ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 8 , August 2016

An Efficient COT based key management scheme for Secure Data storage

Mr.D.Stalin David, Dr.A.Jayachandran

PhD Research Scholar, Department of CSE, PSN College of Engineering & Technology, Anna University,Tamilnadu, India
Research Supervisor, Department of CSE, PSN College of Engineering & Technology, Anna University,Tamilnadu, India

ABSTRACT: Attribute-based encryption (ABE) with outsourced decryption not only enables fine-grained sharing of encrypted data, but also overcomes the efficiency drawback (in terms of cipher text size and decryption cost) of the standard ABE scheme. In Particular, an ABE scheme with outsourced decryption allows a third party to transform an ABE cipher text into an El Gammal-type cipher text using public transformation key provided by a user so that the latter can be decrypted much more efficiently than the former by the user. However, a shortcoming of the original outsourced ABE scheme is that the correctness of the cloud server's transformation cannot be verified by the user. An end user could be cheated by accepting a wrong or maliciously transformed output. In this paper, we first formalize a security model of COT with verifiable outsourced decryption by introducing a verifiable Key in the output of the encryption algorithm. Then, an approach to convert an ABE scheme with outsourced decryption into an ABE scheme with verifiable outsources decryption. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user's and the cloud server's computation costs and the cipher text size. We show a concrete construction based on Green et al's cipher text text-policy COT scheme with outsourced decryption and provide a detailed performance evaluation to demonstrate the advantages of our approach.

KEYWORDS: Communities of Trust (COT), Energy Efficient Cluster Head (EECH), General self organized tree based energy Balanced routing algorithm (GSTEB), Data Security, Encryption, Access Control.

I.INTRODUCTION

Access controls to data operate on the assumption data servers can be trusted to keep data confidential and enforces access control policies correctly. However, this assumption is no longer true today since services are increasingly storing data across many servers that are shared with other data owners. An example of this is cloud data storage where cloud service providers are not in the same trusted domains as end users and hardware platforms are not under the direct control of data owners. To mitigate user's privacy concerns about their data, a common solution is to store data in encrypted forms so that it will remain private, even if data servers or storage devices are not trusted or compromised. The encrypted data however must be enabling to sharing and access control. Cloud shares infrastructure between several organizations and it managed internally or by a third party. the user stores the data in encrypted format.ABE is an encryption scheme used by the user to store data in the cloud.ABE is a public key cryptography based one to many encryption techniques which allows users to encrypt and decrypt data based on user attributes. Access control of encrypted data stored in the cloud is, by using access policies and ascribed attributes associated with private keys and cipher texts. An ABE system with outsourced decryption eliminates the decryption overhead. Here user provides data to the cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied with the user's attributes or access policy in to a simple cipher text.

II. RELATED WORK

Wireless Sensor Network (WSN) consists of collection of sensor nodes. The sensor node is a tiny device that includes four basic components such as sensing subsystem, processing subsystem and power supply subsystem. The major issue in WSN is energy consumption and lifetime of the network.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 8 , August 2016

C. Santhi , D. Sharmila, (2013) proposed Data aggregation and it is a way to consume energy in WSN and interfere acquiring the sensed data from the sensors to the gateway node. Data aggregation plays a vital role in Wireless Sensor Networks since the data aggregation involves in reducing the amount of power consumed during data transmission between the sensor nodes. Data aggregation is mainly performed in clustering.CH will perform Data aggregation and send to base station.

Changlin Yang and Kwan-Wu Chin, (2013) proposed joint design of asynchronous sleep-wake schedules and opportunistic routing called ASSORT, to maximize the network lifetime. The advantage of opportunistic routing i.e., path diversity and the improvement of transmission reliability, are exploited to develop a lifetime-extended opportunistic routing for wireless sensor networks. Joint design of asynchronous sleep-wake schedules and opportunistic routing, called ASSORT, to maximize lifetime.

Guojun Wang,, Md Zakirul Alam Bhuiyan, Jiannong Cao and Jie Wu, Fellow, (2013) proposed EECC scheme is used to improve the transmission performance along the energy consumption and it will reduce the packet loss during transmission. When a node fails to receive a packet then the nearby nodes start the cooperation then the transmission begins without failure cooperation is carried out by selecting a co-operator and the co-operator is elected through nearby nodes have successfully overhead the election. After selecting a co-operator from qualified neighbors of the relay nodes on the routing path will be allowed to participate in the transmission. EECC will reduce the total number of transmission time with the help of cooperator present in the transmission. Drawback of EECC is does not work in node mobility.

Nicholas Roseveare, and Balasubramaniam Natarajan, (2014) proposed “alternative perspective of energy harvesting” In cluster formation Phase- initially depends upon size, range individual small clusters are formed. Data forwarding phase-At the same time, Inter clustering and Intra clustering transmission can be done. Cluster Maintenance Phase- All the control and the CH in each round. The power of all sensor nodes is same in beginning and CH variation depends on its own residual energy.
Clustering significantly reduces the energy consumption of each sensor nodes and increase the communication load on CH. Unequal clustering is an effective way to reduce the load in CH. Energy Balancing Unequal Clustering Approach for Gradient based Routing algorithm is used.

Pengfei Zhang ,Gaoxi Xiao, (2013) proposed Clustering algorithm for maximizing the lifetime of wireless sensor networks with energy-harvesting sensors. Clustering algorithm is of 2 types heterogeneous clustering and homogeneous clustering. Clustering is the most important algorithm for energy consumption, so clustering is chosen as best technique for energy consumption and to increase the lifetime of node.

Xenofon Fafoutisa, Thomas Sørensenb, Jan Madsena, (2014) proposed an Structure-Free and Energy-Balanced Data Aggregation Protocol (SFEB). We assume that SFEB operate simulation hop network where sensor nodes are synchronized and aware of the locations of the sink and their own. Location information can be obtained by applying a localization protocol that is either GPS-based. Each node had similar transmission and carrier sensing range. Packets with the event identification (EID) can be aggregated. Our SFEB consists of two phases. In phase one, some nodes as aggregators together as many packets as possible. Then, these aggregators end the collected packets back to the sink.

Zaixin Lu, Wei Wayne Liand Miao Pan, (2013) proposed The Group Key Agreement (GKA) is used for secure group communication and used to utilize the remaining energy of sensor nodes to the CH of individual clusters. Filtration of sensed data by removing the redundancy in the sensed data pattern reduces the energy consumption during transmission. The filtered data at the sensor node undergoes entropy based processing prior to the transmission to the cluster head. Entropy based processing selects some random samples from sensed data to check whether redundancy exist or not. Energy can be consumed by removing redundant data and lifetime also increased up to 47%. Data aggregation is an effective approach to save energy because the number of transmission can be reduced after aggregation. Structure-free and Energy-balanced data aggregation protocol.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 8 , August 2016

III. PROPOSED SYSTEM

WSN senses the information and then transmits the data to the base station. The transmission of data from the source node to the BS uses various methods and all routing methods are concentrated for the energy consumption reduction. As the LEACH protocol is mainly used for the energy Consumption but it does not provide an efficient cluster head selection and energy consumption in CH. Our proposed system, we have modified the existing LEACH protocol by EECH and Sleep Awake Scheduling algorithm to efficiently consume energy and to increase the lifetime of the sensor nodes.

ARCHITECTURE DESIGN OF ENERGY EFFICIENT SCHEDULING:
Fig. 1. Describes Energy efficient scheduling of the system to determine or to find energy consumption. The following modules described about the Energy Efficient scheduling. The modules are focussed on

- Cloud Environment
- Role Manager
- Admin
- User

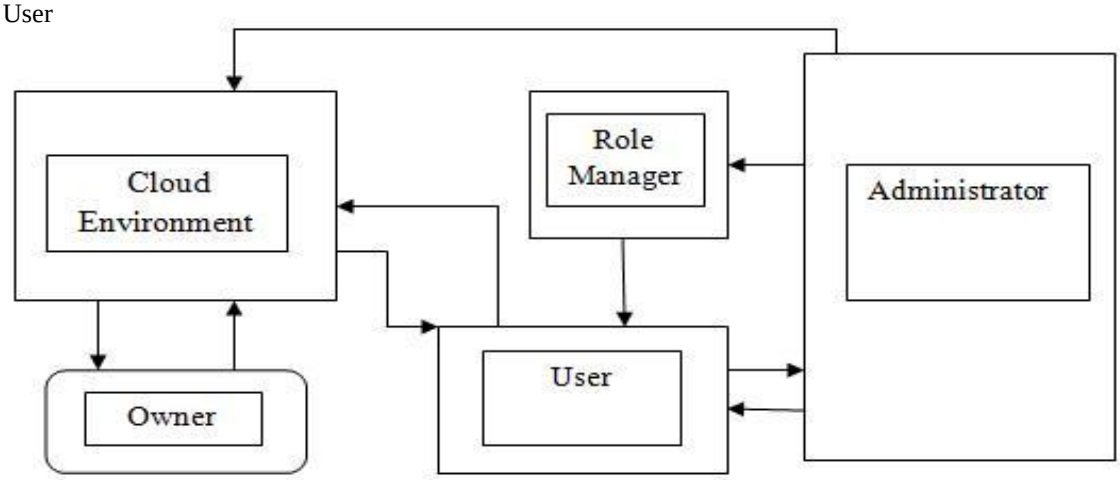

Fig. 1. System model of role based access control

A.CLUSTER HEAD ELECTION:

The Cluster head election module is designed to form clusters and to elect cluster head. Cluster head are chosen based on the energy of the sensor node. CH is used for communicating with the BS. CH will collect the information from its group members and the send information to BS.EECH algorithm is used for selecting cluster head. The cluster head will introduce to its members, then neighbourhood table is formed which contains **node** position and its neighbourhood member.

B.DATA TRANSMISSION:

In this phase first the data is sensed. Data are collected in cluster head. The sensed data are sent to the Base station.

C.SELECTION OF ACTIVE NODES:

For each node energy is assigned. The node which has high energy is set as active node. Through active nodes the packet will be routed to the Base Station. The energy is assigned for each node and the slots are allocated for each node.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 8 , August 2016

D.PACKET FORWARDING:

The GSTEB algorithm is used for routing the packets to the base station. Select the next hop node which has high energy. Then routing table has to be updated. The remaining nodes which act as active node form a child node for that root node. In this protocol tree is formed.BS assigns a root node and broadcasts this selection to all sensor nodes. The algorithm includes four steps namely, Initial phase, Tree constructing phase, Self organized Data collecting and transmitting phase, Information Exchanging phase.

IV.EXPERIMENTAL RESULTS

The experiment was checked with various users and all registration; role based key generation, encryption and decryption. In the first page, the user select the registration button, store the full details of user, mainly the category and security questions which are used for two level of authentication of our proposed work.

The roles are assigned from the registration and registered user got the identity token unique id. The every user got the different unique id from random id generator and it is shown in the Fig 3 and Fig 4.

The user set the password for the first level authentication and it is shown in the Fig 4. The keys generated for the registered user with their file is shown in the Fig 3.

The system will ask randomly any security questions to the user registered. This is second level of authentication. If both the level of authentication is successfully completed, then the user is authenticated to use the system. Now user, role based key is generation is generated by the public key crypto system, here which role is entered first his appropriate key is generated

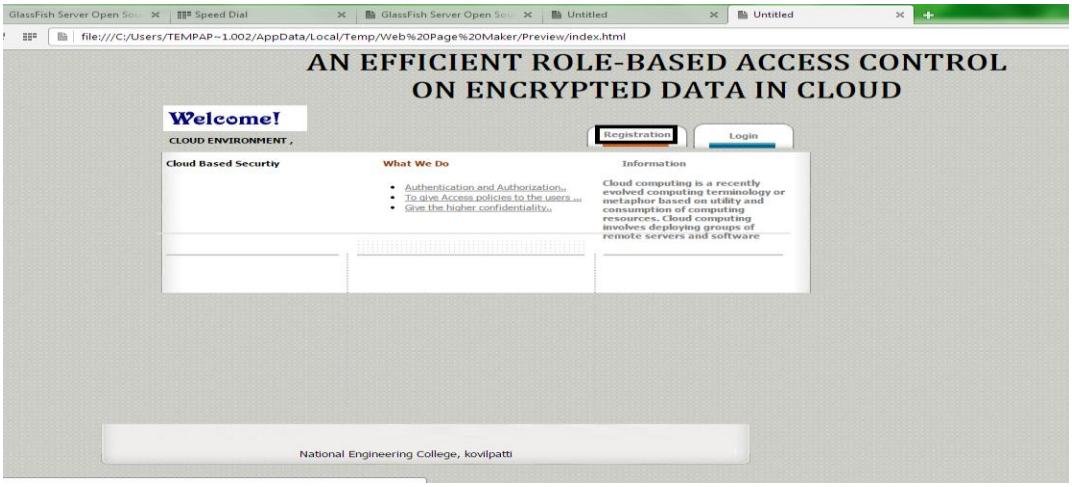

Figure 2.User Interface of our proposed work

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 8 , August 2016

Figure 3.Checking Password Mismatch

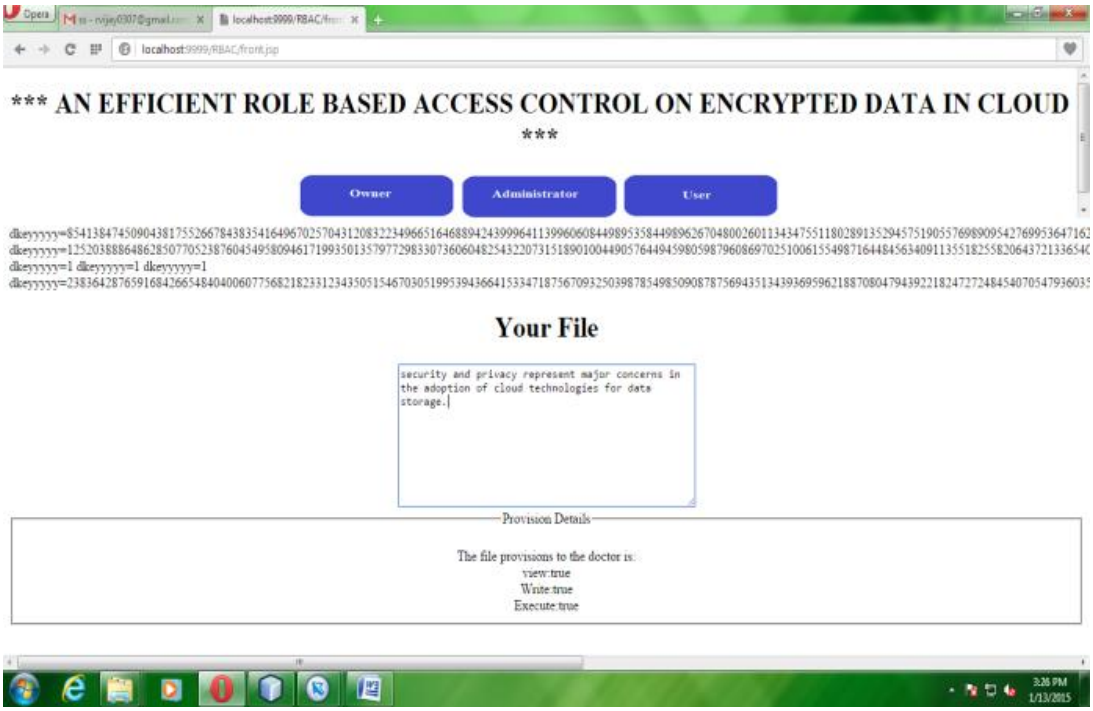

Figure 4.Decrypted File with its access policies

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 8 , August 2016

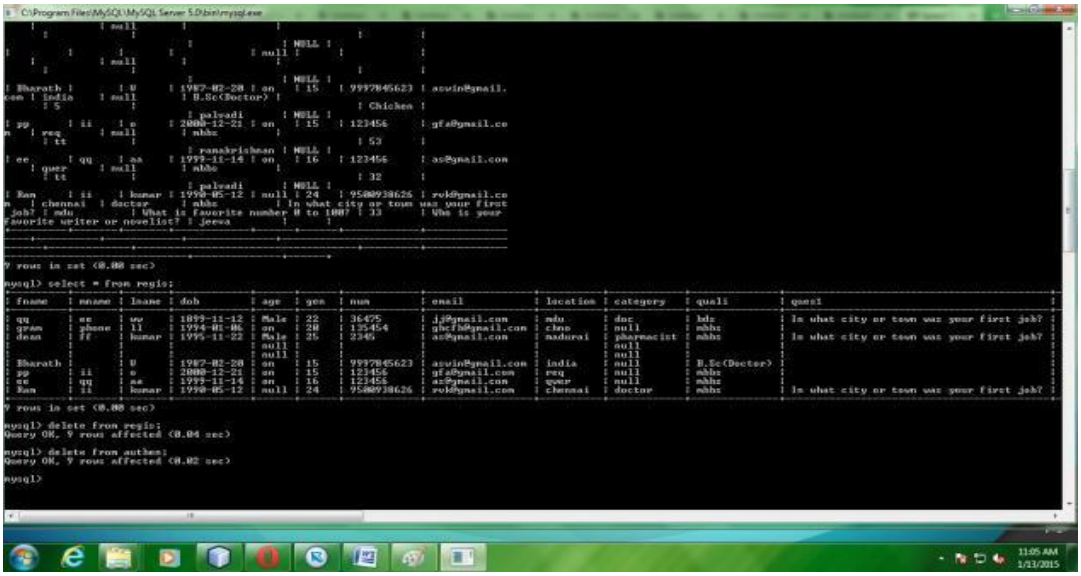

Fig. 5. Key Storage in MySql

First, the user registers their details and generate the user identity token unique id is generated and stored in the cloud database. Unique id is used for further login purpose. The second level authentication is based on security questions.

After the registration and login is successful the user is valid user. Role based key was generating for further encryption and decryption. Administrator fig: have the all sensitive information of user. This is shown, only for explain purpose because this information is maintained by the cloud environment. The Fig 4 shows the doctor role details. The access rights are shown in the Fig 4. It shows the doctor role have the access rights Read, Write, Execute. In this work we use a mysql database as the back end to store all details of the user involved in the system. The database is shown in Fig 4.

V. CONCLUSION

In this paper, we proposed a simple and generic method to convert any COT scheme with non-verifiable outsourced decryption to an ABE scheme with verifiable outsourced decryption to a COT scheme with verifiable outsourced decryption in the standard model. To concretely assess the performance of the new method, we presented an instantiation of our generic method based on green et al.'s outsourced CP-ABE scheme without verifiability. Experiment results showed that our method is nearly optimal in the sense that it introduces minimal overhead in exchange for verifiability. In future we can consider these solution on the multimedia files and the system is lacking reliability factor, improvement in these pin holes can be done.

REFERENCES

[1] C. Santhi , D. Sharmila, 'A self-organized location aware energy efficient protocol for wireless sensor networks', Elsevier-Wireless Networks,(2013), vol 17, pp. 1007-1014.

[2] Cheng Hsu, Ming-Shing Kuo, Shi-Chen Wang, and Cheng-Fu Chou, 'Joint Design of Asynchronous Sleep-Wake Scheduling and Opportunistic Routing in Wireless Sensor Networks', Elsevier-Porcedia Technology (2013), vol 22, pp.234-237.

[3] Guojun Wang,, Md Zakirul Alam Bhuiyan, Jiannong Cao and Jie Wu, Fellow, 'Detecting Movements of a Target Using Face Tracking in Wireless Sensor Networks', IEEE-Wireless Communication, (2013),vol 8, 186-194.

[4] Nicholas Roseveare, and Balasubramaniam Natarajan,' An Alternative Perspective on Utility Maximization in Energy-Harvesting Wireless Sensor Networks', IEEE transaction on vehicular technology, (2014).

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 8 , August 2016

[5] Pengfei Zhang ,Gaoxi Xiao , Hwee-Pink Tan, 'Clustering algorithms for maximizing the lifetime of wireless sensor networks with energy-harvesting sensors', Elsevier-Wireless Networks, (2013), vol 67, pp.410-416.
[6] Xenofon Fafoutisa, Thomas Sørensenb, Jan Madsena,'Energy Harvesting - Wireless Sensor Networks for Indoors Applications using IEEE 802.11', Elsevier-Procedia computer science, (2014), vol 32, pp.991-996.
[7] Zaixin Lu, Wei Wayne Liand Miao Pan, "Maximum lifetime scheduling for target coverage and data collection in wireless sensor networks", IEEE- Wireless Communication, (2013), vol 33, pp.639-647.
[8] Pratyay Kuilab, Prasanta K. Janaa, 'Energy Efficient Load-Balanced Clustering Algorithm for Wireless Sensor Networks', Elsevier –Procedia Technology, (2012), vol 6, pp. 771-777.
[9] T. Shah, N. Javaid, T. N. Qureshi, 'Energy Efficient Sleep Awake Aware (EESAA) Intelligent Sensor Network Routing Protocol', Elsevier-COMSATS Institute of Information Technology, (2014), vol 21, pp.456-459.
[10] S. Mini, Siba K. Udgata, and Samrat L. Sabat ,'Sensor Deployment and Scheduling for Target Coverage Problem in Wireless Sensor Networks', Elsevier-Porcedia Computer Science (2013), vol 29, pp. 245-247.
[11] Xingfa Shen a, Cheng Bo a, Jianhui Zhang a, Shaojie Tang b, Xufei Maob, Guojun Dai a, 'EFCon: Energy flow control for sustainable wireless sensor networks', Elsevier-Institute of Computer Application Technology, (2013), vol 11, pp.1421-1431.
[12] Ting Zhu, Ziguo Zhong, Tian Hi, Zhi-Li Zhang, 'Energy-synchronized computing for sustainable sensor networks', Elsevier- Adhoc Networks, (2013), vol 11,pp. 1392-1404