ISSN: 2456-9348
Vol (03) _Issue (12) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

AN EFFICIENT ENCRYPTION METHOD FOR SECURING ACCESS TO CLOUD DATABASE

Swati Vithal Khidse [*1]
Dr. Santosh S. Lomte[2]
*[1]Ph.D Research Scholar, Department of Computer Science & Engg, Aurangabad, Maharashtra
[2]Radhai Mahavidhyalaya, Aurangabad, Maharashtra, India

ABSTRACT
Cloud computing is growing enormously in public and private sector organization. With the increase in number of users of cloud, there are so many concerns that need to be look out. One such major concern is about security and privacy of data being stored in cloud database. When the user is accessing his data from the cloud he should be assured about security, the data should not be accessible to unauthorized users. Unauthorized user performs number of attempts for accessing the data till he gets some information of use, which results into denial-of-service attack, brute-force attack and etc. Honey Encryption algorithm is used for protecting data by providing the bogus information to the user whenever unauthorized access is performed by the user. Thus unauthorized user will not be able to distinguish between original data and fake data; he will consider fake or bogus data as the original one. On every unauthorized attempt, it will provide different key. If the attacker has found the data then also he is not able to identify the correct one. He will work on that data and will get fake results. In this way the original data will only be accessed by authorized user only. We are proposing algorithm for secured access to cloud database using AES Encryption and Honey Encryption algorithm that will prevent unauthorized users from accessing any real sensitive information.

KEYWORDS:
AES; Homomorphic Encryption; Honey encryption

INTRODUCTION

With the exponential use of Internet, cloud computing has emerged as one of the most successful computing models in recent years and thus demand for provisioning of database services is increasing. Cloud database runs on the cloud computing platform. It is accessible from the cloud and delivered to users via the Internet from the provider's servers, on their demand. It is also referred to as Database-as-a-Service (DBaaS).

Cloud database can achieve optimized scaling, high availability, multi-tenancy and effective resource allocation using cloud computing. Now a day's many organizations data are being transferred and shared via devices from the cloud database. So it is very important to properly protect information.

One of the method for protecting electronic messages and other types of data is encryption. Encryption method is used for protecting user's sensitive data. Only authorized users will read the original message, and it will be inaccessible to unauthorized users.

Secured access to cloud database ensures only authorized user is able to access information. This trust of secured access by cloud provider is very important for promising usage of cloud services. For this strong authentication mechanism should be employed by the cloud provider. Apart from secured access there are several issues related with the maintenance of cloud database for its proper functioning. Among these, security issues are of prime concern, which provides trust and confidence to the user that there data is in safe hands. They need not to think about how their data is operated, where it is placed, what happened to data after deletion, which else can have access to data, how to recover accidental loss of data, data integrity, ease of portability for data migration, auditing and many more. This also provides guidelines to the cloud database provider regarding promising deployment of cloud database service. Security concern has created research scope in maintenance for cloud database.

iJETRM
International Journal of Engineering Technology Research & Management

LITERATURE SURVEY

Authentication is the first primary step for preventing unauthorized access to the application. It assures correct identity of authorized users to access resources, or to deny them and reassure protection of resources from unauthorized access.

There are three different types of authentication mechanism used in security:

1. Something you know- password, PIN, or piece of information
2. Something you have – ATM card number, smart card, or token
3. Something you are as a biometric- There are two types
   i. Physical biometrics authentication- finger-prints; hand or palm geometry; and retina, IRIS, or facial recognition characteristics.
   ii. Behavioral biometrics authentication- signature, voice, typing rhythm, and speaking style.

Keystroke dynamics is one of the promising behavioral biometric authentications, which works on typing pattern of person that is generally unique. It does not require any extra hardware so there is no effect on overall cost of the system. Keystroke dynamics is used for user identification and verification [1]. It uses flight time, dwell time and some other parameters using machine learning techniques for calculating person typing pattern.

Mean and standard deviation are calculated from keystroke features to form the template. Hybrid model based on combination of Gaussian probability density function (GPDF) and Support Vector Machine (SVM) will convert test features into scores [2].

Human minds are much more proficient to recognize previously learnt pictures as compare to alphanumeric codes and PIN. Graphical passwords are introduced as an alternative technique to textual passwords. According to psychological studies human mind can easily remember images as compare to alphabets or digits; this is the major reason behind using graphical passwords as an authenticating mechanism. Most of the graphical schemes are vulnerable to shoulder surfing. In order to avoid this graphical password authentication can combined text with images or colors for generating session passwords. Use of session passwords is only once and every time a new password is generated. Two techniques are described for generating session passwords using text and colors which are resistant to shoulder surfing [3].

Generally the passwords tend to follow patterns which are easier for attackers to guess. A literature survey shows that text-based password suffer this security problem Pictographic passwords are provided as replacement to text based passwords. Pictographic passwords may prone to shoulder surfing. Pictographic passwords may suffer with the usability issue. Color code authentication provides two step authentications for the user [4]. Every time user will log-in with different one time password. This scheme is tested with different kinds of security attacks. User has to memorize only the sequence of three colors and three shades selected at the time of registration. This scheme is useful for secure authentication method for data protection on cloud. To ensure confidentiality of data stored in cloud database, encryption is the common technique. But it alone doesn't guarantees maximum protection. For achieving the efficient cloud storage confidentiality, encryption and obfuscation techniques were used to protect the data in the cloud storage [5].

In recent years security has become a critical issue in cloud computing. Encryption plays an important role in security system. Many techniques are required to protect the shared data. Cryptography is used to secure the data while transmitting in the network [6]. Firstly, data should be encrypted using encryption algorithm in cryptography. Secondly, with decryption technique the receiver will view the original data. A comparison of encryption techniques like AES, DES and RSA algorithms is performed and their results are shown in Table 1.

Various recent trends for securing access to cloud database is discussed [7]. It includes techniques like Symmetric Encryption, Asymmetric Encryption, Biometric Authentication, Two/Three Factor Authentication, Out-of band authentication, Bring Your Own Encryption (BYOE). Honey encryption technique is used for providing security in cloud computing [8]. It generates ciphertext, if it is provided with wrong key, it produces a believable plaintext. Thus using this way it provides assurance against brute force attack.

iJETRM
International Journal of Engineering Technology Research & Management

Table 1: Comparison between AES, DES and RSA Algorithms

Sr. No.	Factors considered	AES	DES	RSA
1.	Developed	2000	1977	1978
2.	Key size	128,192,256 bits	56 bits	>1024 bits
3.	Block size	128 bits	64 bits	Minimum 512 bits
4.	Ciphering & Deciphering	Same	Same	Different
5.	Scalability	Not scalable	Scalable	Not scalable
6.	Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
7.	Encryption	Faster	Moderate	Slower
8.	Decryption	Faster	Moderate	Slower
9.	Power Consumption	Low	Low	High
10.	Security	Secured	Not Secure Enough	Least Secure
11.	Deposit of keys	Needed	Needed	Needed
12.	Inherent Vulnerabilities	Brute Force Attack	Brute Force Attack, Linear and differential cryptanalysis attack	Brute Force and Oracle Attack
13.	Key	Same key for Encryption and Decryption	Same key for Encryption and Decryption	Different key for Encryption and Decryption
14.	Hardware and Software Implementation	Faster	Better in Hardware than in Software	Not Efficient
15.	Ciphering and Deciphering Algorithm	Different	Different	Same

A framework of 5-layered architecture in cloud database management system has been given [9]. First layer is External Layer, it is closest to the user, in which manageability, providing transparency and security are the important issue that should be considered. Second layer is the Conceptual Middleware Layer, interoperability is the major issue because of heterogeneous databases and clouds. Third layer is the Conceptual Layer in which programming techniques, transaction management, query processing and optimization are the issues that should be considered. Fourth layer is the Physical Middleware Layer, interoperability between various platforms and the last layer is the Physical Layer in which how data can be stored so that it can be easily accessible without so much overhead so here data security, storage, backup, load balancing, partitioning, scaling, elasticity, fault tolerance and replication are the important issues that should be considered.

Honey Encryption

Honey Encryption was developed by Ari Juels, former chief scientist of RSA, and Thomas Ristenpart from the University of Wisconsin.[10] Honey Encryption is best-suited where encrypted data is obtained from the passwords. When attacker try to perform brute force attack, Honey Encryption makes it complicated for an attacker to know if he has correctly guessed a password or key. Wrong guesses of an attacker generates results which appear to be real, but not real. In this way the attacker is misguided by using honey Encryption.

A) DTE (Distributed Transforming Encoding)

The DTE (Distributed Transforming Encoding) is the main idea behind working of pure honey encryption method. It manages the space of plaintext via DTE. Let probability distribution over the message space be p over the message L. The DTE encodes the message L as a K bit seed $S \in \{0, 1\}K$ and decodes the message by inverse DTE method, $decode\ (S) = L$. The internal structure of the HE includes DTE encryption and DTE decryption. These two

algorithms describe the functioning of the Honey Encryption.

Honey Encryption Algorithm:

H← Enc(*X*, *L*)
S← $ encode (L)
R← $ {0, 1} n
S‟← H(R, X)
C← S'⊕S

Honey Decryption Algorithm:

H ← Dec(X, (R, C))
S‟← H(R, X)
S ← C ⊕S‟
L ← decode(S)
Return L

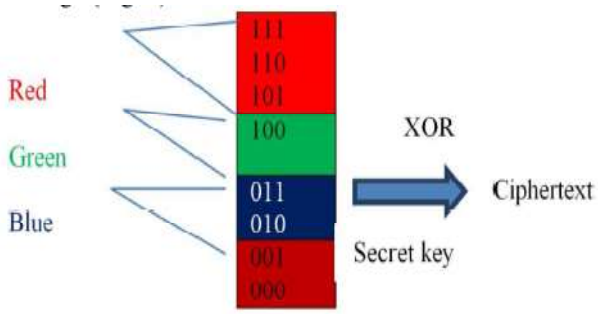

Fig. 1: Honey Encryption

METHODOLOGY

A new algorithm is proposed by using keystroke dynamics, color code authentication, AES and honey encryption algorithm. It will provide a correct, safe and efficient algorithm for securing data saved in cloud storage. This algorithm suggests encryption of the files and data to be uploaded on the cloud, based on the keystroke parameters and color code authentication as given in Fig. 2.

iJETRM
International Journal of Engineering Technology Research & Management

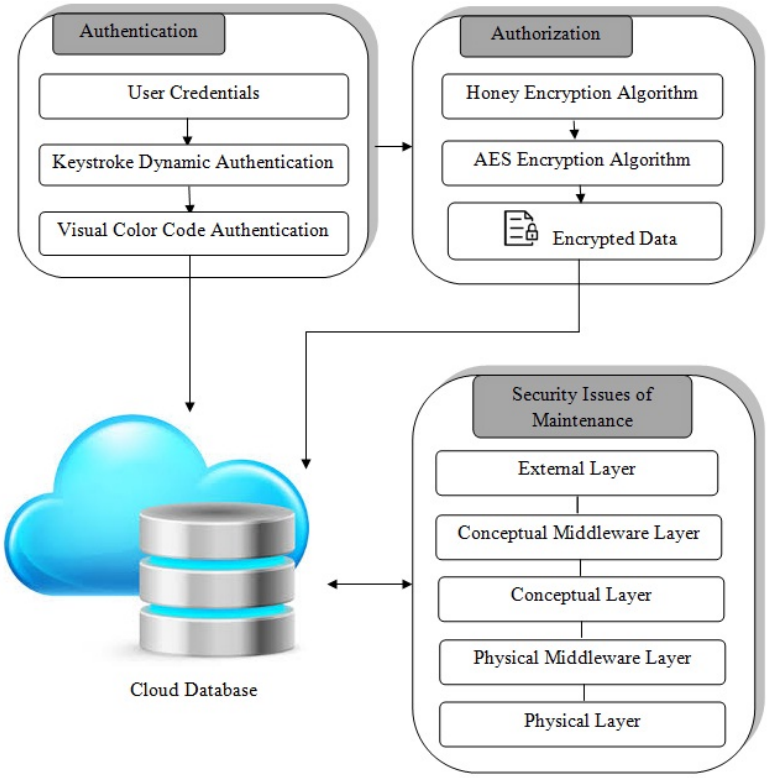

Fig. 2: Proposed Model of Algorithm

First of all the data will be encrypted using honey encryption and if is authorized user he will be directed to the correct data by using AES encryption. If the user is unauthorized then he will be directed to the fake entry database or bogus message will be displayed. By using this algorithm possibility of brute force attack has been eliminated, because the user is provided with the fake data. He plays with that, he will not get valid results.

For the unauthorized user, after downloading file he will get the fake encrypted text. We are modifying the basic working of the honey encryption. Instead of providing a valid looking message, it will display encrypted text. Simple concept of encryption and decryption is used in honey encryption. For every click of download different encrypted text will be generated. It becomes very difficult to find out the correct text.

By using this new algorithm for cloud database ensures integrity as well as confidentiality of the data uploaded by the user doubly by encrypting it and also providing access to the data only on successful authentication. The file will be encrypted using AES algorithm and will be stored in cloud database. The authorized user can download any of the uploaded encrypted files and read it on the system at any time.

Each different invalid key will generate different fake file with different extensions (pdf, docx, txt, pptx). When an imposter is entering invalid keys; he will get different fake files and he will not able to identify which one is correct.

iJETRM
International Journal of Engineering Technology Research & Management

Table 2: Key Pair Combination and their effect for Individual User

Case	HE key	AES key	Access to Cloud Database	Corresponding Action
1.	✓	✓	Granted	Original file
2.	✓	×	Not granted	Fake file
3.	×	✓	Not granted	Fake file
4.	×	×	Not granted	Fake file

Therefore, the attacker is kept under the false assumption that he has got hold of the original data while he is being fed with the false messages and at the same time, the system is also flagged about the potential threat. On the server side, a notification will be received about attempt of the attack. On the contrary, if the attacker somehow manages to get the key of this layer of protection right, there is very little chance that he/she will be able to break another layer of AES security. Therefore, the system becomes more secure. For group of users based on HE key account will be classified as active or inactive account and after that AES key will be checked. Table 3 represents all these cases with results.

Table 3: Key Pair Combination and their effect for Group of Users

Case	HE key	Account Type	AES key	Corresponding Action
1.	✓	Active Account	✓	Original file
			×	Fake file
2.	×	Inactive Account	✓	Fake file
			×	Fake file

After providing secured access to cloud database; cloud database provider should also provide promising services to their users for enhancing adoption of cloud technology. In order to ensure this there are several security issues of maintenance for cloud database, which need to take care for promising usage and making its working transparent to the users and build their trust.

These several issues are analyzed and represented according to the framework of five-layered architecture in cloud database management system. According to the layer position in cloud database management system, issues are enlisted. When this framework will be integrated with the cloud computing services it will ensure proper working of cloud database from maintenance point of view, and thus making sure to user that there data is in safe hands.

CONCLUSION

In this paper, we have suggested a new algorithm which allows secure access to the cloud database. It is provided by implementing the AES and honey encryption algorithm. Only authorized users will have access to their data based on the keystroke and the visual color code authentication. When an intruder (unauthorized user) gets data accidentally or intentionally, he will not be able to distinguish between the real and fake data. This technique can be used in credit card application, online data storage and retrieval applications.

REFERENCES

[1]. Chandralekha Jadhav; Siddhi Kulkarni; Sagar Shelar; Kaustubh Shinde; Nagaraj V. Dharwadkar;*BiometricAuthentication Using Keystroke Dynamics.*International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017 IEEE, pp. 870-875

[2]. Ramu Thanganayagam; Arivoli Thangadurai*; Fusion Approach on Keystroke Dynamics to Enhance the Performance of Password Authentication*. 2015 IEEE.

[3]. M SREELATHA; M SHASHI; M ANIRUDH; MD SULTAN AHAMER; V MANOJ KUMAR; *Authentication Schemes for Session Passwords using Color and Images*. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, pp. 111-119.

[4]. Manish M. Potey; Dr. C. A. Dhote; Deepak H. Sharma; *Secure Authentication for Data Protection in Cloud Computing using Color Schemes* . 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, 2016 IEEE, pp. 424-427.

[5]. Dr. L. Arockiam S. Monikandan*; EfficientCloud Storage Confidentiality to Ensure Data Security*. 2014 InternationalConference on Computer Communication and Informatics (*ICCCI* -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.

[6]. Dr. Prerna Mahajan & Abhishek Sachdeva; *A Study of Encryption Algorithms AES, DES and RSA for Security*. Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013, pp.15-22.

[7]. Dr. Santosh S. Lomte; Swati V. Khidse; *Recent Trends for Efficient and Secure Accessing Scheme for Cloud Database*. 2017 IJEDR | Volume 5, Issue 4 | ISSN: 2321-9939, pp.396-399.

[8]. Fancy Arora; *Security in cloud computing using honey encryption*. April 12,2017, pp. 1-9.

[9]. Bashir Alam ; M.N. Doja ; Mansaf Alam ; Shweta Mongia; *5-Layered Architecture of Cloud Database Management System*. 2013 AASRI Conference on Parallel and Distributed Computing and Systems, ELSEVIER Procedia 5 (2013) pp. 194-199.

[10]. Ari Juels; Thomas Ristenpart; *Honey Encryption-Encryption beyond Brute Force Barrier*. IEEE Security and Privacy July/August 2014.