ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Authenticated File Access using Random Key Encryption via message as OTP

Shifani [1], J. V. Gorabal [2]

P.G. Student, Department of Computer Science and Engineering, Sahyadri College of Engineering and Management, Adyar, Mangalore, India[1]

Associate Professor, Department of Computer Science and Engineering, Sahyadri College of Engineering and Management, Adyar, Mangalore, India[2]

ABSTRACT: Most of the sensitive data is either stored or shared over the network by using third-party authorities. Hence there exists a need for data encryption stored on these authorities. One of the common drawbacks that occur in network security is to encrypt the data by using private key that is being shared by another party. In such case, the private key that is being used for encryption must be kept secure so that an unauthorized person would not be able to obtain any of the private key. In this proposed system, we develop an application in which the sender sends his confidential data or files by encrypting the data or files to the other authenticated user. The receiver can then retrieve the file by using the One-Time-Password. The proposed system provides an efficient technique to upload the file and to retrieve the file.

KEYWORDS: File Upload, File Retrieval, One-Time-Password (OTP).

I. INTRODUCTION

The network is mainly used to connect people who reside in very distant place. Due to network people can connect to each other via messaging one another or by talking over cell phones. The two users who communicate with each other reside in two ends of network. Hence a connection has to be established between them. File sharing is a private or public sharing of computer data or space in a network with various levels of access privilege. File sharing allows a many number of people to use the same file by combining the features of being able to read or view it or to modify it.

In networking, the internet service models is based on few critical assumptions such as (i) there need to be existence of an end to end path connection between source and destination pair, and (ii) there must be a lower value of round trip latency between any pair of nodes. However, these assumptions do not hold in some emerging networks. The main issue in networking is its security; it mainly deals with how the network is kept secure from being pruned to security attacks. In military network scenarios, connection of the wireless devices that are carried by the soldiers and commander may be not be permanently connected due to signal jamming, moving of mobile devices especially when they need to be operated in remote environments. Most often, when there do not exists end-to-end connection between a source and the destination pair, the messages from the source node may have to wait in the intermediate nodes for quite period of time until the connection is fully established.

The proposed system provides an efficient method by which one user can send message to another user by encrypting the message while sending it, and another user would download the message by decrypting the message and then downloading the file or message that was sent.
In early days, when the sender sends confidential messages to the receiver over network, the sender would not ensure its security.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

As the days passed, scientist and researchers found a method to secure the message over network and they named this method as cryptography. Cryptosystem is a technique that allows a user to encrypt the message from being misused by unauthorized users.

II. RELATED WORK

In military network, Roy [4] and Chuah [5] used the concept of Disruptive Tolerant Network (DTN) wherein storage nodes were used to store or replicate the data so that unauthorized users or mobile nodes are not allowed to access the necessary information quickly [1].
Most of the applications developed for military applications require increased security of confidential data which included access control mechanisms that were cryptographically enforced [6]. Some access services were provided such that data access policies are defined over user attributes or roles, which were managed by key authorities.
The concept of attribute-based encryption (ABE) [7]-[8], this features a mechanism that enabled an access control over the data encrypted using access policies. However, the problem that arose by applying ABE to DTNs had introduced several security and many privacy challenges. Since some of the users might wish to change their associated attribute by some point, some of the private keys must be compromised, key revocation for every attribute was necessary to ensure that the system is secure.

The work in this paper is divided into two stages. 1) File Upload after encryption 2) File download after decryption. The file is uploaded while the message is being composed and sent to another user. Meanwhile, before sending message, the file is encrypted. On other hand in receiver side, the file is downloadable only after the receiver obtains a secret password that is One Time Password (OTP) via message. The encryption technique used is Standard AES algorithm which makes use of 128 bits.
Paper is organized as follows. Section II describes the message being composed, how the message is encrypted and being sent. The message is being retrieved on the receiver end, after the receiver obtains secret password via message as OTP. The flow diagram represents the system architecture and the modules that are present in the proposed system. Section III describes the proposed system, Section IV describes the analysis of the proposed system, and Section V describes conclusion and future scope.

III. PROPOSED SYSTEM

The confidential message that is sent by sender to the receiver has to be encrypted before sending it. The sender has to select a file from the computer system and upload it before he sends it to the receiver. The file has to be encrypted by using AES algorithm.
The AES algorithm follows few steps:
Step 1: Get Random Key as input.
Step 2: The Key length of the Random Key is noted and it is converted into its byte format.
Step3: The Encryption function takes 2 inputs, filename and the Random Key RK1 i.e ENCRYPT (FILENAME, RK1); returns an output with random alphanumeric characters.
Step 4: The file is now encrypted and sent to the user.
Step 5: In the receiver end, Second Random Key RK2 is generated. This RK2 is sent to receiver as message via OTP.
Step 6: The RK2 is encrypted again using RK1 i.e ENCRYPT (RK2, RK1). This encryption technique is used as a method for decryption.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

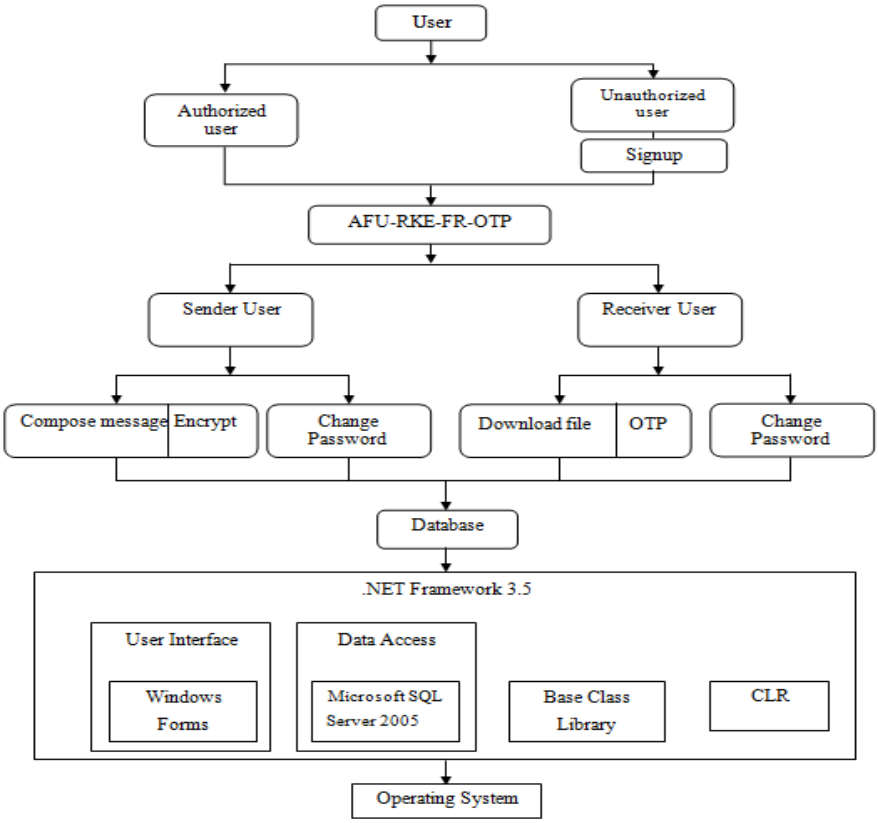

Fig (a)

Fig(a): System architecture shown above depicts the flow of implementation of the application. Authorized sender user sends encrypted message to the user, who will receive the message and download the file via OTP.

In the proposed system, the authenticated user can send message to another user who is also authenticated. The system architecture is shown in the above figure fig (a). When the sender sends message he encrypts the filename and sends it to the user. The user can view the message and download the message only after he obtains the message via OTP. OTP is One-Time-Password that is used to confirm the authenticity of the user. There would be timestamp for entering this OTP. If the user delays in entering OTP, he does not get access to download the file. Thus authenticity of the receiver user is maintained and message is kept secure from unauthorized access.

IV. EXPERIMENTAL ANALYSIS

The sender would compose the message to the receiver, by uploading the file and upon sending the filename of the file will be encrypted. The receiver can view and download the file only by entering the correct OTP. Once the entered OTP is valid, then the receiver selects the destination to download the file.

In this section, discussion about the existing systems its advantages and disadvantages are made. By considering the features of previous existing systems a brief analysis on how the proposed system is better that the existing system is discussed in Table I as shown below.

i) The first feature is Independent Authenticity: In the existing system, multiple users have to co-inside to perform any single task. Whereas in the proposed system, single user can any perform task.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

ii) The second feature is File-route level encryption: In the existing system the file route level encryption is partially done. Whereas in the proposed system, the file route level encryption is done completely.

iii) The third feature is Usage of master secret key: The existing system makes use of master secret key to encrypt the key. Whereas in the proposed system, the key is encrypted using another randomly generated key.

Features	Existing System	Proposed System
Independent Authenticity	No	Yes
File route-level Encryption	Partially	Complete
Usage of Master Key	Yes	No
OTP	No	Yes
OTP timestamp	No	Yes
User Collusion to Decrypt	Multiple users	Single user

Table I : Analysis based on the features of existing system and proposed system

iv) The fourth feature is OTP: The existing system does not make use of the concept of OTP, but proposed system uses OTP for authentication.

v) The fifth feature is OTP Time stamp: The existing system does not make use of OTP. Whereas the proposed system makes use of the OTP and the lifetime of this OTP is very important aspect. Once the lifetime expires, the OTP will be invalid.

vi) The last feature is User collusion: In the existing system multiple users had to collude to decrypt a message. Whereas the proposed system makes use of only single user to decrypt the complete message.

V. CONCLUSION AND FUTURE SCOPE

The proposed system provides a secure and encrypted mechanism to send file and to retrieve the file over the network. Usually, in remote area where there does not exist an end-end connection between two systems, in such cases the proposed system provides an efficient mechanism that allows two users to access this application, provided they would have network connection that allows users to access the database information. The admin database is created, which gives access only to the admin and no other users can access the database. Thus the data is kept secure from unauthorized access. The database information is kept secure from unauthorized access and only authorised user can access the information wisely.

This paper deals with encrypting the name of the file. Whole message details are encrypted by considering the filename as a parameter in the encryption algorithm. In future, file path and the complete file can be encrypted and sent to the receiver. Also, one can adopt the technique of message retrieval by sending OTP via mails.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang,"Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE TRANSACTIONS ON NETWORKING, VOL:22 NO:1 , pp1-11, 2014.
[2] P.Bhavana and Yugandhar Garapati," Secure Data Retrieval For Decentralized Disruption Tolerant Military Network", International Journal & Magazine of Engineering, Technology, Management and Research, vol2,issue 3,ISSN No: 2348-4845,pp 247-254, 2015.
[3] C. Rajeshwar Reddy1, N.V. Sailaja,"Secure Data Retrieval Using CP-ABE for Decentralized Disruption Tolerant Military Networks",International Journal of Computer Science and Information Technologies, Vol. 6 (5) ,pp 4201-4205 ,2015.
[4] Vipul Goyal, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", pp 1-28,2010.
[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Cryptology ePrint Archive: Rep. 2010/351, 2010.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

[6] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular adhoc networks," Ad Hoc Netw., vol. 7, no. 8,pp. 1526–1535 , 2009.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *ACM Conf. Comput. Commun. Security*, pp. 89–98, , 2006.
[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc.Eurocrypt*, pp. 457–473, 2005.
[9] www.indi.ca.