ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Improving Efficiency and Security Based Data Sharing in Large Scale Network

B. SakthiSaravanan., M.Tech[#1], R.Dheenadayalu M.Sc (Engg)[#2] A.Vijayaraj. ME, (Ph.D)[#3],
Department of Information Technology, Saveetha Engineering College, Chennai, India

Abstract — The Key Generation Center (KGC) could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users key. To overcome this problem we propose escrow problem which means a written agreement delivered to a third party and Attribute-Based Encryption (ABE). Attribute-based encryption is a promising cryptographic approach, is a fine-grained data access control which provides a way of defining access policies based on different attributes of the requester, environment and the data object. The KGC can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the data sharing systems.

Keywords— **Attribute based Encryption, Access Control, Cipher text Policy, Revocation, Data Sharing**

I. INTRODUCTION

Network and computing technology enables many people to easily share their data with others, using online external storages. People can share their lives with friends by uploading their private photos or messages into the online social networks; or upload highly sensitive Personal Health Records (PHRs) into online data servers such as Microsoft Health Vault, Google Health for ease of sharing with their primary doctors or for cost saving. The Security Management of PHRs is shown in Fig. 1. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-Based Encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. It provides a way of defining access policies based on different attributes of the requester, environment and the data object. Especially, Cipher text-Policy Attribute-Based Encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data as per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access, which is the traditional access control approach such as the reference monitor Nevertheless, applying CP-ABE in the data sharing system has several challenges. In CP-ABE, the Key Generation Centre (KGC) generates private keys of users by applying the KGC's master secret keys to users' associated set of attributes. Thus, the major benefit of this approach is to largely reduce the need for processing and storing public key certificates under traditional Public Key Infrastructure (PKI). However, the advantage of the CP-ABE comes with a major drawback which is known as a key escrow problem. The KGC can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the data sharing systems. Another challenge is the key revocation. Since some users may change their associate attributes at some time, or some private keys might be compromised, key revocation or update for each attribute is necessary in order to make systems secure. This issue is even more difficult especially in ABE, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a set of users as an attribute group).

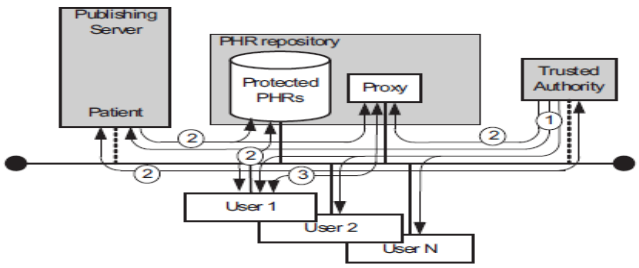

Fig. 1 Security Management of PHRs

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

This implies that revocation of any attribute or any single user in an attribute group would affect all users in the group. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability.

A. *Related Work*

Cipher text-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the cipher text is associated with an access policy over attributes. The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control [2].

In [3], they created public key revocation encryption systems with small cryptographic private and public keys. Their systems have two important features relating respectively to public and private key size. First, public keys in our two systems are short and enable a user to create a cipher text that revokes an unbounded number of users. This is in contrast to other systems where the public parameters bound the number of users in the system and must be updated to allow more users. Second, the cryptographic key material that must be stored securely on the receiving devices is small. Keeping the size of private key storage as low as possible is important as cryptographic keys will often be stored in tamper-resistant memory, which is more costly. This can be especially critical in small devices such as sensor nodes, where maintaining low device cost is particularly crucial [3].

Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, the identities (e.g. emails or IP addresses) of the latter are sufficient to encrypt. Any setting, PKI- or identity-based, must provide a means to revoke users from the system. The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority [4].

Cipher text-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control of shared data. In CP-ABE, each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a cipher text if and only if his attributes satisfy the cipher text access structure. Beside this basic property, practical applications usually have other requirements [5].

In cipher text policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the cipher text access structure. This provides fine-grained access control on shared data in many practical settings, e.g., secure database and IP multicast. The communication model is one-to-one, in the sense that any message encrypted using a particular public key can be decrypted only with the corresponding secret key. The same holds for identity-based encryption (IBE), where user public keys can be arbitrary bit strings such as email addresses [6].

II. EXISTING SYSTEMS AND PROPOSED SOLUTION

The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation centre and the data storing centre, fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system

A. *Existing System*

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information Thus, the key escrow problem is inherent such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time.

- The key generation centre could decrypt any messages addressed to specific users by generating their private keys.
- This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

III. PROPOSED SOLUTION

In this paper, we propose a novel CP-ABE scheme for a secure data sharing system. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing centre with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing centre in the proposed scheme.

- The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation centre and the data storing centre.
- Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.

IV. ATTRIBUTE BASED DATA SHARING SYSTEM

As shown in Fig. 2, the architecture of data sharing system consists of the following entities:

A. Data Owner

It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. Data Owner to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

B. Data Storing Centre

It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data storing centre is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. Data storing centre store the data. Data Storage Centres provides offsite record and tape storage, retrieval, delivery and destruction services.

C. User

This is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the cipher text and obtain the data.

D. Key Generation Centre

It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

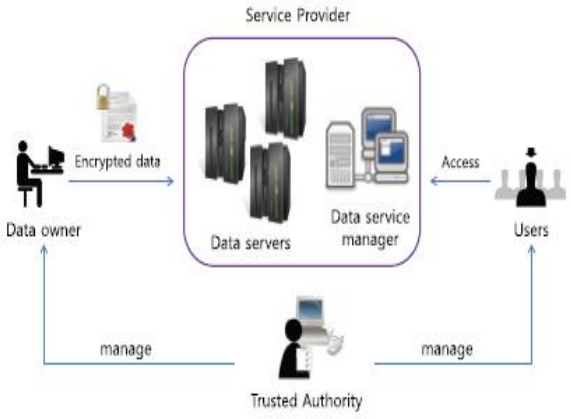

Fig. 2. Architecture of a Data Sharing System

The node structure of the Attribute based data sharing system is shown in Fig. 3. The nodes involved are admin and clients which stands as UI for the system. The nodes are Key Generation Centre (KGC) is a key authority that generates public and secret parameters for CP-ABE. Data storing center is an entity that provides a data sharing service. The data storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

fine-grained user access control. It is a client who owns data, and wishes to upload it into the external data storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. User is an entity who wants to access the data.

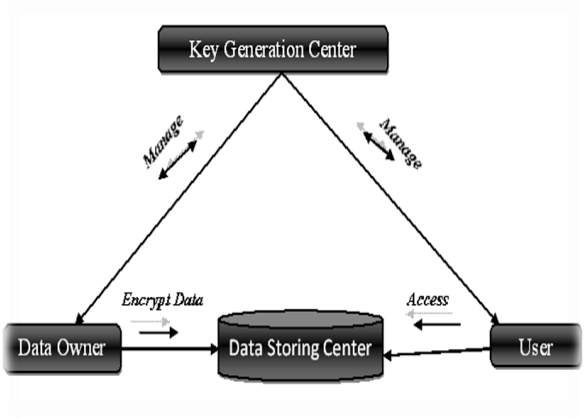

Fig. 3. Node Structure of a Data Sharing System

V. FUNCTIONAL AND NON FUNCTIONAL REQUIREMENTS

A. Functional Requirements

The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing center in the proposed scheme.

B. Non Functional Requirements

Efficiency Attribute Based Data Sharing System encrypting the content, hence solving the performance degradation problem of distributed approach.

VI. METHODOLOGY

The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing centre with their own master secrets.

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information Thus, the key escrow problem is inherent such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time.

A. Cipher text – Policy Attribute Based Encryption with User Revocation

We define the CP-ABE with user revocation capability scheme. The scheme consists of the following six algorithms:

Setup: The setup algorithm is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public key PK and a master key MK.

AttrKeyGen: The attribute key generation algorithm takes as input the master key MK, a set of attributes and a set of user indices. It outputs a set of private attribute keys for each user in U that identifies with the attributes set.

KEKGen: The key encrypting key (KEK) generation algorithm takes as input a set of user indices and outputs KEKs for each user in U, which will be used to encrypt attribute group keys.

Encrypt: The encryption algorithm is a randomized algorithm that takes as input the public parameter PK, a message M, and an access structure AA over the universe of attributes. It outputs a cipher text such that only a user who possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

ReEncrypt: The re-encryption algorithm is a randomized algorithm that takes as input the cipher text including an access structure and a set of attribute groups. If the attribute groups appear in AA, it re-encrypts for the attributes; else, returns specifically, it outputs a re-encrypted cipher text such that only a user who possesses a

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

set of attributes that satisfies the access structure and has a valid membership for each of them at the same time will be able to decrypt the message.

Decrypt: The decryption algorithm takes as input the cipher text which contains an access structure AA, a private key SK, and a set of attribute group keys for a set of attributes.

VII. IMPLEMENTATION OF ALGORITHM

A. C# and .NET Implementation

The implementation of Attribute Based Data Sharing System consists of the following components

- Data Owner:
  - Login
  - Key Generation Center (KGC)
  - Data owner (set Access Policy, Encrypt File)
  - Send Data Storing Center
- Data Storing Centre
  - Store Data
- User
  - Authentication (Registration /Login)
  - User Access
  - View Available Files
  - User Get File
  - Decrypt File

Data Owner:

Login: If the user enters a valid username/password combination they will be granted to access data. If the user enter invalid username and password that user will be considered as unauthorized user and denied access to that user.

Key Generation Centre (KGC): It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

Data owner (set Access Policy, Encrypt File): It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. Data Owner to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. This operation is shown in Fig. 4.

Send Data Storing Centre: Data storing centre store the data of data owner in the encrypted form.

Data Storing Centre

It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data storing centre is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. Data storing centre store the data. Data Storage Centres provides offsite record and tape storage, retrieval, delivery and destruction services.

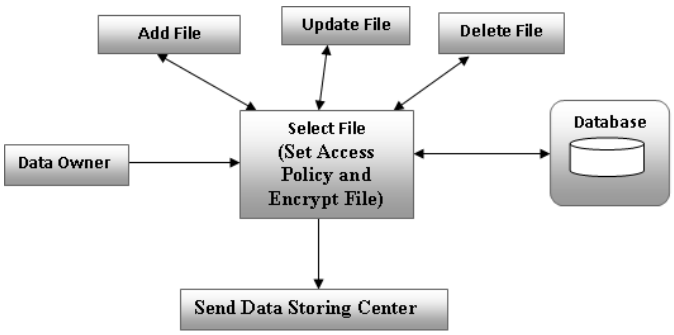

Fig. 4 Data Owner (Set Access Policy, Encrypt File)

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

User:

Authentication (Registration /Login): New user access data storing means must, new User can enter our details and register here. In Login Form module presents users a form with username and Password fields. If the user enters a valid username/password combination they will be granted to access data. If the user enter invalid username and password that user will be considered as unauthorized user and denied access to that user.

User Access: In this module the user to check our attributes and access policy.

View Available Files: Data Storing Centre Store the number of files that files are displayed authorized user based on user access policy.

User Get File: It is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the cipher text and obtain the data User to select particular file and get Key from Key Generation Centre.

Decrypt File: Decryption is the reverse process to Encryption. Frequently, the same Cipher is used for both Encryption and Decryption. While Encryption creates a Cipher text from a Plaintext, Decryption creates a Plaintext from a Cipher text. User uses that particular file key decrypt and save that file

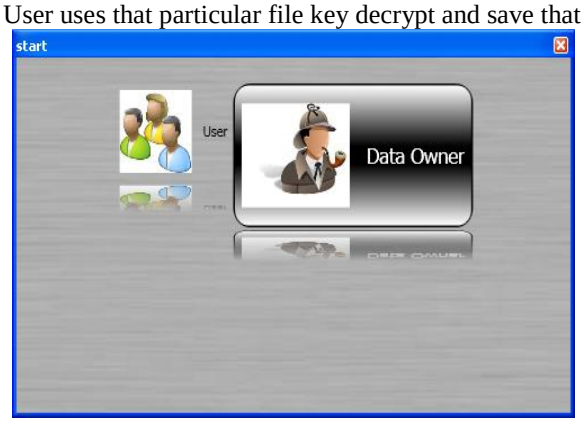

Fig. 5 Data Owner

Fig. 6 Data Owner Login Form

Data Owner Login Screen is shown in Fig. 6. If the user enters a valid username/password combination they will be granted to access data. If the user enter invalid username and password that user will be considered as unauthorized user and denied access to that user.

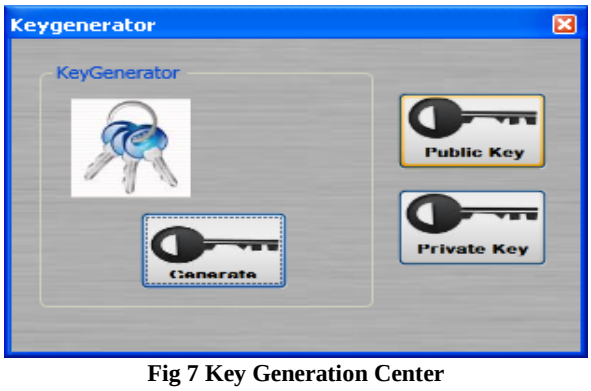

Fig 7 Key Generation Center

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Key generation process is shown in Fig. 7, generating keys for cryptography. It provides public key and private key. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

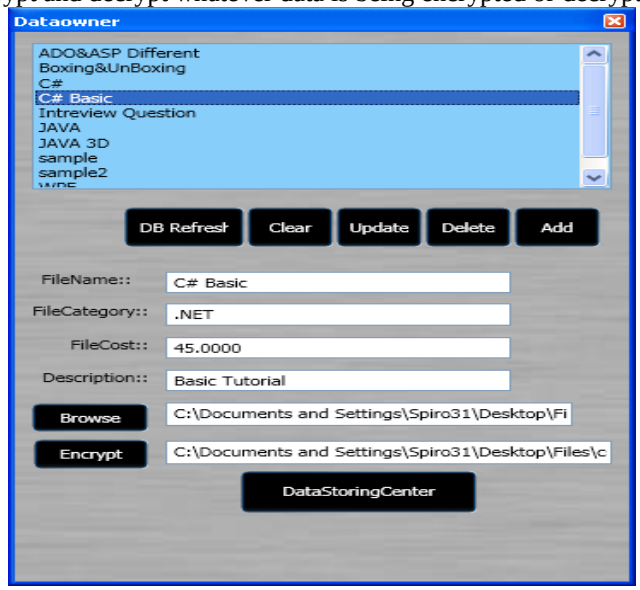

Fig. 8 Data Owner File Entry

Data Storing Centre Process is shown in Fig. 9. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. Data storing centre store the data. Data Storage Centres provides offsite record and tape storage, retrieval, delivery and destruction services.

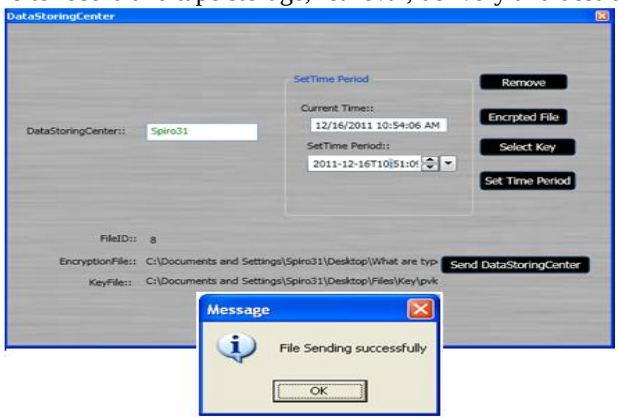

Fig. 9 Data Storing Center

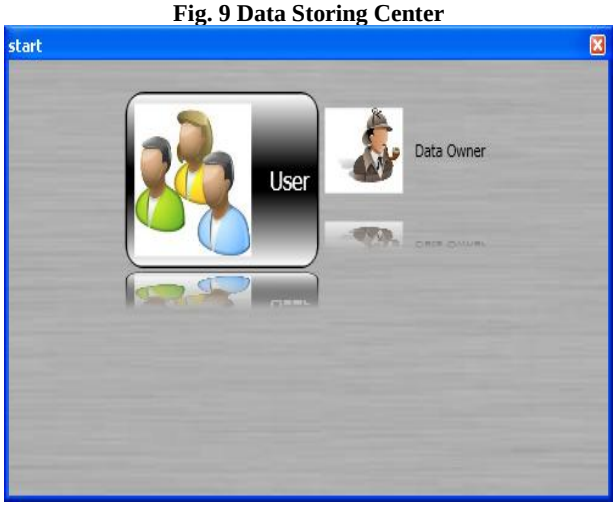

Fig. 10 User

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

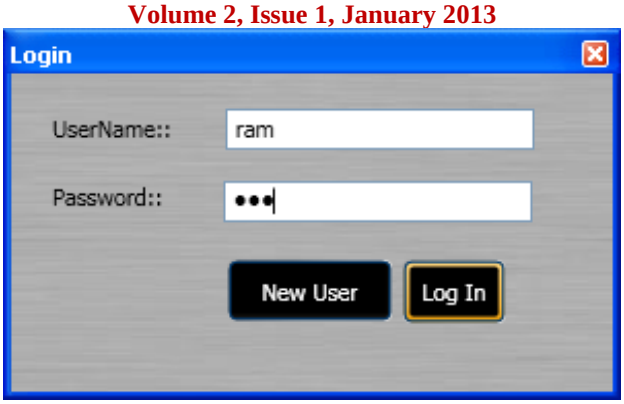

Fig. 11 User Login

Fig. 12 shows how the Data Storing Centre Store the number of files that files is displayed authorized user based on user access policy. It is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the cipher text and obtain the data User to select particular file and get Key from Key Generation Centre.

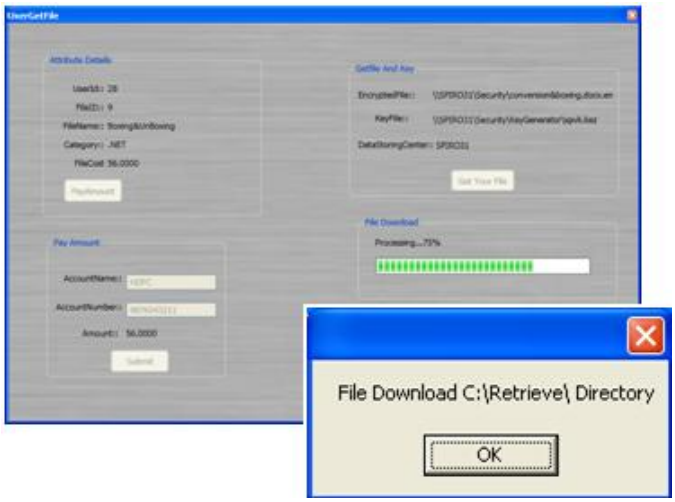

Fig. 12 File Download

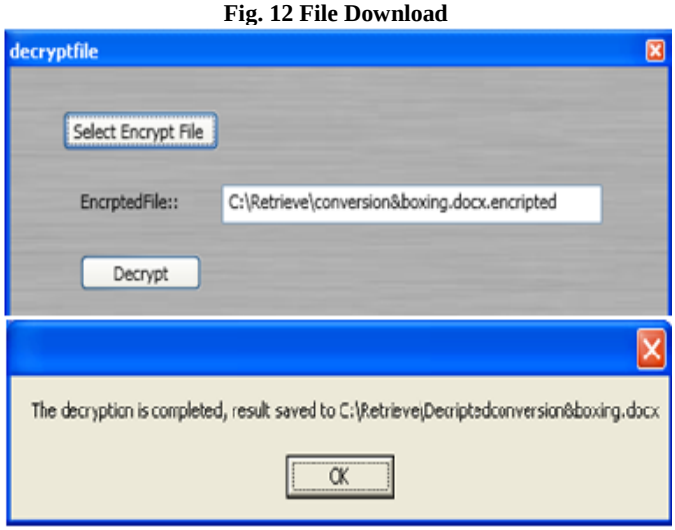

Fig. 13 Decrypt File

Decryption of a file is shown in Fig. 13. Decryption is the reverse process to Encryption. Frequently, the same Cipher is used for both Encryption and Decryption. While Encryption creates a Cipher text from a Plaintext, Decryption creates a Plaintext from a Cipher text. User uses that particular file key decrypt and save that file.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

VIII. CONCLUSION AND FUTURE ENHANCEMENT

A. Conclusion

To achieves more secure and fine-grained data access control in the data sharing system. We demonstrated that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system. Data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials.

B. Future Enhancement

In the future, it would be interesting to consider attribute-based encryption systems by applying advanced cryptosystem for data sharing. In future, we encrypt multimedia content, Solve the performance degradation of fully distributed approach, Neglected key expired time, we can use multi Data Storing Centre, Proxy servers to update user secret key without disclosing user attribute information.

REFERENCES

[1] Junbeom Hur and Dong Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Transactions on Parallel and Distributed Systems, pp 1214-1221, 2011.

[2] Luan Ibraimi, Milan Petkovic, Svetla Nikova, Pieter Hartel and Willem Jonker, "Mediated Cipher text-Policy Attribute-Based Encryption and Its Application", Information Security Applications, Lecture Notes in Computer Science, DOI: 10.1007/978-3-642-10838-9_23, pp 309-323,2009.

[3] Lewko, Allison; Sahai, Amit; Waters, Brent, "Revocation Systems with Very Small Private Keys", Security and Privacy (SP), IEEE Symposium, May 2010, 978-1-4244-6895-9, pp 273 – 285, 2010.

[4] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar, "Identity-based encryption with efficient revocation", Proceedings of the 15th ACM conference on Computer and communications security, ISBN: 978-1-59593-810-7, pp 417-426, 2008.

[5] Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, "Attribute based data sharing with attribute revocation", Proceedings of the 5th ACM Symposium on Information, ISBN: 978-1-60558-936-7, pp 261-270, 2010.

[6] Ling Cheung, Calvin Newport," Provably secure cipher text policy ABE", Proceedings of the 14th ACM conference on Computer and communications security, ISBN: 978-1-59593-703-2, pp 456-465, 2007.

AUTHOR BIOGRAPHY

B.Sakthisaravanan has received B.TECH from Anna University, Chennai. He also received M.Tech (IT) from Satyabama University, Tamilnadu, India. He has 3 years of experience as Lecturer. He is currently working as an Assistant professor in Saveetha Engineering College, Chennai. He has Published number of national and international conferences .His area of interest are Data Structures, Data Base Management Systems, System Software, Computer Networks and Computer Architecture.

Prof. R. Dheenadayalu, B.E., M.Sc(Engg), **Dean(ICT) & Professor.** He Specialized in Software development, OS and data centre administration. He has years of service in teaching, industry, education & training in various colleges(including IIT, Chennai & College of Engg, Guindy). He has written 12 books on various topics in Computer Science. Prof.R.Dheenadayalu has authored modules for DOESEC examinations and IGNOU. He received special training on computers in Germany and has executed projects in India & Malaysia.

A.Vijayaraj is an Associate Professor in Department of Information Technology at Saveetha Engineering College. He received his Master of Computer Application in Bharathidhasan University, in 1997 and his Master of Engineering in Computer Science and Engineering from Sathyabama University at 2005. He has 12 years of teaching experience from various Engineering Colleges during tenure he was Awarded **Best Teacher Award** twice. He is a Member of, CSI and ISTE. He has Published 2 papers In International journal 10 Papers in International and National Level conferences. His area of interest includes Operating Systems, Data Structures, Networks and Communication.