International Journal of MC Square Scientific Research Vol.11, No.4,2019

Deduplication with Attribute Based Encryption in E-Health Care Systems

Amit Pandey[1], Gyan Prakash[2]

[1]Assistant Professor, College of Informatics, Bule Hora University, Bule Hora, Ethiopia ,Africa

[2]Explorer, Startup India, Government of India

&

Co-Founder, Emsoft Technologies, Chennai

E-mail:amit.pandey@live.com, gyanprakash.95@gmail.com

Abstract

Attribute Based Encryption (ABE) algorithm is the one of the most familiar one in cloud computing environment. While with the influence of data Deduplication technique is more effective to secure any kind of data bases. The existing system of this paper is based on Health Care Systems. In this system, large amount of data bases can be stored and retrieved day by day. So the problem arises in privacy module and storage module. Because in recent period, data's structure in health care system can be stored heavily. So it is vulnerable to Bruce force attack. In this paper, the proposed system is overcome the drawback of privacy and storage problem in Health care systems. Attribute based encryption with data Deduplication is the best way to avoid the privacy problems.

Keywords: Health care System, Deduplication, Attribute Based Encryption, privacy and storage problems.

1. Introduction

Uses of cloud computing in modern computer world had done a remarkable job of storing data's, sharing data's and outsourcing computation. It is a problem solving technique for many resources. Most of the problem came as privacy and storage issues in data's structure. In Health care system large amount of data's can be stored continuously in day by day. Data's in the system module are patient details, doctor details, medical report, appointment details and so on. So that kind of data's are must need privacy module and storage module to take care of patient infrastructure. In this proposed system with the use of ABE algorithm, we have concluded the problem of privacy and storage issues in health care systems. In this algorithm, the

process of Access Control and Digital Rights Management (DRM) to make a complete way of encrypting data's in such manner. According to deal with cloud computing services, the cost of efficiency also comes to small. That's why cloud server is the one of the best online services in the world right now.

2. Literature Survey

In [1] it proposed a scheme of privacy preserving key policy of de-centralized ABE scheme. It is used to rewrite the problem of privacy and storage issues with key generation. In [2] it acknowledges a scheme of CP-ABE and KP-ABE to provide a model of black box decryption. Both the scheme supported the model of traitor tracing, revocation and large universe. In [3] this paper modifies an ABE model and decryption technique with the use of key encapsulation mechanism. It is used to enforce the cipher text policy to overcome the drawback of attacked data's. In [4] the proposed work of this paper is archived by the way of white box traceability in Cipher text Policy Attribute based encryption. It is used for social network to enable the storing of large amount of data.

In [5] the process of sharing a hierarchical file in cloud computing is the proposed model of this paper. Then the hierarchical file was encrypted to cloud for DBDH assumption. In [6] the scheme of VMKS- ABE is applied in to this article. It is used for multi keyword search in Attribute Based Encryption. In [7] this paper describes the concept of Wild card policy in CP-ABE for AND gate constructions. In [8] the concept of Internet of Things (IOT) is used in this paper. Because it is used to support KS-ABESwET scheme for privacy and storage problems in keyword search. In [9] the process of sharing a data's in multiple groups in cloud computing storage devices is the proposed system of this model, it is used to distribute the key generation for protecting the data's from attacks.

In [10] multiple authorities for ABE algorithm to help a mobile social network in cloud computing services are the proposed model of this paper. In [11] the scheme of access controls policies to solve a key escrow issues. CP-ABE is the one who solved this issue with providing a free key escrow generation. In [12] the proposed model targets, the outsourcing of decryption process in ABE algorithm. It is used to split the decryption key for formatting the kind of approaching in cloud computing services. In [13] this paper guiding the elevation of multiple authorities reduces the trusted authority on single AA. In [14] MPRE-CPABE algorithm is used in this paper. By use of this algorithm it is used to perform the task of re-encrypting multi authority proxies. In [15] this paper discussing about the privacy of collaborative E-health System, the proposed model of this paper was overcome the drawback of privacy and storage issues by the help of Attribute based encryption in cloud computing environment.

By the influence of literature survey, we have witnessed some idea about the Attribute based encryption. The process of Attribute Based Encryption (ABE) is with the influence of data

access control to converting the Control Policies (CP) in to Access Policies (AP).When encryption key update the access policies by the practical demands, the process of de-duplication and access control will be supported. Then also supported the process of Digital Rights Management (DRM).some of the uses of DRM is

- It is the way of systematic approach to copyright the protection for digital media's support.
- In case you get the privacy from DRM, no other people to copy your data's from any resources.
- This service only based on expectations of data owner's only.
- This scheme will support CSP storage, when it stores only one copy of same data.

By storing de-duplication records in DRM, it will occupy some storage memory in that system. But the cost of comparing and storing a large de-duplication data is smaller than other services. For example...email system.

3. Proposed design

The process of making a secure E-Health system is the proposed system of this paper, with the influence of Deduplication in attributes Based Encryption model. In E-Health system a lot of databases have been stored frequently. The purpose of using data Deduplication is the only way to handle large amount of databases. While talk about privacy in E-Health systems, Data access control technique is used to overcome the drawback of this system. The implementation of this technique was mainly depending upon on the encrypted data's. Once the encryption was complete, data Deduplication process is come to fill the remaining part of the Attribute Based Encryption technique. Some of the important modules of E-Health Systems are

- Log in
- Appointment
- Doctor's
- Patient
- Report

The function of ABE algorithm with de-duplication process was efficient one to protect data's from the attackers. The experimental structure of ABE algorithm with E-health system has shown in the figure 3.1

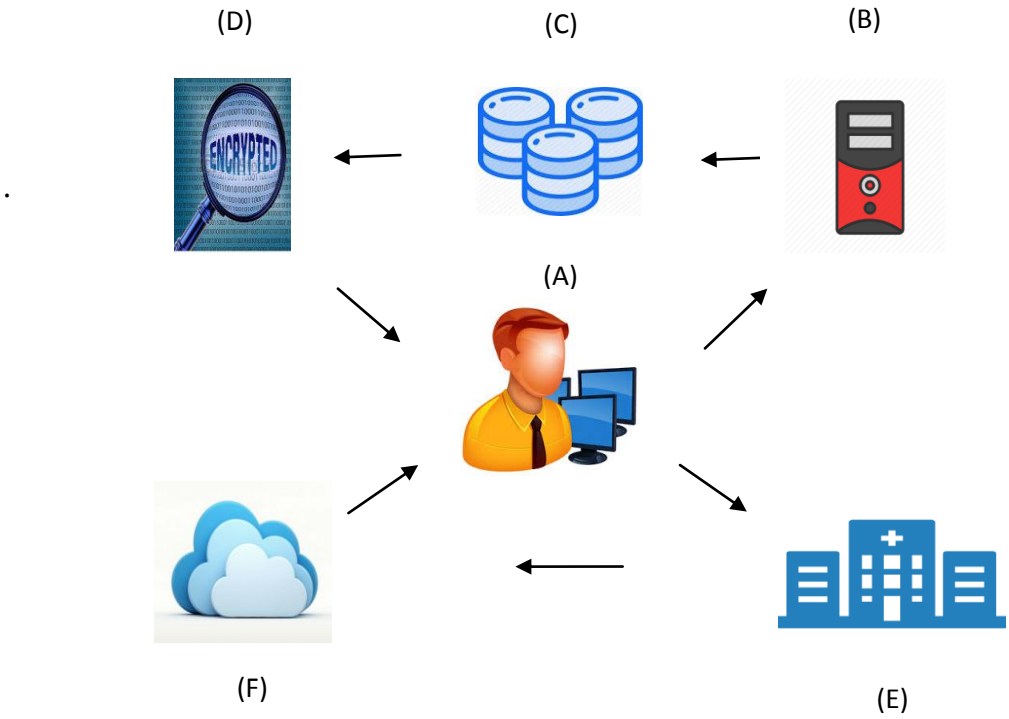

Figure. 1 Structure of secure E-Health System

Where (A) denotes the Admin server, (B) denotes the attribute key generation module, (C) denotes the modified E-Health System data, (D) denotes the encrypted modified data, and (E) denotes the E-H management System and (F) denotes the cloud data base.

4. Implementation steps

4.1 Log in

It is the first module of the E-Health System. In this module, it is used to register a patient log in form. After the procedure of complete the registration, that module admin provide a admit card for the E-Health System. That admit card is used to move the way of doctor's appointment fixing module. It include all the databases of patient registration.

4.2 Appointment

It is the second module of E-Health System. The process of this module was fixing the appointment of doctor's based on health problems. For instance a patient register a disease as eye problem, that module admin fix the appointment of eye doctor.

4.3 Doctor

This module gathers information about doctor's period of time that available in that hospital. It denotes how many doctor's worked in that hospital and how many specialist doctors currently available in that hospital also mentioned in that module.

4.4 Patient

After visiting the doctor's that admin module stores the information about patient details. It contains several number of databases can be stored and retrieved day by day.

4.5 Report

At the end of all the check up in hospital and consulting with doctor, that admin module provide a patient medical report and stored in a report databases in that module. In case sometime patient misses a medical report, that time with the use of this module, retrieved their medical report immediately. It also contains large amount of data bases.

5. Result and discussion

Development of Encrypting data's with the use of cloud computing has done a remarkable job of store and secure data's from vulnerable attacks. In E-health system before the arrival of encrypting technique, lot of problems had raised in that period. With the support of ABE algorithm and data Deduplication technique is used to overcome from those issues. Now days with the improvement of technologies, lot of advanced algorithm of encryption has developed. Some of the popular algorithm is Advanced Encryption Standard (AES) and Data Encryption Standard (DES).AES is more efficient than DES. Because, the Key length of AES is 128 bits, 192 bits and 256 bits instead of key length that available in DES are only 56 bits. Then number of rounds in AES are 10(128 bits), 12(192 bits), 14(256 bits) instead of DES have only 16 rounds of identical operations. AES was developed by Vincent risinen and Joan dawn.

Some of the important benefits of AES are

- Infrastructure is depended on substitution permutation network
- Rounds are based on Byte substitution, swift row, mix column and key addition.

- Plaintext of 128 bits can be encrypted in such manner.

It is the best example of cipher text policy. It was invented by the place of National Institute of Standards and technology (NIST).While talk about cipher text, some of the popular cipher used in cloud are substitution cipher-it is used to replace the plain text in to cipher text with the use of letters of single, double or triple. The design of AES algorithm has shown in the fig 2 and table 1 denotes the comparison of AES and modified AES algorithm. Talk about AES algorithm, that must discuss about the concept of DES,3DES,Blow fish and RSA algorithms.

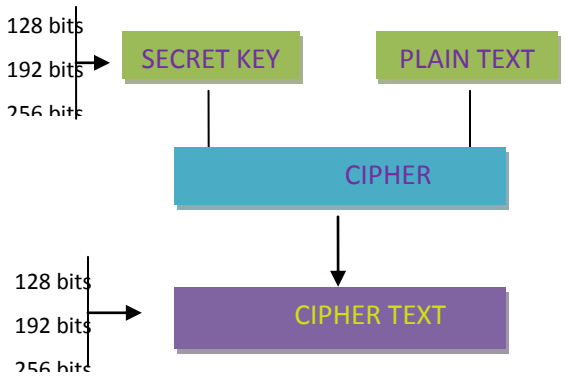

Figure. 2 Structure AES design

Table 1: Comparison of AES and modified AES algorithms

File Size	AES	Modified AES
128k	00:00:00:233	00:00:00:84
256k	00:00:00:607	00:00:00:156
512k	00:00:00:887	00:00:00:204

3Des is the process of cipher that encrypt the three time of its data. It is based on Feistal network algorithm. It is used to protect against Bruce force attacks. Blow fish is an another encrypted algorithm for replace the DES or IDES algorithms.RSA algorithm is the cryptography algorithm for asymmetric data's that used to process the private key and public key configuration. Fig 3 denotes the chart for file size calculation in 3DES,AES,DES,Blow fish and RSA algorithms.

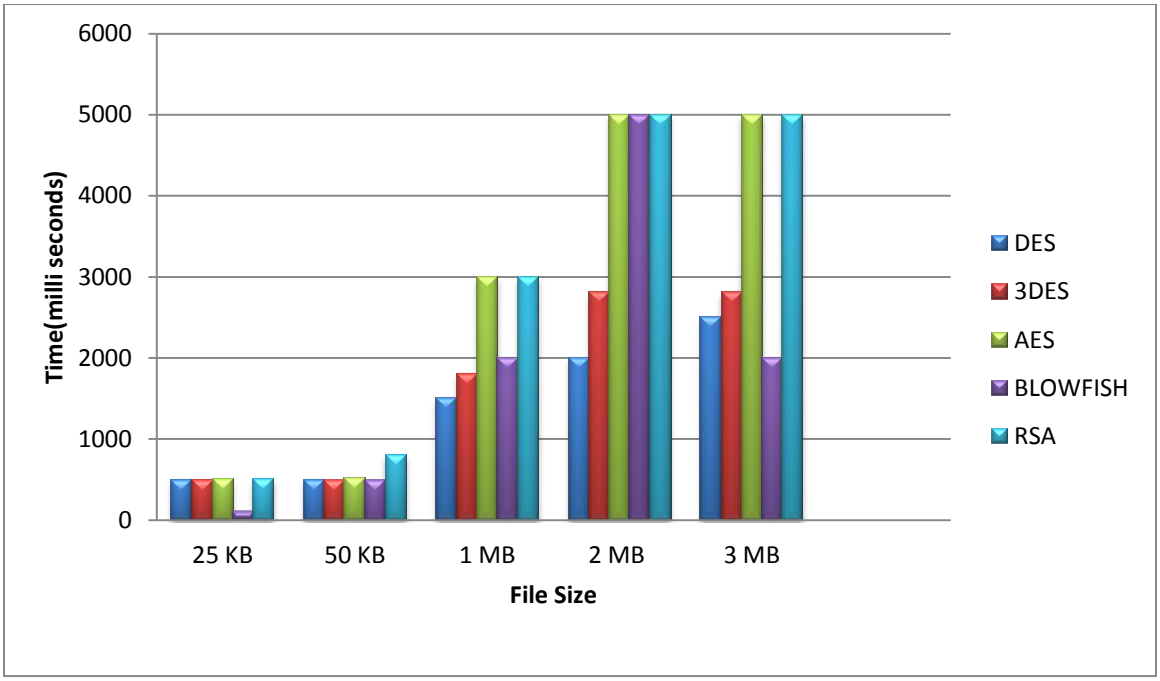

Figure. 3 File size chart for AES algorithm

6. Conclusion

Due to the process of Attribute Based Encryption (ABE) with Deduplication technique is helpful for most of the online web based application. In this paper it supported the progress of E-Health System environment with privacy and storage modules. In early days without the help of encrypted algorithms, data's are vulnerable to Bruce force attack, due to the reason of large amount of repeated data's in management system. Deduplication technique is overcome the drawbacks of repeated data's in database environment. The likes of E-Health system is should needed on privacy module. Because it contains patient medical reports, patient databases, doctor's details etc…once the information's are hacked it will be a bigger problem of this society right now. So security and storage module is very important one to develop a E-Health organization System.

References

1. Ge, Aijun, et al. "Security analysis of a privacy-preserving decentralized key-policy attribute-based encryption scheme." IEEE Transactions on Parallel and Distributed Systems: 2319-2321, 24.11 (2012).

2. Liu, Zhen, and Duncan S. Wong. "Practical attribute-based encryption: traitor tracing, revocation and large universe." The Computer Journal 59.7 pp: 983-1004.2016.

3. Surjati, 3. Lin, Suqing, et al. "Revisiting attribute-based encryption with verifiable outsourced decryption." IEEE Transactions on Information Forensics and Security: 2119-2130, 2015.

4. Liu, Zhen, Zhenfu Cao, and Duncan S. Wong. "Traceable CP-ABE: how to trace decryption devices found in the wild." IEEE Transactions on Information Forensics and Security: pp.55-68. (2014).

5. Bah, 5. Wang, Shulan, et al. "An efficient file hierarchy attribute-based encryption scheme in cloud computing." IEEE Transactions on Information Forensics and Security 11.6 pp: 1265-1277.2016.

6. Wang, S., Jia, S. and Zhang, Y., "Verifiable and Multi-Keyword Searchable Attribute-Based Encryption Scheme for Cloud Storage". IEEE Access, 7, pp.50136-50147,2019.

7. Phuong, Tran Viet Xuan, Guomin Yang, and Willy Susilo. "Hidden ciphertext policy attribute-based encryption under standard assumptions." IEEE transactions on information forensics and security 11.1 pp: 35-45 2015.

8. Wang, Shangping, et al. "KS-ABESwET: A Keyword Searchable Attribute-Based Encryption Scheme with Equality Test in the Internet of Things." IEEE Access 7 pp: 80675-80696. 2019

9. Xiong, Hu, Hao Zhang, and Jianfei Sun. "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing." IEEE Systems Journal 2018.

10. Luo, Entao, Qin Liu, and Guojun Wang. "Hierarchical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks." IEEE Communications Letters 20.9 pp: 1772-1775, 2016

11. Xia, Zhihua, Liangao Zhang, and Dandan Liu. "Attribute-based access control scheme with efficient revocation in cloud computing." China Communications 13.7 pp: 92-99, 2016

12. Qin, Baodong, and Dong Zheng. "Generic Approach to Outsource the Decryption of Attribute-Based Encryption in Cloud Computing." IEEE Access 7 pp: 42331-42342,2019

13. Cui, Hui, and Robert H. Deng. "Revocable and decentralized attribute-based encryption." The Computer Journal 59.8 (2016): 1220-1235.

14. Xu, Xiaolong, et al. "Multi-authority proxy re-encryption based on CPABE for cloud storage systems." Journal of Systems Engineering and Electronics 27.1 pp: 211-223, 2016.

15. Edemacu, Kennedy, et al. "Privacy Provision in Collaborative Health with Attribute-Based Encryption: Survey, Challenges and Future Directions." IEEE Access 7 pp: 89614-89636, 2019