ENERGY EFFICIENT DATA SHARING METHOD USING LIGHTWEIGHT ALGORITHM FOR MOBILE CLOUD ENVIRONMENT

[1]Gurram Sai Kumar, [2]Dr. R. Jegadeesan, [3]Alla Pravalika, [4]Gurram Varsha, [5]Narla RamyaSai,

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

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

Abstract :As the popularity of cloud computing increases on mobile devices, this can store or retrieve personal data from anywhere at any time. At the same time, the problem of data security also increases day by day and substantial studies have also been conducted to improve cloud security, but most of them are not applicable to the mobile cloud, since mobile devices they have a very limited capacity and capacityresources. In this we provide a solution through a light data exchange scheme (LDSS) for mobile cloud computing. Adopts CP-ABE, which changes the structure of access control and even access control technology used in normal cloud environments. This scheme moves a large part of the transformation of the CP-ABE intensive computing access control tree from mobile devices to external proxy servers. Attribute description fields are used to implement deferred revocation in order to reduce the cost of user revocation, which is a thorny problem in systems based on CP-ABE programs. When users share data in mobile cloud environments, this LDSS can effectively reduce the overhead on the mobile device side.

Index Terms **– Lightweight algorithm, cloud computing, computational overhead, Lazy-revocation, encryption.**

1. INTRODUCTION

With the improvement of distributed computing and the ubiquity of enthusiastic cell phones, people are slowly becoming familiar with another moment of information exchange where information is kept in the cloud and cell phones are used to store / recover the information. from the cloud. Commonly, cell phones only have restricted storage space and computing capacity. Actually, the cloud has a huge amount of assets. In such a situation, to achieve an attractive execution, it is basic to use the assets provided by the specialized organization in the cloud (cloud service provider) to store and share the information.
Currently, different portable cloud applications have been used in general. In these applications, individuals (information owners) can transfer their photographs, recordings, reports and different documents to the cloud and offer this information to other individuals (information clients) who wish to share. Cloud service providers also provide information about the utility of the board to the owners of the information. Because individual information documents are sensitive, the owners of the information can choose whether they want to open their information records or they must be informed to the clients of explicit information. Obviously, the security of individual sensitive information information is a major concern for some information owners.

The above problem can be solved using LDSS in a mobile computing environment.

The main tasks in LDSS are the following:
1. To increase the efficiency of access control over the ABE cipher text, we structured an algorithm called LDSS-CP-ABE.
2. Normally, the encryption and decryption process is performed on the devices themselves, which leads to a large computational overload, but in our design the calculation is done on the proxy server itself and also maintains the privacy of the data, in order to access to the structure. it was also added. The decryption key is also loaded into proxy servers in a secure manner.
3. To reduce the revocation problem caused by revocation overload, we introduce a new encryption and an attribute description field.

Finally, a data exchange framework is implemented in LDSS. The experimental results show that this scheme (LDSS) greatly reduces the computation overhead on the client side, which represents a minimal additional cost on the server side. Access control schemes based on ABE on encrypted text.

2. PRELIMINARY AND ASSUMPTIONS

In this segment, we first quickly present the start procedures firmly identified with LDSS and then present the framework model and some safety assumptions in LDSS.

2.1 Preliminary Techniques

2.1.1 Bilinear Pairing:

Define a function l in the following way: $l: g_0 * g_{0=} g_1$

In this function, both $g_0$and g_1 are multiplicative cyclic groups of the prime order p.

Suppose that g is a generator of g_0, F_f is a finite field. So l is a bilinear pair if l has the following properties:

(1) Bilinear: $\forall x, y \in g_0, \forall c, d \in F_f,\ \ l(x^c, y^d) = l\,(x, y)^{cd}$

(2) No degeneration: l ((G, G)) is a memberg_1 of is G is a member of g_0.

(3) Computability: $\forall x, y \in g_0, e(u, v)$ can be calculated.

In our implementation, we usually take xx as a group consisting of points on an elliptic curve over a finite field. Other descriptions of how these parameters are defined and generated can be found in [11].

2.1.2 Attribute-based encryption:

Sahai and Waters [12] propose attribute-based encryption (ABE). It is obtained from identity-based encryption (IBE) and is especially reasonable for one-to-many information exchange situations in an open and running cloud condition. Character-based encryption is divided into two classes: one is encryption based on encrypted text policy attributes (CP-ABE), in which the input control arrangement is inserted into the encrypted text; the other is encryption based on key policy attributes (KP-ABE), in which the input control approach is implemented in the key qualities of the client. In genuine applications, CP-ABE is increasingly reasonable, since it resembles job-based access control. In CP-ABE, the owner of the information structures the entry control agreement and assigns information clients.

2.1.3 Secret exchange scheme

Shamir's secret exchange is used to protect secret information. It can be explained as follows. Suppose that p is a prime number, the secret information to share is $e \in E = F_f$. Divide e into n pieces through the following steps:

(1) Randomly select a polynomial of order (s-1)

$h(i) = a_{s-1}n^{s-1} + \cdots + a_1 n + a_0 \in F_f[n]$and let $a_0 = e$

(2) Select n nonzero elements and differentI_n from F_f, calculate $t_i = j(n_i)$, 1≤i≤m.

(3) Distribute$t_i(1 \le i \le m)$as shared resources and publish the corresponding$n_1, n_2 , \ldots\ldots, n_m$.

The process to reconstruct j (n) of t random parts through the Lagrange polynomial interpolation is the following:

$$j(n) = \sum_{z=1}^{s} t_{i_z} \prod_{\substack{x=1 \\ x \neq z}}^{s} \frac{n - n_{i_x}}{n_{i_z} - n_{i_x}}$$

All these operations are performed inF_f, that is, they are all operations in p mode.

After obtaining (n), we can obtain the secrete$e = a_0 = j(0)$:

$$e = j(0) = \sum_{z=1}^{s} t_{i_z} \prod_{\substack{x=1 \\ x \neq z}}^{s} \frac{-n_{i_x}}{n_{i_z} - n_{i_x}}$$

As $n_1, n_2, \ldots\ldots\ldots, n_m$is public, we can get the coefficient of lagrange in advance:

$$\lambda_s = \prod_{\substack{x=1 \\ x \neq z}}^{s} \frac{-n_{i_x}}{n_{i_z} - n_{i_x}}$$

Thus, the formula to recover the secret k can be put in a simpler way:

$$e = \sum_{z=1}^{s} \lambda_s t_{i_z}$$

2.2Security assumptions:

2.2.1 Semi-reliable servers:

We assume that the CSP is honest but curious. It performs all the operations required by the users, but it can see the data of the users stored in the cloud. therefore, LDSS is designed based on these assumptions. In LDSS we have a proxy encryption and decryption server for data encryption and decryption respectively. Through these proxy servers we can reduce the user's general expenses. These proxy servers are also machines in the cloud. Therefore, we consider that they are honest but curious as well as the CSP.

2.2.2 Trust authority:

In order to make the LDSS more viable in practice, we present a reliable authority that is used to generate public and private keys and distribute attribute keys to users. Therefore, by using this TA, we can share and access the data without having knowledge of the encryption and decryption operations. There is a reliable channel between TA and each user to transfer keys securely between users.

2.2.3 Lazy Recording:

When the user revokes the access control privileges of the data, the data must be re-encrypted. But frequent re-encryption can generate a computational overload. This access data can be stored in these data users. Therefore, we adopt Lazy re - encryption method. In this method, whenever the owner of the data revokes the access privileges, the file containing these access privileges is marked and when the DO updates the data, it checks whether the file is marked or not. If the file is Marked then the data is encrypted.

3. METHODOLOGY

In this segment, we represent the structure of the LDSS structure. To begin with, we give the LDSS diagram, and then we present the calculation of LDSS-CP-ABE and the framework activities, which are the basis of the LDSS calculation. Finally, we represent LDSS in subtleties.

3.1 Summary:

We propose LDSS, a lightweight data exchange plan structure in the portable cloud (see Fig. 1). It has the six segments that accompany it.

(1) Data owner (DO): the DO transfers information to the versatile cloud and offers it with companions. DO decides on entry control strategies.

(2) Data user (DU): DU retrieves versatile cloud information.

(3) Trust Authority (TA): TA is responsible for creating and transmitting feature codes.

(4) Encryption service provider (ESP): ESP assigns information encryption tasks to DO.

(5) Deciphering Service Provider (DSP): DSP provides information decoding activities to DU.

(6) Cloud service provider (CSP): CSP stores information for DO. Loyally execute the tasks requested by the DO, while you can review the information that the DO has saved in the cloud. As it appeared in Fig. 1, a DO sends information to the cloud. As the cloud is not solid, the information must be encoded before being transferred. The DO characterizes the access control provision as an access control tree in the information documents to assign the traits that a DU must acquire in case it needs to access a specific information record. In LDSS, information records are completely mixed with the symmetric encryption component, and the symmetric key for information encryption is additionally encoded using feature-based encryption (ABE).

3.2 LDSS-CP-ABE Algorithm

To more easily delineate the calculation of LDSS-CP-ABE, we first characterize the terms that accompany it.

Definition 1: Attribute

An owner of characteristic information can characterize a lot of qualities for the information documents that characterizes the entry benefit for a given record of information. The credits are assigned to information clients by the owners of the information. An information client can have different characteristics related to various information documents. A. The information received is supervised by the access control strategy determined by the owners of the information. Let a = $\{a_1, a_2, \ldots\ldots, a_m\}$provide the characteristics for an information owner. Each reference or additional client has many properties Au, which is a non-empty subset of An, in particular $a_{du} \subseteq \{a_1, a_2, \ldots\ldots, a_m\}$.

Definition 2: Access control tree

The access control tree is the particular articulation of access control approaches, in which the leaf centers are features, also, the leaf centers are not social managers, for example, and, or, n of m limit Each concentrator in an input control tree talks about a mystery, and the mystery of a better concentrator can be divided into numerous privileged ideas through a plan to share the mystery and transmit it to bring down the dimension concentrators. Consequently, in the event that we know the privileged knowledge of the leaf centers, we can reason out the mystery of the leafless centers by recursion from the base to the top.

Definition 3: Version attribute.

The version attribute is entered in the LDSS-CP-ABE algorithm to guarantee security. It is an addition to the original access control tree, which forms a new root node of y. We have the following definitions.

C: The new access tree with version attributes.

T: The secret related to the root of C.

Ca, Sa, Ta: Ca is the initial access control tree and the left subtree of C. Sa is the root of Ca. Ta is the secret related to Sa.

Cv, Sv, Tv: Cv is the right subtree of C and contains only one node, which represents the Sv version attribute. Tv is the secret related to Sv.

Both Ta and Tv are derived from T based on the secret exchange scheme.

The calculation of LDSS-CP-ABE is structured using the above definitions. It incorporates four subcapacities: Configuration (A, V): generate the key MK, the open key PK depends on the set of properties An of the owner of the data and the variant property V. KeyGen (Au, MK): Generates SKu quality keys for an information client U that depends on its Au feature set and the MK ace key. Encryption (K, PK, T): Generates the encrypted text CT based on the symmetric key K, the open key PK and the access control tree T. Decryption (CT, T, SKu): decrypt the CT encrypted text using the input control tree T and the feature keys SKu. We clarify these capabilities explicitly below. To begin with, the work () configuration is invoked by a third party (TA) to create the ace key and the open key. The ace key is used to create characteristic keys and the open key is used to encode information records.

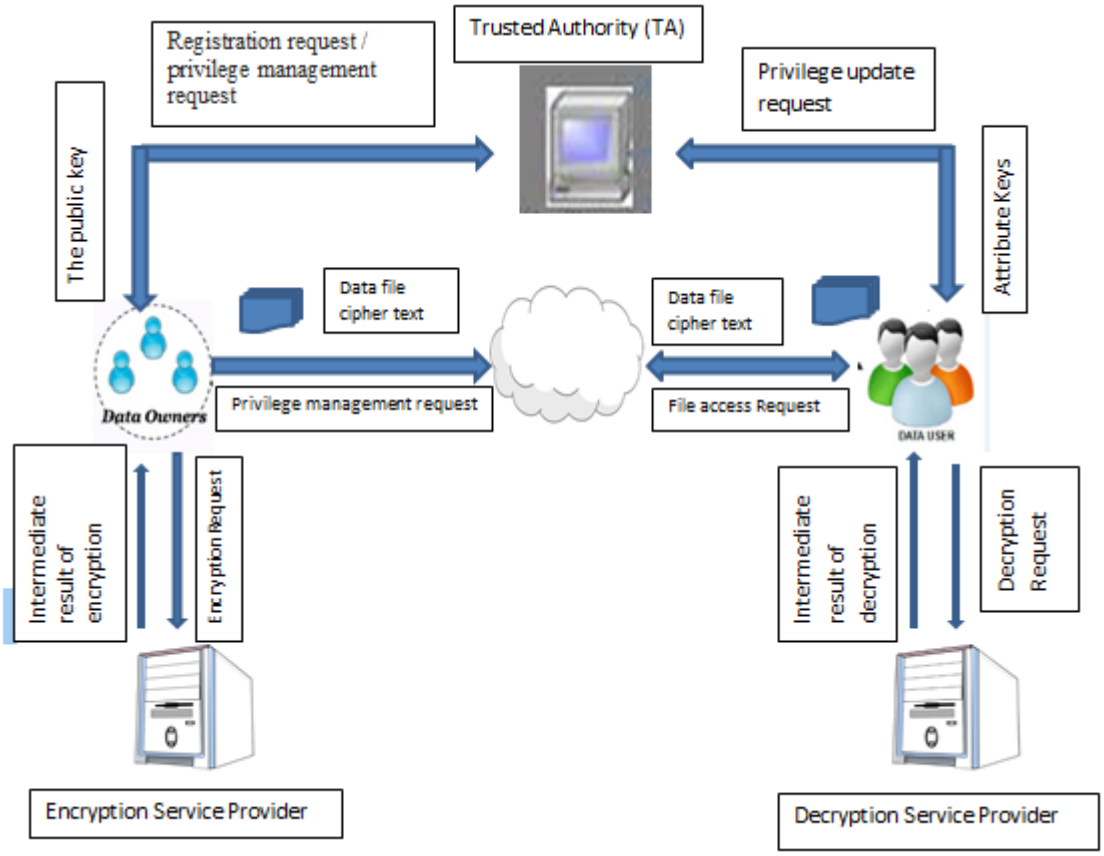

Fig.1: A lightweight data sharing scheme framework

.

3.3 Operations of the LDSS system:

The LDSS chart is intended for information that participates in the versatile cloud. The complete LDSS procedure incorporates the creation of frames, the exchange of documents, the approval of the client and the registration of tasks. In addition, you must help the activities of denial of ownership and updating of documents.

3.3.1 Initialization of the system:

In the introduction to the frame, Function 1 is executed. The particular procedure is described as persecutions.
(1) When the owner of the information (DO) is registered in TA, TA executes the calculation configuration () to create an open key PK and an ace key MK. PK is sent to DO while MK remains on TA itself.
(2) DO characterizes its own set of characteristics and assigns credits to its contacts. All this data will be sent to TA and the cloud.
(3) TA and the cloud obtain the data and store it.

3.3.2 File exchange:

The document exchange procedure is used to encode information records. The particular procedure is described as persecutions.
(1) DO chooses an M record to be transferred and mixes it using a symmetric cryptographic instrument (for example, AES, 3DES calculation) with a symmetric K-key, which produces the ciphertext C.
(2) DO assigns to arrive at the control arrangement for M and codes K with the help of ESP , producing the encrypted text of K (CT).
(3) DO transfers C, CT and the access control agreement to the cloud.

3.3.3 User authorization:

The client approval procedure is executed to produce property keys for information clients. The particular procedure is described as blinds.

(1) DU starts session in the framework and sends a request for approval to TA. The approval request incorporates the property keys (SK) that DU has from now on.

(2) TA acknowledges the approval request and verifies if DU has previously signed. In case the client has not previously logged in, go to step (3), generally go to step (4).

(3) TA calls Function 2 to produce property keys (SK) for DU.

(4) TA thinks about the property representation field in the feature key with the characteristic representation field saved in the database. In case they are not coordinates, go to step (5), generally go to step (6).

(5) For each conflicting piece in the representation field, in the remote possibility that it is 1 on the information client side and 0 on the TA side, it shows that the DU property has been denied, at that time TA does not do anything in this bit. In the remote possibility that the situation is changed, it shows that the DU has been distributed with another quality, at that moment, TA creates the corresponding feature key for the DU.

(6) TA verifies the variant of each DU feature key. In case it is not the equivalent with the current versions; At that point, TA updates the comparison quality key for DU.

3.3.4 Access files

At the time when DU requests to obtain a specific information record, Function 4 is used to decode information.

The particular procedure is described as follows:

(1) DU sends a request for information to the cloud.

(2) Cloud obtains the claim and verifies if the DU meets the entry prerequisite. In case DU can not satisfy the need, it rejects the demand, but sends the encrypted text to DU.

(3) DU obtains the encrypted text, which incorporates the encrypted text of the information documents and the encrypted text of the symmetric key. At that point, DU executes function 4 to decode the encrypted text of the symmetric key with the help of DSP.
(4) DU uses the symmetric key to decipher the encrypted text of the information records.

3.3.5 Privilege revoked

DO can deny qualities of a DU.The procedure is as follows.

(1) DO educates TA and the cloud that a property has been repudiated from a particular DU.

(2) TA and the cloud update the DU data in the database.

(3) DO marks the comparison bit of the property description field of the information documents. This procedure executes the unconventional handling of the repudiation of traits and the updating activities of the property keys. At the moment when the DO must renounce a DU quality, TA simply updates the database and does not update the DU ownership keys at the same time.

3.3.6 Documentation updates

Due to the new languid cipher, when the DO relinquishes a feature of a DU, the denied quality is not updated. At the time the information record is updated, in the event that it has a feature that has been rejected, this feature must be updated. The particular procedure is as follows.

(1) DO check if there are any pieces in the field of representation of the information documents that have been set in '#'.

(2) EDUCATE the TA which characteristics should be updated. Each of the properties that must be updated in the structure of a set is called New.

(3) TA chooses another incentive in G0 for each assignment in Anew to supplant the first, and updates the DO description field in the DO-PK / MK table, changing the comparison bit of the credit representation to the new estimate.

(4) TA sends another PK to DO, and DO uses the new PK to encode information records.

(5) You MUST set bit '#' of the description field of the related information record in 1.

4.RELATED WORK

In this segment, we focus around the data produced by encrypted text to control the plans that are firmly identified with our exploration. Access control is an essential component of the information security guarantee to guarantee that the information is obtained by authentic clients. Important research has been done on the subjects that information can control in the cloud, generally focusing on the power of access over the encrypted text. Regularly, the cloud is seen as legitimate and inquisitive. The sensitive information must be encoded before sending it to the cloud. Customer approval is achieved through key dispersion. The scan can be commonly divided into four territories: basic encryption text is controlled, level access control, control depends on fully homomorphic encryption [1] [2] and control depends on feature-based encryption (ABE). Straightforward the encrypted text that is obtained to the control alludes to that after the encryption of the information document, the encryption keys are spread securely to obtain the approval of the clients [3]. To reduce the overload of the huge dispersion of the client key, Skillen and Mannan [4] structured a framework called Mobiflage that enables the PDE (possibly deniable encryption) in cell phones by storing volumes encoded by irregular storage information. external of a device. Be that as it may, the framework needs to obtain an extensive measure of the key data. [5] acquires the entry control strategy used in the appropriate traditional storage [4] [6], isolating clients in several meetings as indicated by access rights and assigning various keys to meetings

The progressive access control has a great execution to reduce the overload of the dispersion of keys in the encrypted text that can be controlled [7]. Therefore, there is important research on ciphertext to control [8] [9] [10] that depends on several level access control strategies. In various level access control strategies, private key keys and an open token table can be obtained. Be that as it may, the task in the token table is confused and creates a surprising expense. In addition, the chip table is saved in the cloud. Your protection and security can not be guaranteed. In this document, we propose a light information exchange plan

(LDSS) for versatile cloud applications. It encompasses CP-ABE, an innovation used in access control in the typical cloud condition, but changes the structure of the access control tree to be reasonable for the portable cloud. LDSS is demonstrably safe, and is shown to be more competent and adaptable than the best ABE plans of its kind.

5. CONCLUSION

Lately, numerous exams on access control in the cloud depend on the calculation of feature-based encryption (ABE). Be that as it may, the usual ABE is not reasonable for the versatile cloud, since it is computationally concentrated and cell phones only have restricted assets. In this document, we propose LDSS to address this problem. It presents a new LDSS-CP-ABE calculation to relocate a significant computation overload from cell phones to intermediary servers, so it can address the problem of the secure exchange of information in the versatile cloud. The results of the test show that LDSS can guarantee the protection of versatile cloud information and decrease overhead costs on the client side of the portable cloud. Later in the job, we will structure new ways to deal with the reliability of the warranty information. To take advantage of the versatile cloud capacity, we will also think about how to perform the recovery of encrypted text on the existing information exchange plans.

6. REFERENCES

[1] Gentry C, H alevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: continuing of IEEE conference on Foundations of technology. California, USA: IEEE press, pp. 97-106, Oct. 2011.

[3] Qihua Wang, Hongxia Jin. "Data discharge mitigation for discertionary access management together clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the twentieth Annual Network and Distributed System Security conference (NDSS), Feb. 2013.

[5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. In: Proceedings of the 2009 ACM workshop on Cloud registering security. Chicago, USA: ACM pp. 55-66, 2009.

[6] Maheshwari U, Vingralek R, Shapiro W. How to build a sure information system on untrusted storage. in: Proceedings of the fourth conference on conference on software package style & Implementation-Volume four. USENIX Association, pp. 10-12, 2000.in: Proceedings of the 2009 ACM workshop on Cloud registering security.

[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.

[9] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of conference on Security and Privacy (SP), IEEE press, 2007. 350- 364

[10] Cong Wang, KuiRen, Shucheng Yu, and KarthikMahendraRajeUrs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud information. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[11] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. in: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, pp. 213−229, 2001

[12] Sahai A, Waters B. Fuzzy identity based encryption. in: Proceedings of the Advances in Cryptology. Aarhus, Denmark: Springer-Verlag, pp.457-473, 2005.

[13]Shamir A. How to share a secret. Communications of the ACM,1979, 22 (11): 612-613

[14] Zhou Z, Huang D. Efficient and secure information storage operations for mobile cloud computing. in: Proceedings of eighth International Conference on Network and repair Management (CNSM 2012), Las Vegas, USA: IEEE, pp. 37-45, 2012.

[15] Bethencourt J, Sahai A, Waters B. Cipher text-policy attribute based encryption. in: Proceedings of the 2007 IEEE conference on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

[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.