International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

An Attribute based Cryptography Mechanism for Minimum Disclosure of Sensitive Patient Health Information at Emergency in m-Healthcare

Miss. Priti Khodankar

Computer Science Department,TGPCET,Nagpur, India

Prof. Roshni B. Talmale

Computer Science Department,TGPCET,Nagpur, India

Abstract - *Today Mobile Healthcare system is being part of regular healthcare system. In mobile healthcare system Body Sensor Node(BSN) collects heath data such as blood pressure, blood sugar level and others of patients and further transmitted to smartphone. Finally these collected data is transmitted to remote Healthcare Center via modem. These transmitted data is being observed by medical professionals at healthcare center and able to observe patient continuously. The proposed SPOC framework is provide high reliability to this information of patient which is confidential and critical so that proper help could reaches to the patient.*

Key Words: Mobile-Healthcare emergency; opportunistic computing; user-centric privacy access control; PPSPC component …

1. INTRODUCTION

Medical healthcare center experiencing a huge change now days. In this changes information digitization plays important role which improves healthcare quality and saves lives of people. These days smartphones are being use to monitor the patient condition regarding health on different parameters such as diabetes, heart disease etc. After equipped with smart phone patient need not to be stayed at home or hospitals necessarily rather they can walk outside and receive high quality healthcare monitoring from anywhere.

The data about his personal health is inputted by patient in the smartphone application. This information is stored in database and used at the time of emergency. Using these information particular doctor with specification in that field can be appointed according to the information. The data is maintained and accessed using attribute which identifies medical user according to their specification.

This information sharing between doctors and patient occurs through the internet. As information is more sensitive, it should be protected and need to be encrypted to ensure confidentiality. We develop new cryptosystem based on attribute known as Key-Policy Attribute Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

1.1 Existing System

Existing system is using smartphone and advance Body Sensor Network (BSN) for better health monitoring. Mobile Healthcare (m-healthcare) has attracted considerable interest recently as use of smartphone is common today.

But m-healthcare system still faces many challenges regarding data security and privacy preservation.

Fig -1: Pervasive health monitoring in m-Healthcare system

1.2 Limitations of Existing System

- Existing system faces many problems such as information security and privacy preservation.
- The smartphone's energy may become insufficient at the time of emergency.

2. Proposed System

In this paper, we propose another secure and protection saving astute figuring structure, called SPOC, to address this test. With the proposed SPOC structure, every restorative client in crisis can accomplish the client driven security access control to permit just those qualified partners to take an interest in the sharp registering to adjust the high reliability of PHI process and minimizing PHI protection

revelation in m-Healthcare crisis. We present an effective client driven security access control in SPOC structure, which depends on a property based access control and another protection saving scalar item calculation (PPSPC) strategy, and permits a medicinal client to choose who can take part in the entrepreneurial figuring to help with handling his staggering PHI information.

2.1. System Model

In our framework, a restorative work force at the human services focus who is viewed as reliable is in charge of instating and controlling the whole social insurance framework. A client who wishes to get the advantages of the versatile social insurance framework registers himself as a restorative client under a specific social insurance focus, then a therapeutic expert inspects the client and creates his well being profile. In view of the well being profile, the clients are then given the specific kind of sensors, for example, heart rate, glucose level etc. Once being outfitted with the sensors the clients can move anyplace not at all like in clinic .The sensors start to gather the detected information and transmit them to the client's advanced mobile phone which is then transmitted to the human services focus. The sensors and the advanced cell assume a key part in portable observing of patients. The sensors are utilized just to sense thus they can be energized each day and utilized though the advanced mobile phones are utilized for different purposes, the force of the PDA may not be adequate under crisis circumstances. In the proposed system we added one more functionality using (LAS) Location Awareness Services. At the time of emergency to all nearest doctor lie within the 10 km distance from patient will get the notification. But visible to only those doctors who is having specialty in the disease patient had.

Here we are using KP-ABE algorithm to make patient sensitive data more secure.

Fig -1: Location Aware Services

2.2 System Architecture

In the proposed framework our principle rationale is to secure the data inputted by the therapeutic clients in the framework. After the clients include the data, it is gone to the encryption calculation. We build up a much wealthier sort of quality based encryption cryptosystem and exhibit its applications. In our framework, every figure content is marked by an encryptor with an arrangement of enlightening qualities. Every private key is connected with an entrance structure that determines which kind of figure messages the key can unscramble. We call such a plan a Key-Policy Attribute-Based Encryption (KP-ABE), since the entrance structure is indicated in the private key, while the figure writings are basically marked with an arrangement of engaging properties. We take note of this setting is reminiscent of mystery sharing plans. Utilizing known methods one can construct a encryption sharing plan that indicates that an arrangement of gatherings must collaborate so as to reproduce a mystery. For instance, one can determine a tree access structure where the inside hubs comprise of AND/OR entryways and the leaves comprise of distinctive gatherings. Any arrangement of gatherings that fulfill the tree can recreate the mystery. In our setting, the part of the gatherings is taken by the properties. In this way, the entrance structure A will contain the approved arrangements of properties. We limit our thoughtfulness regarding monotone access structures. Nonetheless, it is additionally conceivable to (wastefully) acknowledge general access structures having so as to utilize our methods the NOT of a quality as a different property inside and out. Along these lines, the quantity of qualities in the framework will be multiplied. In our development every client's key is connected with a tree-access structure where the leaves are connected with properties. A client can decode figure content if the properties connected with figure content fulfill the key's entrance structure. Therefore, just if the client or a gathering is validated to utilize the information he/she is took into consideration that generally a decoded key is required for it. This ensures the information is open just if the gatherings give the right get to key. Generally the client is precluded the solicitation from claiming getting to the information which they require.

2.3 Description

Let {P1,P2,...,Pn} be an arrangement of gatherings. An accumulation A⊆ 2P{P1,P2,...,Pn}P is monotone if ∀B,C : if B ∈A and B ⊆ C then C ∈A. An entrance structure (individually, monotone access structure) is an accumulation (separately, monotone gathering) An of non-void subsets of {P1,P2,...,Pn}, i.e., A ⊆ 2P{P1,P2,...,Pn}P\{∅}. The sets in An are known as the approved sets, and the sets not in An are known as the unapproved sets. In our setting, the part of the gatherings is taken by the characteristics. Consequently, the entrance structure A will contain the approved arrangements of characteristics. We limit our thoughtfulness regarding

monotone access structures. Be that as it may, it is likewise conceivable to (wastefully) acknowledge general access structures having so as to utilize our strategies the not of a quality as a different trait through and through. Subsequently, the quantity of properties in the framework will be multiplied. Starting now and into the foreseeable future, unless expressed generally, by an entrance structure we mean a monotone access structure.

3. Conclusion

Mobile Healthcare Emergency Platform has revolutionized the way people used to store and access their medical records. The digitization of the health information has not only saved money but also has saved additional overhead that occurred earlier. This is a new topic which is drawing attention because of the secured framework that helps user in maintaining their health information private to themselves and the other medical users with similar symptoms so that he can be a helper in the opportunistic framework. This process is becoming more and more user- centric to let users identify and mitigate emergency cases thus helping them save lives of their close ones and others as well. The system has an attribute based encryption mechanism which limits the visibility of the information to only authenticated users thus minimizing the disclosure of information to the unauthorized ones. Since this system has evolved over the years but still it faces the threat of misuse of information. So, in this project, a secured system has been proposed to minimize the threat and thus benefit its users to a large extent. The scope of this platform is not limited and hence is an important field of research especially in terms of security.

4. Future Work

In this undertaking, we have proposed a client driven methodology (through property based system) towards portable social insurance crisis by investigating the present security issues that make it defenseless against access by unapproved sources without trait based structure. Sooner rather than later, we expect to perform tests that are firmly identified with hacks and other security issues of the proposed system. Furthermore, we additionally expect to actualize other conceivable mechanical progressions incorporating counterfeit consciousness in our task so that the system can be robotized totally in this manner minimizing the time slacks above and beyond. Notwithstanding this, we plan to further improve the system by actualizing body sensors nodes usefulness in India too.

5. References

1. Rongxing, Xiaodong Lin, and Xuemin (Sherman) Shen, “SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency”, IEEE Transaction.
2. SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency, IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 5, July 2014. ISSN 2348 – 7968.
3. Secure and Privacy Approach in Mobile-Healthcare emergency Using PPSPC technique, International Journalof Research in Computer and Communication Technology, Vol 2, Issue 10, October-2013.
4. Toninelli, R. Montanari, and A. Corradi, “Enabling secure service discovery in mobile healthcare enterprise networks,” IEEE Wireless Communications, vol. 16, pp. 24–32, 2009.
5. R. Lu, X. Lin, X. Liang, and X. Shen, “Secure handshake with symptoms- matching: The essential to the success of mhealthcare social network,” in Proc. BodyNets’10, Corfu Island, Greece, 2010.
6. Y. Ren, R. W. N. Pazzi, and A. Boukerche, “Monitoring patients via a secure and mobile healthcare system,” IEEE Wireless Communications, vol. 17, pp. 59–65, 2010.