Indo American Journal of Multidisciplinary Research and Review (IAJMRR)
ISSN: 2581 - 6292 / Impact Factor: 6.885 / Website: www.iajmrr.com

A SECURED FRAMEWORK FOR DATA STORAGE IN CLOUD

B. N. Karthik*, K. Aishwarya, R. Swathi*** & S. Vaishnavi******
Department of Information Technology, AVC College of Engineering, Mayiladuthurai, Tamilnadu

Cite This Article: B. N. Karthik, K. Aishwarya, R. Swathi & S. Vaishnavi, "A Secured Framework for Data Storage in Cloud", Indo American Journal of Multidisciplinary Research and Review, Volume 4, Issue 2, Page Number 9-13, 2020.

Abstract:
Cloud computing is one of the popular technologies used by both large and small scale organizations. Its popularity is increased with the use of services like Amazon Web Service (AWS), Google cloud, Drop box, Office 365 and so on. Cloud provides access to information and resources from anywhere when network is available. Security of information plays vital role today. There are many open challenges in cloud security environment. In this paper we propose a framework to solve the data security related issues in cloud.
Key Words: Cloud Computing, Homomorphic Encryption, Honey Encryption, Framework & Security

Introduction:

Cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3].

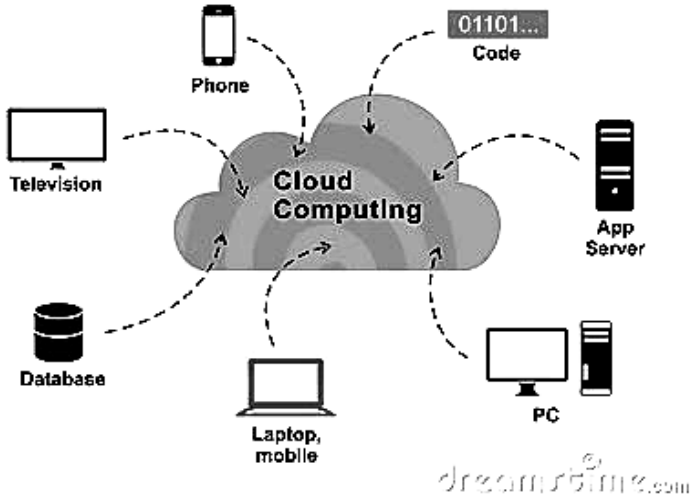


Figure 1: Cloud computing services

There are *four essential cloud deployment models*, taking into an account who gives the cloud administrations which are Public cloud, Private cloud, Community cloud and hybrid cloud [5].

A. Public Cloud: Every user can access the public cloud from anywhere. It can be accessed using interfaces such as Web browsers. Users have to pay only for that time duration in which they user the cloud service i.e., pay-per-use model. Example of public cloud providers includes Amazon AWS, Microsoft etc.

B. Private Cloud: Private cloud exists within an organization's internal enterprise data centre. Only that user can access the private cloud that is having authorized access by the organization. Security can be easily managed using private cloud. Example of private cloud is intranet.

C. Hybrid Cloud: It provides the functionalities of both public and private cloud. Data and applications can be secured in an efficient manner. In hybrid cloud, one can take advantage of third party cloud providers in either a full or partial manner, thus increasing the flexibility of cloud computing.

D. Community Cloud: A community cloud is a multitenant cloud service model that is shared among various organizations. It is managed and secured by every organization participating. It is hybrid form of private clouds designed specifically for a targeted group.

Depending on the type of service provided, there are three types of cloud services also termed as delivery models which are SaaS: Software as a service, PaaS: Platform as a service and IaaS: Infrastructure as a service.

The *five characteristics* of cloud computing are: on-demand service, self-service, location independent, rapid elasticity and measured scale service. The feature of cloud computing is unique. Most of the organization and institute utilized of this characteristics of the cloud computing and take benefit to

gain profit. Hence, industries are shifting their businesses towards cloud computing. Cloud computing uses increased day by day, however, Data security is main concern in cloud computing [4].

Cloud Computing:

As per the National Institute of Standards and Technology (NIST) standards, there are five main characteristics which need to be available in any service to be treated as cloud service which is:

On-Demand Self-Service: user can carry out operation whenever he wants to use the service without any interference from anyone else.

Network Access: is accessible with any Internet connected device.

Location Independent Resource Pooling: resources should be shared across the users irrespective of their location.

Physical Transparency: user can change their resource capacity as per their requirement.

Pay per Use: customer need to be charged based on the resources used [1].

Security:

The Data Owner(s) would worry that the data could be tampered (or deleted) in the cloud. They have this concern because they know that data can be lost in any infrastructure, irrespective of the extent of reliable measures to prevent this from happening .In addition, sometimes cloud service providers may be dishonest. The server may discard some file blocks that have not been accessed or rarely accessed to save storage space and claim that all of the files are still intact. Gradually, the security of files has become a big problem in the field of cloud storage. Users are beginning to worry about the security of their files [6]. So that data security in cloud becomes an important issue today.

In the existing system we need to encrypt the plain data using the homomorphic encryption technique. Once the data has been encrypted, we can store the data in the cloud. As the data is encrypted using homomorphic encryption, we can perform computations in the cloud. The computations carried on encrypted data will same as the computations carried on the plain data because of the usage of homomorphic encryption. So when attacks are made to compromise the key, the attackers are able to know our original data and the result of computations also able to modify the original text. Our proposed framework is helpful to overcome this issues.

Securing data is always of vital importance as shown in figure 2 and because of the critical nature of cloud computing and large amounts of complex data it carries, the need is even important. Therefore, data privacy and security are issues that need to be resolved as they are acting as a major obstacle in the adoption of cloud computing services [11].

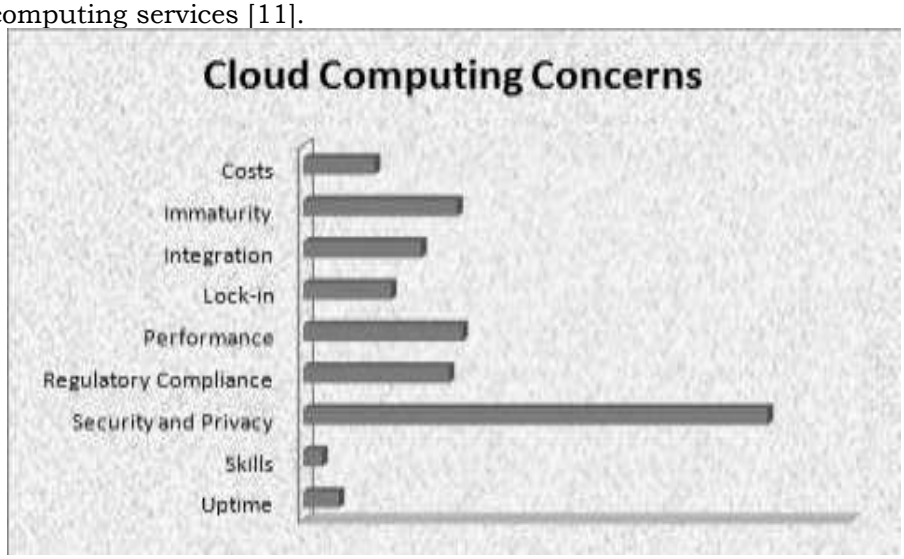


Figure 2: Cloud computing concerns

The major security issues with cloud are:

Privacy and Confidentiality: Once the clients outsource data to the cloud there must be some assurance that data is accessible to only authorized users. The cloud user should be assured that data stored on the cloud will be confidential.

Security and Data Integrity: Data security can be provided using various encryption and decryption techniques. With providing the security of the data, cloud service provider should also implement mechanism to monitor integrity of the data at the cloud.

Proposed Framework:

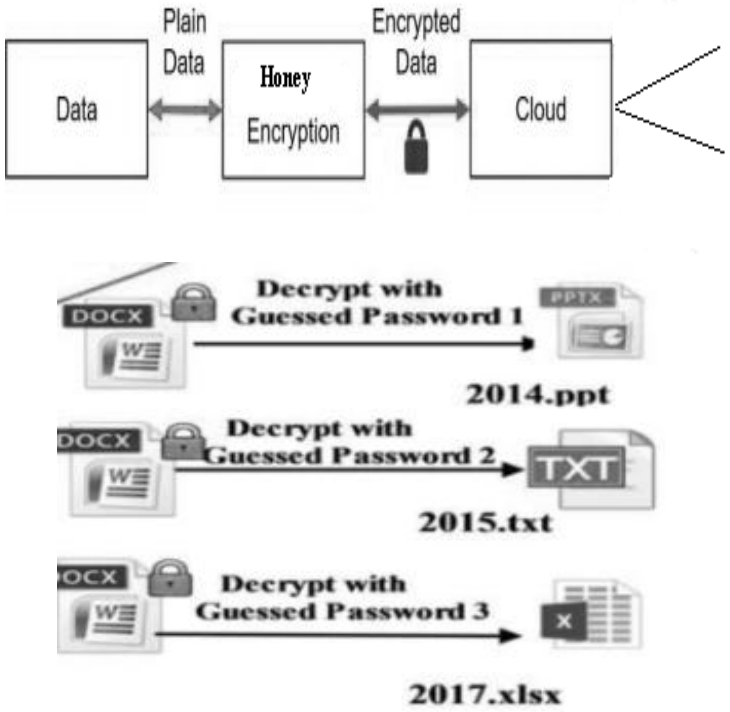
To solve some of the issues in current cloud environment i.e., attacks to compromise the key and possibility of modifying the original text, we propose a simple and powerful secured cloud framework with the use of Honey Encryption.

Honey encryption protects a set of messages that have some common features (e.g., credit card numbers are such messages). A message set is called a message space. Before encrypting a message, we should determine the possible message space. All messages in the space must be sorted in some order. Then the probability of each message (PDF) that occurs in the space and the cumulative probability (CDF)

of each message are needed. A seed space should be available for the distribution-transforming encoder (DTE) to map each message to a seed range in the seed space (-bit binary string space).

The DTE determines the seed range for each message according to the PDF and CDF of the message and makes sure that the PDF of the message is equal to the ratio of the corresponding seed range to the seed space. The -bit seed space must be big enough so that each message can be mapped to at least one seed. A message can be mapped to multiple seeds and the seed is randomly selected.

The diagram shown below (fig.3) describes the architecture of our proposed framework with the use of honey encryption and with the description of what happens when attacks are made.



The innovation of honey encryption is the design of the distribution-transforming encoder (DTE). According to the probabilities of a message in the message space, it maps the message to a seed range in a seed space, then it randomly selects a seed from the range and XORs it with the key to get the cipher text. For decryption, the cipher text is XOR'ed with the key and the seed is obtained. Then DTE uses the seed location to map it back to the original plain text message. Even if the key is incorrect, the decryption process outputs a message from the message space and thus confuse the attacker.

The principle is very simple: instead of returning a 'fail' or nothing or garbage when a password or key is incorrectly entered, it returns fake but plausible information. It is designed to make brute forcing stolen password/credit card databases more difficult.

Pseudo Code:

- A user inputted password.
- A user inputted secret message.
- A hard coded dictionary of secret messages.
- A dictionary containing manipulated passwords (Sweet words) in addition to the real password.
- A dictionary containing seeds. (Seed generator) seeds are simply pointers that point to the secret message.
- The encryption algorithm: $c = sk \wedge sm$
  Where, C - cipher text
  SK - seed value of key
  SM - seed value of message
  (the cipher text = seed value of the key XOR seed value of the message.)
- The decryption algorithm: $m = sk \wedge c$
  Where, M - message
  SK - seed value of key
  C - Cipher text
  (the message = seed value of the key XOR cipher text.)
- A try/catch block to search for passwords that do not exist in the dictionary of sweet words.
- A query to prompt the user for another attempt.

Related Works:

Jayachander Surbiryala et al [1] proposed a simple yet powerful framework using homomorphic encryption for solving data security problems in cloud environments. Adoption of the proposed framework will solve many of the issues in cloud environment related to ethical and security aspects.

Mostafa Taha et al [2] proposed a lightweight key-updating framework for efficient leakage resiliency. Their solution utilized two rounds of the underlying AES itself achieving negligible area overhead and very small performance overhead. It provides a complete solution to protect the implementation of any AES mode of operation.

Karun Handa et al [3] Proposed it revolves the problem of data security with the help of encryption at client side and steganography at server side which provides a highly secure model that will not only solve the issue of data safety but also simple in its implementation and usage.

Taware Sang ram et al [4] presented a new approach which provides Security for data outsourced at CSP. Some approaches are given to secure outsourced data but they are suffering from having large number of keys and collision attack. By employing the threshold cryptography at the user side, they protect outsourced data from collision attack.

Neha, Mandeep Kaur [5] Shows comparison on the basis of encryption/decryption time and hybrid of AES and Two fish takes less time to encrypt and decrypt the file as compared to AES and Blowfish. This work can be extended to determine the performance of cloud in terms of throughput, power consumption and memory consumption. It can also be extended to the use of large size of text files, images, audio files and video files for encryption and decryption.

Bin Feng et al. [6] proposed a new, remote data-auditing system that supports bi-directional verification and further validation for data storage security in cloud computing. In addition, they presented an additional validation scheme to solve the problem of file errors. If there are some important blocks in the user's file, the Data Owner can check the integrity of these important blocks at less cost and CSP cannot acquire any information about the important blocks.

Shabnam Kumari et al [7] Designed model of a complex data security in cloud computing has adequately increased data security in all three attributes of data security which are confidentiality, integrity and availability in the use of encryption algorithms.

Vaibhavi Bharvada et al. [8] proposed Security of data is main issue for this technology. It provides a review of different issues and possible solution for data confidentiality and authentication of Cloud computing.

S. Meena et al. [9] proposed scheme is used to provide for enhancing security on the cloud server. They use ECC and MD5 as a hybrid security mechanism. Encryption and decryption is done by ECC and MD5 is used for data digestion form which enhances the security.

Amjad Alsirhani et al [10] proposed a combination of approaches by using the encryption algorithms. The encryption algorithms provide the user with confidentiality and also support the query processing of encrypted data. The distributed technique provides greater security and prevents cloud providers from procuring meaningful information.

Comparison:

S.No	Criteria	Homomorphic Encryption	Honey Encryption
1.	Computation on Encrypted data	It allows computation	It does not allows computation
2.	Attacks to compromise key	Possible	Impossible
3.	Modification	It allows modification	It doesn't allows to compromise key

Conclusion:

Cloud computing was one of the emerging techniques today but it has problems related to its security i.e., it has lots of security issues such as suffering of attacks like collision attack and also suffered from having lots of keys. In this paper ,we proposed a new framework which provides the security on the data. Even though some approaches are helpful in securing the cloud data, they are suffered from having more number of keys and attacks like collision attacks. In our proposed framework we use Honey Encryption to solve the security issues in cloud data. The number of keys and security attacks are also reduced by the proposed framework.

Acknowledgement:

We like to express our sincere gratitude to Mr. B. N. Karthik Assistant Professor- IT whose guidance and supervision has make us to complete this thesis successfully. It is not possible for us to complete this without his guidance and supervision.

References:

1. Jayachander Surbiryala, Chunlei Li, Chunming Rong," A Framework for Improving Security in Cloud Computing" the 2nd IEEE International Conference on 2017.
2. Mostafa Taha, Patrick Schaumont, "Key Updating for Leakage Resiliency with Application to AES Modes of Operation" IEEE transactions on information forensics and security, vol.10, no. 3, march 2015.
3. Karun Handa , Uma Singh , "Data Security in Cloud Computing using Encryption and Steganography" International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, Page 786-791.
4. Taware Sangram, Zargad Ameya, Waghmare Raju, Ghodke Omkar, Prof. A. A. Chavan," Secure Data Access in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 4, April 2016.

5. Neha, Mandeep Kaur, "Enhanced Security using Hybrid Encryption Algorithm" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 7, July 2016.
6. Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, Tie Qiu 12," An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing" DOI: 10.1109/ACCESS.2016. 2621005, IEEE Access.
7. Shabnam Kumari, Reema, Princy,Sunita Kumari, "Security in Cloud Computing using AES & DES" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5 Issue: 4,April 2017.
8. Vaibhavi Bharvada, Sohil Gadhiya, "Review: Data Privacy and Data Confidentiality in Cloud Computing"Vol-3, Issue-2 2017, IJARIIE-ISSN (O)-2395-4396.
9. S. Meena,Dr. N. Kowsalya, "Achieving High Secure Data Storage in Cloud Computing" International Journal for Research in Applied Science & Engineering Technology (IJRASET),Volume 5 Issue, May 2017.
10. Amjad Alsirhani, Peter Bodorik, Srinivas Sampalli, "Improving Database Security in Cloud Computing by Fragmentation of Data" 2017 International Conference on Computer and Applications (ICCA).
11. Sanjoli Singla, Jasmeet Singh," Cloud Data Security using Authentication and Encryption Technique", ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 7, July 2013.