An Enhanced Attribute Based Encryption Technique that Reduce Computation Complexity of Fine Grained File Access Control in Cloud

Dinesh Raja
Project Manager, Shiro Software Solutions, Nagercoil.

Dr.K.Selva kumar
Assistant Professor, Department of Mathematics, University College of Engineering, Nagercoil.

Manibharathi R
Senior Developer, Shiro Software Solutions, Nagercoil.

Abstract –Advance development of cloud computing, outsourcing data to cloud server attracts millions of attentions due to any where access though with low price. To ensure the safety and security of data and flexibly fine-grained file access management, attribute based encryption (ABE) was projected and employed in cloud storage system. However, user revocation is that the prime issue in ABE techniques. Our proposed work, we provide an Enhanced Attribute Based Encryption Technique with efficient user revocation reduce computation for cloud storage system.

Index Terms – cloud computing, attribute-based encryption, access control, computation complexity.

1. INTRODUCTION

Cloud computing is the process of sharing system resource and application services over internet based on demand which reduce the total cost of organization. Cloud computing defined by Amazon web services as follow as, "Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing"[1].

Cloud are divided into four type based on cloud location public cloud, private cloud, hybrid cloud and community cloud. Cloud Computing provides the following types of services such as Infrastructure-as-a-Service, Platform-as-a-Service,Software-as-a-Service,Storage-as-a-Service, Database-as-a-Service, Information-as-a-Service, Process--as-a-Service, Application-as-a-Service, Integration-as-a-Service, Security-as-a-Service, Management-as-a-Service, Testing-as-a-service [2].

There are two imperative difficulties in secure cloud outsourcing services. To start with, the put away data must be secured against unapproved access. Second, both the data and the access to data should be shielded from cloud service providers. In these situations, depending on secret key and different access control instruments are lacking.

According to wikipedia, The cloud data security threat differ with traditional security threat. It is explained detail manner here. A number of security threats are associated with cloud data services: not only traditional security threats, such as network eavesdropping, illegal invasion, and denial of service attacks, but also specific cloud computing threats, such as side channel attacks, virtualization vulnerabilities, and abuse of cloud services. The following security requirements limit the threats.

Data confidentiality is the property that data contents are not made available or disclosed to illegal users. Outsourced data is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive data while others, including CSPs, should not gain any information of the data. Meanwhile, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and data sharing, without the leakage of the data contents to CSPs or other adversaries.

Access controllability means that a data owner can perform the selective restriction of access to her or his data outsourced to cloud. Legal users can be authorized by the owner to access the data, while others cannot access it without permissions. Further, it is desirable to enforce fine-grained access control to the outsourced data, i.e., different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in un-trusted cloud environments.

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that her or his data in a cloud can be stored correctly and trustworthily. It means that the data should not be illegally tampered, improperly modified, deliberately deleted, or maliciously fabricated. If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users.

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are based upon attributes such date of birth of the user country in which he/ she belong to etc. The term encryption refers to converting the original data into human unreadable form (encoding). The conversion of the encoded data into original form is known as decryption. By encrypting the data only the authorized person can decode the original data. Thus data confidentiality is achieved by the encryption. There are many encryption algorithms currently available and has its own advantages. The attribute based encryption is a proven algorithm for cloud computing environment .The limitations of some of attribute based encryption method are to be analyzed. Attribute based encryption generally involves encrypting the attributes neither encrypting the whole data. Encryption in ABE is easy and secure and inexpensive compared to other encryption discussed. The ABE is secure because the encrypted data contains the attributes rather than the data. In case of any malicious attacks the data never is leaked.

The limitation of the attribute based encryption is decryption of data is expensive .The attribute based encryption makes the application to be secure .the performance of the ABE is high compared to other encryption methods. Thus attribute based encryption is the solution to all cloud applications in future. The cloud is moved to next generation computing with critical applications and real time applications. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.[1] ABE is a public key pair encryption. The cipher text and the secret key that the user holds depends on the attribute value (eg: the profession he attained, place he resides). This allows the user to secure the data by encrypting it or view the secured data by decryption. Encryption takes place using the user attributed. The decryption can be done only if the key matches the attributes of user specified. Access policy is classified into key-policy and cipher text policy based on the user policies. The first Key-Policy Attribute Based Encryption (KP-ABE) was proposed by Goyal which allows a specific access structure. The first Cipher-Policy Attribute Based Encryption was proposed by Bethencourt and many such schemes were proposed later. There are numerous schemes proposed recently using multiple authorities generating private user keys. The main security advantage of Attribute Based Encryption is collusion resistance.

2. RELATED WORK

Jin Li,Jingwei Li,Xiaofeg Chen and Wenjing Lou (2013) proposed Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation.

Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally.

This goal is achieved by utilizing a novel collusion-resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. However If a revoked user and either of the KU CSPs collude, it is unable to help such user re-obtain his/her decrypt ability.

Qinlong Huang, Zhaofeng Ma, Jingyi Fu and XinxinNiu (2015) proposed Ciphertext-policy attribute-based encryption (CP-ABE) is becoming a promising solution to guarantee data security in cloud computing. In this paper, we present an attribute-based secure data sharing scheme with Efficient revocation (EABDS) in cloud computing. This scheme first encrypts data with Data encryption key (DEK) using symmetric encryption and then encrypts DEK based on CP ABE, which guarantees the data confidentiality and achieves fine-grained access control. In order to solve the key escrow problem in current attribute based data sharing schemes, our scheme adopts additively homomorphic encryption to generate attribute secret keys of users by attribute authority in cooperation with key server, which prevents attribute authority from accessing the data by generating attribute secret keys alone.

This scheme presents an immediate attribute revocation method that achieves both forward and backward security. The computation overhead of user is also reduced by delegating most of the decryption operations to the key server. The security and performance analysis results show that our scheme is more secure and efficient. However it is not comfort for multi user environment.

PiotrK.Tysowski, M.AnwarulHasan and Xinxin Niu (2013) proposed Outsourcing data to the cloud are beneficial for reasons of economy, scalability, and accessibility, but significant technical challenges remain. Sensitive data stored in the cloud must be protected from being read in the clear by a cloud provider that is honest but- curious.

Additionally, cloud-based data are increasingly being accessed by resource-constrained mobile devices for which the processing and communication cost must be minimized. Novel modifications to attribute based encryption are proposed to allow authorized users access to cloud data based on the satisfaction of required attributes such that the higher computational load from cryptographic operations is assigned to the cloud provider and the total communication cost is lowered for the mobile user. Furthermore, data re-encryption may be optionally performed by the cloud provider to reduce the expense of user revocation in a mobile user environment while preserving the privacy of user data stored in the cloud. The proposed protocol has been realized on commercially popular mobile and cloud platforms to demonstrate real-world benchmarks that show the efficacy of the scheme.

A simulation calibrated with the benchmark results shows the scalability potential of the scheme in the context of a realistic workload in a mobile cloud computing system. However it is not protected from cloud service provider.

AijunGe, JiangZhang, RuiZhang and ZhenfengZhang (2012) proposed decentralized attribute-based encryption (ABE) system, any party can act as an authority by creating a public key and issuing private keys to different users that reflect their attributes without any collaboration. Such an ABE scheme can eliminate the burden of heavy communication and collaborative computation in the setup phase of multi authority ABE schemes, thus is considered more preferable.

Recently in IEEE Transactions Parallel Distributed Systems, Han et al. proposed an interesting privacy-preserving decentralized key-policy ABE scheme, which was claimed to achieve better privacy for users and to be provably secure in the standard model. However, after carefully revisiting the scheme, we conclude that their scheme cannot resist the collusion attacks, hence fails to meet the basic security definitions of the ABE system.

They also claimed that they solved the challenging open problem left by Chase and Chow by constructing a privacy-preserving multi-authority ABE scheme without interactions among the authorities. However, after carefully analyzing their scheme, we have found that this scheme is vulnerable to the collusion attack, which is a basic security requirement for ABE systems. Furthermore, a user can decrypt a cipher text only if his attributes simultaneously satisfy all the access structures at all the authorities (implicitly) involved in the cipher text (also because of the GID). However, such a binding guaranteed by the GID seems too weak to prevent users' collusion. However It cannot resist the collusion attacks.

ZhenLiu, ZhenfuCao and DuncanS.Wong (2012) proposed cipher text-policy attribute-based encryption (CP-ABE) system, decryption keys are defined over attributes shared by multiple users. Given a decryption key, it may not be always possible to trace to the original key owner.

As a decryption privilege could be possessed by multiple users who own the same set of attributes, malicious users might be tempted to leak their decryption privileges to some third parties, for financial gain as an example, without the risk of being caught.

This problem severely limits the applications of CP-ABE. Several traceable CP-ABE (T-CP-ABE) systems have been proposed to address this problem, but the expressiveness of policies in those systems is limited where only AND gate with wildcard is currently supported. In this report we propose a new T-CP-ABE system that supports policies expressed in any monotone access structures.

Also, the proposed system is as efficient and secure as one of the best (non traceable) CP ABE systems currently available, that is, this work adds traceability to an existing expressive, efficient, and secure CP-ABE scheme without weakening its security or setting any particular trade-off on its performance. However CP-ABE scheme is not secure with respect to black-box traceability.

Sahai et al.[9] introduced the concept of another modified form of ABE called CP-ABE that is Cipher text Policy Attribute Based Encryption. In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. CP-ABE works in the reverse way of KP-ABE. In CP-ABE the cipher text is associated with an access tree structure and each user secret key is embedded with a set of attributes. In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system MK, PK, and user secret keys. Only authorized users (i.e., users with intended access structures) are able to decrypt by calling the algorithm Decryption. In CP-ABE, each user is associated with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP ABE technique, encrypted data can be kept confidential and secure against collusion attacks.

To enable more general access control, V. Goyal, O. Pandey, A. Sahai, and B. Waters [4] proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. In this scheme, data is associated with the attributes for which a public key is defined for each. Encrypter, that is who encrypts the data, is associated with the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access tree structure over the data attributes. The nodes of the access tree are the threshold gates. The leaf nodes are associated with attributes. The secret key of the user is defined to reflect the access tree structure. Hence, the user is able to decrypt the message that is a cipher text if and only if the data attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with cipher text and the user's decryption key is associated with a monotonic access tree structure [10]. When the attributes associated with the cipher text satisfy the access tree structure, then the user can decrypt the cipher text. In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and a re-encryption technique used together. It enables a data owner to reduce most of the computational overhead to the servers. The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure. The encrypted data file is stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK. That can be used to decrypt the file or message.

3. PORPOSED SYSTEM

The proposed Enhanced Attribute Based Encryption Technique model is explained using the Figure1.The work enhanced the existing system Jiguo Li [8] work. To reduce the complexity of the work we remove the TA is a trusted authority who authenticates user's attribute sets and generates corresponding private keys for them. The proposed system the Data Owner is responsible for authenticates the user's attributes. The performance validation results show the better result in reducing complexity of the proposed system.

3.1 File Access Control Architecture

Data owner has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access structure and executing Encrypt operation. And it uploads data and cipher text to CSP.

Data User wants to access a large number of data in cloud system. The entity first downloads the corresponding cipher text. Then it executes Decrypt operation of the proposed scheme.

Cloud Server is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible. In the proposed system, it provides ciphertext storage and transmission services.

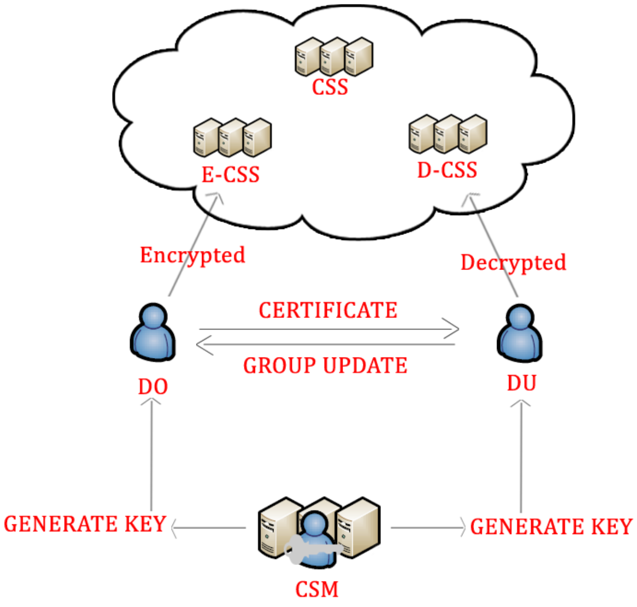


Figure 1 our proposed System model

Cloud Security Manager is security provider for cloud system, such as key creation, key updating, user authorization and revoke users. It would like to find out as much sensitive information. In the proposed scheme, it provides all security related information.

There are following entities in total in our scheme. They are given in Table 1.

TABLE 1 ENTITIES

Symbol	Description
CSS	Cloud Storage Server
E-CSS	Encryption-Cloud Service

	Provider
D-CSS	Decryption-Cloud Service Provider
DO	Data Owner
DU	Data User

1.2 ABE Algorithm Model

In basic ABE, both the secret key of user and cipher text used will be labeled with attributes. A key can decrypt the cipher text to get access to the data only if it has a certain combination of attributes present on both cipher text and the secret key of user. So the decryption takes places in a KP-ABE or CP-ABE schemes only if the attribute set used in the secret key and cipher text abides the access structure.ABE basically has four algorithms. They are Setup, Encryption, Decryption and Key generation which consists of sender to send, authority to validate the data and receivers with participants.

A. Setup: (K, U)->(PP,MSK): This algorithm uses the parameter K as input and returns Public Key and master Secret Key as output. The senders use PP to encrypt the data. The authority alone knows the MSK which is used to create secret keys.

B. Key Generation: (K,PP,MSK,S)->SK: Key generation algorithm uses the inputs as public parameter PP, master secret key MSK, attribute set S and it generates a key to decrypt SK, this key helps the user to decrypt the data using an access tree structure T only if T matches

C. Encryption: (K, PP, M, T)->CT : In the Encryption algorithm, the sender would encrypt a message M, using a public parameter PP, an access structure T and an attribute set S. The output of this algorithm is a ciphertext CT.

D. Decryption: (K, PP, SK,CT)->M: In this algorithm, public parameter PP and ciphertext CT are taken as input with a secret key SK for an attribute set SK. The output of this algorithm is a message only if the associated ciphertext matches the access structure.

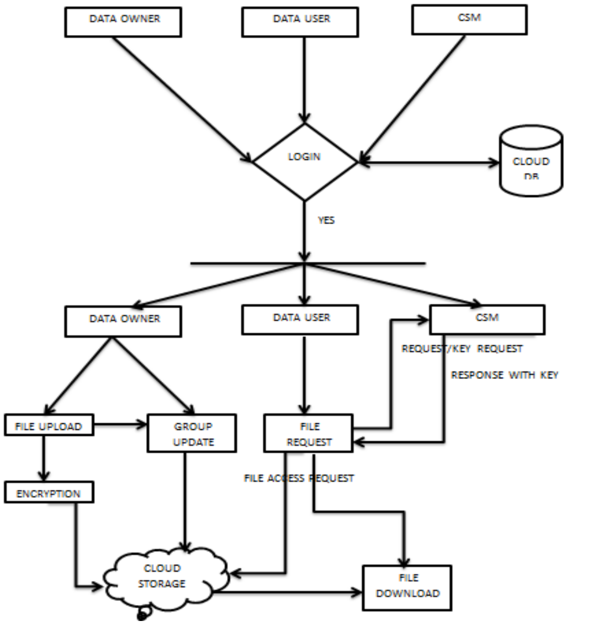


Figure 2 Data Flow Diagram

The Figure 2 explains the data flow diagram of the proposed Enhanced Attribute Based Encryption Technique model in details manner.

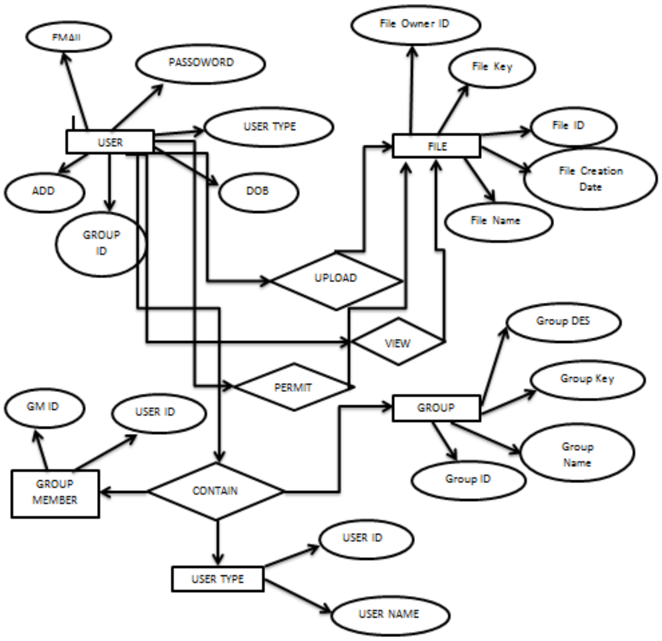


Figure 3 E-R Diagram

The Entity Relationship Diagram explains that the database design of Enhanced Attribute Based Encryption Technique model in details manner. The system has the following list of entities such as user, file, group, group member, user type and group. The user entity has the following entity attributes such as login email, password, group id, add, user type and date of birth etc. The file entity has the following entity attributes such as file owner id, file key, file id, file creation date, file name etc. The group entity has the following attributes such as group id, group name, group key, group DES etc. The user type has the following attributes user id and user name. The group member has GM Id and user id. The entity user has upload relationship with file entity. The group member have contains relationship with user type and group. The user have view, permit relationship with file.

4. RESULTS AND DISCUSSIONS

The following list of the figures show the implementation of the proposed system. We implement our scheme and the model on Windows system with an Intel Core i3 CPU 2.13GHz and 2.00 GB RAM.

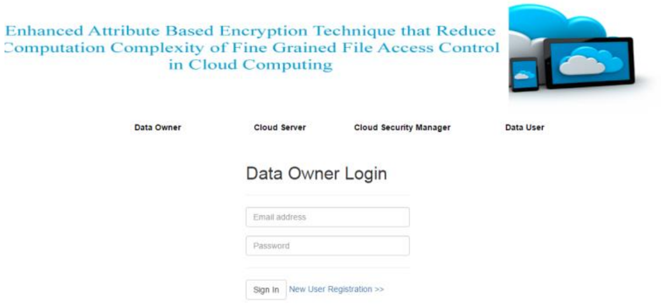


Figure 4 Data Owner Login

The Above figure 4 shows that Data Owner Login screen in An Enhanced Attribute Based Encryption Technique that Reduce Computation Complexity of Fine Grained File Access Control in Cloud.

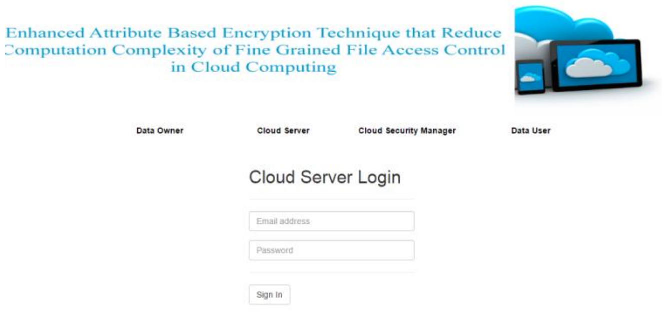
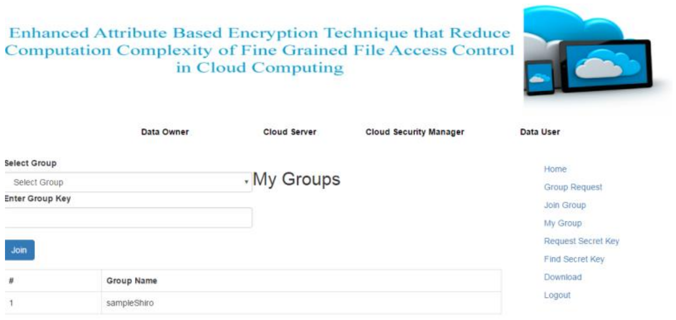


Figure 5 Cloud Server Login

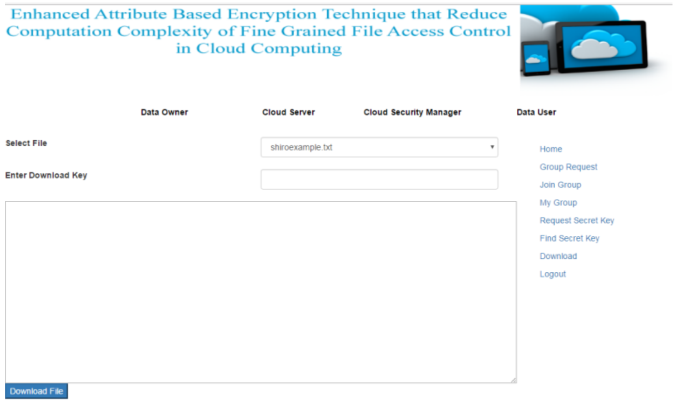
The Above figure 5 shows that Cloud Server login screen in An Enhanced Attribute Based Encryption Technique that Reduce Computation Complexity of Fine Grained File Access Control in Cloud.



#	Group Name
1	sampleShiro

Figure 6 Group Creation

The Figure 6 shows that Group creation process of the data owner. Data User who below to the particular group only can access the data.



Select File: shiroexample.txt

Figure 7 Cloud Server Login

Performance Analysis

The file size, upload time and file size, encryption of the proposed An Enhanced Attribute Based Encryption Technique is compared with existing scheme. The proposed scheme provides the better results. Here proposed system means encryption of the proposed An Enhanced Attribute Based Encryption Technique. The existing system means the Jiguo [8] proposed Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing.

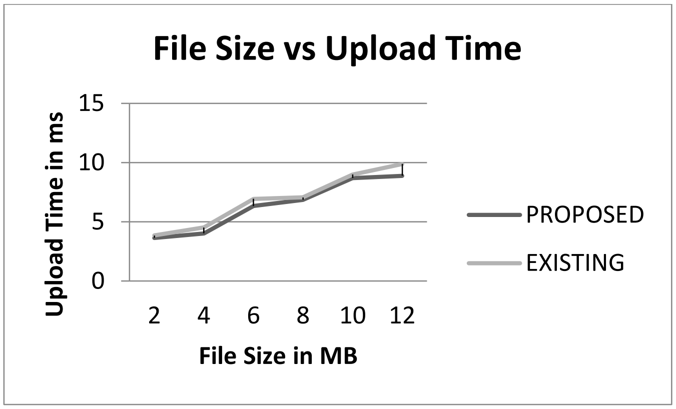


Figure 8 File Size vs Upload Time

The figure 8 shows the comparison of size of file upload to cloud against time required to upload the file. The size of the file is represented in megabytes and the time required to upload is represented using microsecond. The result shows that the computation complexity is reduced in proposed system against existing scheme.

The figure 9 shows the comparison of size of file upload to cloud against time required to encrypt the file. The size of the file is represented in megabytes and the time required to encrption is represented using microsecond. The result shows that the computation complexity of encrypt the files are reduced in proposed system against existing scheme.

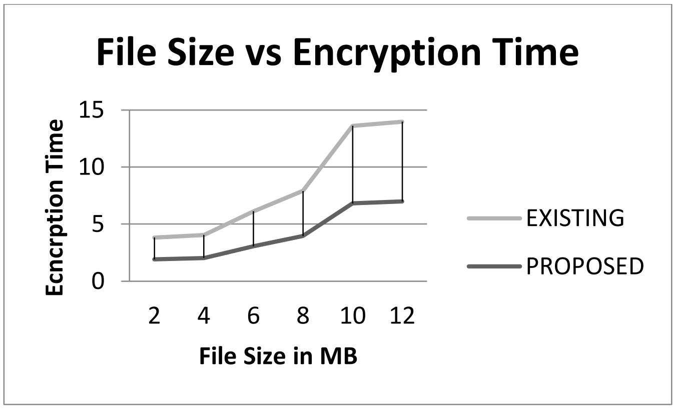


Figure 9 File Size vs Encrpytion Time

5. CONCLUSION

Our work Enhanced Attribute Based Encryption Technique that Reduce Computation Complexity of Fine Grained File Access Control in cloud environment which provide user revocation solution to file sharing system in cloud and also provides better computation complexity in file access. The proposed work is compared with existing scheme it provides better result.

REFERENCES

[1] https://aws.amazon.com/what-is-cloud-computing/

[2] https://www.globaldots.com/cloud-computing-types-of-cloud/

[3] Jin Li, Jingwei Li, Xiaofeng Chen, ChunfuJia, Wenjing Lou, “Identity-Based Encryption with Outsourced Revocation in Cloud Computing,” IEEE Transactions on Computers, Pages: 425 – 437,2013.

[4] Qinlong Huang; Zhaofeng Ma, Yixian Yang, Jingyi Fu, XinxinNiu, “EABDS: Attribute-Based Secure Data Sharing with Efficient Revocation in Cloud Computing,” Chinese Journal of Electronics, Pages: 862 – 868,2015.

[5] Piotr K. Tysowski, M. AnwarulHasan, XinxinNiu, “Hybrid Attribute-and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds,” IEEE Transactions on Cloud Computing, Pages: 172 - 186, 2013.

[6] AijunGe, Jiang Zhang, Rui Zhang, Chuangui Ma, Zhenfeng Zhang, “Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme” IEEE Transactions on Parallel and Distributed Systems, Pages: 2319 - 2321, 2012.

[7] Zhen Liu, Zhenfu Cao, Duncan S. Wong, “White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures” IEEE Transactions on Information Forensics and Security, Pages: 76 – 88,2012.

[8] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian and Jinguang Han, Member, IEEE,Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing.

[9] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute based encryption,” IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[10] R.Ostrovsky, A. Sahai, and B. Waters. “Attribute-based encryption with non-monotonic access structures”. In Proc. of CCS’06, New York, NY, 2007.

Authors

Mr. Dinesh R has obtained his Bachelor Degree in Physics from Manonmaniam Sundaranar University. The obtained his Masters Degree from Anna University. Currently He is working as Project Manager in Shiro Software Solutions. He has 6 years experience in Software industries. He also has 4 years experience in teaching as Assistant Professor. His Specializations include Cloud Computing, Big data and Networkig.

Dr. K. Selva kumar started my research and teaching works from April 1987 at Bharathidasan University, Trichy, Tamilnadu, India. Received Ph.D. from Bharathidasan University in 1992. At present working as Assistant Professor in Mathematics at University College of Engineering, Anna University, Nagercoil Campus, Tamilnadu, India. Developing software for Networking , cloud computing. Image Processing, Singular perturbation problems in control design, aircraft optimal control guidance, Numerical methods for engineering related research problems.

Mr. R. Manibharathi completed MCA from Institute Of Road and Transport Technology, Erode, Anna University, Chennai. He graduated BSc Information Technlogy from Manonmaniam Sundaranar University. He is currently working as Senior Developer at Shiro Software Solutions. His research interest in Cloud Computing, networking and Big Data.