International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(1), pp.005-008
DOI: http://dx.doi.org/10.21172/1.101.02
e-ISSN:2278-621X

OVERVIEW ABOUT SECURE SHARING ENCRYPTION TECHNIQUES IN CLOUD COMPUTING

KavithapriyaCJ[1], AncyS[2]

Abstract- Patient details in cloud is shared among users in cloud .To make it secure we encrypt the data using FH-CP-ABE (File Hierarchy- Cipher text Policy-Attribute Based Encryption).Previously there is no hierarchy followed. Also data has been encrypted within some time intervals. So that it can be secured. For viewing data user and doctor should request hospital admin. Hospital should register in cloud to store user data, hospital is provided with license number and password .Hospital should register doctor and patient details, user and doctor is provided with id and password. User can select what are the details that should be hidden or to be encrypted. Sharing data by securing personal information.
Keywords- ABE,Hospital, User Data,Secure Sharing.

1. INTRODUCTION

Cloud computing ,a network based information processing system which has wide characteristics of distributed computing , interactivity, real time dynamic and so on in the application . Discussing about the benefits it provides a timely adjustments on network performance , rapid recovery from fault etc. Cloud computing describes a new class of network based computing that takes place over the internet. It is an upgrade from utility computing. It uses a collection of integrated , network hardware, software and internet infrastructure. It uses internet as a intermediate bridge for communication and transport which provides hardware, software and networking for clients. These platforms hide a complexity and details of underlying infrastructure from users and applications by providing very simple Application Programming Interface (API)[5].Cloud is used as storage location and database can be accessed and computed from anywhere. It provides scalable computing format to extend the distributed storage location. It is a model for enabling a convenient, on demand network access for shared pool of configurable computing resources. Example: networks, servers, storage, application and services. It is a way to increase a capacity or add capabilities on the fly without introducing the new infrastructure. Cloud computing includes any of the subscription based or service in form of pay-per-use service that in real time over the internet by extending its existing capabilities. Previously it required a tremendous hardware/software investments and professional skill to acquire those jobs. It reduces a technical complexities and complicated deployment worries.

2. COMPLEXITIES

Most user now a day's least bother about the complexities involved in computers and technologies so there is no use in visualizing the things to end user. What they just need is the computer or a technology should work properly for what the purpose it designed for. So hiding the complexity from end user is needed. The way we can hide is "Cloud". Most people wants to deal with application, they don't need software. Most of us prefer automation now a days , in future we expect that extension of cloud may take place in its own without any human intervention. Currently all the software which are hidden from us are taken care by some professionals or a system that is provided for that purpose. Today's high speed networks, sophisticated PC graphics processors and fast inexpensive servers has tilted engineers to house more datacenters. Reliability, scalability , security and host to other problems will prevent most business from moving their mission critical applications to hosted services or cloud based services[6]. The risk of failure is too great.

3. ONLINE/OFFLINE ATTRIBUTE BASED ENCRYPTION

ABE is a significant type of public key encryption which allows user to encrypt and decrypt messages based on user attributes. For example any message can be encrypted by anyone to any user by satisfying some Boolean formula (i.e combinations of AND & OR Operations).Its disadvantage is encryption and its computational costs scale with complexity of access policies or no of attributes user uses. This above method creates encryption and the user key generation a possible restricted access for applications. In this paper a new technique for ABE[3] as in Fig.1[1] that split these algorithms into two phases has been developed:

[1] Assistant Professor, Department of Information Technology, Jeppiaar Institute of Technology, Sriperumbudur, India
[2] Assistant Professor, Department of Information Technology, Jeppiaar Institute of Technology, Sriperumbudur, India

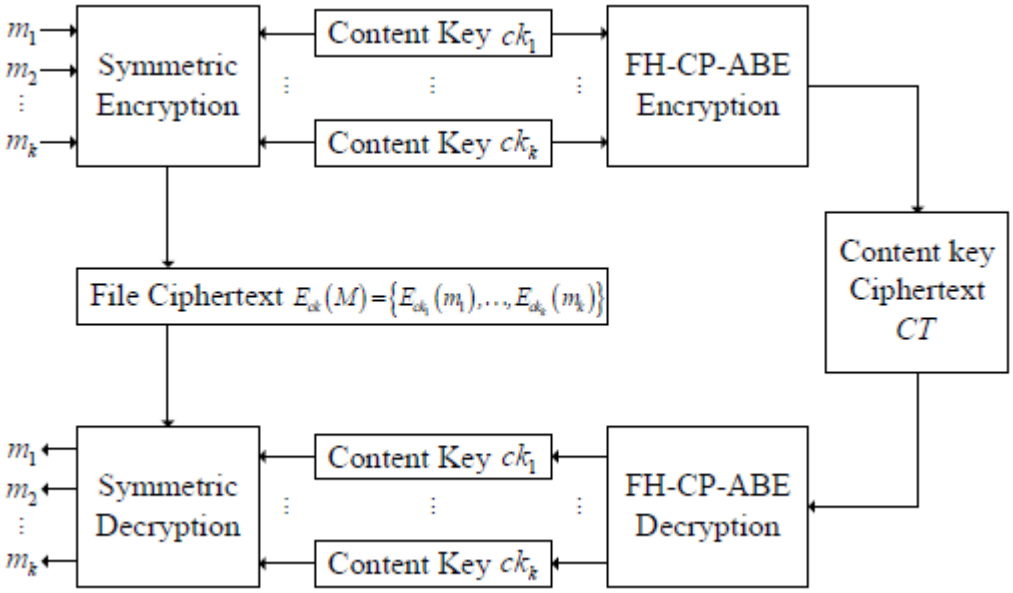

Fig. 1. Depiction of ABE-Framework

A preparation phase that does the majority of work to encrypt a message or to create a secret key before it knows the message or attribute list/access control policy that will be used. A second phase can rapidly assemble an ABE cipher text or key when the specific become known. This process is some times called online/offline encryption when the message is unknown during the preparation phase. Toting up of unknown attribute lists and it's access makes ABE[1] significantly more challenging. One of the application for the new technique is mobile phone : the preparation can be performed when plugged into a power source, then it can later battery. The graph depicted as in Fig2. Gives the details about the cost of storage of the data comparison of the two ciphertext files.

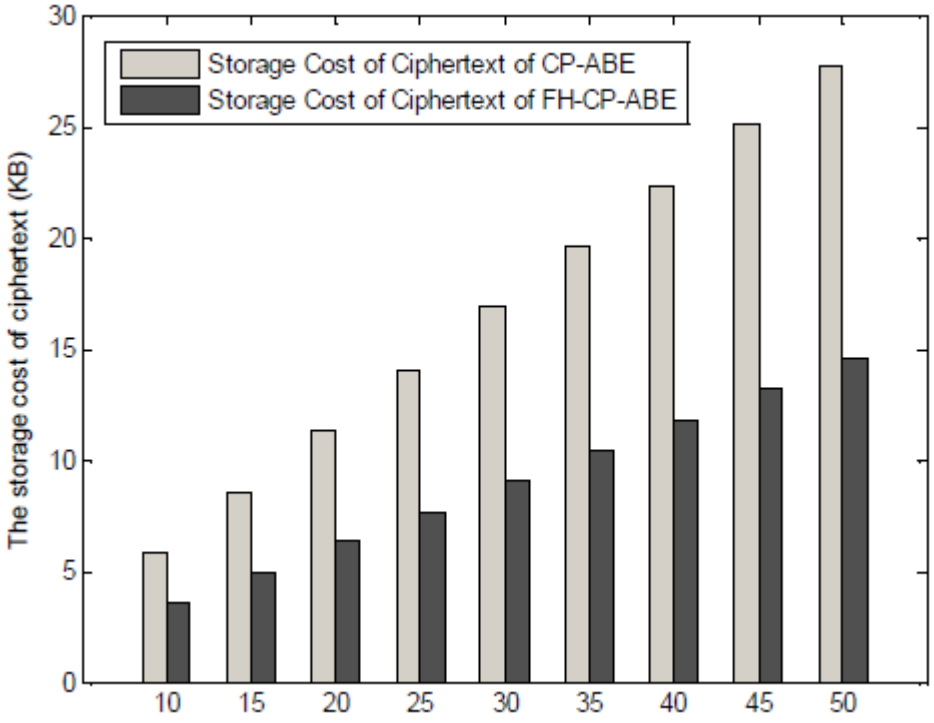

Fig2. Comparison of two cipher text files based on storage cost.

4. CP-ABE WITH CONSTANT-SIZE KEYS FOR LIGHTWEIGHT DEVICES

Light weight devices such as RFID(radio frequency identification) tags has limited storage capacity. In many applications this is not enough specially in security applications. Ciphertext policy attribute based encryption (CP-ABE) technique is a more capable cryptographic tool in which a encryption will be deciding the access structure that will be used to protect the sensitive data. But this CP-ABE has the issue of holding long decryption keys. In this the size is linear and dependent on of attributes . This drawback prevents the use of light weight devices in practice of storing decryption keys. In this paper they provide a affirmative answer to long standing issue which will make the CP-ABE very practical. They propose the novel CP-ABE scheme with constant size decryption keys independent of no of attributes, according to this project the size can be as small as 672 bits. It has express access structure which is suitable for CP-ABE key storage for light weight devices. ABE has the potential to deploy in cloud computing environment to provide scalable and fine-grained datasharing[2] as in Fig.3. However, a challenging issue to overcome within ABE deployment is the user revocation exists, particularly when there is large no of users . In this paper they introduced extended proxy assisted approach . This weakens the trust required of cloud server. Based on all-or-nothing principle , this approach is designed to discourage a cloud server from colluding with third party to hinder the user revocation functionality .This demonstrate the utility of approach by presenting the construction of proposed approach, designed to provide efficient cloud sharing and user revocation. A prototype was then implemented to demonstrate the particularity of our proposed construction.

Fig. 3. Use of Decryption Keys in Secure Decryption accumulate in Constrained Devices

The fine grained two factor(2FA)[1] which access control system for web based cloud computing services.But it is not as like the attribute based encryption which has both user secret key and a lightweight device.It enables the cloud server to restrict the access the users with the same attributes.The cloud server only knows the user fulfills the predicate but has no idea of the user.Here we using the simulation for demonstration.Here we are using the Cloud computing technology which is a host computer system which enables the enterprises to buy or distribute software and other digital resources over the internet as on demand service.The user secret key could be easily stolen or used by an unauthorized party even though the the computer is locked by passwords, to overcome this we are using the two factor authentication (2FA).It is a very common among web based e-banking services.In addition to a username/password user is also required to have a device which displays the one-time password.The OTP is sent to the mobile phone through the SMS during the login process.By,this service the user will get the confidence that our details are secured and couldn't not be shared to the intruders.By our contribution we propose the 2FA control protocol and lightweight security device which can compute some lightweight algorithms e.g., hashing and the device is tamper resistant(it is assumed that no one can break into it to get the secret information which stored inside. The process may be like this,1) the user secret key is required. In addition, the secret device should be also connected to the computer(e.g., through USB) for authenticate the user for accessing the cloud.

5. IDENTITY-BASED ENCRYPTION WITH POST-CHALLENGE AUXILIARY INPUTS FOR SECURE CLOUD APPLICATIONS AND SENSOR

Identity based encryption is useful for providing end-end across control access control and data protection in many scenarios such as cloud applications and wireless sensor networks. There are some threats for the data owner, who encrypts raw data and the data user or the control centre, who decrypts the cipher text and recovers the raw data. We are discussing the open problem of proposing a leakage-resilience encryption model that can capture leakage from both the secret key owner (the data user or control centre) and the encryptor (the data owner or sensor),in the auxiliary input model. The existing models only allow the leakage information after seeing the challenge cipher text of the security games. This problem can be solved by defining the post-challenge auxiliary input model in which the family of leakage functions must be defined before the adversary is given the public key. We propose the transformation from the auxiliary input model to our new post-challenge auxiliary input model for both public key encryption(PKE) and IBE. The customer requirements and constraints must be fulfilled which is specified Service Level Agreement. Confidentiality, integrity and access control are important issues for security and privacy of such open infrastructure. Access control is classified as one to the top 10 challenges in big data security by the Cloud Security Alliance(CSA)[4].The sensitive data must be protected by using cryptographically secure algorithm and suitable access control. The use of IBE as one of the possible cryptographic approach to enforce the big data applications. Sensor networks is

similar after getting raw data it encrypts the information.IBE which eliminates costly certificate verification process and thus it is preferred in sensor networks.

6. FINE-GRAINED ACCESS CONTROL OF ENCRYPTION DATA

In cipher text policy attribute based encryption (CP-ABE) scheme[3], a private key holder is related with a set of attributes while the data is encrypted under an access structure defined by the data provider. In this paper a scheme is proposed under a different hierarchy of attributes with the name of cipher-text policy hierarchical attribute based encryption. Encryption is the cryptographic primitive which provides confidentiality to the digital communication. The public key encryption provides a powerful mechanism for protecting the confidentiality of stored and transmitted information. User needs information which data provider has to be shared to the user, the provider must know exactly the one he/she wants to share with.ABE has prominent advantages over the traditional public key encryption which can be exemplified, by the fact that the one to one encryption.

7. FUTURE SCOPE

According to desired outcome, the approach proposed has high applicability in service oriented environments like as cloud. In this paper, we proposed a ciphertext policy- Attribute Based Encryption (CP-ABE), which efficiently shares the files in hierarchy in cloud computing. The files which are hierarchical are encrypted with an access structure and ciphertext components which is related to the attributes. In this we implemented the time based control in which we can secure the private information of the user and doctor can view the user report only at the particular time. Direct user is the user they meet the requirements directly from the doctor. Indirect user is the one who meets the requirements through an intermediate. Unauthorized user is the one who has no rights to access the user information and reports.

8. REFERENCES

[1] Shulan Wang, Junwei Zhou, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing," Ieee Transactions On Cloud Computing, Vol. 11, No. 6, June 2016.

[2] Fuchun Guo, Willy Susilo, Duncan Wong, Vijay Varadharajan "CP-ABE with constant-size keys for lightweight Devices", University of Wollongong Research Online.

[3] Ximeng Liu, Jianfeng Ma, Jinbo Xiong, and Guangjun Liu,"Ciphertext-Policy Hierarchical Attribute-based Encryption for Fine-Grained Access Control of Encryption Data", International Journal of Network Security, Vol.16, No.6, PP.437-443, Nov. 2014

[4] Saraswati Gore1 , Ashokkumar Kalal2," A Survey on Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 10, October 2016.

[5] Archana Srivastava," A Detailed Literature Review on Cloud Computing", Asian Journal of Technology & Management Research [ISSN: 2249 –0892]Vol. 04 – Issue: 02 Jul - Dec 2014.

[6]]Rajani Sharma, Rajender Kumar Trivedi, "Literature review: Cloud Computing –Security Issues, Solution and Technologies", International Journal of Engineering Research, ISSN:2319-6890)(online),2347-5013(print), Volume No.3, Issue No.4, pp : 221-225, April 2014.