SECURE DATA SHARING TECHNIQUE FOR ELECTRONIC MEDICAL RECORD WITH MOBILE DEVICES

[1]L. Rachna, [2]Dr. CH. Srinivas, [3]Dr. R. Jegadeesan, [4]Amsha Sumeen, [5]Shaistha Shireen,

[6]N. Sandeep

[1,4,5,6]Final year Student Computer science and Engineering , [2,3]Associate Professor- CSE,

[1,2,3,4,5]Jyothishmathi Institute of Technology and Science, Karimnagar, India

ABSTRACT To get medical treatment if high quality and efficiently, patients share their Medical Health Record (MHR) digitally on public storage with mobile devices. Nonetheless data privacy protection, flexible data sharing, computation efficiency optimization are some pf the obstacles which remaining accomplishing fine - grained access control in Electronic Medical Record (EMR) system. Here, we have come up with an ingenious access control model & fine grained data sharing mechanism for EMR which concurrently achieves the above mentioned features & it is relevant for resource - constrained mobile devices complex computation is externalized to public cloud server. Having approximately no complex computation left for PKG, sender & receiver with optimized communication cost. Further an extensible library is developed that is appropriate with android devices on realistic environment, access control mechanism along with public cloud servers is deployed with constrained resources. The results indicate that mechanisms is compelent, dynamic and practically cost effective.

Index Terms—Data sharing mechanism, attribute based encryption, secure outsourced computation, cloud computing, Electronic Medical Record.

INTRODUCTION

For digital information processing, EMR enables doctors & patients to conveniently share medical records and personal health information it also assets patients to high quality medical treatment. EMR system can outsource medical records to public cloud where doctors & patients ca store manage and share medical records in order to diminish maintenance cost of specialized data centre and to attain data sharing.

Diversified server based access control mechanism like Role Based Access Control (RBAC) [1], Temporal - RBAC [2],[3] and GEO - RBAC [4], have been sharing. A reliable access control server is employed to act as a supervisor. As the record are stored on public cloud, the cloud and user are not in same trusted domain, so conventional access control mechanism may not be suitable for cloud assisted

EMR system. Medical records must b encrypted to protect privacy before outsourcing to the cloud. To reinforce imperative access control, key assignment scheme can be used which is a symmetric cryptography primitive. A class lower down in the hierarchy in (KAS) [5],[6],[7],[8],[9],[10] which is set in advance which is used for computation. It is not flexible enough & access policy should follow the fixed classes.

As associate degree innovative science answer, attribute based mostly encryption (ABE) [11] integrates versatile access management with encryption practicality. the flexibleness denotes that each single file may be encrypted with a versatile access policy. Fig. 1 presents the standard access management model of ABE. In specific, cipher text-policy ABE (CP-ABE) [12] that's conceptually nearer to RBAC has potential to be applied in ERM systems. so as to fulfil the immediacy and quality, doctors use mobile devices to form, browse and update medical records anyplace, at any time. A doctor is assigned with several attributes supported his/her role, like “Surgery”, “Director”, “Male” etc., and uses a mobile device to inscribe patients’ medical records related to access policy, e.g., “Pediatrics” ∧ (“Doctor” ∨ “Head-nurse”), before uploading to the EMR cloud. different doctors WHO have non-public keys containing attributes will decipher encrypted medical records if the attributes satisfy the access policy.4

Multi-authority ABE ,traceable[13] and revocable multi-authority ABE[14] ,multi-authority ABE with semi outsourced decryption [15] are the examples of a series of work existed

on ABE for EMR, through which several sensible features can be delivered.Although ABE is deployed in a large scale EMR system there are various serious challenges that still exists.

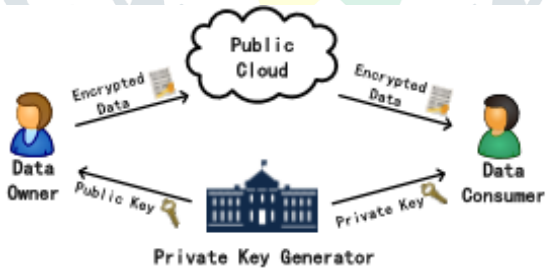

Fig. 1: Traditional Access Control Model of ABE

- **Computation Potency:** Heavy computation is a significant disadvantage that disrupt ABE from a wide range preparation complexness of access policy is grown for most paring & exponentiation transaction reserve-strained mobile device in EMR faces a large burden for PKG & users. Therefore the way for synchronously dwindle]the estimation cost for PKG & users is the first confrontation.

- **Authority/ Investiture:** To private doctors the compelling patient records need to be promptly accredited. Accomplishment of efficient authority delegation without divulging the data confidentiality in ABE is the second confrontation.

- **Economic Constructivity:** To shop for a high-end mobile devices for every staff is not commercial for an outsize health care enterprise with distinct thousands of staff the way to picture an economical ABE system that can be reasonable for resource-constrained mobile device is the third confrontation.

Our Contribution

Intending outsourced at resolution of the above challenges competent data sharing mechanism for EMR accomplishing data privacy, fine-grained access control, authority delegation. It enhances the computation potency and is appropriate for resource constrained mobile devices.

a) **New Access Management Model.** Powerful outsourced capability of public cloud is employed by ABE by proposing a new access control model. Our new model will considerably improve the computation potency for PKG and user by computing only one addition public cloud service supplier when correlated with conventional model.

b) **High Computation Potency.** The intense computation of all the ABE algorithms (i.e, key generation,encryption,&decryption) is deployed to public and cloud servers, exploiting zero exponentiation for PKG (key generation) and data owners (encryption) and one exponentiation for data consumers (decryption) based positioned on the new model.Moreover the new model will restrict public cloud servers from learning secret information.

c) **Economical Authority Delegation.** A fully outsourced cipher text - policy attribute based proxy re-encryption(FO-CP-AB-PRE) system is recommended which can re-encrypt an ABE cipher text into a current cipher text beneath anew access policy without revealing the plain text.To perform one authority delegation operation for the doctor it takes virtually no complex computation.Furthermore, security model is designed and security verification is given.

d) **Low Communication Price.** Addition communication cost in our system which is yet "imperceptible" for the PKG is delivered by the outsourced computation. Because computation could be done once the servers recurving public key and the results are downloaded by the PKG in the spare time (while being charged). Waiting for the cloud's response and draining

battery, operation could be later promptly completed. Thus our method is applied for resource-constrained mobile devices.

e) **Performance Analysis.** Theoretical comparison with numerous sensible ABE schemes is provided by us. Moreover on extensible library "Libabe" that is compatible with android device is developed. An epitome of our mechanism within Libabe on two cloud servers, a portable system and a low-end mobile is enforced. The consequences illustrate high potency and economy of our methodology.We consider that ABE is made a step closer to the actual deployment on EMR by the prototype with mobile devices.

Related Work

To achieve cryptographic access control, Akl and Taylor [5] initially considered the Key assignment scheme(KAS). Based on a binary tree a space-efficient KAS was designed by Alderman et al [6] and a key based cryptographic access control mechanism was intended in recent times.cryptographic hierarchical access control was proposed by Castiglione et al[7]. for dynamic structures [16]. It shows in what way we can enact outsourced publicly verifiable computation on KAS [8] from access control.shared key assignment schemes [9] on symmetric encryption and two hierarchical.[10] Castiglione suggested two hierarchical and shared key assignment schemes supported bilaterally symmetric coding and public key threshold broadcast coding on an individual basis.

The concept of attribute-based encryption was first proposed by Amit Sahai and Brent Waters [2] and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters[11].There are mainly two types of attribute-based encryption schemes: Key-policy attribute-based encryption (KP-ABE)[11] and cipher text-policy attribute-based encryption (CP-ABE).[12]. In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attributes. However, CP-ABE uses access trees to encrypt data and users' secret keys are generated over a set of attributes.

M. Blaze first bought up Proxy re-encryption (PRE) schemes cryptosystems. It allow third parties (proxies) to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. Unidirectional PRE scheme was proposed by Ateniese et al [23], and CCA-secure PRE scheme was proposed by Hanaoka et al [24]. There are various PRE schemes like anonymous proxy re-encryption [25], attribute based proxy re-encryption [26]. In recent times, to reducing the online computation cost on the mobile devices side[20] Shao et al. proposed online/offline attribute based proxy re-encryption (OOABPRE).

SYSTEM MODEL AND SECURITY MODEL

Here,we present the system and security model.

SYSTEM MODEL

To achieve secure outsourced computation, like outsourced key generation/encryption/re-encryption key generation/decryption, we have a tendency to adopt 2 totally different public cloud servers when compared with the standard model of ABE in fig1. For outsourced secret writing,one public cloud server (e.g.public cloud 2) as all the key can be exposed to the distinctive cloud server,it is not enough for different operations.Concretely, once the server that helps information owner generate the intermediate cipher text (IT), obtains the ultimate original cipher text (CT), it can simply recover the key in CT . Consequently, two non-collusive cloud servers area unit adopted in our system, where a data owner initial obtains IT one, IT two from 2 cloud servers respectively, then generates the ultimate IT by combining IT one and IT 2 . Since 2 public cloud servers cannot conspire with each other, the ultimate combined IT ought to be information- theoretically hidden from 2 cloud servers.

The access management model consists of 5 entities: personal key generator (PKG), public cloud one, public cloud two, data owners and information customers. Table one lists the acronyms used in this paper. Fig.2 shows the organization of those entities.

- PKG is accountable to line up the system parameters and distributes all the cryptologic keys PK, MSK, SKs, TKs and RtK s to different entities.
- Knowledge owner defines access policies and encrypts knowledge under these policies before uploading them to public cloud 2. He/she also can delegate (re-encrypt) the encrypted knowledge to unauthorized knowledge shoppers. All the significant computation within the on top of operations is completed with the assistance of public cloud one and public cloud two.

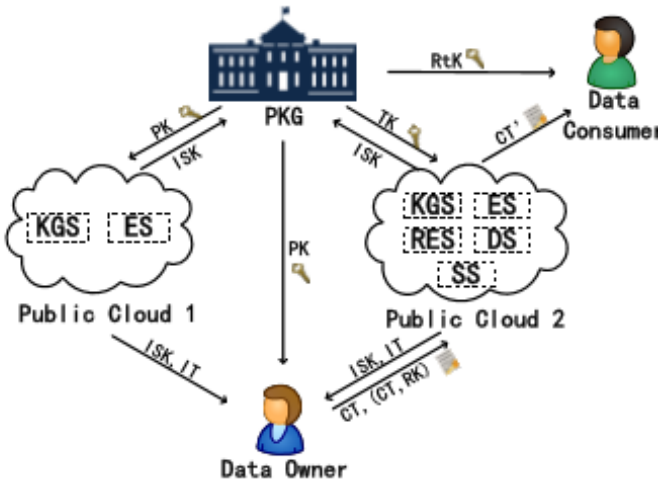

Fig. 2: Access Control Model of FO-CP-AB-PRE

- Public cloud 2 equipped with PK and TK is deployed to provide outsourced computation service and cloud data storage service, like KGS, ES, RES, DS and SS. The description of the services is as follows.

  – KGS generates ISK s to assist PKG/data house owners with key generation/authority delegation.

  – metallic element generates IT s to assist knowledge house owners with encryption and authority delegation.

  – RES generates RCT s to assist knowledge house owners with authority delegation.

  – DS generates CT to assist knowledge customers with decryption.

  – SS stores all the encrypted cloud knowledge.

- Public cloud 1 equipped with PK is another totally different cloud service supplier. it's deployed to produce solely outsourced computation service, like KGS and E.

- Data shopper equipped with a retrieval key Rtk will download any encrypted information of his/her interest from public cloud a pair of and check out to rewrite the ciphertext.

SECURITY MODEL

Adversarial Model. In our system, public cloud one and public cloud two area unit "honest-but-curious"[18][17]. More precisely, they can follow the protocol however strive to realize out as a lot of personal info as doable. Most of the information consumers area unit honest, whereas few of them area unit corrupt and will outflow their secret keys within the collusion. On the contrary, PKG and information

owner area unit assumed to be absolutely trustworthy . Besides, public cloud one and public cloud two cannot conspire with one another. The non-collusive assumption is reasonable, as a result of the consumer will demand that 2 cloud severs cannot reveal users' info by contract.

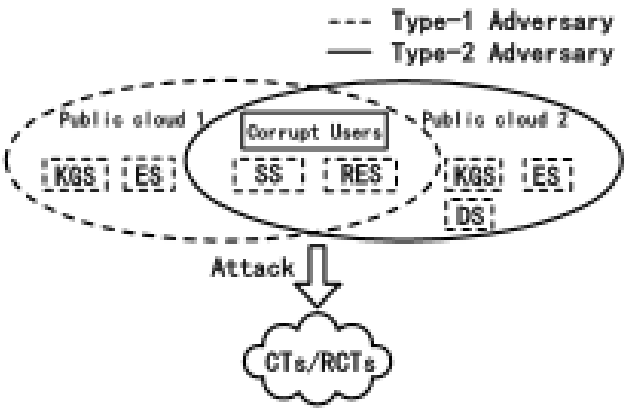

Fig. 4: Two Types of Adversaries

The channels that transmit ISK;IT;TK;RtK should be secured and this could be simply enforced by SSL. Because the secret keys TK;RtK are forever distributed in camera, and the intermediate computation results ISK;IT cannot be accessed by outsiders. If the channels that transmit ISK;IT are public, meaning ISK;IT can be accessed by any entities, the outsourced key generation/encryption/re-encryption generation area unit not secure. Since we tend to adopt 2 non-collusive public cloud servers, we tend to ought to take into account the circumstances that every cloud server colludes with alternative entities. As delineated in Fig. 4, we tend to contemplate the following 2 styles of adversaries.

- Type-1 resister refers to corrupt knowledge shoppers colluding with public cloud one, who will acquire Sks of corrupt data consumers,all the 1SK1s/IT1sat public cloud 1, some RKs of RES and every one the CTs/RCTs of SS4. It intends to decipher unauthorized Cts/RCTs.

- Type-2 someone refers to corrupt knowledge consumers colluding with public cloud a pair of, UN agency will acquire SKs of corrupt knowledge customers,ISK2s/IT2s/RKs5/TKs/CTs/RCTs at public cloud a pair of. It intends to de-crypt unauthorized Cts/RCTs. Next, according to the capabilities of 2 completely different adversaries and also the attack targets (CT or RCT), we tend to outline the following selective accountant security game.

Next, according to the capabilities of 2 completely different adversaries and also the attack targets (CT or RCT), we tend to outline the following selective accountant security game.

PERFORMANCE EVALUATIONS

Theoretical Analysis.

Communication Price Analysis. Even so, outsourced computation definitely brings further communication price, e.g.,a user must watch for the cloud server's response and downloads the computation results on-line. within the on top of process, the user's mobile device can expertise the facility consumption and therefore the network latency.The power consumption continually will increase with the transmission size. The network latency may be influenced by several factors,but solely the transmission size depends on the theme[17],[18], [19], [22], [21], [23].

Experimental Analysis

An extensible library Libabe , that overtures imperative APIs for implementing ABE schemes is developed by C language to appraise the practical performance. To be compatible with android OS, Libabe is solely captivated with Pairing-Based Cryptography (PBC) library [36] and OpenSS-L [37].The assessment program with Java Native Interface(JNI) is developed depending upon the Libabe.We select the 224-bit MNT ellipsoidal curve from PBC library.

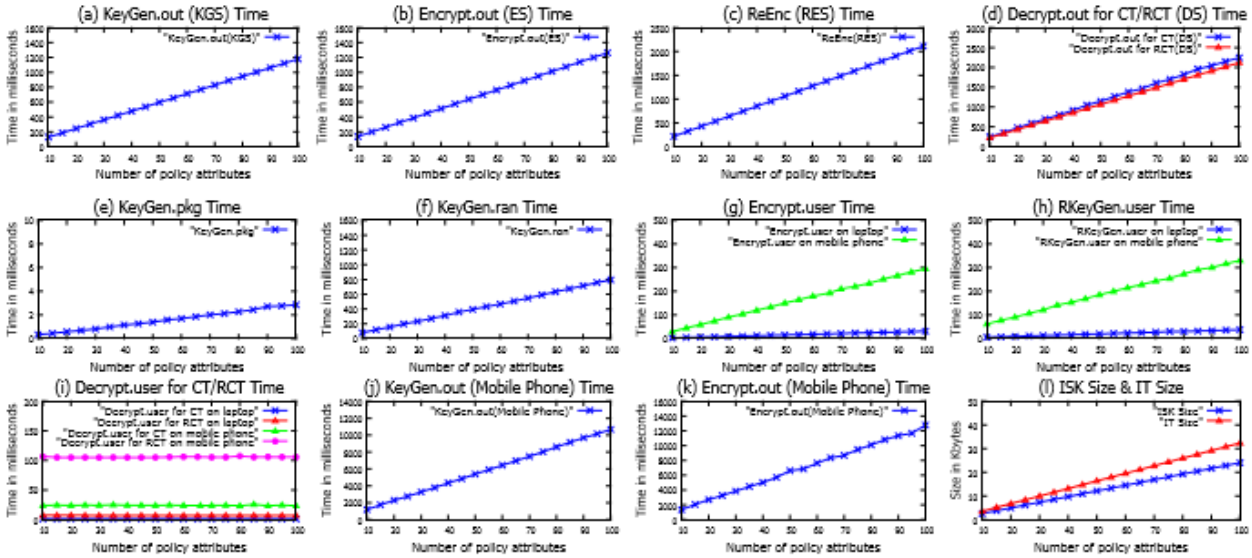

Fig. 6: Experimental Results

To execute interrelated algorithms, two public cloud service providers(Alibaba cloud and Tencent cloud) are employed. To act as the PKG,we use a system and the same system and a low-end mobile phone perform the part of users.The device configuration we elect a low-end mobile phone whose worth is about ₹5,000($66) to assert the economy of our theme.

CONCLUSION AND FUTURE WORK

Here, we tend to propose a fine-grained data sharing mechanism for the EMR system, that not solely achieves data privacy, non-interactive fine-grained access management, and authority delegation at the same time, however is also appropriate for low-end mobile devices. Moreover, we tend to develop an extensible library known as Libabe that is appropriate with android devices, and our mechanism is implemented on realistic environment. The experimental results signify that our mechanisms competent, sensible and cost-effective.The economical revocation mechanism will be focussed within the future.

REFERENCES

[1] D. F. Ferraiolo, R. S. Sandhu, S. I. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 224–274, 2001.

[2] 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

[3] J. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A generalized temporal role-based access control model," IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 1, pp. 4–23, 2005.

[4] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "Geo-rbac: a spatially aware rbac," in 10th ACM Symposium on Access Control Models and Technologies,SACMAT2005,Stockholm,Sweden,June1-3, 2005, pp. 29–37.

[5] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," ACM Transactions on Computer Systems, vol. 1, no. 3, pp. 239–248, 1983.

[6] J.Alderman,N.Farley,and J.Crampton,"Tree-basedcryptographic access control," in Computer Security - ESORICS 2017 - 22nd European Symposiumon Researchin Computer Security,Oslo,Norway, September 11-15, 2017, pp. 47–64.

[7] 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)

[8] A. Castiglione, A. D. Santis, and B. Masucci, "Key indistinguishability versus strong key indistinguishability for hierarchical key assignment schemes," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 4, pp. 451–460, 2016.

[9] J. Alderman, J. Crampton, and N. Farley, "A framework for the cryptographic enforcement of information flow policies," in 22nd ACM on Symposium on Access Control Models and Technologies, SACMAT 2017, Indianapolis, IN, USA, June 21-23, 2017, pp. 143– 154.

[10]A.Castiglione,A.D.Santis,B.Masucci,F.Palmieri,A.Castiglione, J. Li, and X.Huang,"Hierarchical and shared access control," IEEE Transactions Information Forensics and Security, vol. 11, no. 4, pp. 850–865, 2016.

[11] 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

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA. IEEE, 2007, pp. 321–334.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-baseden cryption," IEEE Transactionson Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[14] J. Zhou, Z. Cao, X. Dong, and X. Lin, "Tr-mabe: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," in IEEE Conference on Computer Communications, INFOCOM 2015, Kowloon, Hong Kong, April 26 - May 1, 2015, pp. 2398–2406.

[15] 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.

[16] J. Alderman, C. Janson, C. Cid, and J. Crampton, "Access control in publicly verifiable outsourced computation," in 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '15, Singapore, April 14-17, 2015, pp. 657–662.

[17] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with check ability,"IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2014.

[18] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe cipher texts," in 20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011.

[19] R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system based on fully outsourced attribute-based encryption," Journal of Systems and Software, vol. 125, pp. 344–353, 2017.

[20] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009, Sydney, Australia, March 10-12, 2009, pp. 276–286.

[21] R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system based on fully outsourced attribute-based encryption," Journal of Systems and Software, vol. 125, pp. 344–353, 2017.

[22] J. Shao, R. Lu, and X. Lin, "Fine-grained data sharing in cloud computing for mobile devices," in 2015 IEEE Conference on Computer Communications, INFOCOM 2015, Kowloon, Hong Kong, April 26 - May 1, 2015, pp. 2677–2685.

[23] S. Luo, J. Hu, and Z. Chen, "Cipher text policy attribute-based proxy re-encryption," in Information and Communications Security 12th International Conference, ICICS 2010, Barcelona, Spain, December 15-17, 2010, pp. 401–415.

[24] 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

[25] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006, pp. 89–98.

[26] A.Castiglione,A.D.Santis,B.Masucci,F.Palmieri,A.Castiglione, and X. Huang, "Cryptographic hierarchical access control for dynamic structures," IEEE Transactions Information Forensics and Security, vol. 11, no. 10, pp. 2349–2364, 2016.

[27] 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

[28] 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

[29] 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

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

[31] 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

[32] 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

[33] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal rolebased access control model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191–233, 2001

[34] 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)

[35] I. E. Ghoubach, F. Mrabti, and R. B. Abbou, "Efficient secure and privacy preserving data access control scheme for multiauthority personal health record systems in cloud computing," in 2016 International Conference on Wireless Networks and Mobile Communications, WINCOM 2016, Fez, Morocco, October 26-29, 2016, pp. 174–179.

[36] 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

[37] 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.