Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

File Keyword Based Search Over Encrypted Data

A. Saleem[1], G. Priyanka[2], P. Archana[3], M. Sharanya[4]

[1]*Assistant Professor, Computer Science and Engineering, BVRIT Hyderabd College of Engineering for women*
[2,3,4]*Computer Science and Engineering, BVRIT Hyderabd College of Engineering for women*

Abstract — *This paper presents a searchable encryption mechanism over encrypted data stored in traditional databases. We focus on secure storage using Advanced Encryption Standard (AES) and information retrieval by performing keyword search on this encrypted data and MD5 algorithm to secure the personal information of the user and owner.*

Keywords- *Search, AES, MD5, File, Keyword, Encryption, Decryption, Security, Encode, Decode,*

I. INTRODUCTION

As more and more information is stored in traditional databases such as emails, documents, phone numbers and so on. By storing their data in databases data owner is relieved from carrying the documents, and from maintaining them. Data owners and database server are not in the same trusted domain, they may put the outsourced data at risk, as the database server may no longer be fully trusted. It follows that sensitive data usually should be encrypted prior to outsourcing for data privacy and combating unsolicited accesses

In this paper, we focus mainly on three things. First one is encrypting passwords using MD5 before it can be stored in the database. Most of the web sites require users to register before they could use the website. As a result, most websites store user's password as plain text in the database or any file. Anyone with some efforts can get to the password. Second one is encrypting File path and keywords using AES, before it can be stored in the database and the last one would be keyword search over encrypted data while maintaining keyword privacy. By employing keyword search the usability of our system is enhanced. Users can search their text with possible values and get the desired result when exact keyword matches other-wise failure. This failure of exact keyword could be because of some spelling or morphological error

II. EXISTING SYSTEM

The data must be encrypted before stored in database to protect the files from intruders but the encryption restricts the power of the user and makes the traditional plaintext scenario not suitable for cloud. Beside this, data encryption it demands the protection of keyword privacy, that makes the plaintext search technique unsuitable in encrypted files. There are many existing systems which are implemented using Data Encryption Standard (DES) algorithm.

III. PROPOSED SYSTEM

We found that Advanced Encryption Standard(AES) is more secure , supports larger key size and six times faster than DES algorithm. So, we have chosen this AES algorithm to secure the keywords and file path in our paper and a searchable encryption mechanism.

3.1. Advantages

We focus on enabling effective yet privacy preserving keyword search in traditional databases.

3.2. Application

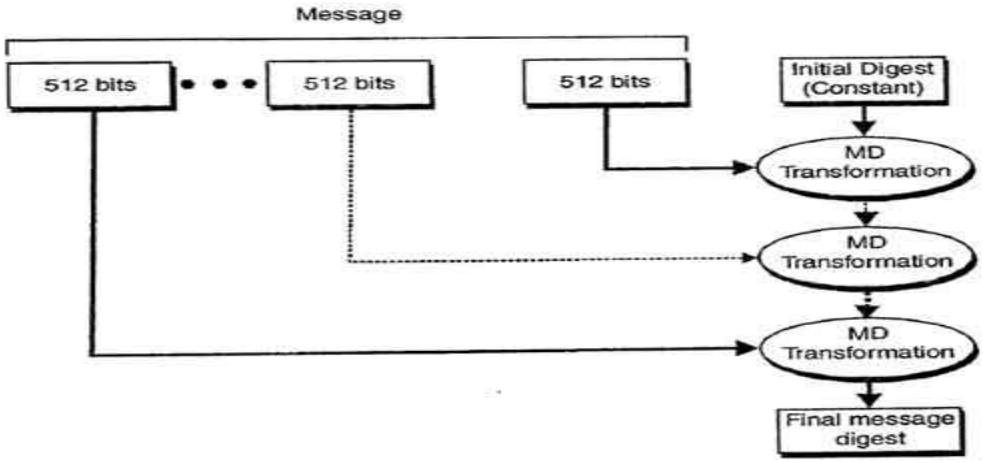
This is used in mobile healthcare application where the resource of memory, computation and connectivity are extremely limited.

IV. IMPLEMENTATION

First of all, the user initiates a request to the owner of the file to register on the portal . The owner then allows the user to register as a new user on the portal. The password is encrypted using MD5 algorithm before it is stored in the database. Once the user is registered, then he/she can easily login by providing the login credentials. All the users are managed by the owner and the credentials are matched from those saved in the database.

ALGORITHM: **Message digest algorithm (MD5)**

The MD5 algorithm is a widely used hash function producing a 128-bit hash value. "The MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA."



Generation of message digest using MD5.

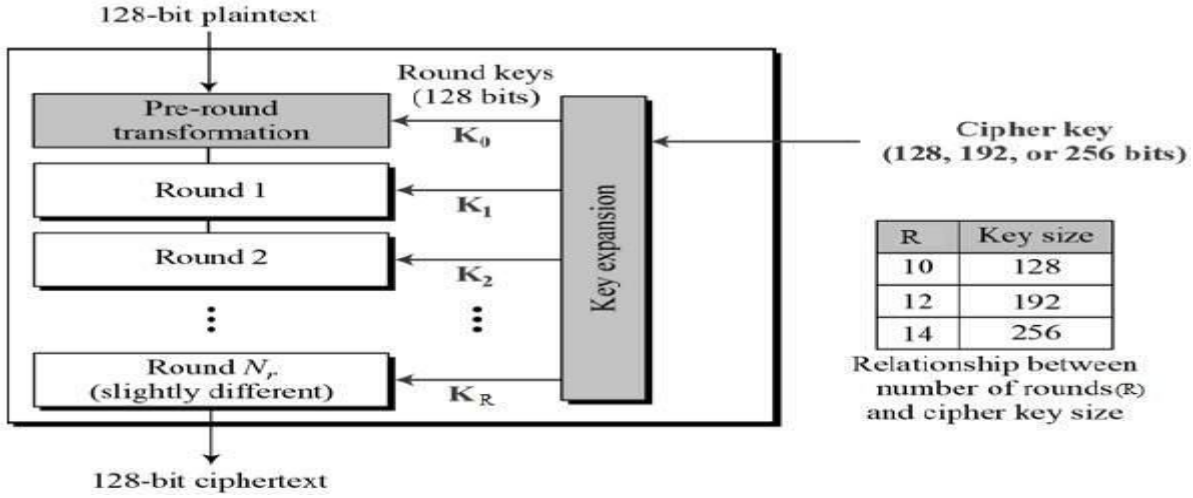
A registered user can upload any file which follows the guidelines set by the owner. While uploading a file, a keyword is to be specified for the file which is used for searching the file. The user can upload as many files as he/she wants but each and every file must have a unique keyword. As soon as the file is uploaded, the system encrypts the keyword specified by the user using AES (Advanced Encryption Standards) algorithm.

ALGORITHM: Advanced encryption standard

AES is based on Rijndeal Cipher and works on the substitution permutation network principle and uses a 128-bit key for encryption. All these features make AES extremely secure and accomplishes the first requirement of searching that is 'security must never be compromised'.

Features:

- Symmetric key symmetric block cipher
- supports larger key sizes than 3DES's 112 or 168 bits.
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java
- AES is required by the latest U.S. and international standards
- AES's 128-bit block size makes it less open to attacks via the birthday problem than 3DES with its 64-bit block size.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

A user can search a file by the help of the keyword used to upload the file. As soon as the user enters the keyword, the system again matches it with that of the files stored on the server. After this, the server sends the files that match with the keyword provided. System then decrypts the results that are provided by the system. The user, hence gets the relevant files and can easily choose the file he required from the provided list of files.

V. CONCLUSION

In this paper, we formalize and solve the problem of supporting efficient yet privacy preserving file keyword search for achieving effective utilization of encrypted data. The proposed system helps in accomplishing the task in a simple and yet efficient manner. It also enhances the overall performance by increasing the speed of the operation.

VI. SCOPE FOR FUTURE ENHANCEMENT

As a future work, we will continue to work on search semantics that takes into consideration conjunction of keywords, sequence of keywords, and even the complex nature language semantics to produce highly relevant search results.

VII. REFERENCES

[1]N. Raghavendrasai, Innovative Journal, Available: http://www.innovativejournal.in/index.php/ajcsit.

[2] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposiumon Security and Privacy'00, 2000.

[3] S. Ji, G. Li, C. Li, and J. Feng, "Efficient merging and filtering algorithms for approximate string searches",in Proc. Of ICDE' 08, 2008.

[4] Abha Sachdev, Mohit Bhansali Enhancing Cloud Computing Security using AES Algorithm, International Journal of computer Applications, volume 67, issue 9, 2013.

[5] Techniques for Efficient Keyword Search in Cloud Computing , P.NiranjanReddy,Y.Swetha ,Department of CSE , Kakatiya Institute Of Technology & Science, Warangal Dist-506002,India.

[6] Fuzzy Keyword Search over Encrypted Data in Cloud Computing Jin Li, Qian Wang, Cong Wang†, Ning Cao ‡, KuiRen †, and Wenjing Lou‡ †Department of ECE, Illinois Institute of Technology ‡Department of ECE, Worcester Polytechnic Institute Email: †{jinli, qian, cong, kren}@ece.iit.edu, ‡{ncao, wjlou}@ece.wpi.edu

