A SYSTEMATIC AND SECURE DEDUPLICATION SCHEME FOR CLOUD ASSISTED e-HEALTH SYSTEMS

[1]A.Bhavani, [2]Dr. R. Jegadeesan [3]A.Shwetha Sri,[4]G.Anjali,[5]G.Sai Teja, [6]K.Mahesh Raj

[2,6]Associate Professor - of Jyothishmathi Institute of Technology and Science

Dept of CSE,

JYOTHISHMATHI INSTITUTE OF TECHNOLOGY & SCIENCE, KARIMNAGAR, T.S., INDIA.

ABSTRACT:

The widespread use of Electronic Health Record (EHR), and building a secure EHR sharing environment has attracted a lot of attention in both the academic community and health care industry. The Cloud computing paradigm is one of the most popular health IT infrastructure for facilitating EHR sharing and EHR integration. Privacy into mobile healthcare systems is built with the help of the private cloud. The desire to protect privacy is in part an outgrowth of a common human wish to live free of encroachment, judgment, inferiority complex. This technique provides important characteristics like privacy-preserving data storage and retrieval and audit ability to avoid miss using of health records. In this, we search over encrypted data thus hides access and search patterns. Searchable symmetric algorithm and elliptical curve cryptography are used here.

I. INTRODUCTION

The widely deployed electronic health (e-Health) system has changed people's daily life for its extraordinary advantages, such as more efficiency, high accuracy, and broader availability. Whereas, privacy concern is arguably the major barrier that hinders the development of the EHR stored in public storage with a direct connection to a network. For most e-Health systems, physicians periodically upload their observations and diagnosis to one particular store, where the Protected Health Information (PHI)[1] is seamlessly bound to the real identity of a specific patient. When physicians are authorized, they can easily obtain both the real identity and designated diseases of a particular patient, which apparently discloses the patient's privacy. To some extent, patients are reluctant to contact a doctor or a medical facility based on the real identities, instead, they prefer to show a token which can represent their diseases or other attributes rather than exposing real identities, and physicians can treat them using the token only. This perfect solution leads us to separate attributes from identity, which brings several open problems related to the system architecture.

First, if the authentication process takes place on centralized authority, even if the identity is isolated from the corresponding attributes, it still needs to disclose certain information regarding the relationship between attributes and identity to the authority for verification, so that the centralized authority can process requests and grant privileges to the designated user. On the other hand, if users directly communicate without the help of a central authority, it can guarantee that the privacy issues related to attributes are well preserved[2]. However, purely relying on the distributed user’s attributes cannot fulfill the requirement of verifiability of the isolated attributes. In a word, existing e-Health systems lack the ability to satisfy the requirements of preserving the privacy and the verifiability of the corresponding attributes simultaneously. As a result, patients face those security breaches and authentic verification problems when they share the same situation and want to talk with each other via cyber-space. Furthermore, those kinds of concerns become the major barrier that impedes patients from easily communicating. Thus, there is an urgent need for designing a framework where users can authenticate each other using verifiable attributes while keeping their attributes and identities undisclosed[3].

Fast access to health data enables better healthcare service provisioning, improves quality of life, and helps to save a life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in daily life services supported by mobile devices, such as home care and remote monitoring, enable patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces hospital occupancy, allowing patients with a higher need for in-hospital treatment to be admitted. Private cloud introduced which can be considered as a service offered to mobile users. Mobile users outsource private cloud data processing tasks that store the results processed on the public cloud. The cloud-assisted service model supports implementing practical privacy mechanisms as intensive computing and storage can be moved to the cloud, leaving mobile users with lightweight tasks. The electronic health care systems are dominantly increasing day by day as large amount of personal data for the medical purpose are involved and once the health record is exposed to cyberspace it becomes vulnerable to the outside world. According to a survey of government website [4], around 9 million patient's health record was leaked in the past three years. Despite the highest importance, privacy issues are not addressed efficiently at the technical level and efforts to keep health record secure have often fallen short. Automated decision support algorithms in mobile health monitoring [5] which is cloud-based was considered a future trend. Unfortunately, the cloud-assisted mobile-access of health data is promising and offers a great advance in healthcare systems and improves quality of life thus reducing the healthcare costs, there is a dominant opposing force in making a technology reality. Without properly addressing the health record maintenance and data management the complete health record is subject to get breached during data collection. This is because of protecting privacy in cyberspace is significantly more challenging. Thus, there is an urgent need for the development of reliable protocols and architectures, which will assure the privacy and security to stand as a guard against the adversaries and possible threats[6].

II. RELATED WORK

As far as emergency medical services are concerned, one of the earliest works on e-healthcare is medical information privacy assurance (MIPA) [7]. It was one of the few works that pointed out the important challenges for the privacy of medical information. It has also put on lights on devastating privacy breaches that were caused by inefficient technology. MIPA developed privacy-protecting infrastructures and technology to facilitate the personalized development of health information.

Winandy and colleagues [8] have pointed out various drawbacks of current e-health solutions and standards. In particular, they have not proposed the client platform security, which is a sensitive aspect of security in e-health systems.

Liang [9] and colleagues proposed an efficient and patient-centric access control scheme which allows data requesters to have different access privileges which are called as role-based access and then assigns different attribute sets to them. Performance analyses and extensive security mechanisms and demonstrate that the scheme is able to achieve desired security requirements with a little amount of communication delay.

The cryptographic key-management solution for e-health care systems was proposed by Lee and Lee [10] and in their solution, the trusted server has the ability to access the health record at any time which could result in a possible threat. Zhang and colleagues [11] proposed a framework for privacy-preserving attribute-based authentication system in e-health networks. The attribute - based authentication schemes designed for higher levels of privacy preserve the greater privacy of attributes and values of attributes, but cost more resources for computation and communication.

Terry and Gunter [12] designed a system so that it accurately captures the state of the patient at all times and represent data in a suitable form. The system also had the ability to view the entire patient's history without the need to keep track of the patient's previous medical record volume. It also assists in ensuring data is accurate, appropriate and legal. It has significantly reduced the chances of data replication as there is only one modifiable file, which means that the file is updated constantly when viewed at a later date or day and removed the issue of lost forms or paperwork.

Ren and colleagues [13] proposed e-health care system to which allows patients to encrypt their personal health records (PHR) before storing it on central authority. Because of the fact that the encrypted PHR prohibits the centralized server from obtaining the information it still faces the problem of data verification. Another drawback of this scheme is that it is vulnerable to a single point of failure. The concept of patient-controlled encryption (PCE) was proposed by Horvitz [14] in which the health records are divided into a hierarchy of smaller piece of information which will be encrypted using the key which is under patient's control. They provided a symmetric-key PCE for fixed hierarchy, a public-key PCE for fixed hierarchy, and asymmetric-key PCE for flexible hierarchy from RSA.

Personal Health Record (PHR) service is an emerging model for health information exchange [15]. Mobile devices help in reducing this clutter, such as home care and remote monitoring enable the people in their flexible lifestyle and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital Update EMT Info Download file Cloud Verify by TPA TPA occupation, allowing patients with a higher need for in-hospital treatment to be admitted. Fine! All these scenarios are possible but people admit to realize that they would completely lose their personal information and identity once it activates in the cyberspace. This takes place around because in a survey 8 million patients‘ health information was leaked over a couple of years. But why this medical data should be kept private rather than allowing somebody to have research on it. Of course, there are some quite good reasons for it. An employer may not find convenient to hire someone with certain diseases. A mutual fund or brokerage insurance firm may refuse to provide features once they know about the history of the disease of the patient. Despite the paramount importance, privacy problems are not addressed adequately at the technical level and efforts to keep health data secure have continually fallen short. This is because protecting privacy in the cyberspace is significantly more challenging[16].

III. HEALTH CARE CLOUD

An electronic health record (EHR) is a digital version of a patient's paper-based record. EHRs are nothing but the systematic and well-organized patient's health record database which is real-time and patient-centered in nature that makes information available instantly and securely to authorized users. Theoretically, EHR is recorded in a digital format which can be considered as capable of being shared across different health care systems. An electronic health record (EHR)[17] is defined as a systematic collection of electronic health information about individual patients. EHRs may consist of a variety of health - related information, including medical history, demographics, medication and allergies, laboratory test results, radiology images, immunization status, age and weight personal statistics, vital signs, and billing information. Health record in digital form and information systems are expected to improve quality of life and efficiency which will eventually lead to cost-effective health care systems. The EHR typically includes:

- Basic contact information.
- Life insurance information.
- Medications.
- Allergies.
- Blood group and other health-related data
- Reference person in case of emergencies.
- Family Background.

This paper presents the taxonomy of healthcare clouds based on the cloud service models and the cloud deployment models. Based on cloud service models, we can divide healthcare cloud product offerings into three layers:

Applications in the cloud (Software as a Service – SaaS).

This layer provides the capability for consumers to use the provider's applications running on a cloud infrastructure. For instance, the applications are accessible from various client devices through a thin client interface such as a Web browser. Consumers do not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even the capabilities of individual applications. In this type of cloud service model, security and privacy protection are provided as an integral part of the SaaS to the healthcare consumers [18].

Platforms in the cloud (Platform as a service – PaaS).

This layer offers the capability for consumers to deploy consumer-created or acquired applications written using programming languages and tools supported by the cloud provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Two levels of security and privacy protection are required in this type of cloud service model. The cloud provider can provide basic security mechanisms like end - to - end encryption, authentication, and authorization at the lower system level. At the higher application level[19], the consumers need to define application dependent access control policies, authenticity requirements, and so forth.

Infrastructure in the cloud (Infrastructure as a Service – IaaS).

This type of cloud service model provides consumers with the ability to deliver processing, storage, networks and other key computing resources where consumers can deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). In the Infrastructure cloud model, the healthcare application developers hold full responsibility for protecting patients' security and privacy[20].

IV. PROPOSED METHOD

The application can also use the cloud deployment models which give the taxonomy of healthcare clouds as shown in Fig 1.

Private cloud. The cloud infrastructure is operated for the sole purpose of providing healthcare. The organization or a third party may manage it and may exist on or off premise. The cloud provider provides the same security and privacy capability in this type of cloud deployment model as in the EMR system running a CDO[21].

Public cloud. The cloud infrastructure is made available by a cloud service provider to the general public or a large industry group. In this deployment model, developers and consumers of healthcare applications are fully responsible for protecting the security and privacy of patients. This infrastructure[22] provides the capability to the consumers to deploy their developed application using programming languages and tools supported by the cloud.

To sum up, security and privacy are more than just user privileges and enforcement of passwords.. Cloud computing platforms must have detailed, robust policies and procedures in place to ensure the highest possible physical security, network security, security of applications, security of internal systems, secure data backup strategy, secure internal policies and procedures, third-party certification. Security should be the top priority from day one in the health cloud. Here the patients' data is protected with comprehensive physical security, data encryption, user authentication, and application security as well as the latest standard-setting security practices and certifications, and secure point-to-point data replication for data backup[23].

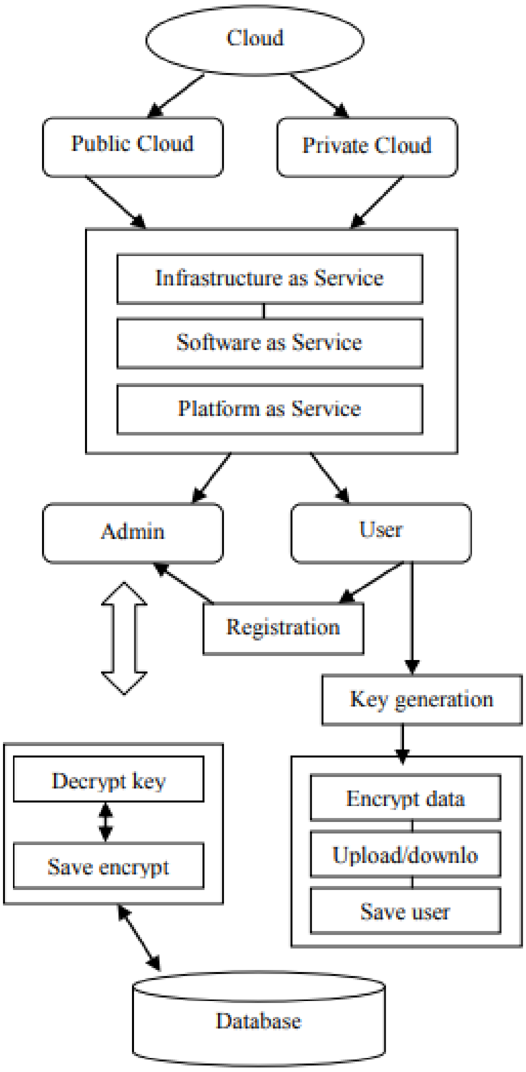

Fig1. System architecture

V. SYSTEM MODEL

The main entities involved in this system are depicted in Fig.2. Emergency Medical Technician (EMT)[24] is a physician who performs an emergency treatment. By user and EMT, which refer to the person and the associated computing facilities. The computing facilities are mainly mobile devices carried around such as a smart phone, tablet, or personal digital assistant. Each user is associated with one private cloud. This can be very desirable in situations like medical emergencies. Public cloud is the cloud infrastructure owned by cloud providers such as Amazon and Google which offers massive storage and rich computational resource. By assuming that at the bootstrap phase, there is a secure channel between the user and his/her private cloud, e.g., secure home Wi-Fi network, to negotiate a long-term shared-key. After the bootstrap phase, the user will send health data over an insecure network to the private cloud residing via the Internet backbone. Note that, we do not focus on the location privacy of mobile users which can be leaked when sending health data to the private cloud. There is a large body of location privacy schemes [25] in the literature. The user fully trusts the private cloud to perform computational health data. It is assumed that the public cloud is honest but curious in that it will not delete or modify the health data of users, but will try to compromise their privacy. Public cloud is not permitted to access health data.

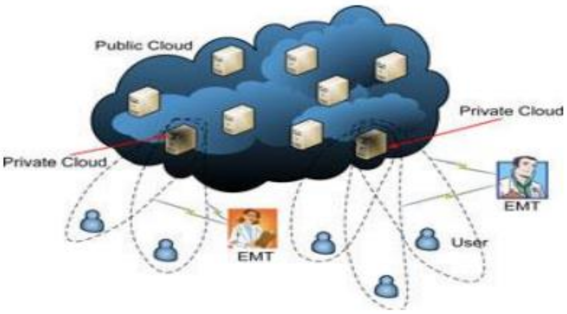

Fig. 2. Cloud-assisted mobile health network.

Searchable Symmetric Encryption (SSE):
This method consists of the following algorithm.

KeyGen(s): This function is used by the users to generate keys to initialize the scheme. It takes the security parameter s and outputs a secret key K.

building (D, K): The user runs this function to build the indexes, denoted by me, for a collection of document D. It takes the secret key K and D and outputs I, through which document can be searchable while remaining encrypted.

Trapdoor(K,w): The user runs this function to compute a trapdoor for a keyword w, enabling searching for this keyword. A trapdoor Tw can also be interpreted as a proxy for w in order to hide the real meaning of w. Therefore, Tw should leak the information about was as little as possible. The function takes the secret key K and the keyword w and outputs the respective trapdoor Two.

Search(I, Tw): This function is executed by the remote server to search for documents containing the user-defined keyword w. Due to the use of the trapdoor, the server is able to carry out the specific query without knowing the real keyword. The function takes the built secure index I and the trapdoor Tw and outputs the identifiers of files which contains keyword w.

VI. EXPECTED RESULTS

The proposed method provides secured health data access. In this work, anonymization is done using l-diversity techniques, which add more security for private data present in the dataset. Then the whole dataset is encrypted using the DES technique.

Now we will see some results performed over data with both algorithms FHE and SPHS and then we will easily understand how effectively our algorithm works. Fig. 3 shows the computation cost required for existing FHE algorithm and proposed SPHS system. We can see that as the number of aggregated data increases the cost required for FHE algorithm is also increased significantly and cost for SPHS is so negligibly increases with data increase. It is obviously observed that as the number of aggregated data increases, the computational cost and communication cost of SPHS negligibly increases which mainly focused on the most costly one-way trapdoor function, which contains a number of the most energy consuming modular exponentiation operations and has the most ciphertext expansion. These two elements significantly contribute to both the computational and communication cost.

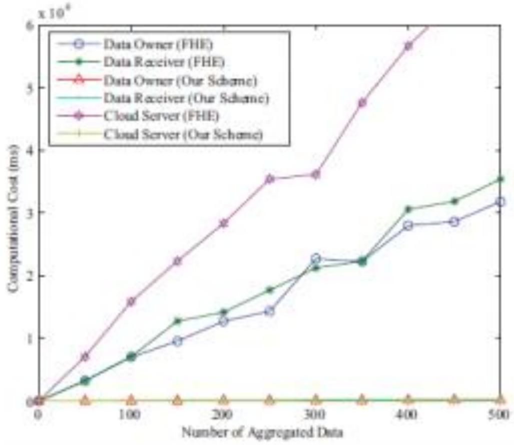

Fig. 3: Computational Cost Comparison of Privacy-preserving Data Aggregation

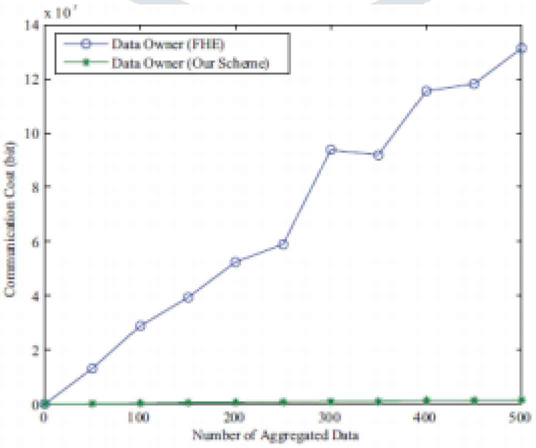

Fig. 4: Communication Cost Comparison of Privacy-preserving Data Aggregation

Fig. 4 shows a comparison between the communication cost required for FHE and SPHS. I figure we can see the cost of FHE highly increases with a number of aggregated data and a very opposite situation in SPHS cost increases in a very small amount.

VI. CONCLUSION

Building privacy with the help of the private cloud into mobile health systems. It provides a data storage solution for privacy by integrating a PRF-based key management system for unlink ability, a redundancy-based search and access pattern hiding scheme, and a secure indexing method for keyword search for privacy. We also looked at techniques that provide access control (in both normal and emergency cases) and Auditing the authorized parties ' ability to prevent misconduct by combining ABE-controlled threshold signing with role-based encryption. The proposed work builds privacy with the help of the private cloud into the mobile health systems. Bootstrapping is the secure channel used by authenticated and authorized cloud users for private communication. As a future work, in instantly accessible electronic devices such as cell phones and PDA's, the illegal access patterns can be made known, so that the basic level distribution of authorized data can be controlled and protected.

REFERENCES

[1] Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin, „„„PPDM: Privacy-Preserving Protocol For Dynamic Medical Text Mining And Image Feature Extraction From Secure Data Aggregation In Cloud-Assisted E-Healthcare Systems‟, IEEE Journal of Selected Topics In Signal Processing, Volume:9, Issue No: 7, pp.1332 – 1344, September 2015.

[2] Xiaokui Shu, Danfeng Yao, „„„Privacy-Preserving Detection Of Sensitive Data Exposure ", IEEE Transactions On Information Forensics And Security, Vol. 10, Issue-4, pp. 5, May 2015.

[3] K. Lauter, M. Naehrig and V. Vaikuntanathan, „ Can Homomorphic Encryption Be Practical?‟, In ACM Conference, vol. 1, no. 4, pp. 485– 509, 2011.

[4] P. Paillier, „ Public Key Cryptosystems Based On Composite Degree Residuosity Classes‟, In Eurocrypt 1999, vol. 20, o. 5, pp. 725–739, May 2009.

[5] Larry A. Dunning And Ray Kresman, „ Privacy-Preserving Data Sharing With Anonymous Id Assignment‟, IEEE Transactions On Information Forensics And Security, Vol. 8, No. 2, pp. 249–257., February 2013.

[6] Jian Liu, Kun Huang, Hong Rong, Huimei Wang And Ming Xian, „ Privacy-Preserving Public Auditing For Regenerating-Code-Based Cloud Storage‟, IEEE Transactions On Information And Security, vol. 57, no. 18, pp. 4047–4064, Dec. 2013.

[7] Kaitai Liang, Willy Susilo, Senior Member, IEEE, And Joseph K. Liu, „ Privacy-Preserving Ciphertext Multi-Sharing Control For Big Data Storage‟, IEEE Transactions On Information Forensics And Security, vol. 18, no. 6, pp. 333–340, 2015.

[8] Jason Croft, Matthew Caesar, „ Towards Practical Avoidance Of Information Leakage In Enterprise Networks‟, in NSDI journal on research and science, vol. 41, no. 4, pp. 23–28, Apr. 2012.

[9] Xiaokui Shu and Danfeng (Daphne) Yao, „ Data Leak Detection As A Service‟, in Securecomm Conference, vol. 31, Issue no 11, Pp. 222– 240, 2013.

[10] J. Sun, X. Zhu, and Y. Fang, "Privacy and emergency response in healthcare leveraging wireless body sensor networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 66–73, Feb. 2010.

[11] J. Sun, X. Zhu, C. Zhang, andY. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.

[12] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for eHealth networks," in Proc. IEEE Intl. Conf. Distrib. Comput. Syst., Jun. 2012, pp. 224–233.

[13] J. Sun, X. Zhu, C. Zhang, and Y. Fang, Security, and Privacy for Mobile Healthcare (m-Health) Systems, in Handbook on Securing Cyber-Physical Infrastructure, S. Das, K. Kant, and N. Zhang, Eds. Amsterdam, The Netherlands: Elsevier, 2011.

[14] E.-J. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[15] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, Jan. 2008.

[16].Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[17]. Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013 "A Recent Approach to Organise Structured Data in Mobile Environment" R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[18]. Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[19]. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013) "Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[20]. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014 "NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD" Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[21]. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 "SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[22]. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology

[23].Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[24]. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[25]. Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[26]. Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[27]. Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[28]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

[29]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.