ENHANCED SECURITY SERVICES TO SHARE OF PERSONAL HEALTH DATA IN THE CLOUD

[1]N.Venkateswaran, [2]Dr. R. Jegadeesan [3]G.Kalyani,[4]G.Ravali, [5]P.Sravanthi, [6]M.Sahithi
[1,2]Associate Professor, [3,4,5,6]SB.Tech Final Year Student-Department of Computer Science and Engineering
[1,2,3,4,5,6]Jyothishmathi Institute of Technology and Science , Karimnagar, India

Abstract - The cloud service in the health care zone has evolved in cost effective and suitable exchange of personal health data. Storing the personal health information to cloud is capable to theft (or) report and calls for the evaluation of method that makes sure security to the personal data. Therefore we suggest method called Enhanced Security Services to Share of Personal Health Data in the Cloud. These schemes protect Patient-Centric control on the personal health data and maintain the privacy of the PHR's. Patients store the encrypted data on the cloud servers and they provide access to different users on different parts of the health data. A semi-trusted proxy is set up and re-encryption server (SRS) is present to set up the public and private key pairs and to create the re-encryption keys. This method is secure opposed to insider warnings and implement a forward and backward access control. We formally study and confirm the working of this method with the High Level Petri Nets (HLPN). Performance assessment with regard to time consumption indicates that the personal health data methodology has the ability to securely share data in the cloud.

Index terms: Access control, security, personal health data, patient centric control.

1. INTRODUCTION

The cloud computing model showed great potential for increased cooperation intensification among many health care stakeholders as well to ensure the continued availability of health information, and scalability. Moreover, cloud computing it also integrates various important entities of health care Areas, such as patients, hospital staff including Doctors, nursing staff, pharmacies and medical laboratories individuals, insurance providers and service providers.

In general, PHR files contain information, such as: Demographic information, medical history of patients including diagnosis, allergies, past surgeries, and treatment, laboratory reports, and data on health insurance claims, and special notes for patients about some important health conditions. More formally, PHRs are managed through inter Web - based tools to allow patients to create and manage their health information as life recorders can be available for those who need access. Thus, PHRs enable patients to work effectively communicate with doctors and other caregivers report symptoms, seek advice, and maintain health records for diagnosis and treatment update from him. And PHRs either in cloud storage or in transit from patient to patient cloud or cloud to another user may be vulnerable to unauthorized access due to malicious behaviour of external entities. Moreover, there are some threats by good insiders on data. For example, PHRs either in cloud storage or in transport from the patient to the cloud or cloud to another user who may be vulnerable to unauthorized access due to malicious behaviour of external entities. Individuals working in the cloud service provider can act maliciously.

The HIPAA provides that the integrity and confidentiality of electronic health information stored by health care providers must be protected by the terms of use and disclosure and with the permission of patients. Furthermore, while PHR files are stored on third-party cloud storage, must be encrypted in a way that does not allow cloud service providers or unauthorized entities should be able to access PHRs. Instead, only entities or individuals who have the privilege of "right to know" should be able to access PHR's. In addition, the patient must administer the mechanism to grant access to PHRs to avoid unauthorized alterations or misuse of data when sent to other stakeholders in a healthy cloud environment. Many methods have been used to ensure the privacy of PHR stored on cloud servers. Privacy policies include privacy, confidentiality, authenticity, accountability, and audit experience. Confidentiality ensures that health information is completely hidden from unauthorized parties.

This methodology called Enhanced Security Services to Share of Personal Health Data in the Cloud to manage the access control mechanism for PHR administered by the patients themselves. The methodology maintains confidentiality of PHRs by restricting unauthorized users. In general, there are two types of PHR owners and non-owner PHRs, such as family members or friends of patients, doctors, doctors, representatives of health insurance companies, pharmacists and researchers. Patients as PHR owners are allowed to upload encrypted PHR files to the cloud by providing selective access to users across different parts of the PHR each member of the late user group is granted access to PHRs by PHR owners to a certain level based on the user role. The access levels for different groups of users in the access control list (ACL) are determined by the PHR owner. In contrast to the approach to achieving safe control of access to accurate, scalable and fine data in cloud computing that proposes multiple key management by PHR owners.

2. LITERATURE SURVEY

In this modern healthcare environment, the personal health data owners ready to store their personal health information in the cloud. They can determine which users shall have access to their medical record. At the same time provide the confidentiality [1] and authenticity of personal health data. In this the user wants to access the data then the cloud storage will provide the different types of keys. The re-encryption scheme is one in which the proxy possesses both parties keys simultaneously. The goal of this proxy re-encryption schemes is to avoid revealing either of the keys or the underlying plaintext to the proxy, [2] this method is not ideal. Attribute based encryption is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon attribute. A crucial security aspect of ABE is collusion resistance an adversary that holds multiple keys. Now a day's data is not secure if the person wants to store the data then he will check the security [3].

Now a day's healthcare providers are moving their electronic data into the cloud. Because of security purpose and storage. Instead of building data centers we use the cloud storage. In this cloud also raise many security challenges that are authentication, identify management, access control and trust management [4]. In this the patients will maintain their personal own information stored in the cloud.

In this the owner stores data in the third party such as cloud providers. However, there have been wide privacy concerns as personal health information cloud be exposed those third party server and to unauthorized parties. In this security schemes are protect their personal data from public access [5]. Here we are testing the challenges of maintaining patient's privacy in electronic health record systems. Furthermore, we argue for approaches that will allow patients to generate and store encryption keys, so that the patient's privacy is protected should the host data center be compromised [6].

Sharing of personal health records (PHR) in cloud is a serious issue in recent trends. The data which is stored in the cloud is not secure because everything depends upon the cloud service provider (CSP).An unexpected cloud fail suddenly may expose all data in cloud. In order to overcome that problem a new symmetric key encryption that uses a constant key for encrypting PHR is proposed [7]. Cloud computing provides better opportunity for both small and large organizations to change from traditional data centers to cloud services, where the organizations will be more worried with their applications, services, and data rather than the underlying network infrastructures and their associated cost. These are the major problems, however, with data security, reliability, and availability in the cloud [8]. In this paper, we are going to propose an efficient fine-grained access control system for secure Personal Health Records (PHRs) in cloud computing. In this system, the patients have fine-grained access control for their health records. The underlying denoting of this system is a newly designed identity-based conditional proxy re-encryption scheme with chosen-cipher text security [9].

Cloud computing mainly focuses on maximizing the effectiveness of the shared resources. Cloud storage provides a convenient means of storing and retrieving of large amount of data. Personal Health Records (PHRs) should remain as a lifelong property of patients and should be displayable conveniently and securely to selected caregivers [10]. Cloud computing is emerging computing a model those resources computing infrastructure they are offered as online services. As it is a missionary as it is, this model also brings many new data challenges security and access control when users use sensitive information to share on cloud servers, which are not within their scope trusted domain as data owners [11]. PHR is a kind of Maintain and record health records by individuals. To an ideal personal health record can incorporate personalized medical information from different sources and provide complete and personal Health and Medical treatment summary by internet or portable media under security requirements and privacy [12]. The cloud, along with mobile technology, has enabled doctors to function properly monitor and evaluate patient health while the patient is in the comfort of his home. This requires Share health information among health care teams such as doctors and nurses to provide them better and safer care for patients [13].

At present, the sensors are everywhere like mobile phones, laptops, GPS, etc. allow one to access not only him private data, but also to others on the cloud servers. To enhance security, data is usually encrypted before being sent to servers. However, take advantage of other encrypted data without decryption the keys are very difficult. In this paper, we propose a framework which allows cloud-based social networking users to share data in a secure manner [14]. Cloud computing is one of the most advanced technologies in recent years. Since this new computing technology requires users to entrust their data to cloud service providers. PHR is patient-centered a model for the exchange of health information in which information is outsourced for storage in a third-party server, called cloud service providers, so that the security and privacy of data outsourcing must be maintained[15]. This is an exploratory invitation paper studied on Petri-graphical networks and mathematical modeling tool. Petri Networks is a promising tool to describe and study information processing systems it is synchronized, asynchronous, and distributed parallel or non-deterministic and / or random [16].

In multiple power ABE Schema, multi-monitor different attribute authorities sets of features and the corresponding decryption version keys for users, can require encryption that gets the user keys to the proper attributes of each power by decrypt a message. Chase gave multiple authority ABE schemes using the concepts of Centralized Authority (CA) and Global Identifiers (GID) [17]. Plutus is an encryption storage system that can be secured file sharing without putting too much trust in the file servers. In particular, it makes use of new encryption priority to protect and share files. Features Plutus too manage scalable key while allowing individual users to maintain direct control over who has access to its files [18]. The Personal Health Record Online (PHR) enables patients to manage their medical records in a centralized manner, which is largely personal health data is easy to store, access, and share.

However, by storing PHRs in the cloud, patients lose physical control for their personal health data, making it necessary for each the patient has to encrypt their PHR data before uploading it to the cloud servers [19]. Security and privacy are crucial issues in the protection of health information. The goal is to maintain the medical privacy of confidential information about the patient. The successful implementation and application of the Electronic Medical Record (EMR), EHR and Personal Health Record (PHR) prove to be a difficult task due to a combination of technical, regulatory and policy issues. Personal health records, HIPAA privacy rule, authentication, health privacy protection, encryption and electronic health records [20].

3. FRAMEWORK

The method imposes access to fine granules .The control allows patients or PHR owners to Manage access through their health information. In the professionals Methodology development, patients load encrypted Health bills by encrypting PHRs sections separately, For example: (i) personal information, (ii) medical information and insurance information, and (iii) before Book Information Moreover, the client application for PHR also generates re-encoding parameters. They are later transferred to the SRS. If the user wants To access any part of the PHR, the user downloads PHR of the cloud after authentication It is important to say that it is still at this point, the user cannot decrypt PHRs, because the user needs to receive correspondence parameters for decoding from SRS.SRS checks ACL to the student's user and determine whether it is Access the section that the user requested The decoding parameters are given by PHR owner or not.

3.1 PERSONAL HEALTH DATA:

PHRs can be defined as the electronic version of health information for patients, which is controlled by patients themselves. Primary health organizations allow patients to manage them Information, such as demographics, diagnosis, and treatment monitoring and self- control. Primary health reports differ from e-health Records (EHRs) meaning that EHRs are managed by health organizations and contain information Income by doctors and hospital staff instead of patients.

3.2 EL-GAMAL ENCRYPTION:

Cryptography is a public key cryptography system Proposal by T. EL-Gamal. The sentences are based on different-Hellman Key exchange. Difficulties in computing separate logarithms establish the cryptography Security system. The steps consists mainly which are initialization, encryption and decryption.

3.3 PROXY RE-ENCRYPTION:

The third- party proxy re-encryption policy is used Possess the ability to convert encrypted text which has been encrypted for one of the connected parties to be decrypted by the user or the other party. The main key Re-programming modules include re-encoding, setup, key encryption, and decryption.

4. RESEARCH METHODOLOGY

In this system is used to re-encrypt the proxy Secure and secure sharing of PHR files through the general cloud. This methodology for the participation of PHRs in the cloud environment includes three entities:

i. The cloud: The plan suggests storing the PHRs on the cloud by PHR owners for subsequent participation with other users in a safe manner. The cloud is assumed as an unreliable entity and users download or download PHRs to or from the cloud servers. This methodology uses cloud resources just download and download PHRs by both types of users, therefore, have no changes related to the cloud necessary.

ii. Server Setup and Re-encryption (SRS): SRS is a semi-trusted server responsible for preparing public-Private keys/ Home users in the system. SRS .It also generates encryption keys for the purpose PHR is safe between different user groups. The statistical evaluation strategy is considered in this methodology is trusted entity. So, suppose to be honest the protocol is generally low but quaint in nature. The Keys are maintained by SRS, but PHR data is never referred to SRS. Encryption and decryption tasks are performed at the end of users. Beside the key management, SRS also implements access control over shared data. SRS is a standalone server cannot it took more than a general cloud due to cloud failure trusted entity. SRS can be maintained by trusted a third party organization or by a group of hospitals to Patient comfort. They can also be kept a group of connected patients. However, SRS maintained by hospitals or by a group of patients will generate more confidence is due to the involvement of health professionals and or self-control of SRS by patients.

iii. Users: In general, the system has two types of users: (a) Patients (b) family members Or friends of patients, doctors, doctors and health representatives of insurance companies and pharmacists researchers. In this methodology, friends or families members of me are considered private domain users while all other users are considered to be the public domain users. Users of both public and private sectors the domain may be granted different levels of access to PHRs by PHR owners. In other Words, this methodology allows patients exercise control over obtaining good lines on health care references. All users in the system are required to register with SRS to receive SRS services. Record based on user roles, for example, Researcher, and Pharmacist.

This system provides the following services for the personal data shared over the public cloud.

•Confidentiality

•Secure sharing in PHR between groups Users designers

• Secure health care reviews (PHR) from unauthorized access to Insiders on identity

• Control forward and backward access

In this system, we do not consider the cloud trusted entity tends. Cloud computing features Such as the Common Resource Group, virtualization can generate many types of internal and external threats for PHR groups that are shared across the cloud. It is therefore important that human rights organizations do so they are encrypted before they are stored in the third-party cloud server verse. The PHR is first encoded at the end of the PHR holder they are later uploaded to the cloud. The cloud only works as a storage service in this methodology. Encryption keys and other control data are never stored on the cloud. So, at the end of the cloud Data confidentiality is achieved well. Even if the user is unauthorized in the cloud by some means wipe the encrypted PHR file, the file cannot be decrypted because the control data does not exist in the cloud guaranteed Privacy PHR.

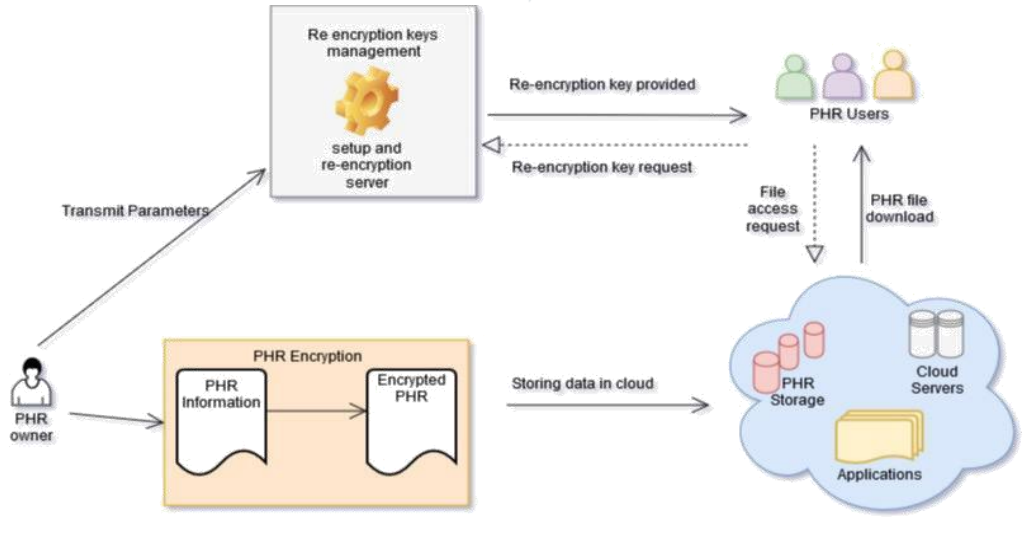

Fig1: Architecture of the personal health data

4.1 ENCRYPTION and DECRYPTION

Encryption:

Suppose that any patient needs to load personal data on the cloud. Patient client application generates a random number equal to the personal data sections set in user-defined access level groups. In this case, we consider all four sections listed in have different access levels. The system does not need to change keys for each user also do not require a reboot Encrypt the entire data. The variable is used to encrypt section of the personal data. Each partition is encrypted separately by the client position.

Decryption:

Suppose the user wants to access the encrypted personal data loaded by the patient. The user downloads data directly from the cloud (after cloud authentication Processing). After that, the user asks the SRS to calculate and send the corresponding parameters used for decryption. The SRS checks the ACL for a restart the age of the user and determine whether to access the partition that the user request is granted by the PHR owner or not. According to the access permissions specified in the ACL, the SRS will generate the corresponding parameters and will send those to the requesting user. The process of making a encrypted message recognizable with a cipher algorithm.

Private Key: The secret component of a pair of cryptographic keys used for asymmetric cryptography. In a public key cryptosystem that key of a user's key pair which is known only by that user.

Public key: A public key which encrypts a message. (RFC 2828) the publicly-disclosable component of a pair of cryptographic keys used for asymmetric cryptography. In a public key cryptosystem, that key of a user's key pair which is publicly known.

For this encryption and decryption algorithms are used they are SHA1 hashing algorithm is used, HLPN (High Level Petri Nets), EL-Gamal encryption, and proxy re-encryption. These algorithms produce high security to the personal health data.

Table1: comparison of models

Attribute-Based Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing	**Scalable and secure sharing of personal health records in cloud computing using attribute based encryption**	**Analysis of Various Encryption Algorithms in Cloud Computing**	**A Methodology for Secure Sharing of Personal Health Records in Cloud Environment**
In this method a new structure Safe distribution of personal health records in the cloud Computing. we are taking into consideration cloud servers are moderately responsible, we oppose it to, they fully understand the patient-based model and patient. They must have a wide management of their privacy through encrypt their personal health records files to allow access fine granules. The characteristic method is treated. Goals brought by various users of personal health record owners, in that we completely reduce multiples, main management with enhanced privacy guarantee. We use attribute property encryption to encrypt personal health record data. Patients can therefore allow access not only through personality users, but also many users of public domains with different professional roles, affiliations and qualifications. Here, we reinforce the existing multiple authority. The schema-based encryption scheme is managed on demand user revocation, effectiveness and reliability.	In this method, a novel secure participation framework for personal health records in cloud computing. Consider the cloud is partly trustworthy servers, we call it to achieve the full realization of the patient concept, patients must have full control over themselves privacy by encrypting their PHR files to allow granular access. Handles the unique window. The challenges brought by many PHR owners and users, at we greatly reduce the complexity of key management with enhanced privacy safeguards compared with previous works. We use ABE to encrypt PHR data, so that patients are allowed access not only by personal users, but also different users of public areas with different professional roles, qualifications and affiliations. Furthermore, we reinforce the current MA-ABE scheme for dealing with user revocation efficiently and on demand, and prove it. Security through implementation and simulation, we It turns out that our solution is scalable and effective.	Cloud computing arises a new generation technology in the information world technique. It has a lot of advantages but some challenges still exist in this technology. Security is the most difficult issue in this technology. we discussed different encryption algorithms to overcome this security problems with the advantages and negatives from ression analytical algorithms. Here, we conclude that the homomorphic algorithm is the most appropriate algorithm in cloud computing environment to secure its value data in an open network capacity, symmetric an algorithm to perform operations on encrypted data enables higher security than other algorithms such as RSA,DES and AES. Future work is the implementation of hardware or software technology with symmetric algorithm to provide protection on the cloud of any kind of seconds attack of purity.	Data security is the key problem in cloud storage. Before outsourcing PHR in a different third party server we use attribute-based encryption schemes for safe storage. ABE is used to encrypt PHR data, so that patients cannot allow access only by personal users, but also different users of public areas with different professional roles, qualifications and affiliation. Using MA ABE enhancement system, better when cancelling the order. The status of the process will arise some problems. The main issue in this case is the attempt to implement the workflow on the basis of circumstances. To solve this need encryption-based encryption feature (ABBE). work flow based on attitude is Implemented using ABBE and cost security and account analysis. From the analysis shows that this work is based on flow. The scheme is both scalable and effective. It gives better on revoking user demand as well.

IV.CONCLUSION

This methodology for safe storage of output and sending it to entities that are certified in the cloud. The methodology maintains the confidentiality of PHRs and ensures patient-based access control to different parts of PHRs based on patient access. We have implemented a granular access control so that valid system users can not access the PHR parts they are not allowed to access. PHR owners store encrypted data on the cloud, and only our authorized servers with valid cryptographic keys issued by a semi-trusted agent can decrypt the PHRs. The semi-trusted agent role is to create and store public / private pairs for users in the system. In addition to maintaining confidentiality and ensuring patient-based access control over PHRs, methodology also manages forward-access and back-end access control for newly joined users, respectively in addition, we have formally analyzed and verified the work of the this methodology through HLPN, SMT-Lib, and Z3 solution. Performance was evaluated based on time spent on switches, encryption and decryption operations, and response time. The experimental results show the feasibility of the this methodology for secure exchange of PHRs in the cloud environment.

REFERENCES

[1] Prajakta Solapurkar, Girish Potdar," Patient-Centric Secure Sharing Of Personal Health Record In Cloud Storage," International Journal of Engineering Research and General Science Volume 3, Issue 3, part-2, May-June, 2015.

[2]A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, "Incremental proxy re-encryption scheme for mobile cloud computing environment," The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

[3]Vishal Jagdale, Dinesh Kekan, Ishwar Baride,"Secure Sharing Of Personal Health Record In Cloud Using Attribute Based Encryption," International Journal of Computer Science and Mobile Computing, Vol.4, Issue.4, April 2015, pg.309-312.

[4]R.Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom), 2012, pp. 711-718.

[5]Y. B. Gurav, Manjiri Deshmukh, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358.

[6]Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter," Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,"Sathish kumar V E, K Umamaheshwari," Cryptosystem For Personal Health Records In Cloud," International Journal of Computer Applications (0975-8887) International Conference on Innovations in Computing Techniques (ICICT 2015).
[7]Daniel f. fitch and haiping xu," a Petri net model for secure and fault-tolerant Cloud-based information storage,"
Kaihe1, 2, jian weng1?? Joseph k.liu2, wanlei zhou3," Efficient Fine-Grained Access Control for Secure Personal Health Records in Cloud Computing,"V.M. Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data In Cloud," International Advanced Research Journal in Science, Engineering and Technology Vol. 1, Issue 2, October 2014.
[8]S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.
[9]T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.
[10]D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud," Future Generation Computer Systems, vol. 35, 2014, pp. 102-113.
[11]D. H Tran, N. H.-Long, Z. Wei, N. W. Keong, "Towards security in sharing data on cloud-based social networks," in 8th International Conference on Information, Communications and Signal Processing (ICICS), 2011, pp. 1-5.
[12]T.Radhika, S.Vasumathi Kannagi "secure sharing and access control of personal health record in cloud computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Special Issue 3, July 2014 .
[13]T. Murata, "Petri Nets: Properties, Analysis and Applications, "Proceedings of the IEEE, vol. 77, no. 4, pp. 541-580, Apr. 1989.
M. Chase and S. S. M. Chow. Improving, privacy and security in multi authority Attribute -based encryption. In CCS 2009, pages 121–130. ACM, 2009.
[14]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.
[15]Li, M., Yu, S., Ren, K., and Lou, W., "Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings," Security and Privacy in Communication Networks, pp. 89-106, 2010.
[16]Cheng-Kun Wang (2015) Security and privacy of personal health record, electronic medical record and health information. Problems and Perspectives in Management, 13(4), 19-26
[17]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
[18]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
[19]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
[20]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
[21]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
[22]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

[23]Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology
[24]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
[25]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
[26]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)
[27] 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)
[28] 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
[29] 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
[30] 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.
[31]Prajakta Solapurkar, Girish Potdar," Patient-Centric Secure Sharing Of Personal Health Record In Cloud Storage," International Journal of Engineering Research and General Science Volume 3, Issue 3, part-2, May-June, 2015.
[31] A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, "Incremental proxy re-encryption scheme for mobile cloud computing environment," The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.
[32] Vishal Jagdale, Dinesh Kekan, Ishwar Baride,"Secure Sharing Of Personal Health Record In Cloud Using Attribute Based Encryption," International Journal of Computer Science and Mobile Computing, Vol.4, Issue.4, April 2015, pg.309-312.

[33] R.Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom), 2012, pp. 711-718.
[34] Y. B. Gurav, Manjiri Deshmukh, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358.
[35] Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter," Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,"
[36] Sathish kumar V E, K Umamaheshwari," Cryptosystem For Personal Health Records In Cloud," International Journal of Computer Applications (0975-8887) International Conference on Innovations in Computing Techniques (ICICT 2015).
[37] Daniel f. fitch and haiping xu," a Petri net model for secure and fault-tolerant Cloud-based information storage,"
[38] Kaihe1, 2, jian weng1?? Joseph k.liu2, wanlei zhou3," Efficient Fine-Grained Access Control for Secure Personal Health Records in Cloud Computing,"
[39] V.M. Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data In Cloud," International Advanced Research Journal in Science, Engineering and Technology Vol. 1, Issue 2, October 2014.
[40] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.
[41] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.
[42] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud," Future Generation Computer Systems, vol. 35, 2014, pp. 102-113.
[43] D. H Tran, N. H.-Long, Z. Wei, N. W. Keong, "Towards security in sharing data on cloud-based social networks," in 8th International Conference on Information, Communications and Signal Processing (ICICS), 2011, pp. 1-5.
[44] T.Radhika, S.Vasumathi Kannagi "secure sharing and access control of personal health record in cloud computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Special Issue 3, July 2014 .
[45] T. Murata, "Petri Nets: Properties, Analysis and Applications, "Proceedings of the IEEE, vol. 77, no. 4, pp. 541-580, Apr. 1989.
[46] M. Chase and S. S. M. Chow. Improving, privacy and security in multi authority Attribute -based encryption. In CCS 2009, pages 121–130. ACM, 2009.
[47] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.
[48] Li, M., Yu, S., Ren, K., and Lou, W., "Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings," Security and Privacy in Communication Networks, pp. 89-106, 2010.
[49] Cheng-Kun Wang (2015) Security and privacy of personal health record, electronic medical record and health information. Problems and Perspectives in Management, 13(4), 19-26