M-healthcare cloud computing system for multilevel and single handled privacy preserving cooperative authentication in patient diagnosis

Patil S.N¹, Borkar B.S ²

¹Department of Information Technology, Pune University, Sangamner
Email: sachinpatil6933@gmail.com
²Department of Information Technology, Pune University, Sangamner

Abstract—A patient attribute-based designated verifier signature a patient self controllable multi-level privacy-preserving cooperative authentication security and privacy requirement in distributed m-healthcare cloud computing system. Distributed m-healthcare computing system significantly encourages productive patient treatment for therapeutic discussion by sharing individual wellbeing data. Nonetheless, it brings regarding the challenge of keeping each the information confidentiality and patients’ identity privacy at the same time. Numerous current get to control and unknown validation plans can’t be clearly abused. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. At that point, in light of it, by formulating another method of characteristic based assigned verifier signature, a patient self-controllable multi-level privacy-preserving cooperative validation scheme (PSMPV) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly approved physicians, the indirectly approved physicians and the unauthorized persons in medical consultation can restorative decipher the personal health information and/or verify patients’ identities by satisfying the access tree with their own attribute sets. Privacy in the distributed m-healthcare cloud the formal security evidence and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the past ones as far as computational, communication and capacity overhead.

Keywords—Authentication, Access control, Multi-Level Privacy, Distributed cloud computing, M-healthcare system, Security and Privacy.

I. INTRODUCTION

Distributed m-healthcare cloud computing systems have been increasingly adopted worldwide including the European Commission exercises, the US Health Insurance Portability and Accountability Act (HIPAA) and numerous different governments for efficient and high-quality medical treatment [1-3]. The individual health information is always shared among the patients situated in respective social communities suffering from the similar disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant [9-10]. However, it likewise achieves a progression of difficulties, particularly how to guarantee the security and protection of the patients’ personal health data from different assaults in the remote correspondence channel such as eavesdropping and tampering [16]. As to the security facet, one of the main issues is access control of patients’ personal health information, to be specific it is just the approved doctors or institutes that can recover the patients’ personal health information through the data sharing in the distributed m-healthcare cloud computing system. Most patients are concerned about the confidentiality of their personal health data since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. In this way, in distributed m healthcare cloud computing frameworks, which part of the patients’ personal health information should be shared and which physicians their personal health information should be shared with have become two immovable issues requesting earnest arrangements. There has developed different research comes about [8-9] concentrating on them. A fine-grained appropriated information get to control plan is proposed utilizing the system of characteristic based encryption (CBE). A meet based get to control strategy provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient- driven and fine-grained data access control in multi-proprietor settings is constructed for securing personal health records in distributed computing. In any case, it fundamentally concentrates on the central cloud computing system which is not sufficient for proficiently handling the
expanding volume of personal health information in m-healthcare distributed computing framework. Moreover, it is not enough for [16] to only guarantee the data confidentiality of the patient’s personal health information in the honest-but-curious cloud server model the incessant correspondence 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 the issue 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.

II. INDENTATIONS AND EQUATIONS

A mathematical model is a description of a system using mathematical concepts and language. The process of developing a mathematical model is termed as mathematical modelling.

As the project is having finite input and finite output, it comes under P-Problem.

Let S be the PSMPV system

\[ S = \{ I, K, R, O \} \]

Where

- \( I \) = Information of Patient, Authorised Physician, Unauthorised Physician, Pharmacist, Researcher which are input to System,
- \( K \) = Key generation step, Privacy preserving patient record
- \( O \) = efficient treatment.

\[ I = \{ I_1, I_2, I_3, I_4, I_5 \} \]
\[ K = \{ K_1, K_2, K_3, K_4, K_5 \} \]
\[ R = \{ R \} \]
\[ O = \{ O \} \]

Where

- \( K_1 \) = Setup,
- \( K_2 \) = Key Extract,
- \( K_3 \) = Sign,
- \( K_4 \) = Verify,
- \( K_5 \) = Transcript Simulation.

III. FIGURES AND TABLES

A typical architecture of a distributed m-healthcare cloud computing system is shown in Fig. 1. There are three distributed healthcare providers A, B, C and the medical research institution D, where Dr. Red, Dr. White, Dr. Yellow and Prof. Pink are working respectively. Each of them possesses its own cloud server.

System can be divided in to four parts
1) Patient
2) Clinical Data Collection
3) Administrator
4) Physician

**1.1 Patient**
The patient must register at hospital and he can enter he/her all the information of his/her health information. After stored patient information in hospital server the physician checks patient.

**1.2 Clinical Data Collection**
The Hardware kit contains sensors like temperature and heart bit counter. Using that sensors the patients heart bit and body temperature readings collection are done. Using Radio frequency that readings are send to the mobile device like laptop, tablet etc. the receiver side receive that readings and uploads on physician cloud.

**1.3 Administrator**
This module is use to assign the patient which is registered at hospital to the respective specialist. It manages each patients uploaded files such as CDA files, medical images, medical video files, and any other related medical documents (e.g. medical charts, immunization records, etc.). The files will be uploaded by each individual and may be shared with physicians when necessary for the treatment.

**1.4 Physician**
Physicians are two categories: The directly authorized physicians are identified with green labels in the local health-care provider they are authorized by the patients and these physicians can access the patients personal health information and verify the patients identity. The indirectly authorized physicians identified with yellow labels in the remote health-care providers they are authorized by the directly authorized physicians for medical consultant or some research purposes.

**1.5 Attribute Based Designed Verifier Signature Algorithm**

Input- \( Pr_1, Pr_2, Pr_3 \ldots \ldots Pr_n \)
IV. CONCLUSION

The Paper proposed an effective method used to provide 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.

ACKNOWLEDGEMENTS

I thankful our partners from AVCOE, Sangamner who gave knowledge and mastery that significantly helped the dissertation. I want to demonstrate my appreciation to the Prof. B. S. Borkar for offering his pearls of intelligence to me over the span of this dissertation. I am additionally gigantically greatful to Dr. B. L. Gunjal (H.O.D) for her remarks on a prior rendition of the original copy.

REFERENCES