Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.534 – 540

SECURE AND VERIFIABLE DATA TRANSFER WITH ENCRYPTION TECHNIQUE

G.Geetha Mounika[1], A.Persis[1], A.Sowjanya[1], A.LeelaSaiKrishna[1], Ch.Vijayananda Ratnam[2]

[1]UG Scholar, Department of Computer Science & Engineering, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India
[1]mgitak@gmail.com
[2]Associate Professor, Department of Computer Science & Engineering, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India
[2] vijayanandaratnam@gmail.com

***Abstract:** Now a days hackers are increasing day to day rapidly. As more sensitive data is shared and stored by third-party on the internet, to provide security to that data, there will be a need to encrypt data stored at these sites. Previously there are various techniques proposed but in that computation costs are high to decrypt the data. In this proposed system the computational costs are reduced and to provide more security to the files an encryption technique is used and also a new key is generated whenever the user want to access the same file.*

***Keywords:** Encryption, Security, Blowfish Algorithm, Confidentiality*

I. INTRODUCTION

There is a trend for sensitive user data to be stored by third parties on the internet. For example personal email, data and personal preferences are stored on web portal sites such as google and yahoo. In distributed settings with untrusted servers, such as the cloud many applications need mechanisms for complex access control over encrypted data.Traditionally, encryption is a method in which user encrypts data to another specific targeted party and only the targeted recipient can decrypt this message. Due to the attack of third parties it becomes imperative to have a mechanism for encrypting data according some access policy. Attribute Based Encryption is a new vision of public key encryption in which user is allow to encrypt and decrypt based on some attributes. The problem with existing ABE system is that the decryption involves expensive pairing operations and the number of pairing operations required to decrypt a cipher text grows with the complexity of the access policy. In order to overcome the decryption overhead we are proposing the outsourced decryption mechanism. The user provides a transformation key to the cloud and the cloud uses this key to transform the cipher text into simple cipher text which possess simple steps of computation. Also correctness is essential while transmitting the data from the cloud to the user. This ensures whether the requested file is retrieved to the user. Moreover hash chain mechanism is used for identifying data modification that can be occurred in cloud. Each data is stored in clouds along with random hash blocks and these hash blocks are checked during decryption in order to identify the modification.

II. RELATED WORK

Previously there are various schemes. The main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive due to pairing operations and the number of pairing operations required to decrypt a cipher text involves high complexity. Hohenberger and Waters succeeded in reducing the decryption requirements to two pairings and two exponentiations by making tradeoffs in the private key size. Green introduced outsourced decryption into ABE systems such that most of complex computation of decryption algorithms is outsourced to an untrusted third-party service, leaving only a smaller overhead for users to recover the plaintext.

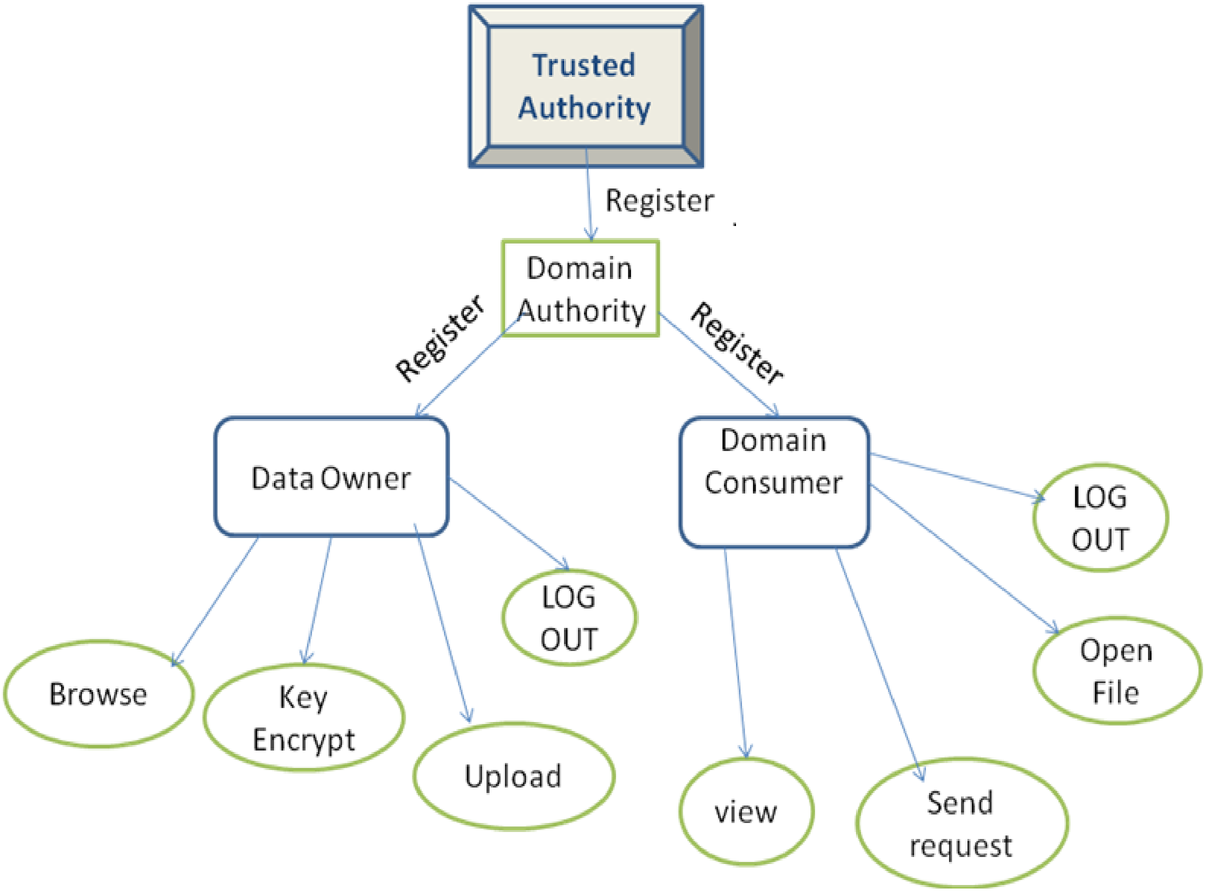
III. PROPOSED WORK

The proposed work is intended to provide the security to the transfer of data. It generates the individual key for every file access. It provides more security. It reduces the computation costs when compared to the existing system. In proposed system whenever the data uploaded on cloud the data will be encrypted. If the user want to access the file they need to request the owner for the key to decrypt the file. The owner verifies the requested person is authorized or not. Then send a key to him. The user can send request to the owners currently who is available only. The user want to revisit the file then the old key is not valid. He has to request for key again because one key valid one time only. If the user access the file with the key then the key changed for another time file access. This is because to provide more secure and confidential data transfer between distributed systems.

Advantages:

- Reduces the computation cost
- Provides more security
- Generates a new key for every file access

System architecture:



Class Diagram:

Class Diagram consists of the classes and the objects and the interaction between them. It mainly deals with the interaction between classes in the system, their behavior and properties of the system. Apart from classes this also provides inheritance relationships in the project. Class diagrams consist of basically two parts: first one is the member variables and class variables and the second part consists of the total number of methods available in the class.

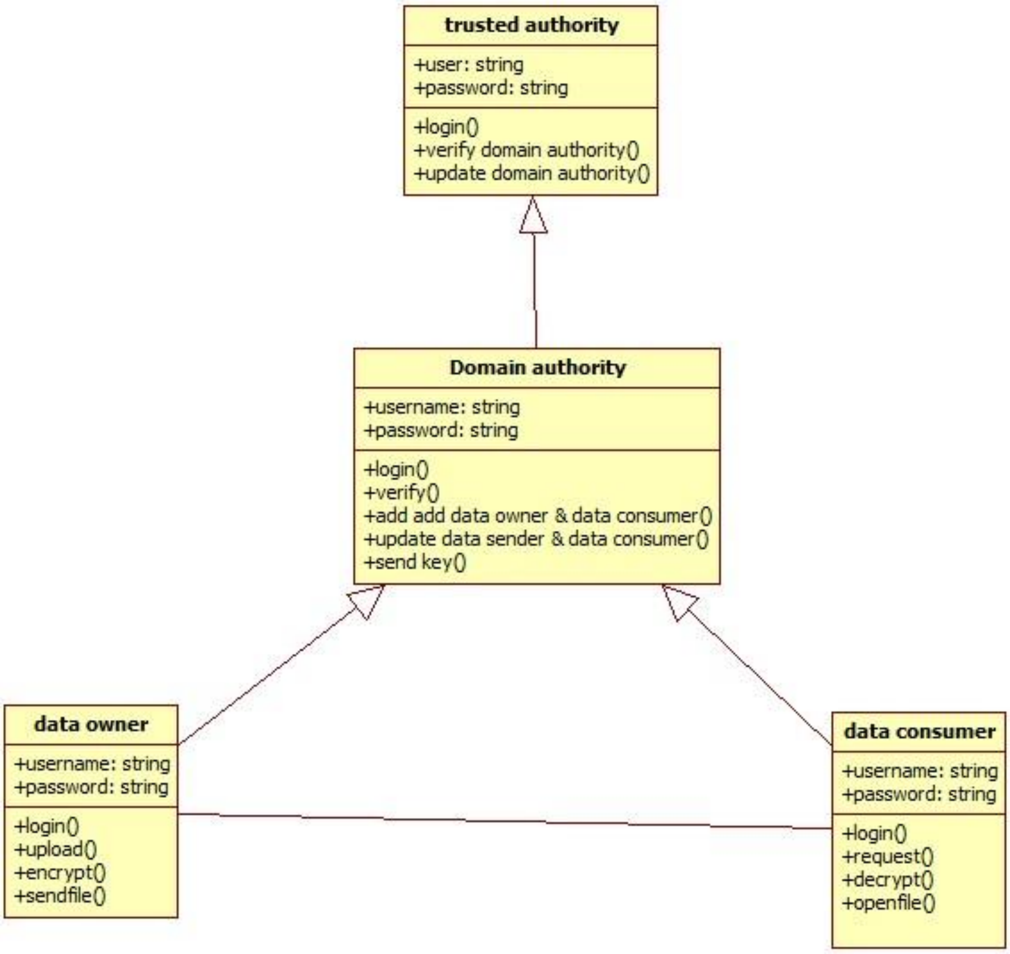
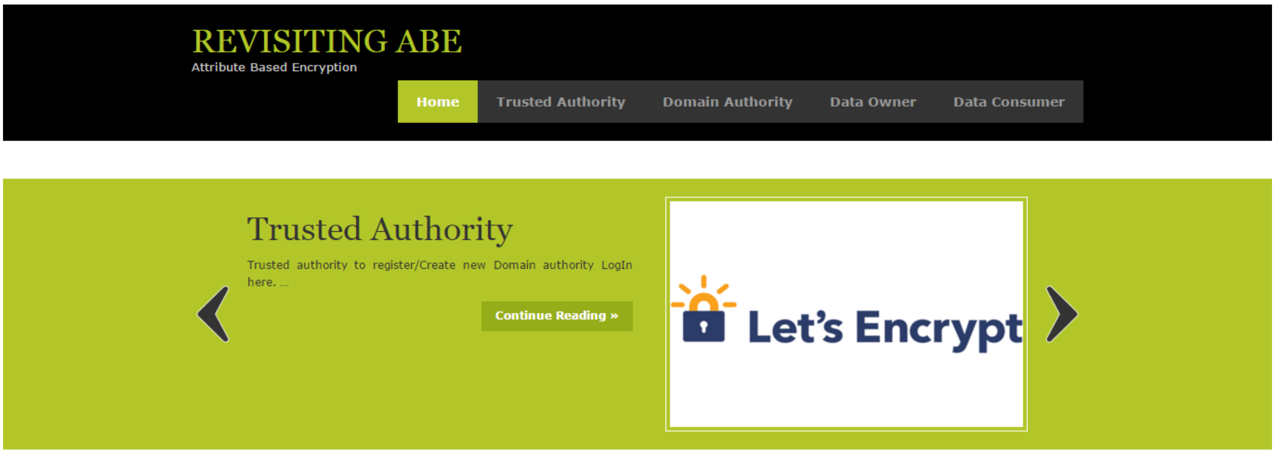


Fig 3.1 Class diagram for proposed work

IV.RESULT & DISSCUSSIONS

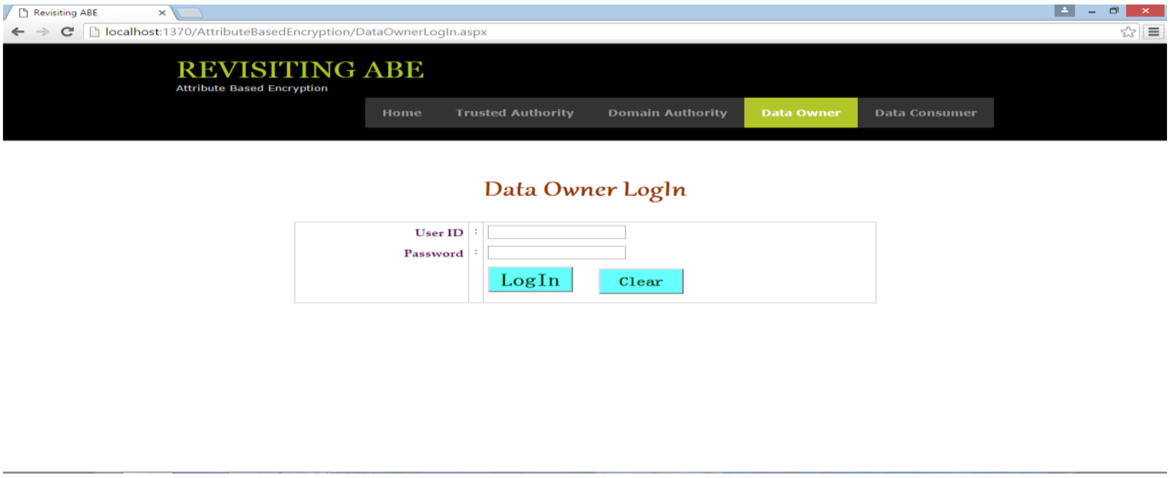
Figure 1:Home page



Trusted Authority

Trusted authority to register/Create new Domain authority LogIn here. ...

Figure 2: Login page

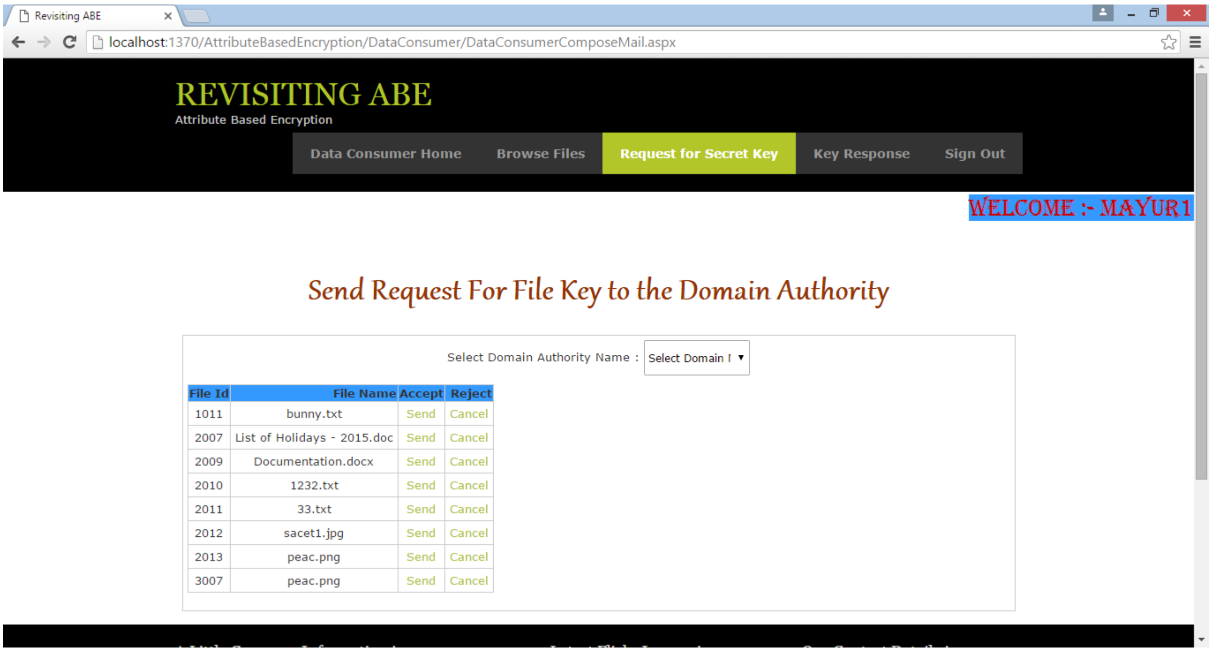


Data Owner LogIn

User ID :

Password :

Figure 3: Requesting for Secret key to view the File:

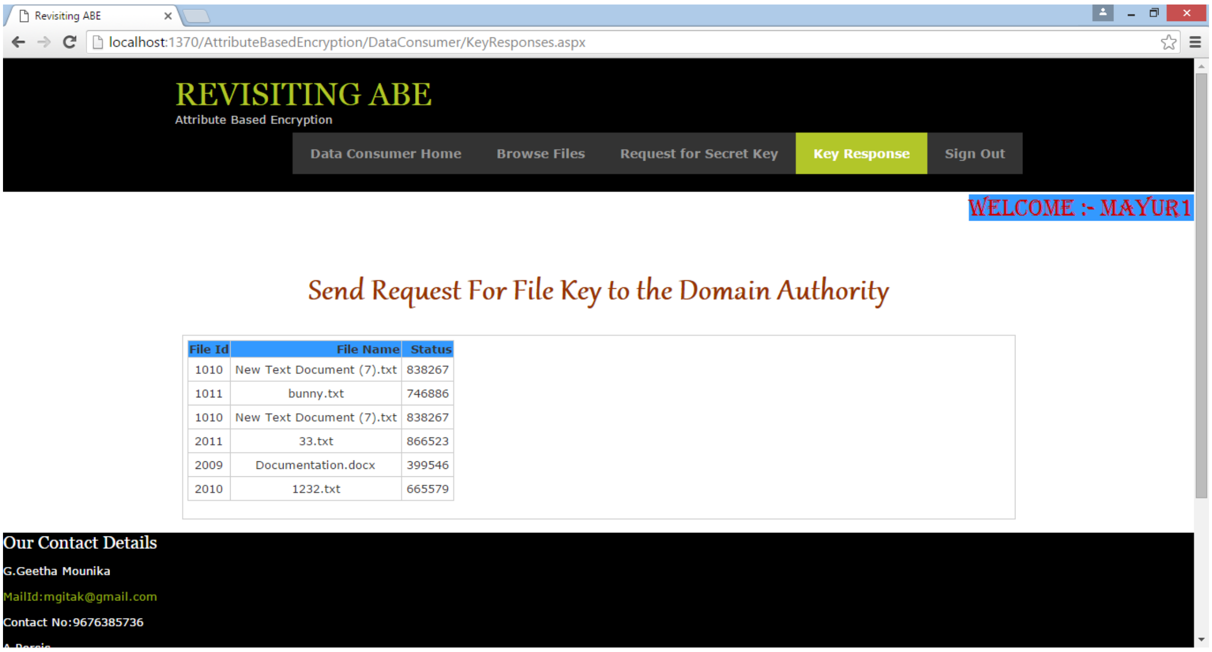


Send Request For File Key to the Domain Authority

Select Domain Authority Name : Select Domain I ▾

File Id	File Name	Accept	Reject
1011	bunny.txt	Send	Cancel
2007	List of Holidays - 2015.doc	Send	Cancel
2009	Documentation.docx	Send	Cancel
2010	1232.txt	Send	Cancel
2011	33.txt	Send	Cancel
2012	sacet1.jpg	Send	Cancel
2013	peac.png	Send	Cancel
3007	peac.png	Send	Cancel

Figure 4: Status of key



WELCOME :- MAYUR1

Send Request For File Key to the Domain Authority

File Id	File Name	Status
1010	New Text Document (7).txt	838267
1011	bunny.txt	746886
1010	New Text Document (7).txt	838267
2011	33.txt	866523
2009	Documentation.docx	399546
2010	1232.txt	665579

Our Contact Details

G.Geetha Mounika

MailId:mgitak@gmail.com

Contact No:9676385736

V. CONCLUSION & FUTURE WORK

In previous system there is no individual key for every accessing of file by the Data consumer. By using symmetrical algorithm, we can able to provide the individual encrypted key for every accessing of file by the Data consumer. By using this algorithm we can able to provide more security with the use of revisiting and efficiency by reducing the computational costs. In future our project is going to be used in various organizations. For the storage of confidential files our project is very useful. Our project can be used for the storage of personal information/company/country's confidential matters.

REFERENCES

[1] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 195–203.

[2] B. Waters, "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, 2011, pp. 53–70.

[3] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. EUROCRYPT, 2010, pp. 62–91.

[4] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in Proc. CRYPTO, 2010, pp. 191– 208.

[5] A. B. Lewko and B. Waters, "Unbounded HIBE and attribute-based encryption," in Proc. EUROCRYPT, 2011, pp. 547–567.

[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertextpolicy attributebasedencryption,” in Proc. IEEE Symp. Security and Privacy, 2007, pp. 321–334.

[7] L. Cheung and C. C. Newport, “Provably secure cipher text policy ABE,” in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 456–465.

[8] Y. He and Z. Han, “User Authentication with Provable Security against Online Dictionary Attacks,” J. Networks, vol. 4, no. 3, pp. 200-207, May 2009.

[9] S. Hohenberger and B. Waters, “Attribute-based encryption with fast decryption,” in Proc. Public Key Cryptography, 2013, pp. 162–179.