IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Secure Cloud Storage of Health Records

P. Vishnu Sagar[1], RVLSN Sastry[2]

PG Scholar, Department of C.S.E, Visakhapatnam, India[1]

Associate Professor, Department of C.S.E, Visakhapatnam, India[2]

Abstract: The Distributed healthcare data Keyword cloud computing system considerably facilitates secure and efficient patient treatment for medical consultation by sharing personal health information among the healthcare providers. This system should bring about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. This research focuses on the secure storage of Patient-Centered e-Health (SSPCEH) concept by introducing its importance and demonstrating a multidisciplinary project that combines advanced technologies. The project links several aspects of SSPCEH functionality a) homecare telemedicine technologies) e-prescribing, referral, e-learning (c) state-of-the-art technologies like cloud computing and Service Oriented Architecture (SOA)(d)privacies preserving and secure storage This paper provides insights of the SSPCEH concept and the current stages of the project. In doing so, we aim to increase the awareness of this significant work and disseminate the knowledge gained so far through our work. In this project we implement and identity-based record retrieval process with uses a cryptography technique of identity-based privacy protection

Keywords: Personal Healthcare Record; Cloud Computing; Healthcare Information Systems Integration, privacy Protection, Identify based Encryption

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Cloud Computing comprises three different service models, namely Infrastructure- as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

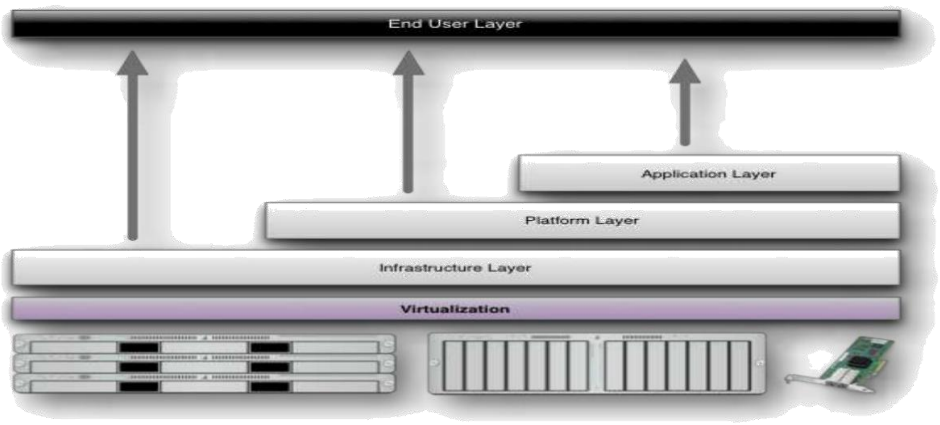

Fig1- Structure of service models

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

In healthcare data Keyword social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how **to ensure the security and privacy of the patients'** personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering and As to the security facet, one of the main issues is access **control of patients' personal health information, namely it is only the authorized physicians or institutions that can recover the patients' personal health information during the data sharing** in the distributed healthcare data Keyword cloud computing system.

In practice, most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. Therefore, in distributed healthcare data Keyword cloud computing systems, 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 intractable problems demanding urgent solutions.

A fine-grained distributed data access control scheme is proposed using the technique of attribute based encryption (ABE). Recently, a patient-centric and fine-grained data access controlling multi-owner settings is constructed for securing personal health records in cloud computing. It mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in healthcare data Keyword cloud computing system.

II. LITERATURE SURVEY

1) Cross-Domain Data Sharing In Distributed Electronic Health Record Systems

Cross-organization or cross-domain cooperation takes place from time to time in Electronic Health Record (EHR) system for necessary and high-quality patient treatment. Cautious design of delegation mechanism must be in place as a building block of cross- domain cooperation, since the cooperation inevitably involves exchanging and sharing relevant patient data that are considered highly private and confidential. The delegation mechanism grants permission to and restricts access rights of a cooperating partner. Patients are unwilling to accept the EHR system unless their health data are guaranteed proper use and disclosure, which cannot be easily achieved without cross-domain authentication and fine- grained access control. In addition, revocation of the delegated rights should be possible at any time during the cooperation. In this paper, we propose a secure EHR system, based on cryptographic constructions, to enable secure sharing of sensitive patient data during cooperation and preserve patient data privacy. Our EHR system further incorporates advanced mechanisms for fine-grained access control, and on-demand revocation, as enhancements to the basic access control offered by the delegation mechanism, and the basic revocation mechanism, respectively. The proposed EHR system is demonstrated to fulfill objectives specific to the cross-domain delegation scenario of interest.

DISADVANTAGE

- Data confidentiality is low.

2) Sage: A Strong Privacy-Preserving Scheme against Global Eavesdropping For E-health Systems

The eHealth system is en visioned as a promising approach to improving health care through information technology, where security and privacy are crucial for its success and large-scale deployment. In this paper, we propose a strong privacy-preserving Scheme against Global Eavesdropping, named SAGE, for eHealth systems. The proposed SAGE can achieve not only the content-oriented privacy but also the contextual privacy against a strong violation in data security.

3) Privacy-Preserving Query Over Encrypted Graph-Structured Data in Cloud Computing

In the emerging cloud computing paradigm, data owners become increasingly motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. For the consideration of users' privacy, sensitive data have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. In this paper, for the first time, we define and solve the problem of privacy-preserving query over encrypted graph-structured data in cloud computing (PPGQ), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Our work utilizes the principle of "filtering-and- verification". We prebuild a feature-based index to provide feature-related information about each encrypted data graph, and then choose the efficient inner product as the pruning tool to carry out the filtering procedure.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

To meet the challenge of supporting graph query without privacy breaches, we propose a secure inner product computation technique, and then improve it to achieve various privacy requirements under the known-background threat model.

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

4) Securing Personal Health Records In Cloud Computing: Patient-Centric and Fine-Grained Data Access Control In Multi-Owner Settings

Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. In this paper, we propose a novel framework for access control toPHRs 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 domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation.

DISADVANTAGE
The challenge of keeping both the data confidentiality and patient's identity privacy simultaneously

III. PROBLEM STATEMENT/SPECIFICATION

- Healthcare integration is a kind of enterprise integration that requires special attention.
- Healthcare information systems refers to such systems that are used to process data, information and knowledge in healthcare environments
- A series of terms have been used in the evolution of this phenomenon from its early foundations in the 1960s.
- Meanwhile health data and information in the past have been created and stored mainly on paper
- While earlier healthcare information systems were limited to departmental units

IV. PROPOSED SYSTEM

Proposed system for a privacy-preserving authentication scheme in anonymousP2P systems based on Zero-Knowledge Proof. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed healthcare data Keyword cloud computing systems where the computational resource for patients is constrained. Suggested patients have to consent to treatment and be alerted every time when associated physicians access their records and also our proposed system is a patient-centric and fine-grained data access controlling multi-owner settings is constructed for securing personal health records in cloudcomputing.Our proposed healthcare The Secure storage of Patient-Centered e-Health (SSPCEH) concept is a new multidiscipline area of research, with crucial aspects as it deals with the wellbeing of patients we focus mainly on views. In more detail depicts that the SSPCEH should integrate three themes such as

- Patient-focus
- Patient-activity
- Patient-empowerment
- Data Security
- The lack of consensus can be attributed, amongst other

(a) on the number of challenges that are involved in transitioning healthcare delivery to a more secure storage of patient-centered system and

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

(b) the lack of proof-of-concept through well documented and effective SSPCEH

- To develop an integrated platform that can be used by other organizations in the future
- better understand and analyze the complexities of the Greek healthcare environment;
- experiment and implement innovative integrated solutions that can be turned into products
- gain expertise and know-how on a complex area
- sell these products and know-how at national and international level

In this paper, we aim to solve the problem with a novel mechanism for Storing and searching of the data using the IBE scheme . With a novel searchable encryption scheme supporting secure conjunctive keyword search function. Compared with existing schemes, this work can achieve Better re-encryption with effective delegation revocation. And Searching technique will avoid the Guessing Attacks.

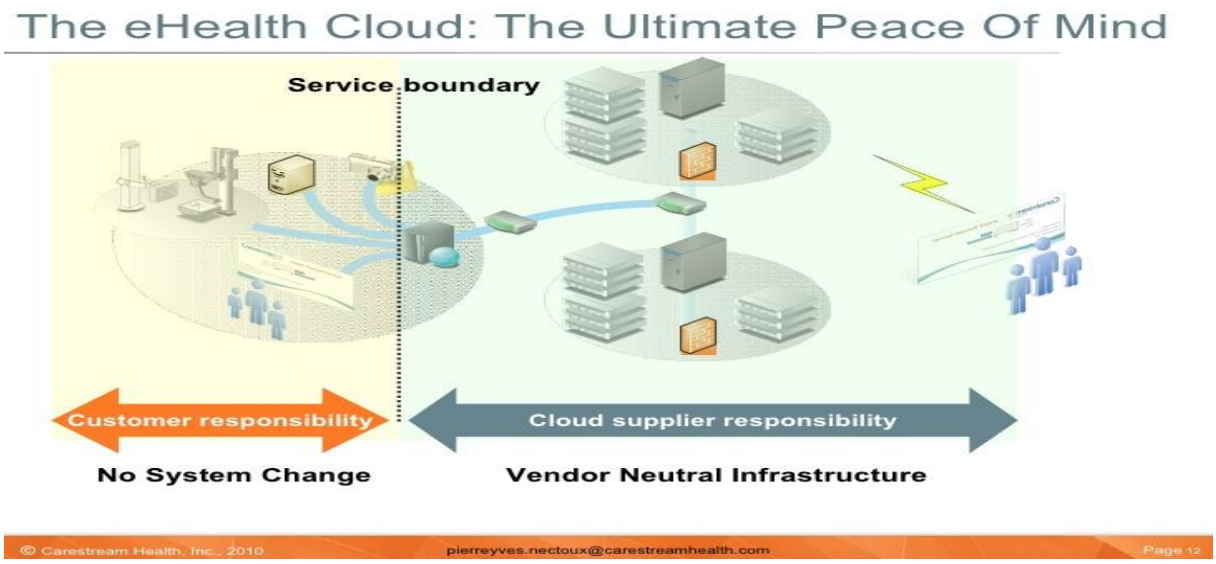

Figure 2: Proposed Model

E-healthcare system framework

E-healthcare System consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud **servers. The patient's personal health information is securely transmitted to** the healthcare provider for the authorized physicians to access and perform medical treatment. Illustrate the unique characteristics of distributed healthcare data Keyword cloud computing systems where all the personal health information can be shared among patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare providers and medical research institutions for medical consultation.

Authorized accessible privacy model

Multi-level privacy-preserving cooperative authentication is established to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates. Propose a novel authorized accessible privacy model for distributed healthcare data Keyword cloud computing systems which consists of the following two components: an attribute based designated verifier signature scheme (ADVS) and the corresponding adversary model.

Security verification

The security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem **and the number of patients' attributes to deal** with the privacy leakage in patient sparsely distributed scenarios. More significantly, without the knowledge of which physician in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfy the access policy can recover the PHI and the access control management also becomes more efficient.

Performance evaluation

The efficiency of PSMPA in terms of storage overhead, computational complexity and communication cost. a patient-

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

centric and fine-grained data access control using ABE to secure personal health records in cloud computing without privacy-preserving authentication. To achieve the same security, our construction performs more efficiently than the traditional designated verifier signature for all the directly authorized physicians, where the overheads are linear to the number of directly authorized physicians

ALGORITHM

HPE Identity-Based Encryption (IBE) takes a breakthrough approach to the problem of encryption key management. HPE IBE can use any arbitrary string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the dynamic generation of private decryption keys that correspond to public identities and the key servers base root key material. By separating authentication and authorization from private key generation through the key server, permissions to generate keys can be controlled dynamically on a granular policy driven basis, facilitating granular control over access to information in real time. The stateless nature of HPE IBE also dramatically simplifies operation and scaling. Key Servers can be distributed independently and geographically and key requests load balanced across them without the need to synchronize data, thus enabling high scale without growing complexity and to enable distributed and federated key management across the world easily and quickly. By eliminating the need for certificates, HPE IBE removes the hurdles of PKI: certificate lookup, lifecycle management, certificate revocation lists, and cross-certification issues. HPE IBE's simplicity enables it to be used in ways PKI could not; HPE IBE can be used to build security systems that are more dynamic, lightweight and scalable.

- **Notation**

For two bit strings X and Y of the same length..n X $\bigoplus$Y is their xor. For an integer n ≥ **1,** $\{0,1\}^n$ is the set of all bit strings of n bits, and {0,1} is the set of strings of m to n bits long. Also Xm..n denotes the substring of X containing bits with indices from m to n, where the first index is 1. We write X ←− $\mathbf{X}^{\$}$ for sampling an element from the set X uniformly at random.

- Description of IBE

Our scheme provides an authenticated encryption of short messages and is based on a fixed it permutation F. Of the n-bit input, k bits are devoted to the key K, l bits to the associated data H, and n−k−l to the message M. As the associated data needs only authentication, we map a possibly long string H to an l-bit value with a cryptographic hash function G. We **define scheme KWF formally as Π = (K**,E[F],D[F]), where:

K = $\{0,1\}^k$ — the key space;

1. H = $\{0,1\}^{0..t}$ — the associated data (AD) space with t ≤ $\mathbf{2}^k$; M= $\{0,1\}^{1..(n-k-l-1)}$ — the message space; C = $\{0,1\}^n$ — the cipher text space.
   G : $\{0,1\}^{0..t}$ −→ $\{0,1\}^l$ — collision-resistant hash function for the associated data;
2. pad : $\{0,1\}^{1..(n-k-l-1)}$ −→ $\{0,1\}^{n-l}$ — invertible padding function; F: $\{0,1\}^n$ −→ $\{0,1\}^n$ — fixed permutation.
3. E[F] : K × H × **M**−→ C —
$$\begin{cases} \mathcal{E}_K[\mathcal{F}](H,M) = \mathcal{F}\left(K||\mathcal{G}(H)||pad[M])\right) \oplus \left(K||0^{n-k}\right), \\ \mathcal{E}_K[\mathcal{F}](H,M) = \mathcal{F}\left(K||0^l||pad[M]\right) \oplus \left(K||0^{n-k}\right), \quad \text{else} \end{cases}$$
encryption function (Figure 1):
if H 6= **∅**;
4. D[F]:K×H×$\{0,1\}^n$−→M∪{⊥}—decryptionfunction.DK[F](H,C) is computed asfollows:
$$(a)\ X \leftarrow \mathcal{F}^{-1}(C \oplus \left(K||0^{n-k}\right)).$$

V. EXPERIMENTAL/SETUP AND RESULTS

In this work, we proposed and evaluated the IBE(Identity based encryption) to securely store the data in the cloud serer and also we have implemented the data owner and the cloud server and doctor to access the data which can enhance the storage for secure data retrieval process in e-health system

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

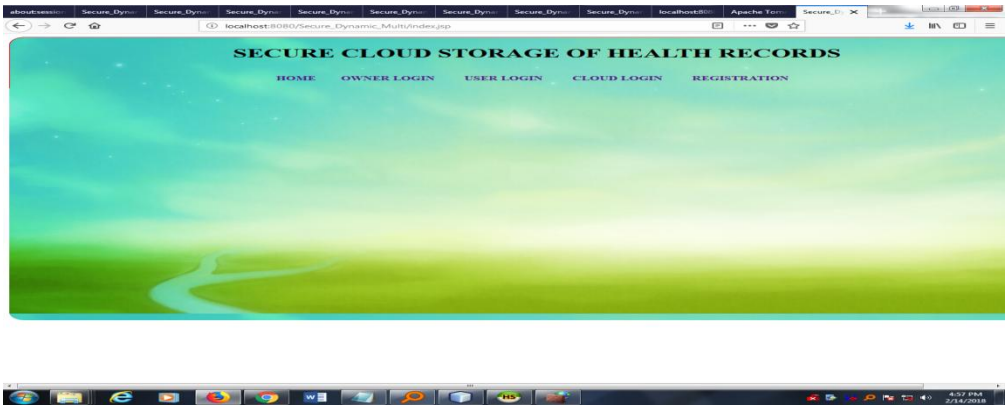

Figure 3: home page for the e-health storage and retrieval process

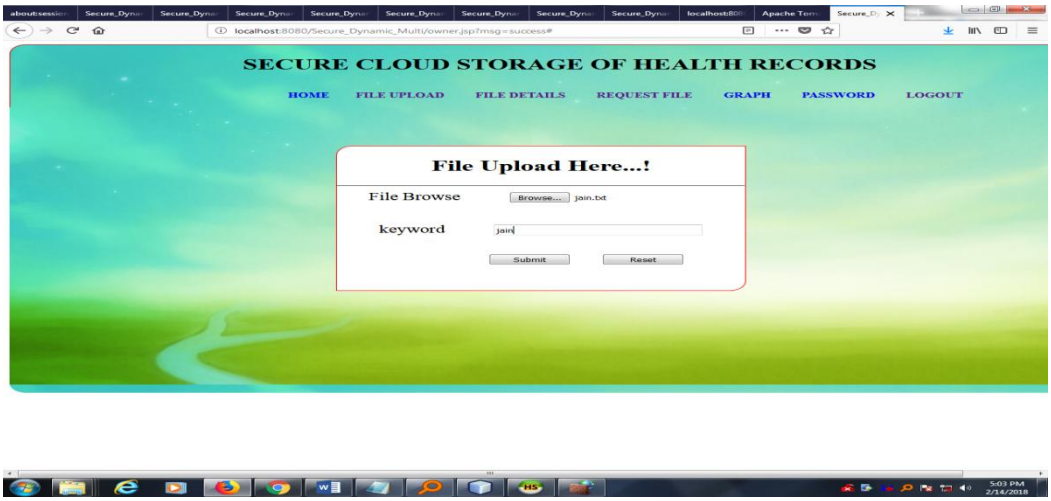

Figure 4: uploading of records in the cloud server

Figure 5: searching of record with security

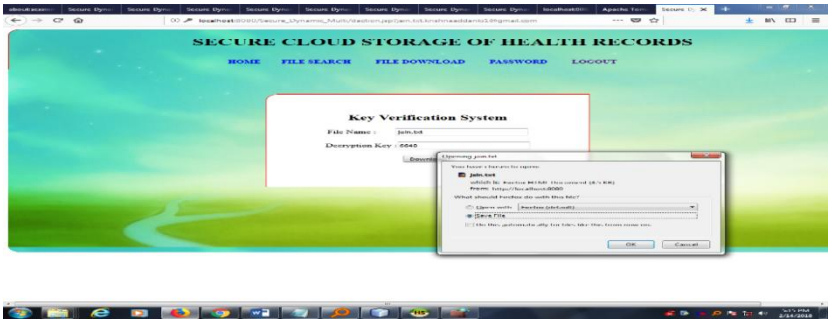

Figure 6: downloading of data with secure decryption key

Furthermore, this approach not only allow to large storage of patient information and also the security for the data accessibility in e-health system

VI. CONCLUSION AND FUTURE SCOPE

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 healthcare data Keyword 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.

Our future work will focus on investigating the relation between patient mobility and privacy under the distributed Environment.

REFERENCES

[1] J. Misic and V. B. Misic, "Implementation of security policy forclinical information systems over wireless sensor network," AdHoc Network, 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 Communication Network. 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 healthrecordsystem," 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] 6, pp. 683–694, Dec. 2011.

BIOGRAPHIES

RVLSN Sastry, Associate Professor, Dept of Computer Science & Engineering, SVCET, Vishakhapatnam(A.P)

P. VISHNU SAGAR, (14MT1D5811), Dept. of Computer Science & Engineering, SVCET, Vishakhapatnam (A.P)