2)b$ is utilized for the secret key for encrypting the details. It prevents the patients' detail from being under surveillance and theft. Computation of different schemes proposed in complexity terms:

Public Key $O(n + d \square k)$
Private Key $O(nD + d)$
Signature $O(n + d \square k)$

Sign $O(n + d \square k)E$
Verify $O(jSrj\ (n + d \square k))(P + E)$

VII. MODULE DESCRIPTION

The work presented above consists of three basic modules with the possibility of further customizations. The first one is the patient module followed by a doctor module which is independent to the first module and the last one is where the treatment is finalized, the prescription module which is where we provide a secure framework so that process is discreet one.

VII.I PATIENT MODULE

The Patient Module includes all the procedures the patient has to undergo. It starts with the registration process with our web application. Next it goes up with signing the agreement of disclosure of all the information about his personal health he agrees upon with research centres. The registration includes sign up of new user into the websites. The registration contains fields for basic information and medical history upon which he/she is given a key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

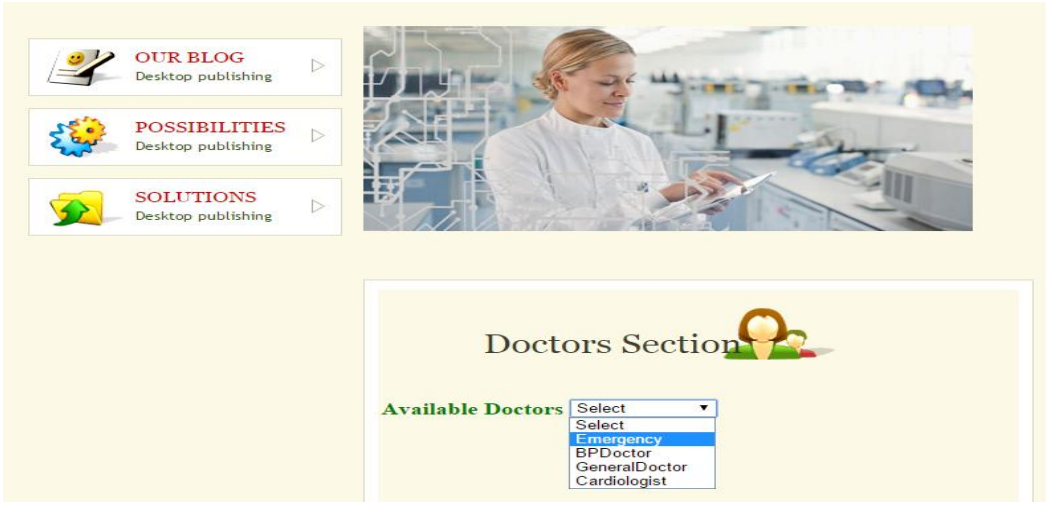
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

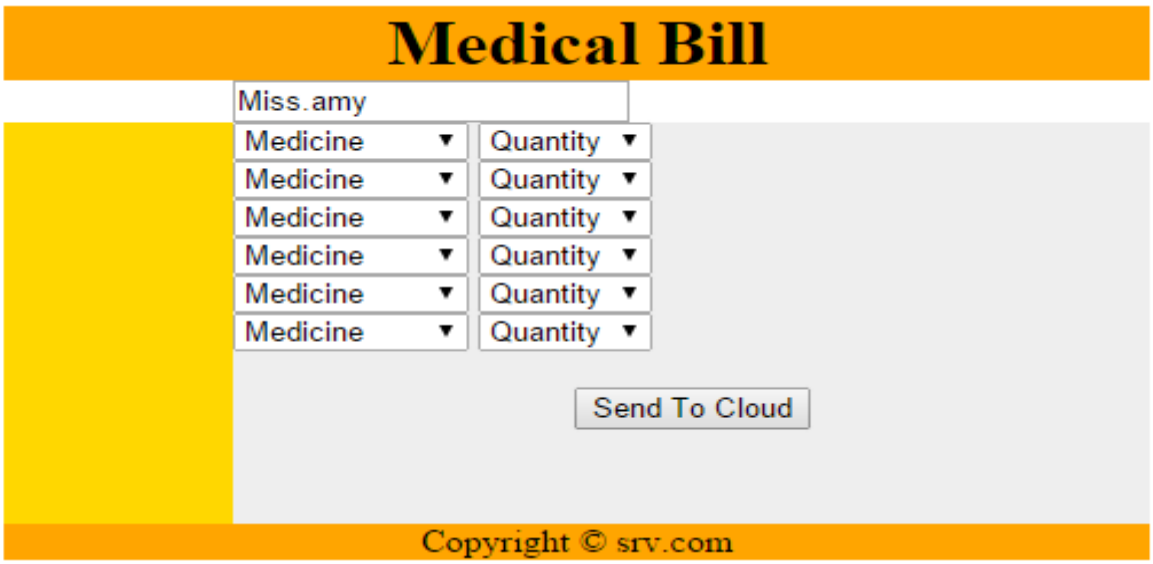
VII.II **DOCTOR MODULE**

The Doctor undergoes the same process of registrations in our web application. They also sign up an agreement for their availability in concerned and required fields and situations. The registration includes sign up of new doctor into the websites. The registration includes the doctor's personal information as well as professional information. The professional information consists of his/her profession, specialization and his/her hospital name. After the registration the doctor's skills are loaded into the training set of access structure



VII.III **PRESCRIPTION MODULE**

This module is where the hospitals and the control of remote centre come into existence. Each medical user's personal health information together with vital health statistics such as symptoms, history, allergies can be first collected by medical facilities. Finally, they are further transmitted to the cloud. Based on these collected data medical professionals at healthcare centre prescribe treatment accessing the detail with their key and can continuously monitor medical users' health conditions.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

VIII. CONCLUSION

In this paper, attribute relying model and a patient centric privacy preserving cooperative authentication scheme ensuring enhanced levels of security and privacy in the multi healthcare system is proposed together with basic experimental set up and efficiency calculations. Medical users can authorize the doctors by setting an access tree supporting optimal requirement and ingress control. The directly authorized physicians, and the third party can access the health details only if patient agrees upon. Eventually, results show this system far exceeds previous ones in terms of efficiency and resource utilization. As the authentication mentioned , are based on key phrase infrastructure the consent of a certificate authority (CA) and one public key encryption for each record at the portal of authorized physicians makes it a great leap in such areas . Furthermore, the confidentiality level is dependent on the size of the anonymity set making the anonymous authentication in specific surroundings where the patients are vulnerable. In this paper, the proposed patient centric framework is developed by making use traditional verifier signature to an attribute relying level. The anonymity level is significantly improved by associating it to bilinear pairings and the number of patients' attributes to deal with the privacy issues. Therefore, it is better suited for healthcare systems where the number of physicians is great and the patients need the timely responses from the healthcare providers. In totality, it is examined that our work differs from the threat prone encryption techniques and designated verifier signature .As the results yield, we achieve the functionalities of patient centric health record management and authentication for medical users. Thus, the CBPP excels in access control for patients' personal health information and in guaranteeing confidentiality in distributed multi healthcare systems.

REFERENCES

1. X. Lin, R. Lu, X. Sheen, Y. Nemoto and N. Kato, SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for E-health Systems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.

2. J. Sun and Y. Fang, Cross-domain Data Sharing in Distributed Electronic Healthcare, IEEE Transactions on Parallel and Distributed Systems, vol. 21, No. 6, 2010.

3. L. Lu, J. Han, Y. Liu, L. Hue, J. Huai, L.M. Ni and J. Ma, Pseudo Trust:Zero-Knowledge Authentication in Anonymous P2Ps, IEEE Transactions on Parallel and Distributed Systems, vol. 19, No. 10, October, 2008

4. B. Riedl, V. Grascher and T. Neubauer, A Secure E-health Architecture based on the Appliance of Pseudonymization, Journal of Software,3(2):23-32, February, 2008

5. Szolovits et al: an entity (patient) based health information system

6. I. Iakovidis, Towards Personal Health Record: Current Situation, Obstacles and Trends in Implementation of Electronic Healthcare Records, International Journal of Medical Informatics, 52(1):105-115,
1998.

7. Microsoft Health Patient Journey Demonstrator

8. Web-based real-time patient tracking and referral management systems and methods

9. Digitization of medical data, identity management, obfuscation of metadata with anonymous authentication

10. Privacy in both the personal health information transferring and storage

11. S. Schechter, T. Parnell and A. Hartemink, Anonymous Authentication of Membership in Dynamic Groups, in Proceedings of the Third International Conference on Financial Cryptography, 1999.

12. PremMithilesh.M, A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency: SPOC

13. V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-based Encryption for Fine-grained Access Control of Encrypted Data, In ACM CCS'06,2006.

BIOGRAPHY

NISHANT KUMAR is an undergraduate student (Final Year) in the Computer Science and Engineering Department, Bharath University, Chennai (India).His areas of technical interest includes Web Data Mining, Algorithm Analysis and Computer Networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

NITISH KUMAR is an undergraduate student (Final Year) in the Computer Science and Engineering Department, Bharath University, Chennai (India).His areas of interest includes Data Mining and Wireless Networks.