International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.179-192
http://dx.doi.org/10.14257/ijsia.2017.11.1.15

Anonymous Authentication with Centralize Access Control of Data Storage in Cloud

Linawati[*1], I Gede Totok Suryawan[2] and [3]Made Sudarma

[*1) 3)] *Electrical Engineering Department, Universitas Udayana, Bali, Indonesia*
[2)] *STMIK STIKOM, Bali, Indonesia*
[*1)]*linawati@unud.ac.id*, [2)]*totok.suryawan@gmail.com*,
[3)]*msudarma@unud.ac.id.*

Abstract

Anonymous authentication will be very useful in some matters that require the protection of the privacy of users, for examples in education is to report incidents of plagiarism, in business is to maintain and protect the rights of consumers, in government is as a place of public complaints about social problems as well as corruption accusation. Therefore this paper investigates the implementation of anonymous authentication with centralized access control on data storage in the cloud. In this investigation, the access control will use the method of Attribute-Based Access Control (ABAC), which would apply access control centralization but supports anonymous authentication. The authentication process will use an algorithm Attribute-Based Encryption (ABE) and Attribute-Based Signature (ABS) with the Key Distribution Center (KDC) as a user management and key distribution. Then the performance of the authentication system has conducted using one year academic data of students in a college, in term of the anonymous authentication user to the KDC as user management and key distribution, encryption and description files using both algorithms of ABE and ABS, the process of uploading and downloading files, as well as the process of file directory movement. In addition, application of anonymous authentication in cloud storage for reporting social problems has been briefly discussed. The results showed that the encryption process and a file description with both ABE and ABS implementation in the Cloud Sever required the average time for encryption of 4.2 seconds for a text file size of 197 byte up to 8116 byte. While the description process spent an average of 3.9 seconds. In term of the file size, the result also proved that the size before encryption is the same as after decryption process. KDC Server also showed a good performance, this was indicated by an ability of the server to distribute keys to the users in 4.6 seconds.

Keywords*: Anonymous Authentication, Data Storage in Cloud, Attribute Based Access Control, Attribute Based Encryption, Attribute Based Signature, Key Distribution Center.*

1. Introduction

Data storage technology is now entering a new era. Before we know the data storage devices such as hard disk in a computer or flash disk that can be taken anywhere. Now technology has offered online data storage, known as cloud storage. Cloud storage is a digital data storage technology utilizing their virtual servers as storage.

Cloud storage technology is one part of a system of cloud computing services. Cloud computing is a basic concept of the cloud storage service. Cloud computing is the delivery of hosted extensively through the Internet. In principle, this technology is based on a collection of some of the technologies of previous research such as Service-Oriented Architecture (SOA), Distributed System, Grid Computing and virtualization which are then modified and updated to a new concept and packaged in such a way become a business model by the name "cloud computing". This technology allows users to manage

ISSN: 1738-9976 IJSIA

these resources effectively in place. Users do not need to invest infrastructure that spend a high cost. Users simply by buying cloud computing services provided according to their need.

Despite the obvious advantages, an important factor in this cloud system is strong enforcement of security mechanisms for data storage, transfer and refineries in the cloud. Moreover, the data stored in the cloud is that sensitive data such as medical records, research results and data users in social media. Ensuring the privacy and data security are important for users to trust the service provider. To achieve that, it must use an adequate authentication and access control techniques.

Research on security and the protection of privacy of data storage in the cloud has been done by many researchers. Study in [1] provides a security mechanism of data storage in the cloud using the RSA algorithm for encryption and description file, key distribution using key manager where the private key is generated from a combination of username, password, and two security questions chosen by the user. The private key has managed by user, and the public key generated from random binary key is created by the key manager. The manager is managed the public key. A cloud user privacy protection by creating some KDC for key management and Third Party Authentication (TPA) for user management and cloud server for file management have been proposed in [2]. Other researches relating to security and privacy protection cloud users are also performed in [3], [4], [5], [6], [7].

In this paper, the research conducts centralize access control that supports anonymous authentication that verifies the cloud without knowing the identity of the user. The authentication process will use algorithms of Attribute-Based Encryption (ABE) and Attribute-Based Signature (ABS) with the Key Distribution Center (KDC) as user management and key distribution. There are several studies that have applied anonymous authentication on data storage in the cloud [8], [9], [10], [11], [12], [13], [14], [15]. However all of the studies utilized decentralized access control with anonymous authentication on data storage in the cloud.

The ABE algorithm will be used for the encryption of processed files in the cloud. However before the user receives services from the cloud, users must enroll in the KDC and get a key. The cloud will provide services to create a file, encryption and file description, and upload and download documents. Detailed user data will be stored in the KDC. Then KDC will distribute keys, where the keys contain of keys for encryption / description and key for signing documents. The process of signing the document is using the ABS algorithm. With the KDC as a key distribution management in the cloud, the anonymous authentication can be implemented. Thus the cloud can verify their validity without knowing the identity of its users.

2. ABE and ABS in Cloud Storage

In this section describes the use of algorithms of ABE and ABS on data storage in the cloud. By ABE, users are given the appropriate attribute set, that only users who have a match set of attributes that can describe the information in the cloud. There are four processes in ABE algorithm [8] such as System Initialization, Key Generation and Distribution by KDC, Encryption by Sender, and Decryption by Receiver.

To prevent replay attacks, the user can make changes to data at any time. The system will revoke user attributes that do not have legitimate access policy, and the system will remove the user. The user will not be allowed to enter the system again. There are six steps involved in ABS algorithm [8], including: System Initialization, User Registration, KDC Setup, Attribute Generation, Sign and Verify.

Many studies have applied algorithms of Attribute-Based [8], [9], [16], and [17]. Then several methods of authentication and encryption have been commonly used in data storage in the cloud such as in [18] uses the SHA to implement SaaS, in [10] uses RSA for encryption / decryption, in [19] uses HBE for encryption / decryption, in [20] uses

Easier for encryption / decryption, and in [21] using DHT Routing for Intrusion Detection System. Finally several other studies conducted literature survey on the implementation of authentication and encryption methods [22], [23], [24], [25].

3. Design of Anonymous Authentication in Cloud Storage and Its Application

In this section will be shown the design anonymous authentication on data storage in the cloud. Overall, the design of anonymous authentication on data storage in the cloud will be created using a model of the Unified Modelling Language (UML) of Use case Diagram which the Use case Diagram consists of Use case Diagram for KDC Server and Use case Diagram for Cloud Server, as shown in Figure 1 and Figure 2.

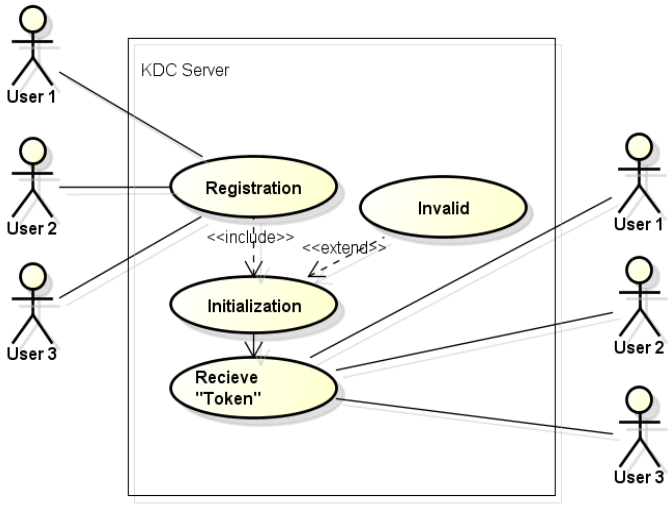

Figure 1. Use Case Diagram KDC Server

As seen in Figure 1 that every user who wants to get the key from the KDC server, the user must register in advance. Each user registration will be validated by KDC Server, then for a valid user status will be changed to be active, while the invalid status to be invalid or inactive. Every user that is already active will get a token that can later be used to log in Cloud Server as shown in Figure 2.

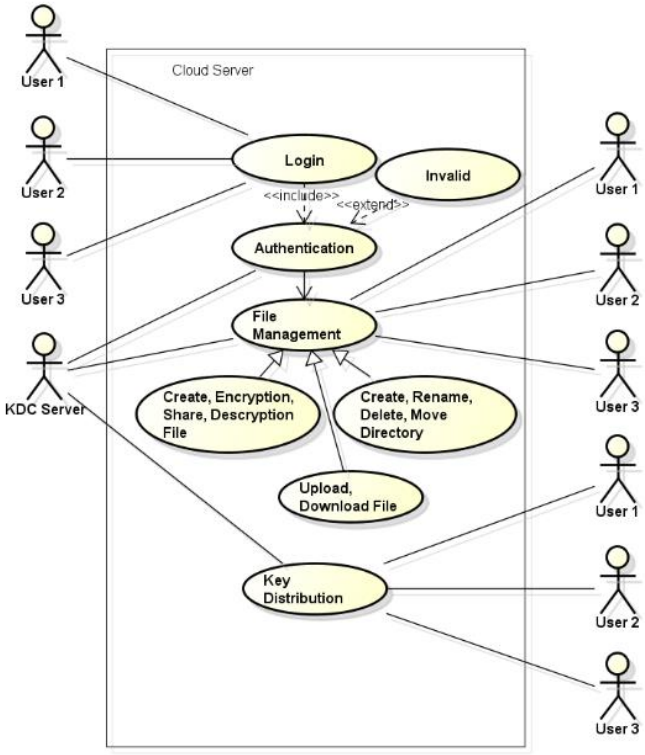

Figure 2. User Case Diagram Cloud Server

Figure 2 shows after the user gets a token from KDC Server, the user can use the token to log in Cloud Server. Cloud Server authenticates each user who logs, if valid then the authenticated user can use the services of Cloud Server. Some of the services are designed in this study, such as create a text file, encrypt text files, share text files, text description file, upload / download files, and the file directory management. The file management user is performed using a key that is distributed by the KDC Server.

One of anonymous authentication in cloud storage applications which is described in this paper is a complaint system in the university. The users of the system are students, academic administration bureau, accounting department, management head of university, *etc*. When a student needs to complaint or report to management head of university about corruption that was done by one accounting staff, confidently that identification of the student is protected and hidden by the system. Only management head of university receives and could read and follow up the report. The management is convinced that the complaint came from an authorized user. Figure 3 explains briefly the complaint or report process. There are two servers, *i.e*. KDC server and server for Complaint Management System (CMS). Student's Id is stored in KDC server and the student could create new report with its supporting documents using CMS server. Then the file is encrypted before sending to the head management. The student can select the receivers and trace the report status.

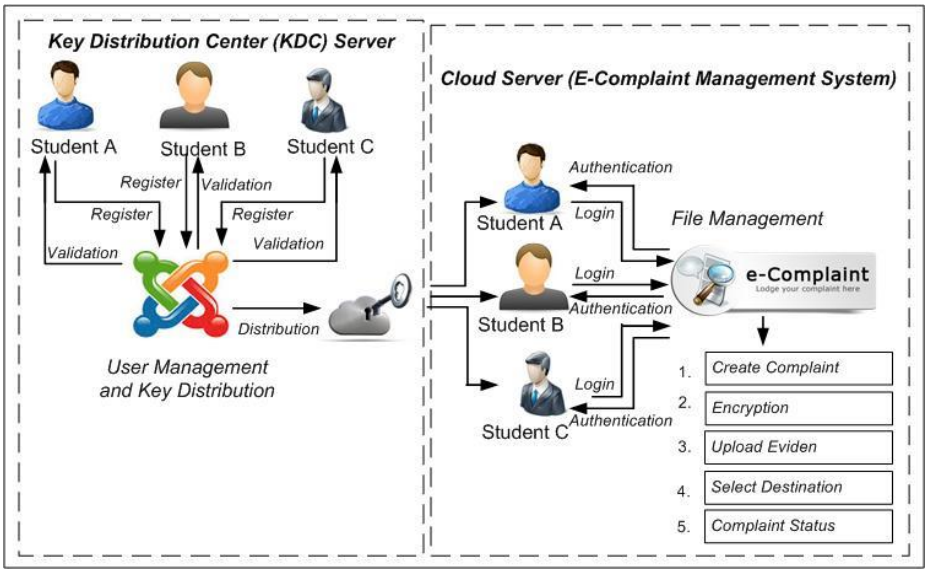

Figure 3. Applied Anonymous Authentication for Complain System

4. Results and Discussions

In this section will describe the implementation of the registration process and user authentication, create and description of the file, share and file encryption, upload and download files, the file directory, and process of complaint management system. Here are the results of each process.

A. User Registration and Approval

To implement the management processes of key distribution, encryption and decryption of files on data storage in the cloud, in this study, two applications have been created, namely an application for user management and key distribution (Key Distribution Center / KDC Server) and an application for file management (Cloud Servers), that each has its own database. Before distributing the keys, the KDC server will validate each user who signed up and subsequently has been declared valid user which can directly receive services from Cloud Server. Validation process in the KDC Server and Cloud Sever Main Menu are shown in Figure 4.

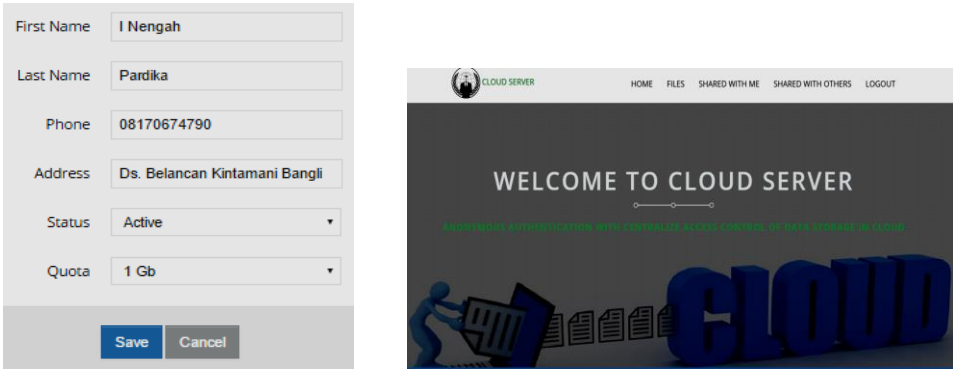

Figure 4. User Validation and Main Menu of Cloud Server

Figure 4 shows the validation process of new user registrations at KDC Server and Cloud Server main menu. With two servers that KDC Server for user management and Cloud Server for file management then anonymous authentication process has been run well.

B. Create and File Encryption

The encryption process has been applied by encrypting the text file. Users can set up a text file in the Cloud server then encrypts the file, or select a file that already exists in the Cloud Server for encryption. Encrypted text file is shown in Figure 5. The Cloud Server has shown that the implementation of both ABE algorithm and ABS algorithm work well in a text file encryption on data storage in the cloud.

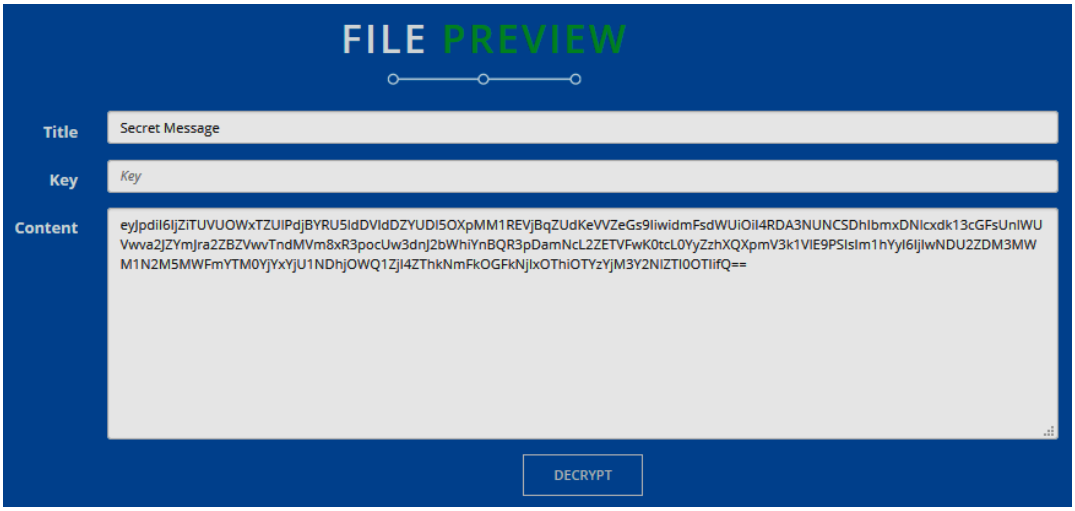

Figure 5. Chypertext File

C. Share and File Decryption

Sharing files is an additional facility after user encrypted the file. For file sharing, user can choose another user as the recipient of the file and specify user access rights received file. In this case there are two types of access granted to the recipient that are read access only and access to modify the file. The process of selecting the recipient user and file access rights are shown in Figure 6.

Once the file is distributed directly, the KDC Server will distribute keys to email recipients that files can then be used to perform file decryption. Accepted locked forms can be seen in Figure 7. Then the user must use the key to convert the file back to be plaintext as seen in Figure 8.

Therefore both Figures 6 and 7 have shown that the KDC Server can perform user management and key distribution well. Finally Figure 8 has displayed that the Cloud Server can implement the ABS algorithm well.

Figure 6. Recipients User List and Their Access Privileges

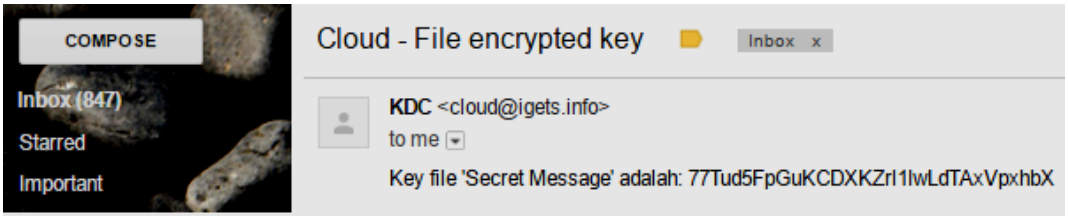

Figure 7. Key for File Decryption

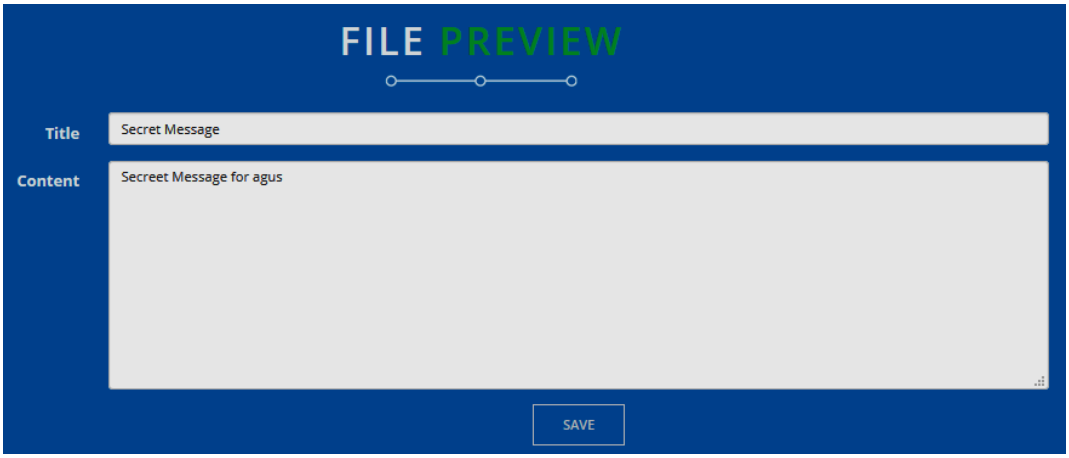

Figure 8. Plaintext File

D. Upload and Download of Files

As a system's primary function of a cloud file storage, then the Cloud Servers have given the facility of uploading and downloading files. Users can upload various types of files to the Cloud Server. When a file has been uploaded, afterward the Cloud Server instantly displays a complete information about the file such as file name, file size, file type, and time of the process. For security reasons the Cloud Server directly renames a file that was uploaded, but the Cloud Server facilitates user button "*Rename*" if a user wants to change the file name as desired by the user. The result of the uploaded file can be

seen in Figure 9. In addition the renamed files are stored in the user private directory. Private directory file storage in the Cloud Servers can be seen in Figure 10.

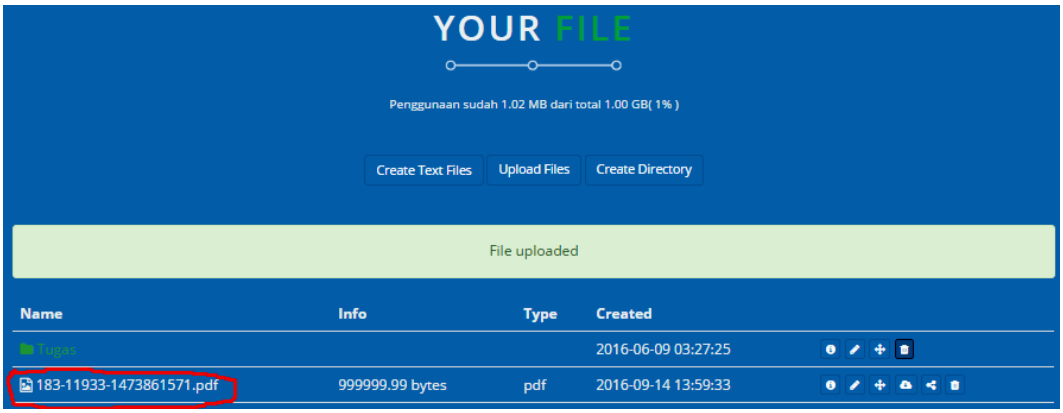

Figure 9. List of Files in the Cloud Server

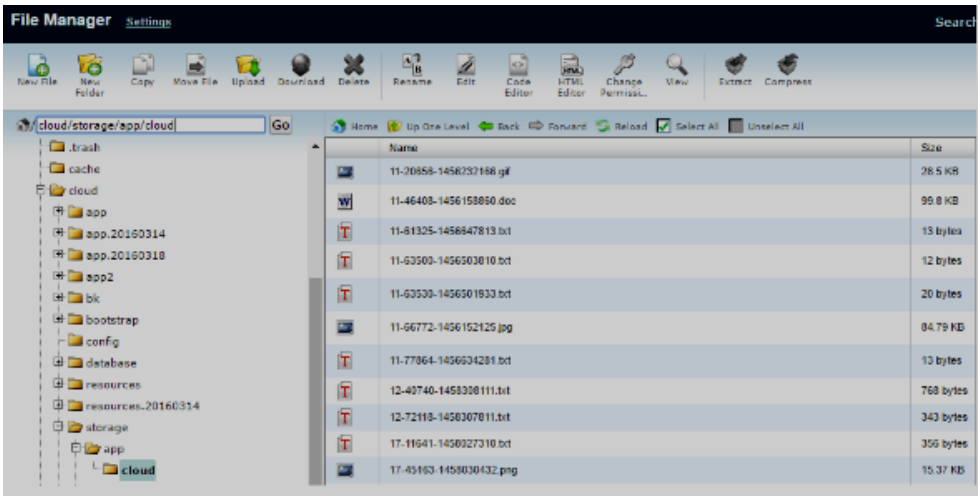

Figure 10. Private Directory File in Cloud Server

Figure 10 proves that the files were uploaded by a user, are stored in a special directory. The directory cannot be accessed by other users, *i.e. home/cloud/storage/app/ cloud*. Files that are public interface for the user are stored in a public directory, as well as a website in a web hosting that is stored in the directory: *home/public html/cloud*. Public Directory Server file storage in the cloud can be seen in Figure 11. Similarly with the process of sharing text files, the uploaded files can also be shared with other user-friend. Accepted form of the file is shown in Figure 12. When the user has accepted the file, the user must use a key to open it. When a file is shared, then the KDC server immediately sends an email to the recipient's key file.

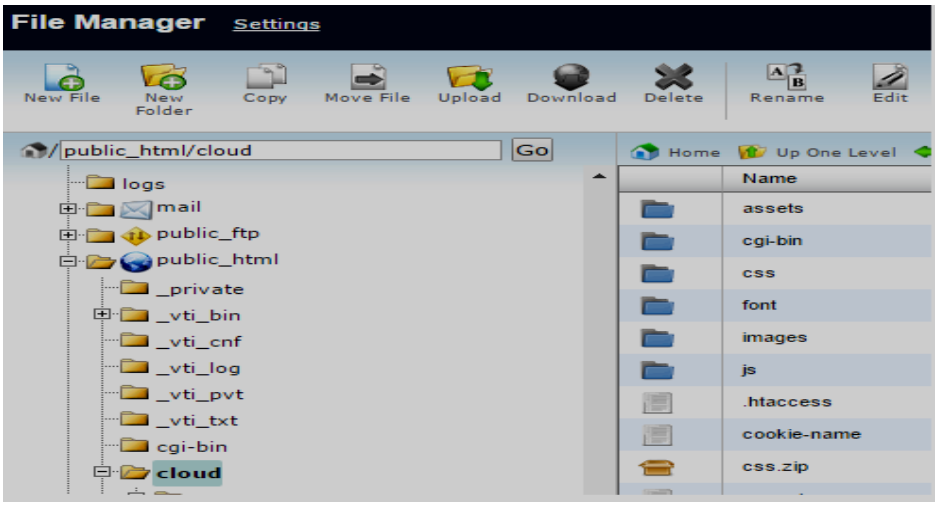

Figure 11. Public Directory File in Cloud Server

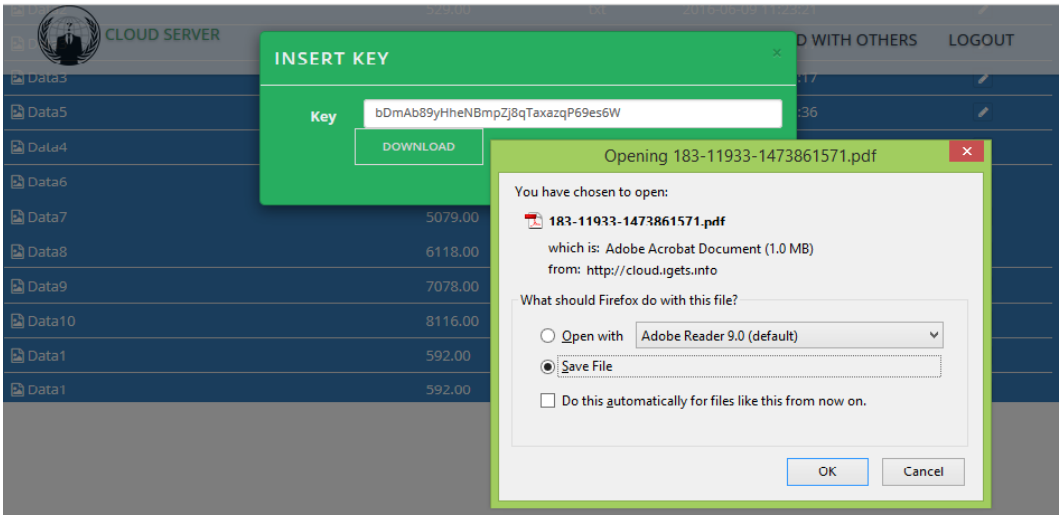

Figure 12. Downloaded File

E. Directory File

Other facilities of Cloud Servers in this study is creating of file directory. With this file directory user will be facilitated in managing files in the Cloud Server. Users can create folders and sub folders and move files from one folder to others using the facilities of this file directory. The process of moving a file from one folder to others can be seen in Figure 13. The figure shows that the Cloud Server has been able to perform file management well. In addition to the file transfer, the Cloud Server users can also see a list of files that have been shared with other users and a list of files received by another user. Cloud server also provides the facility for users to view data storage capacity that has been used and the remaining unused capacity.

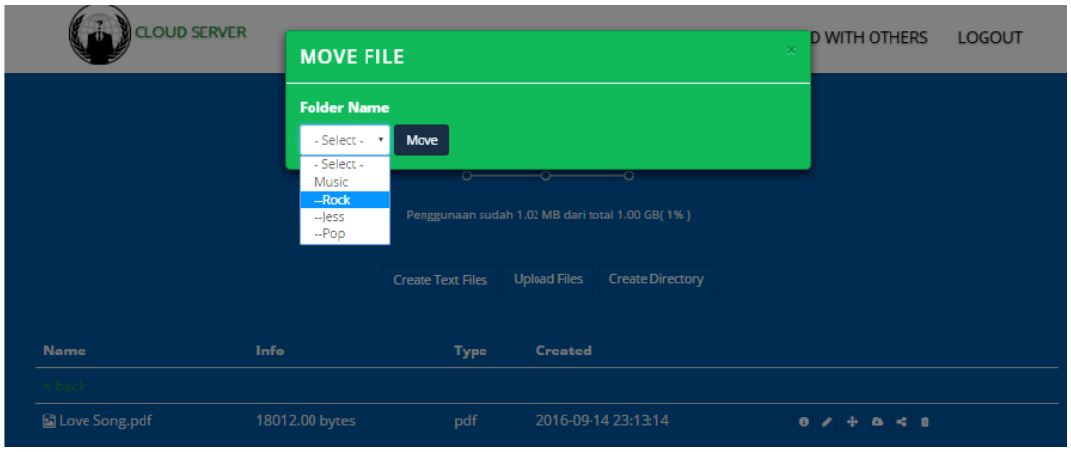

Figure 13. Moving File Process

F. Report or Complaint Submission Process

The implementation of anonymous authentication as stated in Section 3 is for reporting incidents or sending complaints of daily social problems. Only registered users can report or submit complaints. Therefore the system could be protected from junk reports and other abused reports. The user creates report using form as shown in Figure 14. There are selection of issue, recipient unit, subject of report, and report content. Next process is to encrypt the filled form. Non-registered users have no capability to read the report if they have no key to decrypt the file.

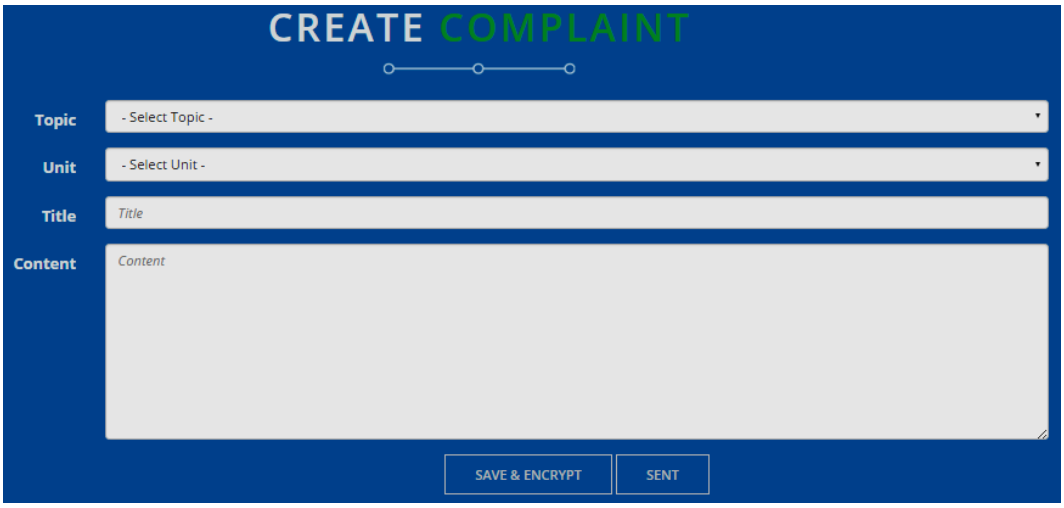

Figure 14. Reporting Form

5. Performance Analysis

In this section will be analyzed the KDC Server performance in accomplishing key distribution, and file encryption and decryption and comparison of the file size before encrypting and after a decryption process in the Cloud.

A. Key Distribution

In this research, the experiments were done 10 times and the results can be seen in Figure 15. The experimental results showed that the average time required by the KDC Server to distribute keys to the user was 4.62 seconds.

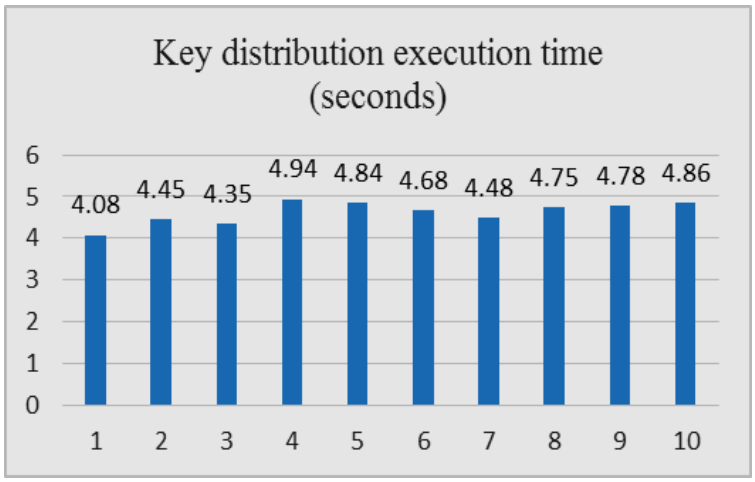

Figure 15. Performance of KDC Server

B. Encryption File

The performance of ABE algorithm in the Cloud Server was examined by using ten (10) encrypted text files with different file size. The test was done 10 times per file. The result is shown in Figure 16. As seen in Figure 16 that number 0 up to 9000 shows the file size in bytes, number 0 up to 6 shows the average execution time in seconds, while number 3 up to 12 shows the first trial until the tenth trial. Of course the bigger the file the longer it takes to perform file encryption.

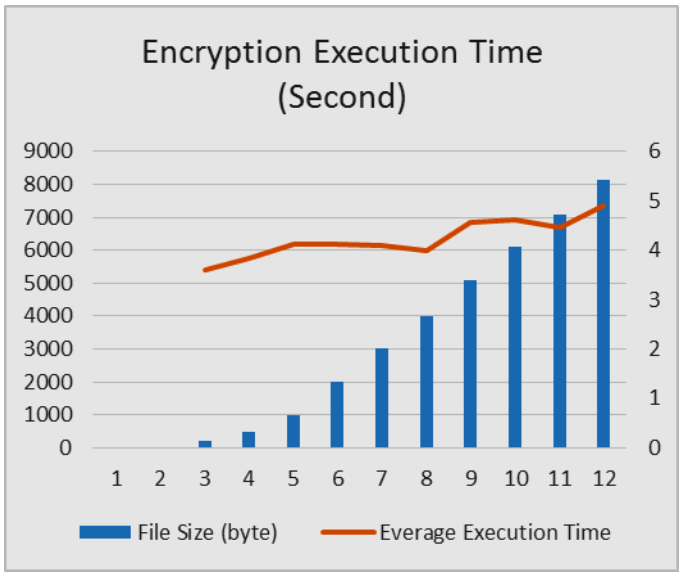

Figure 16. Performance of ABE Algorithm

C. File Decryption

The performance of ABS algorithm was examined by conducting several experiments on file decryption in the cloud. The test was done for 10 different files with different size, and it was performed 10 times per file. The tested files are the same as the files used in the encryption examination. Figure 17 shows the result that the larger the file size, the longer it takes to do the decryption.

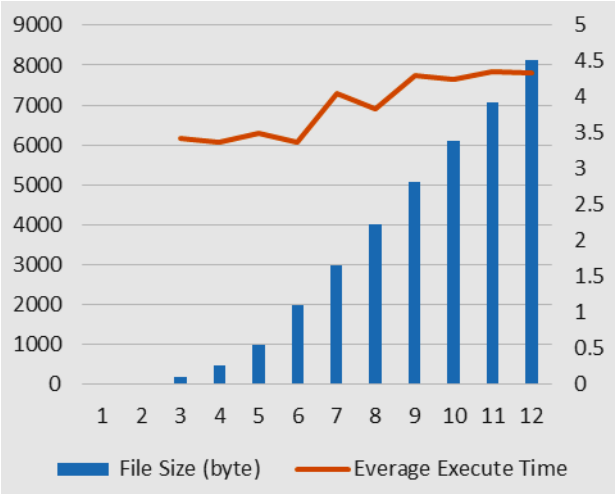

Figure 17. Performance of ABS Algorithm (in Seconds)

D. File Size Comparison

File size without encryption was compared with size of the decrypted file. Using the same files as above, an examination was conducted for 10 text files with different size, and it performed 10 times per file. Figure 18 shows that the file size before encryption is the same as the size of file after decryption.

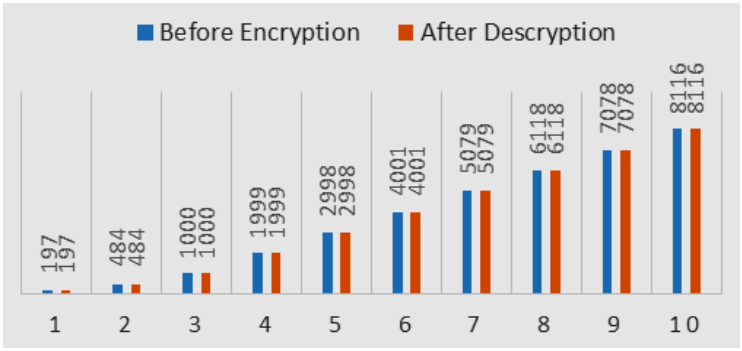

Figure 18. File Size Comparison before Encryption and after Decryption

6. Conclusion

In this study, KDC server and Cloud server have been developed to implement anonymous authentication. Then encryption process and file decryption have been build using Attribute-Based Encryption (ABE) algorithm and Attribute-Based Signature (ABS) algorithm in the Cloud Sever. The results showed that the encryption process and the file decryption performed fast with the average time of encryption of 4.2 seconds for a text file with size of 197 byte up to 8116 byte. While the decryption process spent an average

time of 3.9 seconds for the same file. Then the file size was the same before encrypting process and after decrypting process. Finally KDC server showed that it has good performance by distributing keys to the user in average of 4.6 seconds.

References

[1] C. Engineering, "Secure Data Storage using Decentralized Access Control with Anonymous Authentication Using Cloud," pp. 553–559,**(2015)**.
[2] "Privacy Preserving Authenticated Access Control with Decentralized Key Management in Clouds," vol. 2, no. 1, pp. 838–840,**(2014).**
[3] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," *2012 12th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. (ccgrid 2012)*, pp. 556–563, May **(2012)**.
[4] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, B. S. Lee, and Q. Liang, "TrustCloud : A Framework for Accountability and Trust in Cloud Computing TrustCloud : A Framework for Accountability and Trust in Cloud Computing," **(2011)**.
[5] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," *2011IEEE 10th Int. Conf. Trust. Secur. Priv. Comput. Commun.*, pp. 91–98, Nov. **(2011)**.
[6] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," *2013 Proc. IEEE INFOCOM*, pp. 2895–2903, Apr. **(2013)**.
[7] C. Science and M. Studies, "Cloud Computing," pp. 165–172,**(2015)**.
[8] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 384–394,**(2014)**.
[9] N. Karthika and S. Ranilakshmi, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds," pp. 186–188, **(2014)**.
[10] G. G. Nikhila, A. B. Pramida, P. Jyothsna, and K. Lavanya, "Anonymous Authentication of data storage in cloud computing administration with Decentralized Access," vol. 1, no. 4, pp. 195–198, **(2014).**
[11] P. R. Vyawhare and N. D. Ghuse, "Design and Implementation of User Anonymity and Authentication Scheme for Decentralized Access Control in Clouds : Review," vol. 3, no. 11, pp. 1857–1861, **(2014)**.
[12] S. Murthy, "Cryptographic Secure Cloud Storage Model With Anonymous Authentication And Automatic File Recovery," Pp. 844–849.
[13] "A Literature Survey On Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds Using Kdc," Vol. 3, No. 12, Pp. 1812–1817, **(2014)**.
[14] R. Ranjith and D. K. Devi, "Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication," vol. 2, no. 11, **(2013).**
[15] P. R. Vyawhare and P. N. D. Ghuse, "User Anonymous Authentication Scheme for Decentralized Access Control in Clouds," vol. 6, no. 3, pp. 2441–2447, **(2015)**.
[16] P. Palekar, A. Bharate, and N. Anjum, "A Secure Decentralized Access Control Scheme for Data stored in Clouds," vol. 3, no. 11, pp. 218–223,**(2014)**.
[17] M. Jain and M. Singh, "Identity Based and Attribute Based Cryptography : A Survey," no. 5, pp. 88–92, **(2015).**
[18] C. Science and M. Studies, "Cloud Based Intra-College Information Communication With Bluetooth Attendance System Using Mobile Clients," pp. 43–48, **(2015).**
[19] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," *Proc. 17th ACM Conf. Comput. Commun. Secur. - CCS '10*, p. 735, **(2010)**.
[20] S. Jahid and N. Borisov, "EASiER : Encryption-based Access Control in Social Networks with Efficient Revocation."
[21] C. Science and M. Studies, "Cloud Forensics : Need for an Enhancement in Intrusion Detection System," pp. 369–374, **(2015)**.
[22] M. George, C. S. Gnanadhas, and K. Saranya, "A Survey on Attribute Based Encryption Scheme in Cloud Computing," vol. 2, no. 11, pp. 4408–4412,**(2013)**.
[23] C. Lee, P. Chung, and M. Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments," vol. 15, no. 4, pp. 231–240, **(2013).**
[24] I. Journal, O. F. Engineering, A. S. On, A. Based, E. Techniques, And I. N. Cloud, "A Survey On Attribute Based Encryption Techniques In Cloud," Vol. 4, No. 1, Pp. 494–497, **(2015).**
[25] A. Sheshasaayee, "An Efficient Presentation of Attribute Based Encryption Design in Cloud Data," vol. 5, no. 2, pp. 943–946, **(2015).**

