ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

PSMPV: PATIENT SELF-CONTROLLABLE AND MULTI-LEVEL PRIVACY-PROTECTING COOPERATIVE VALIDATION IN DISTRIBUTED M-HEALTHCARE CLOUD COMPUTING

Nisar Salim Shaikh , Prof.S.Y.Raut
Computer Engineering Department, Pravara rural Engineering college Loni,India

DOI: 10.5281/zenodo.57954

ABSTRACT

Distributed m-healthcare system computing framework fundamentally encourages effective patient treatment for restorative sharing so as to meet individual health data among human services suppliers. On the other hand, it realizes the test of keeping both the information classification and patients' character protection at the same time.Numerous current access control and mysterious validation plans can't be direct misused. To take care of the issue, in this paper, a novel approved open security model (OSM) is built up. Patients can approve doctors by setting an entrance tree supporting adaptable limit predicates it also give the date and time limit to the authorized physician withi that only the physician can access that data . At that point, in view of it, by formulating another procedure of characteristic based assigned verifier mark, a patient self-controllable and multi-level privacy protection safeguarding agreeable confirmation plan (PSMPV) acknowledging three levels of security and security prerequisite in dispersed m-medicinal services distributed computing framework is proposed. The straightforwardly approved doctors, the by implication approved doctors and the unapproved persons in medicinal conference can separately decode the individual health data and/or check patients' personalities by fulfilling the entrance tree with their own quality sets. At last, the formal security verification and re-enactment results show our plan can oppose different sorts of assaults and far outflanks the past ones as far as computational, correspondence and capacity overhead.

KEYWORDS: Distributed cloud computing, access control, security and protection ,m -human services framework Authentication.

INTRODUCTION

Distributed mobile healthcare system reg-istering structures have been logically grasped general including the Commission i europe works out, the US Health Insurance Portability and Accountability Act (HIPAA) and various distinctive governments for capa-ble and first class therapeutic treatment [2], [3]. In m-human administrations interpersonal associations, the individual health information is continually shared between the patients ar-ranged specifically social gatherings encounter-ing the same sickness for regular sponsorship, and transversely over appropriated restorative administrations suppliers (HPs) outfitted with their own cloud servers for remedial guide [11], [12]. Then again, it furthermore understands a movement of troubles, especially how to guard the security and insurance of the patients' up close and personal health information taken away various strikes in the remote correspon-dence channel, for instance, listening in and changing.

Distributed cloud computing [2] Distributed cloud is the appliance of cloud computing me-chanics to couple data and applications pro-vided from multiple geological locations. Cir-culated, in a data innovation (IT) setting, im-plies that something is shared among numer-ous frameworks which might likewise be in various areas.Distributed cloud speeds com-munications for global services and enables more responsive communications for specific regions. Cloud providers use the distributed model to enable lower latency and provide better performance for cloud services. Beyond the cloud provider context, two other examples of distributed cloud are public resource com-puting and the volunteer cloud.

Authentication [3] The procedure of rec-ognizing an individual, generally taking into account a password and username . In security scheme, verification is special from conforma-tion , which is the process of giving people

access to system objects in light of their per-sonality. Verification just assurance that the in-dividual is who he or she claims to be, yet says nothing in regards to the entrance privileges of the person.

Access control [4] In the fields of physical security and data security, access control is the particular limitation of access to a spot or other resource. The demonstration of getting to might mean devouring, entering, or utilizing. Consent to get to an asset is called approval.

Security and Privacy [11] Security is of prin-cipal significance in e-social insurance, since the illicit revelation and inappropriate utilization of EHRs can bring about legitimate question and undesirable or harming results in individuals' lives. For instance, a business might choose not to contract individuals with mental issue, an insurance agency might decline to give extra security knowing a patient's ailment history, individuals with specific sorts of illness might be segregated against by the human services supplier, or uncommon wellbeing states of a pa-tient could be uncovered to the family ignoring his/her will.

M-healthcare system [6] m-Health (likewise composed as m-wellbeing) is a condensing for versatile wellbeing, a term utilized for the act of medication and general wellbeing upheld by cell phones. The term is most regularly uti-lized as a part of reference to utilizing portable specialized gadgets, for example, cellular tele-phones, tablet PCs and PDAs, for wellbeing administrations and data, additionally to influ-ence passionate states.The mHealth field has risen as a sub-fragment of eHealth, the uti-lization of data and correspondence innovation (ICT, for example, PCs, cell telephones, inter-changes satellite, understanding screens, and so on., for wellbeing administrations and data. mHealth applications incorporate the utiliza-tion of cell phones in gathering group and clinical wellbeing information, conveyance of medicinal services data to professionals, scien-tists, and patients, ongoing checking of patient key signs, and coordinate procurement of con-sideration (by means of portable telemedicine).

RELATED WORK

S.Yu,K.Ren and W.Lou (2009) proposed data access control scheme namely FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks which proposed using the technique of attribute based encryp-tion(ABE)[4].The proposed scheme exploits a novel cryptographic primitive called attribute-based encryption (ABE), tailors, and adapts it for WSNs with respect to both performance and security requirements. The main advantage of this system is a distributed data access control scheme that is able to fulfill fine-grained access control over sensor data and is resilient against strong attacks such as sensor compromise and user colluding.The drawback of this system is low fine grained access control.

F.W. Dillema and S. Lupetti (2007) Pro-posed Rendezvous-based Access Control for Medical Records in the Pre-hospital Environ-ment[13].The proposed scheme protect against aggregation threats without letting the patients carry their own medical data.The system pro-vide rendezvous-based access control for access control in the pre-hospital environment. Access is provided locally and does not depend on con-nectivity with remote systems. The drawback of this system is that provides access privilege if and only if patient and health worker meet in the physical world.

M. Li, S. Yu, K. Ren and W. Lou (2010) proposed Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings [14].This system proposed a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients PHR data. To reduce the key distribution complexity, we divide the system into multiple security do-mains, where each domain manages only a sub-set of the users. Advantages of system is flexi-ble, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios. Drawbacks of system are it mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system.it is not enough for to only guarantee the data confidentiality of the patients personal health information in the honest-but-curious cloud server model.

J. Sun, Y. Fang and X. Zhu (2010) pro-posed Privacy and Emergency Response in E-healthcare Leveraging Wireless Body Sensor Networks[5].This scheme provide detailed dis-cussions on the privacy and security issues in e-healthcare systems and viable techniques for these issues. Using this techniques system can provide privacy

ISSN: 2277-9655
Impact Factor: 4.116

to the record of the pa-tients.The drawback of system is they mainly study the issue of data confidentiality in the central cloud computing architecture.

Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato (2009) SAGE: A Strong Privacy-preserving Scheme against Global Eavesdrop-ping for E- health Systems [6]. This paper proposed a strong privacy preserving Scheme Against Global Eavesdropping, named SAGE, for e-Health systems. The proposed SAGE can achieve not only the content oriented privacy but also the contextual privacy against a strong global adversary. The drawback of system is they mainly study the issue of data confiden-tiality in the central cloud computing architec-ture.

PROPOSED SYSTEM

The basic e-healthcare system illustrated in Fig. 1 mainly consists of three components: body area networks(BANs), wireless transmis-sion networks and the healthcare providers equipped with their own cloud servers [2]. The patient's close to home wellbeing data is safely transmitted to the medicinal services supplier for the approved doctors to get to and perform restorative treatment.

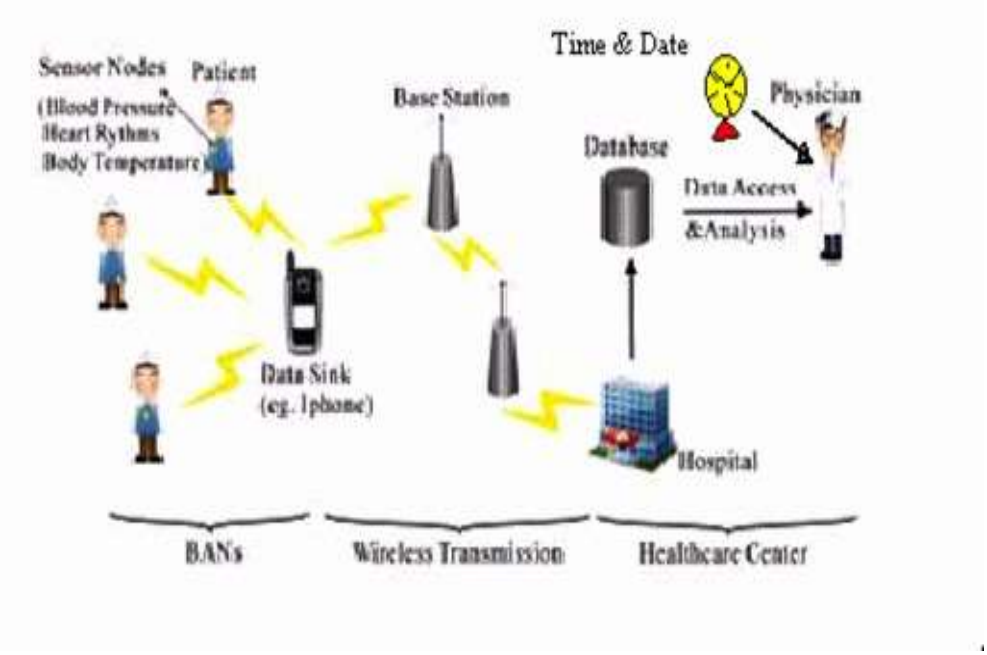


Fig. 1. A basic architecture of the electronic-health system.

The Drawbacks of Existing framework are they predominantly concentrates on the focal distributed computing framework which is not adequate for proficiently handling the expand-ing the volume of individual wellbeing data and most patients are worried about the secrecy of their own wellbeing data since it is liable to raise them in hell for every sort of unapproved accumulation and exposure.

Overcoming of this problem, a novel autho-rized accessible privacy model is established, patients can authorize physician by setting an access tree supporting flexible threshold predicates. A patient self-controllable multi-level privacy-preserving cooperative valida-tion scheme realizing three levels of security and privacy requirement in distributed m-healthcare system is proposed.

A typical architecture of a distributed m-healthcare cloud computing system is shown in Fig. 2. There are three distributed healthcare providers A,B,C and the medical research insti-tution D, where Dr. Brown, Dr. Black, Dr. Green and Prof. White are working respectively. Each of them possesses its own cloud server.

It is assumed that patient P registers at hospital A, all her/his personal health information is stored in hospital As cloud server, patient P gives Date and time limit to the hospital A. and Dr. Brown is one of his directly authorized physicians. For medical consultation or other research pur-poses in cooperation with hospitals B,C and medical research institution D, it is required for Dr. Brown to generate three indistinguishable transcript

ISSN: 2277-9655
Impact Factor: 4.116

simulations of patient Ps personal health information and share them among the distributed cloud servers of the hospitals B,C and medical research institution D.

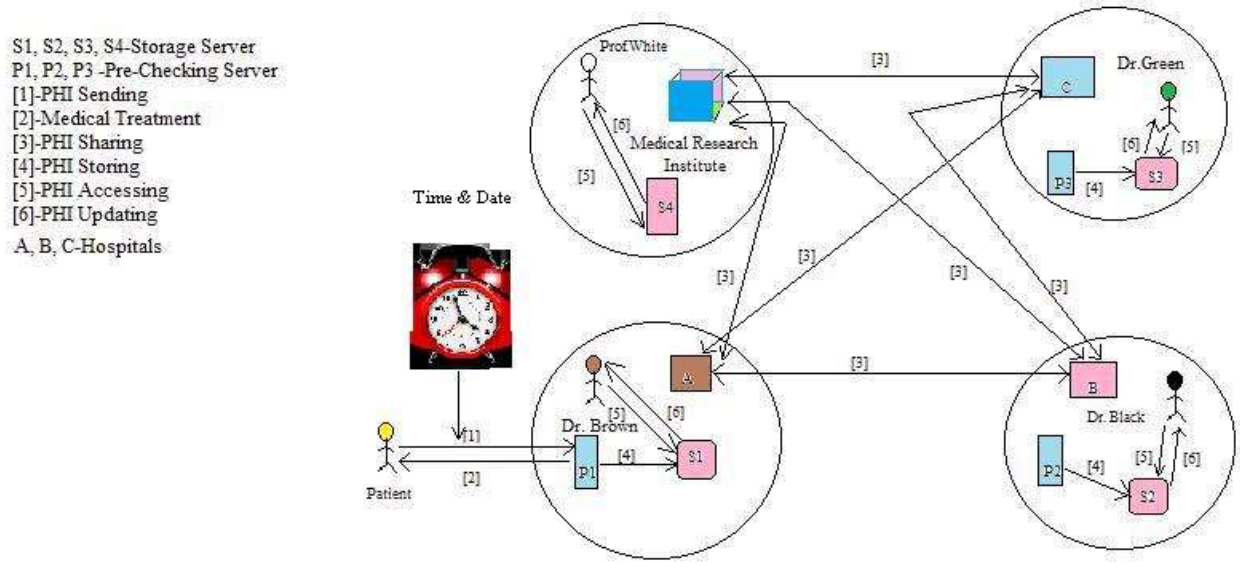


Fig. 2. System Architecture

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

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

Clinical Data Collection
The Hardware kit contains sensors like tempreture and heart bit counter.Using that sensors the patients heart bit and body temperature readings collection are done.Using Radio frequency that readinds are send to the mobile device like laptop ,tablet etc.the receiver side recive that readings and uploads on physicisn cloud.. With the PMHS ,each patient will have control over their personal medical information the information clinical institutions may not have, which will help reduce the complexity of health care delivery to each individual significantly.

Administrator
This module is use to assign the patient which is registered at hospital to the respectivespecialist. 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.

ISSN: 2277-9655
Impact Factor: 4.116

Physician

Physicians are two categories: The directly au-thorized physicians are identified with green labels in the local health-care provider they are authorized by the patients and these physi-cians 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. Since they are not authorized by the patients called 'indirectly authorized physicians. They can only access the personal health information, but not the patients identity.

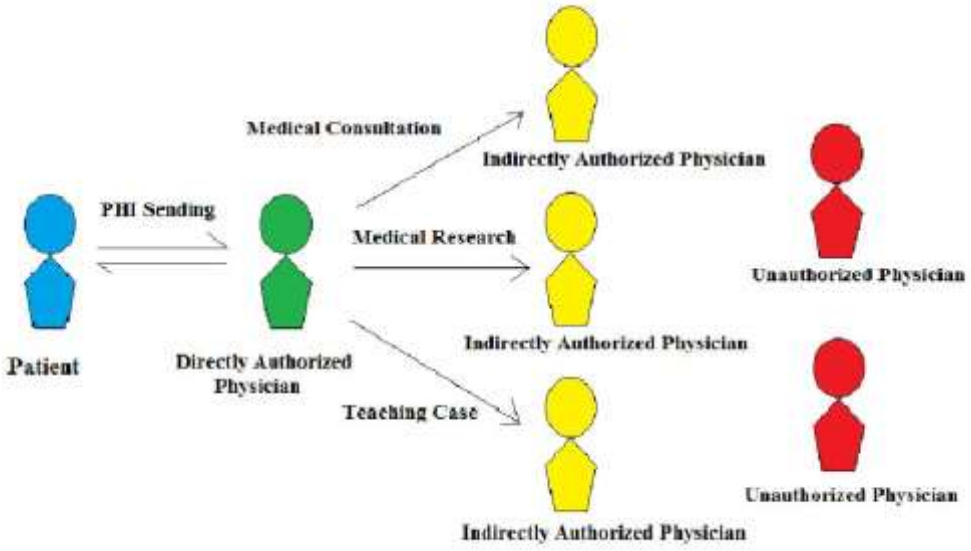


Fig. 3. Multiple Privacy and Security levels in PSMPV System.

ATTRIBUTE BASED DESIGNED VERIFIER SIGNATURE ALGORITHM

Input: Gathered Patient health data Ph

Output: Identically distributed transcript .

1 begin

2 Setup: On input 1^l, where l is the security parameter, this algorithm outputs public parameters and y as the master key for the central attribute authority.

3 Key Extract: Suppose that a physician requests an attribute set $\omega_D \in U$. The attribute authority computes sk_D for him if he is eligible to be issued with sk_D for these attributes.

4 Sign: A deterministic algorithm that uses the patients private key sk_P , the uni-form public key pk_D of the healthcare provider where the physicians work and a message m to generate a signature . That is $\sigma \leftarrow \mathrm{Sign}(sk_P, pk_D, m)$.

5 Verify: Assume a physician wants to verify a signature σ with an access structure A and possesses a subset of attributes $\omega_J \subseteq \omega_D$ satisfying $A(\omega_J) = 1$, a de-terministic verification algorithm can be operated. Upon obtaining a signature , he takes as input his attribute private key sk_D and the patients public key pk_P then returns the message m and True if the signature is correct, or ⊥ otherwise. That is $\{True, \perp\} \leftarrow Verify(sk_D, pk_P, m, \sigma)$.

6 Transcript Simulation Generation: We require that the directly authorized physi-cians who hold the authorized private key sk_D can always produce identically distributed transcripts indistinguishable from the original protocol via the Tran-script Simulation .

ISSN: 2277-9655
Impact Factor: 4.116

Notation in Algorithm
ω_D-The set of attribute owned by the physician.
ω_J- The subset of physicians attribute set of size k_x chosen to satisfy the predicate.
sk_D-Private key of the physician.
k_x-Number of attribute required to be owned by the patient w.r.t. node *x*

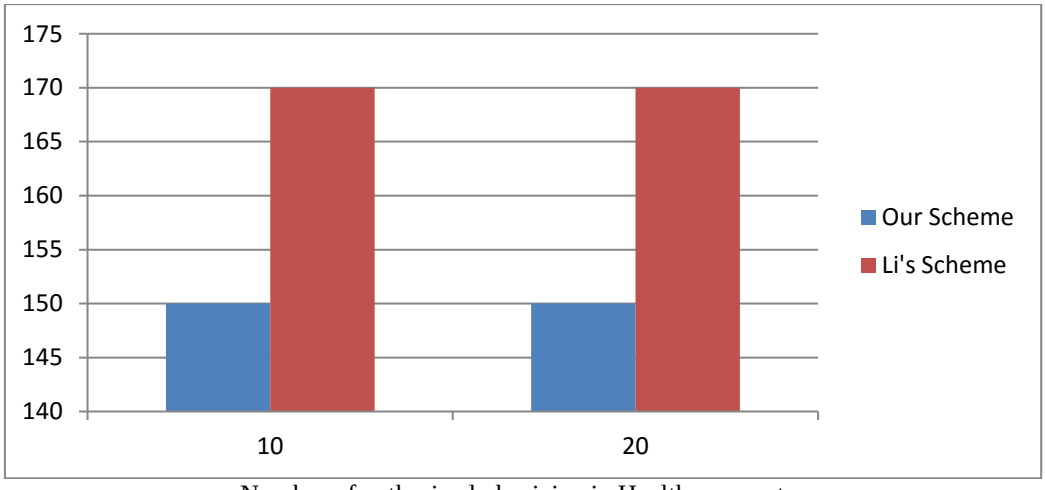
IMPLEMENTATION & PERFORMANCE ANALYSIS

Assume that N represents the no of directly authorized physicians and set n=10, n_D=10,d=6.Li.et al.Proposed a patient-centric and fine grained data access control using ABE to secure personal health record in cloud computing without privacy preserving authentication.for comparison to achieve the same function of PSMPV, it could be considered as the combination of ABE and DVS.Fig.4 Shows the time complexity remain constant even the no of authorized physician increased. Fig. 5 shows that through space complexity of PSMPV is slightly more than the combination construction and it is also independent of the no of directly authorized physician and performs significantly better than traditional DVS scheme all of whose time complexity and space complexity increase linearly to the number of directly authorized physician.

Time Complexity
Sign-*O(n+d-k)E*
Verify-*O(|S_r|(n+d-k))(P+E)*

Space Complexity
Public Key- *O(n + d - k)*
Private Key- *O(n_D +d)*
Signature- *O(n + d - k)*

Where,
n-Size of the required set of attribute
n_D-physicians attribute set
d-Default attribute set
k-Flexible threshold
P-Pairing Operation
E-Exponent operation



Number of authorized physician in Healthcare centre

Fig 4: Comparison of time complexity among Li's Scheme &Our Scheme where k=2

ISSN: 2277-9655
Impact Factor: 4.116

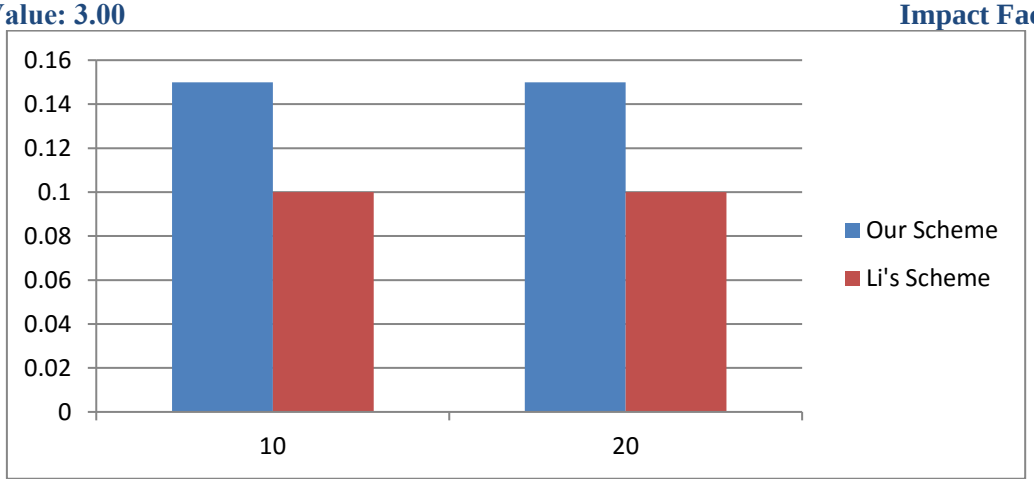


Fig 5: Comparison of space complexity among Li's Scheme &Our Scheme

CONCLUSION

We provide a patient self-controllable multi-level privacy preserving cooperative authen-tication scheme (PSMPV) and authorized ac-cessible privacy mode realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system. our system can resist various kinds of malicious attacks. In future we can implement this system for specially chronic diseases like diabetes.

ACKNOWLEDGEMENT

I thank our colleagues from PREC loni who provided insight and expertise that greatly assisted the dissertation.We would like to show our gratitude to the prof. S. Y. Raut for sharing their pearls of wisdom with us during the course of this dissertation.WE are also immensely greatful to Prof. Jondhale(H.O.D) for their comments on an earlier version of the manuscript.

REFERENCES

[1] Jun Zhou and Xiaodong Lin,PSMPA:Patient self-controllable and multi-level privacy preserving cooperative authentication in distributed m-healthcare cloud computing system, IEEE Transactions on Parallel and Distributed Systems,Vol. 26, No. 6,pp.1693-1703, June, 2015.
[2] L.Gatzoulis and I. Iakovidis, Wearable and Portable E-health Systems, IEEE Eng. Med. Biol. Mag.,26(5):51-56, 2007.
[3] J. Zhou and Z. Cao, TIS: A Threshold Incentive Scheme for Secure and Reliable Data Forwarding in Vehicular Delay Tolerant Networks, IEEE Globecom 2012
[4] S. Yu, K. Ren and W. Lou, FDAC: Toward Fine-grained Dis-tributed Data Access Control in Wireless Sensor Networks, In IEEE Infocom 2009.
[5] J. Sun, Y. Fang and X. Zhu, Privacy and Emergency Re-sponse in E healthcare Leveraging Wireless Body Sensor Net-works, IEEE Wireless Communications, pp. 66-73,In February, 2010.
[6] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for Ehealth Systems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.
[7] L. Lu, J. Han, Y. Liu, L. Hu, 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.
[8] J. Zhou, Z. Cao, X. Dong, X. Lin and A. V. Vasilakos, Secur-ing m-Healthcare Social Networks: Challenges, Countermeasures and Future Directions,IEEE Wireless Communications, vol. 20, No. 4, pp. 12-21, 2013.
[9] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-Plicy Attribte- Based Encryption, In IEEE Symposium on Security and Privacy,2007.
[10] R. Lu, X. Lin, X. Liang and X. Shen, A Secure Handshake Scheme with Symptoms-Matching for m-Healthcare Social Net-work,IEEE Journal on Selected Areas in Communica-tions, Vol.27, No.4, pp.387- 399, 2009.

ISSN: 2277-9655
Impact Factor: 4.116

[11] J. Sun and Y. Fang, Cross-domain Data Sharing in Distributed Electronic Health Record System,IEEE Trans-actions on Parallel and Distributed Systems, vol. 21, No. 6, 20103GPP RP-040461, Study Item: Evolved UTRA and UTRAN, December 200

[12] J. Misic and V. B. Misic, Implementation of security policy for clinical information systems over wireless sensor networks, Ad Hoc Networks,vol.5, no.1, pp.134-144, Jan 2007.

[13] F.W. Dillema and S. Lupetti, Rendezvous-based Ac-cess Control for Medical Records in the Pre-hospital Environ-ment,In HealthNet 2007.

[14] M. Li, S. Yu, K. Ren and W. Lou, Securing Per-sonal Health Records in Cloud Computing: Patient-centric and Fine-grained Data AccessControl in Multi-owner Settings, Se-cureComm 2010,LNICST 50,pp.89-106, 2010.

[15] I. Iakovidis, Towards personal health record: current situation obstacles and trends in implementation of electronic healthcare records in europe,Int. J. Med. Inf., vol. 52, no. 1, pp. 105115, 1998.

[16] E. Villalba, M. T. Arredondo, S. Guillen, and E. Hoyo-Barbolla, A new solution for a heart failure monitoring system based on wearable and information technologies in Proc. Int. Workshop Wearable Implantable Body Sens. Netw., Apr. 2006, pp. 150153.

[17] R. Lu and Z. Cao, Efficient remote user authentication scheme using smart card, Comput. Netw.,vol. 49, no. 4, pp. 535540, 2005. [18] M. D. N. Huda, N. Sonehara, and S. Yamada, A privacy management architecture for patient-controlled personal health record system,J. Eng. Sci. Tech-nol., vol. 4, no. 2, pp. 154170, 2009..

[18] S. Schechter, T. Parnell, and A. Hartemink, Anony-mous authentication of membership in dynamic groups in,in Proc. 3rd Int. Conf. Financial Cryptography, 1999, pp. 184195.

[19]] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrun-ner, and J. Thierry, Anonymity and application privacy in con-text of mobile computing in eHealth, in Mobile Response, New York, NY, USA: Springer, 2009 pp. 148157