International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Implementation of AAPM Model in Distributed M-Healthcare System

P.Chandipriyanka[1], M.Roshini[2], N.Sandhya Rani[3], U.Jothilakshmi[4]
[1,2,3]*B.Tech Student, Dept. of IT, Prathyusha Engineering College, Poonamallee, Tamil Nadu, India*
[4]*Assistant Professor, Dept. of IT, Prathyusha Engineering College,Poonamallee,Tamil Nadu,India*

Abstract: Distributed m-health care system is used for efficient patient treatment and share personal health information among health providers. However, it brings many challenges such as data confidentiality and patients' identity privacy. Many existing system used anonymization, ABE, Access control scheme to solve the above mentioned challenges. But that system failed in satisfying the challenges. To solve this problem, in the paper to enhance data confidentiality and privacy of the patients' identity, a comparison study has been proposed. From this comparison AAPM is considered as best algorithm for enhancing three levels of security and privacy to patient identity.
Key Terms: AAPM, ABE, Access control scheme, privacy, data confidentiality.

I. INTRODUCTION

Distributed m-healthcare cloud computing system has been increasingly adopted worldwide and by many governments for efficient and high quality medical treatment [1] [2]. Initially electronic healthcare systems were used to manage the health records of patients' which were used by healthcare providers. Confidentiality was not enhanced in electronic healthcare system. Mobile health care system was implemented to access the personal health records m- healthcare system was implemented in cloud computing system for usage of all patients to store the health records. Personal health records were shared among patients for mutual support and among other health care providers. However, it brings a challenge of how to ensure the security and privacy of the patients' information. In fact security was one of the main issues in accessing the patients' personal health information records and authorizing the physicians during data sharing in the distributed m-healthcare system. Confidentiality is one of the main concerns to the patient about their personal health records. In distributed m-healthcare system which part of the personal health information should be shared and which physician their personal health information should be shared become a two problem demanding urgent solution. There were emerged lot of research result focusing them [1][2][3][4][5][6][7][8][9][10]. Anonymization technique is proposed [1] for the privacy preserving of patients' identity. It hides the identity of the patient while sharing the information in the cloud system. A fine-grained access control scheme is used to provide confidentiality to the personal health records. Attribute based encryption technique is proposed in many of the papers, which provide encrypted data of the personal health records which is shared among the patients and shared in the cloud system. Moreover many techniques have been used for patient privacy and data confidentiality .Still there exist some lagging in the privacy. In distributed m-health care system the attribute based encryption is also used for data confidentiality and AAPM technique has been proposed for the authorization of physicians and which physician should share the patient personal health records. The technique ensures privacy to the patients' identity and data confidentiality. A comparison study has been taken among various techniques and each technique provides some of data confidentiality and privacy for patient identity AAPM technique is considered as best for providing security to the data and privacy to the patient identity. In these technique doctors are categorized into three levels as authorized physicians, indirectly authorized physicians and unauthorized physicians. Directly authorized physicians can view patients' details and their identity. The other physicians can't view the patients' identity. So, here privacy is considered as one of the main part to the patients.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

II. LITERATURE SURVEY

S.No	Title	Technique/ Algorithm	Model	Pros	Cons	Achievements	Year	Author	Published in journal/ conference
1	A privacy management architecture for patient – controlled personal health record system	Anonymization	Privacy aware patient controlled personal health record	Patient can control their own health record and use some privacy protection techniques	Sharing of health record among patient leads to loss of patient identity	Confidentiality of patient data can be achieved	2009	M.D .Nurul, NoboruSonehara, Shigeki Yamada	Journal of Engineering Science and Technology
2	PSCPA-patient self-controllable cooperative authentication in distributed m-health care system	Attribute based designated verifier signature scheme	Authorized accessible privacy model	Three levels of security and privacy requirement can be obtained	No corrective measure have taken towards various malicious attack in wireless system	Privacy of patient identity can be achieved	2012	Jzhou,Zhcoacoa,Shanghai	International Journal of Advancement in Engineering Technology, Management and Applied science
3	Scalable and secure sharing of personal health records in cloud computing using attribute based encryption	Attribute based encryption	Patient centric framework, data access control	Encryption of health records can avoid the third party to access patient health record	Semi trusted servers only used by the providers.so that complete privacy were not provided	Using cloud for storing health records in secure manner	2012	Y.B.Gurav,ManjiriDeshmukh	International Journal of Computer Application Technology and Research

Volume 4 Issue III, March 2016
ISSN: 2321-9653

4	Enhancing PHR service in cloud computing patient-centric and fine grained data access using ABE	Attribute based encryption	MA-ABE(multiple attribute-attribute based encryption)	Use of multiple domain in cloud reduces key management complexity for owners and users	Maintaining the multiple domain by single owner is very difficult	Secure information protect personal health record in multiple domain write access control	2012	ArpanaMahajan,profYaskpatel	IRACT-International Journal of Computer Application Technology and Security
5	An efficient sharing of personal health record using DABE in secure cloud environment	Distributed attribute based encryption		Provides data confidentiality, there is no center authority who maintain all attribute and secret key due to distribute ABE	Doesn't concentrate on to solve the various attacks	Fine grained access of PHR and reduction of complexity in key management were achieved	2013	T .Parameswran, S. Vanitha, K.SArvind	International Journal of Advanced Research in Computer Engineering and Technology
6	Implementation of mobile-healthcare using cloud computing with access control security and privacy	Access control	Authorized accessible privacy model	Connectivity through internet was well planned and three levels of security can be obtained.	No preventive measure to handle attacks	Multiple level privacy can be obtained	2013	Smitha, Rajashekar	International Journal of Technology and Research
7	NFC-based hospital real-time patient management system	NFC(near field communication)	NFC based real-time HMP	Hospital patient data management made easier with the help of NFC	NFC can be used only for a short distance and can be used only in the availability of internet	Smart card can be used. with the help of this easy accessibility of data can be done	2013	AtluriVenkataGopiKrishna,CheerlaSreevardhan,S.Karun,	International Journal of Engineering Trends and Technology

8	SPHMS: smart patient m-health care monitoring system with NFC and IOT	NFC tags, android application		Patient details can be easily updated with the help of the application	Maintenance of database is very difficult	Reduces use of paper for everything. Papers are replace by android application	2015	HodaRaminHossein	International Journal of Computer Application Technology and Research
9	A novel framework for securing medical records in cloud computing	MA-ABE(multiple attribute-attribute based encryption)		Reduces key management and provide central key management with attribute authorities	There was no special technique used for controlling the attacks	There was no special technique used for controlling the attacks	2013	MD.Irfan ,SayeedYasin	International Journal of Modern Engineering Research
10	Review on PSMPA	Attribute based designated verifier signature	Authorized accessible privacy model	Three levels of security and high level of privacy for distributed system	Patient doesn't know the doctors are authorized one or not	High-level of privacy for patient identity	2014	Gangadhar,Jyothi Sheity	International Journal of Advancement in Engineering Technology, Management and Applied science

Distributed m-healthcare cloud computing system has been increasingly adopted many governments for better medical treatment. A survey has been taken among various paper related to distributed m-health care system .Electronic healthcare system has been proposed to store the patients personal health records and shared among the patients. Limited number of health records can be stored in these systems. Anonymization technique has been used for providing privacy to the patient identity data confidentiality is not provided by these techniques. Attribute based encryption techniques have been proposed that provided data confidentiality by encryptions the personal health records. So that information cannot be hacked by unauthorized person because it will be in unreadable format. ABE can provide only confidentiality for limited data.MA-ABE is proposed where multiple Authorities is used for the authorization of the doctor from the central authority. ABE is used for the encryption of the data to convert the information into unreadable format. Secret key will be provided decrypting the patient data in encrypted format. The secret key will be known only by the authorized doctors who verify the health record of patients. Central authority cannot maintain large amount of data in the network is one of the issues. In real-time healthcare system NFC tags were used within the hospital for patients. With the help of these tags emergency case will be known to the doctors and provide alarm to doctors in the time of patient death. RFID is used in these tags, it will sense only short distance of frequency range. To overcome the distance issue application has been developed with the help of NFC. With the help of this smart phone application updating, registration will be done fast without any paper use. This application can be used only within the health providers. In distributed m-healthcare system health records will be shared among the patients who suffer from same disease for mutual consultation. AAPM model have been used to authorize the doctors. So that authorized doctors can view the patients' details and privacy to patient identity is considered. From the above study AAPM provides both confidentiality and privacy to patients' identity.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. COMPARISION OF M-HEALTHCARE

S .No	Title	Technique	Algorithm	Type of health care system	Encryption type	Key type	Confidentiality level	Privacy level
1	A privacy management architecture for patient – controlled personal health record system	Anonymization	P3-HR	Electronic healthcare	Attribute based encryption	Public key, private key	Low	High
2	PSCPA-patient self - controllable cooperative authenticatio n in distributed m-health care system	Attribute based designated verifier	Authorized accessible privacy model	m-health care system	Attribute based encryption	Private key, shared key	High	High
3	Scalable and secure sharing of personal health records in cloud computing using attribute based encryption	Key policy-Attribute based encryption	Cipher text-attribute based encryption	Real time health care system	ABE one to many encryption, holomorphic encryption	Cipher text	High	High
4	Enhancing PHR service in cloud computing patient-centric and fine grained data access using ABE	Attribute based encryption	MA-ABE(multiple attribute-attribute based encryption)	Electronic healthcare	ABE	Public domain. Personal domain	High	Low
5	An efficient sharing of personal health record using DABE in secure		Distributed attribute based encryption	Distributed healthcare	ABE,MA-ABE	Private key	Low	High

	cloud environment							
6	Implementation of mobile-healthcare using cloud computing with access control security and privacy	Access control	Authorized accessible privacy model	Distributed m-healthcare system	ABE	Random key	High	high
7	NFC-based hospital real-time patient management system	NFC(near field communication)	Unique identification number	Real time patient management system	Public key encryption	Public key	nil	Nil
8	SPHMS: smart patient m-health care monitoring system with NFC and IOT	NFC tags, RFID	ADC	Android application			Low	High
9	A novel framework for securing medical records in cloud computing		Attribute based encryption	Electronic healthcare	ABE,MA-ABE, public key encryption	Symmetric key, public key	High	High
10	Review on PSMPA	Attribute based designated verifier signature	AAPM	Distributed health care system	Identity based encryption	Key policy, cipher text	High	high

IV. CONCLUSION

In this paper a comparison study has been made among various techniques used in different healthcare systems. These techniques are mainly used for data confidentiality and to provide privacy to the patients' identity who shares their own personal health records in online for doctor consultation. Privacy can be provided by encrypting the data of patient by the techniques like ABE, Access control scheme. Authorization of doctors can be provided by AAPM model proposed in distributed m-healthcare system. From these analyses AAPM model is considered as best approach for data confidentiality and privacy for patients' identity.

REFERENCES

[1] MD. Nurul Huda*, Noboru Sonehara, Shigeki Yamada(2009)A privacy management architecture for patient-controlled personal health record system, vol. 4, no. 2 ,154 – 170.
[2] Jun Zhou, Zhenfu Cao(2012) PSCPA: Patient Self-controllable Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Systems.
[3] T .Parameswaran, S.Vanitha, K.S.Arvind(2013) An Efficient Sharing of Personal Health Records Using DABE in Secure Cloud Environment,vol

.2,ISSN:2278-1323.
[4] Gangadhara S M1 , Jyothi Shetty2(2014) Review on Patient Self-contollable and Multi-level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare in Cloud Computing System by using AAPM,vol .1,ISSN NO:2349-3224.
[5] Smitha Kr1 , Rajashekar SA2(2013) Implementation of Mobile-Healthcare using Cloud Computing with Access Control, Security and Privacy, ISSN (Online): 2319-7064.
[6] Arpana Mahajan, Prof . Yask Patel(2012) Enhancing PHR services in cloud computing: Patient-centric and fine grained data access using ABE,vol.2, ISSN: 2249-9555.
[7] Md. Irfan1 , Sayeed Yasin2(2013) A Novel Framework for Securing Medical Records in Cloud Computing,vol.3.
[8] Atluri Venkata Gopi Krishna[1] , Cheerla Sreevardhan[2], S. Karun[3], S.Pranava Kumar[4](2013) NFC-based Hospital Real-time Patient Management System,vol.4.
[9] Hoda Ramin Hossein(2015) SPHMS : Smart Patient m-Healthcare Monitoring System with NFC and IOT,vol.4 956 – 959.
[10] Y. B. Gurav1 , Manjiri Deshmukh2(2012) Scalable and Secure Sharing of Personal Health records in Cloud Computing Using Attribute Based Encryption, ISSN (Online): 2319-7064.