ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Patient Self Controllable and Multi Level Privacy Preserving Co-Operative Authentication in Distributed m – Healthcare Computing System

Dr. K V Prasad, Ph.D
Professor,
Department of CSE,
Sri Vani Educational Society Group of Institutions.

Ankala Naveen Raj
M.Tech (CSE),
Department of CSE,
Sri Vani Educational Society Group of Institutions.

Abstract:
M-healthcare cloud computing system is distributed between the personal health data sharing significantly to the health and medical consultation facilities for the safe and effective treatment. This system of simultaneous data confidentiality and privacy of patients have about the challenge of keeping the two. Anonymous authentication schemes that exist in many access control and should not be exploited directly. Proposed to solve a novel problem (AAPM) the power to set up the accessible privacy model. Support functions by setting a threshold of patients, doctors can allow flexible access to a tree.

The doctors directly, indirectly, the power of personal health information to doctors and medical consultation to decipher a series of unauthorized persons and / or their own attribute sets can verify the identities of patients with satisfactory access to the tree. The main objective of this paper is a novel feature-based designated verifier signature authority has devised a new method based on the available privacy model (AAPM), a patient self-regulation to protect the privacy of the multi-level cooperative authentication scheme (PSMPA) Three realizing the security and privacy of cloud computing healthcare distribution of requirement in the proposed levels.

The scope of this paper is the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.

Key Words: ***Authorised accessible privacy model, attribute based encryption, attribute based designated verifier signature scheme, internet information server***

1. INTRODUCTION:

M-health, social networks, personal health information for mutual support is always suffering from the same disease in patients with relevant community groups, sharing, and medical consultant for the distribution of their own cloud servers equipped health providers (HPS) is over. doctors or institutions, is to control the distribution of patients' access to healthcare in the cloud computing system, data sharing of personal health information.

Therefore, as part of the patients' personal health information to be shared and that doctors demanded immediate solutions to their personal health information to be shared, the two have become intractable problems of delivering healthcare cloud computing systems, in.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Fine-grained access control scheme for the distribution of a data attribute based encryption (ABE) has been proposed using the technology. Recently, a multi-employer settings and fine-grained data access control, a patient-centric cloud computing, personal health records can be constructed safely. M-healthcare cloud computing system which efficiently the growing volume of personal health information is not sufficient for the process focuses on the cloud computing system.

2 EXISTING SYSTEM:

In a m-healthcare system data confidentiality is much important but in existing system framework it is not enough for to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients' data confidentiality and identity privacy in the distributed m-healthcare cloud computing scenario under the malicious model was left untouched.

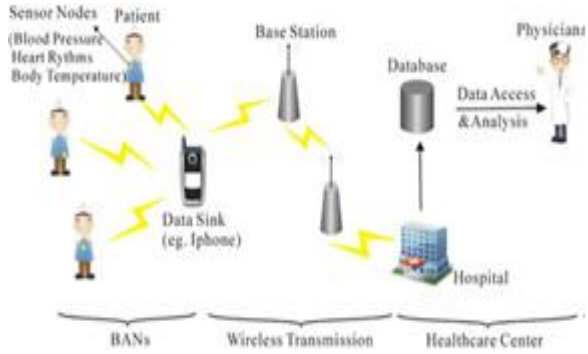

Fig. 2. An basic architecture of the e-health system.

Disadvantages:

- Data confidentiality is low.
- Data redundancy is high.
- There is a violation in data security.

3. PROPOSED SYSTEM:

To protect the privacy of anonymous P2P systems based on zero-knowledge proof authentication scheme Proposed system. However, the distribution of limited computing resources directly to patients, healthcare cloud computing systems applied to the zero-knowledge proof, as if it is a huge computational burden.

The efficiency of our healthcare system proposed by M. healthcare cloud computing system to process the increasing volume of personal health information is not sufficient for the central focuses on cloud computing system. Remote health authority doctors who are authorized by the yellow labels indirectly. They only have access to personal health information of the patient's identity, but it is not. For unauthorized persons red labels, nothing can be accomplished.

Increased security and anonymity of our proposed distribution of scattered cases to deal with the underlying patient privacy leakage gap Bilinear-Heilman (GBDH) is enhanced by the addition of the problem and the number of patients. As a result, doctors are authorized to access this feature also becomes more efficient policy and access control management fee is set to recover satisfied.

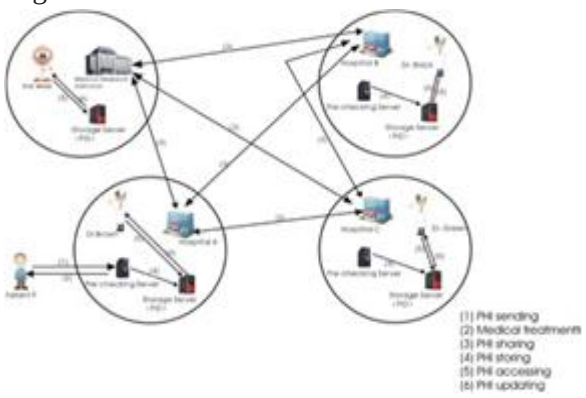

Fig. 3. An overview of our distributed m-healthcare cloud computing system.

Advantages:

- M-healthcare system is fully controlled and secured with encryption standards.
- There is no data loss and data redundancy.
- System provides full protection for patient's data and their attributes.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4. LITERATURE SURVEY

a) Cross-Domain Data Sharing in Distributed Electronic Health Record Systems

Cross-company or cross-domain co-operation and the need for high-quality patient Electronic Health Record (EHR) system, will be held from time to time.

Inevitably, most of the contribution of the exchange and to share personal and confidential patient data is relevant to consider the delegation of the authority to be vigilant so that the design, the building block cross-domain co-operation must be in place. The delegation will be granted permission to the administration and to limit the access rights of a cooperating partner. Patients and their health care data can be easily cross-domain authentication, fine-grained access control can not be achieved without the use of and exposure to it, except for the guarantee did not want to accept the EHR system. In addition, a representative of the rights at the time of the termination of cooperation should be possible at any time. In this paper, we have a secure EHR system, based on cryptography structures, the cooperation of the patient during the delicate start to secure and protect the privacy of patient data have been proposed. Our EHR system establishes a more fine-grained access control for the modern mechanisms; And the prohibition on-demand, providing basic access control mechanism for the delegation, and the basic tools in the cancellation policy. Interest in the proposed EHR system in order to fulfill specific objectives for cross-domain delegation will be displayed on the scenario.

Disadvantage

- Data confidentiality is low.

b) SAGE: A strong privacy-preserving scheme against global eavesdropping for Ehealth systems

EHealth system, information technology, where security and privacy are the key to its success and the largescale expansion through the development of health care are considered to be a good approach. In this paper, we propose a robust privacy-preserving eHealth systems, the global eavesdropping, SAGE against the scheme. The proposed SAGE content-based privacy, but also the concept of privacy around the world only has a strong adversary. A comprehensive analysis of the impact of the proposed scheme and demonstrates practicability.

- There is a violation in data security.

c) Privacy-preserving query over encrypted graph-structured data in cloud computing

The emerging cloud computing model, the data in the public cloud business owners great flexibility and economic savings from local sites to be highly motivated to outsource their complex data management systems. Consideration of the privacy of users, sensitive data, effective data use outsourcing as a very challenging task, should be encrypted before.

Our task is to "filter and verification of the principle of" use. We provide information relating to the motion of the graph for each encrypted data, and then filtering process continues as the crop to choose an effective in-house production of a feature-based index Prebuild. Without the support of the graph is the question of privacy breaches to meet the challenge, we propose a method of calculating a safe internal product, and then operate under a variety of know-themed threat to privacy needs to improve it.

Disadvantage

- Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited

d) Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings

Personal health record (PHR) is a great personal health information storage, access and share the facilities, it is a focused way, which allows patients to manage their own medical records. The emergence of cloud computing, PHR service providers to enjoy the elastic resources and reduce the cost of maintenance, it can be

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

stored in the cloud and their PHR applications is attractive. However, by storing in the cloud PHRs, patients lose physical control PHR cloud servers for each patient before she can encrypt data as it is necessary for the limit of their personal health data.

Under Encryption, it is a scalable and efficient way, PHR data is challenging to achieve fine-grained access control. Each patient, PHR is the norm, so that the number of users that have access to the data should be encrypted. Similarly, in a PHR system with multiple owners (patients), and each owner is a different set of cryptographic keys encrypt files using a PHR is she, it is important to reduce the complexity of the distribution is the key to such multi-employer arrangements. Access control, cryptographic schemes already implemented most of the cases are designed for the same employer. In this paper, we propose a framework for access control in a novel Cloud Computing Environment PHRs. For PHRs sensitive and scalable to enable access control, attribute-based encryption to encrypt the data in each of the patients PHR (ABE) systems leverage. To reduce the complexity of key distribution, we are just a subset of users for each domain name with multiple security domains, divide the system. In this way, each patient has full control over his own privacy, and dramatically reduced the complexity of key management. It is recommended to cancel our proposed scheme is effective and on-demand, is also

Disadvantage

- The challenge of keeping both the data confidentiality and patients identity privacy simultaneously

5. MODULES

A. E-healthcare System Framework:

Body Area Networks (bans), wireless transmission networks and cloud servers equipped with their own health: E- health system consists of three components. Secure access to personal health information and medical treatment of the patient, physicians, healthcare provider to manage the authority vested.

B.Authorized accessible privacy model:

Based designated verifier signature scheme (ADVS) and the adversary nature of the model, the following two aspects of the healthcare supply cloud computing systems available in the privacy model for the authority to propose a novel.

C. Security Verification:

Increased security and anonymity of our proposed distribution of scattered cases to deal with the underlying patient privacy leakage gap Bilinear-Heilman (GBDH) is enhanced by the addition of the problem and the number of patients. As a result, doctors are authorized to access this feature also becomes more efficient policy and access control management fee is set to recover satisfied.

D. Performance Evaluation:

Overhead storage, computational complexity and the cost of communication in terms of the ability of PSMPA. And fine-grained authorization, to protect the privacy of a patient-centric cloud computing without ABE personal health records using a secure data access control. To achieve the same defense, we direct the construction of the high medical costs are simply the direct authority of doctors, will run more efficiently than traditional designated verifier signature

6.INFORMATION SUPER HIGHWAY:

A set of computer networks, a variety of networking protocols that make up a large number of small networks. The world's largest computing network of 20 million users in almost 200 different countries have over two million computers. An unusually high rate of between 10 and 15 per cent of the Internet is increasing. There are no size estimates so quickly.

First, the US Defense Industry was established to meet the needs of Internet research. But the universities, academic research, commercial interest and

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Government agencies, the United States, the two serving overseas has grown into a huge global network. The Internet is a TCP / IP protocols, using a number of Internet hosts running the UNIX operating system.

7. SOFTWARE REQUIREMENT SPECIFICATION

A Software Requirements Specification (SRS) a complete description of the behavior of the software to be developed. It describes all of the interactions users have with the software contains a set of use cases.

Technical details of the figures shows that there are use cases, such as data manipulation and processing, and other special functionality to satisfy, in addition to the use cases, SRS define the functional requirements for the internal workings of the software. It is also the design or implementation (such as performance requirements, quality standards or model) that runs on the obstacles is nonfunctional requirements.

SRS stage has two primary functions:

1) The problem / needs analysis:

And two for the order process is very ambiguous, the problem, the goal and the obstacles to be understanding.

2) Requirement Specification:

Here, as on the representation, specification languages and tools for the analysis of what is found in giving and features mentioned are only handled during this activity.

Requirement will stop production of the document in the correct SRS. The primary goal of this phase of SRS document.

SRS character:

The purpose of the communication between clients and the specification to the software developer is to reduce the gap. The software, which requires a specification of the client and the consumer, however, the medium is strictly specified. It forms the basis of software development. SRS is a good system should satisfy all parties involved.

8. CONCLUSION:

A novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

9. REFERENCES:

1. J. Misic and V. B. Misic, “Implementation of security policy forclinical information systems over wireless sensor network,” AdHoc Netw., vol. 5, no. 1, pp. 134–144, Jan. 2007.

2. J. Misic and V. Misic, “Enforcing patient privacy in healthcare WSNs through key distribution algorithms,” Security Commun. Netw. J., vol. 1, no. 5, pp. 417–429, 2008

3. 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 Proc. 6th Int. ICST Conf.Security Privacy Comm. Netw., 2010, pp. 89–106.

4. J. Sun and Y. Fang, “Cross-domain data sharing in distributed electronic health record system,” IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 6, pp. 754–764, Jun. 2010.

5. R. Lu, X. Lin, X. Liang, and X. Shen, “A secure handshake scheme with symptoms-matching for mhealthcare social network,” J. Mobile Netw. Applications, vol. 16, no. 6, pp. 683–694, Dec. 2011.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Author Details

Ankala Naveen Raj received his B.TECH degree in CSE from R.V.R.&J.C. College of Engineering, Chowda varam, Guntur (Dt), in 2013, M.Tech Degree in CSE from Srivani Educational Society Group of Institutions, Chevuturu, Krishna Dist, in2014-16. At present, he is engaged in "Patient self controllable and multi level privacy preserving co operative authentication in distributed m – healthcare computing system".

Dr. K.V.Prasad ME, Ph.D is working as Director/Principal in Sri Vani Educational Society Group of Institutions, Chevuturu,Vijayawada. He has 12 Years of Teaching Experience including 5 years of Experience as Principal and has 2 Years of Industrial Experience. He has published 6 research publications in International Journals. His research areas of interest are Data Mining and Digital Image Processing.