International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Survey on a Secured Framework for Data Storage in Cloud

B. N. Karthik[1], K. Aishwarya[2], R. Swathi[3], S. Vaishnavi[4]

[1]Assistant Professor-Information Technology, A.V.C College of Engineering, Mayiladuthurai, Tamilnadu, India
[2,3,4]UG Student-Information Technology, A.V.C College of Engineering, Mayiladuthurai, Tamilnadu, India

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 ,Office365 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.

Keywords: Cloud Computing, Honey Encryption, Framework, Security

I. 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"[2].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 [3].

- *Essential Characteristics of Cloud Computing*

1. **On-demand self-service**:

A user can carry out operation whenever he wants to use the service without any interference from anyone else.

2. **Network access:**

It is accessible with any internet connected device.

3. **Location independent resource pooling:**

Resources should be shared across the users irrespective of their location.

4. **Physical transparency:**

A user can change their resource capacity as per their requirement.

5. **Pay per use:**

A customer need to be charged based on the resources used.

- *Issues*

The major security issues with cloud are:-

6. **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.

7. 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.

II. LITERATURE REVIEW

Mostafa Taha et al. [1] 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.[2] 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. [3] 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. [4] 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. [5] 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. [6] 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. [7] 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. [8] 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. [9] 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.

Yong Ding et.al [10] combine the advantages of CP-ABE and homomorphic encryption to construct a fully homomorphic encryption scheme with a fine-grained access control. The secure sharing and cipher text retrieval of multi-user in cloud environment are

realized. Because the number of rows and the number of attributes are the same when the Boolean circuit is transformed into the corresponding LSSS matrix, when the set of attributes is large, the number of lines and the size of the cipher text is relatively large, which affects the speed of encryption and decryption.

III. COMPARATIVE STUDY

RESEARCH PAPER	ALGORITHM	DESCRIPTION	LIMITATIONS	PROPOSED WORK
1.Key Updating for Leakage Resiliency With Application to AES Modes of Operation.	1. Side channel analysis (SCA). 2. Light weight key updating (re-keying / key-rolling)	1. It can provide more detailed information by observing the power consumption of a hardware device such as CPU or cryptographic circuit. 2.It is a Generic framework of lightweight key updating that can protect the current cryptographic standards and evaluate the minimum requirements for heuristic SCA-security	1.Attacks are not avoided.	Attacks are avoided because of using bogus data in honey encryption.
2. Data Security in Cloud Computing using Encryption and Steganography.	1.Steganography	1.The purpose of steganography is covert communication to hide a message from a third party. 2.Steganography techniques can be applied to images, a video file or an audio file.	1.Steganography tools are cracked by expert level intruders.	Intruders cannot be able to crack an encypted data.
3. Secure Data Access in Cloud Computing.	1.Threshold cryptography 2.MD5	1.It provides a way in which data owner can divide users in group and provide single key with the using key each user	1.Hash collision - An attacker can try billions of candidate passwords per second	Hash collisions are avoided because when attackers try to attack data by using incorrect password

		in group can access the data. **2.**It ensures entity authentication and data integrity.	on a single GPU	it yields plausible-looking message.
4.Enhanced **5.**Security using Hybrid Encryption Algorithm.	**1.**AES **2.**Blow Fish **3.**Two Fish	1.AES and blowfish is used for data confidentiality. **2.**It can be used to determine the performance of cloud in terms of throughput, power consumption and memory consumption.	**1.**Attacks like Brute force are not avoided here.	All types of attacks are avoided here.
6.An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing.	**1.**Bidirectional Authentication.	Cloud service provider can verify the authority of the verification party and reject requests that come	**1.**There is no update mechanism, so the verification times are limited. **2.**The usage of space is	Administrator have time to decide how to respond to attacker.

		from unauthorized users.	increased because of the sentinel and error-correcting code.	
7.Security in Cloud Computing using AES & DES.	**1.**AES **2.**DES	**1.**The designed model of a complex data security in cloud computing has adequately increased data security. **2.**Three attributes of data security are confidentiality,integrity and availability in the use of encryption algorithms.	**1.**It could not withstand with the attacks like Brute Force, Linear crypt Analysis, because during its design this attack wasn't invented.	It withstands on any attack.
8.Review: Data Privacy and Data Confidentiality in Cloud	**1.**RSA Encryption with Fermat's Little	It is widely used for secure data transmission. In such a cryptosyste	**1.**It aimed at providing just a review analysis where	This paper aimed at providing a review analysis

Computing.	Theorem	m, the encryption key is public and it is different from the decryption key which is kept secret(private).	the studies became ineffective due to advanced attacks.	to overcome the advanced attacks.
9.Achieving High Secure Data Storage in Cloud Computing.	**1.**Symmetric & Asymmetric Encryption	This technique is a two way secured data encryption system, which focus on the matters related to user's privacy, authentication and accuracy.	**1.**It needs a secure channel for secret key exchange. 2.There is a use of too many keys.	It reduces the number of key usage.
Improving Database Security in Cloud Computing by Fragmentation of Data.	**1.**Data Fragmentation	It allows us to break a single object into two or more segments or fragments.	**1.**Cost and complexity is more. **2.**Integrity control is more difficult. **3.**Database design becomes more complex.	Less complexity.
10. Policy Based on Homomorphic Encryption and Retrieval Scheme in Cloud Computing.	**1.**Homomorphic Encryption **2.**Retrieval Scheme	**1.**It allows us to perform computations on encrypted data. **2.**It provides a method to construct a fully homomorphic encryption scheme with a fine-grained access control.	**1.**Allows modification of original data. **2.**Deletion made easily.	It doesn't allow modification and Deletion.

IV. PROPOSED WORK

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.

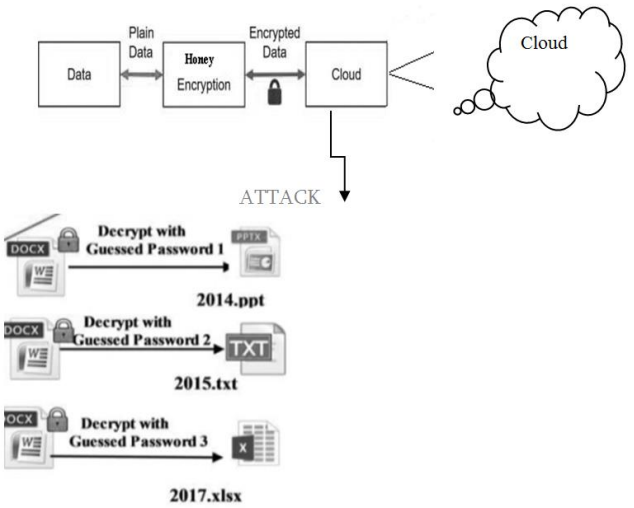

Figure 1 : Proposed framework architecture

The diagram shown above (fig.1) 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.

V. 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. In this paper, we proposed a new framework which provides the security on the data. Eventhough 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.

VI. REFERENCES

[1] Mostafa Taha,Patrick Schaumont,"Key Updating for Leakage Resiliency With Application of AES Modes of Operation"IEEE transactions on information forensics and security, vol.10,no. 3, march 2015.

[2] 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,pg. 786-791.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Vaibhavi Bharvada, Sohil Gadhiya,"Review: Data Privacy and Data Confidentiality in Cloud Computing"Vol-3, Issue-2 2017 ,IJARIIE-ISSN(O)-2395-4396.

[8] 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.

[9] Amjad Alsirhani,Peter Bodorik,Srinivas Sampalli,"Improving Database Security in Cloud Computing by Fragmentation of Data" 2017 International Conference on Computer and Applications (ICCA).

[10] Yong Ding, Xiumin Li,"Policy Based on Homomorphic Encryption and Retrieval Scheme in Cloud Computing", 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC).