ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 5, July 2012

A SURVEY ON CLOUD DATA SECURITY USING ENCRYPTIOIN TECHNIQUE

C.BAGYALAKSHMI
Research scholar, Department of Computer Science
NGM College, Pollachi, Coimbatore, India – 642001
E-mail: bagyachithra@gmail.com

DR.R.MANICKA CHEZIAN
Associate Professor, Department of Computer Science
NGM College, Pollachi, Coimbatore, India – 642001

ABSTRACT

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructures are provided as services of the internet. It allows consumers and business to use application without installation and access their personal files at any computer with internet access. It provides people the way to share distributed recourses and services that belong to different organizations or sites. Since it share distributed resources via the network in the open environment, thus it makes security problems important for us to develop the cloud computing application, when consumers shares their data on cloud servers which is not within the same trusted domain data owners. To keep user data confidential against trusted servers, cryptographic methods are used by disclosing data decryption keys only to authorized users. This paper explores various data encryption technique such as Hybrid algorithm, DES algorithm, Identity based encryption.

Key Terms: Cloud Computing, Encryption, Cryptography, Plaintext, Security.

I INTRODUCTION

Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to computers on a pay-as-you-use basis. The world of computation has changed from centralized to distributed systems and now we are getting back to the virtual centralization. During the past few years, cloud computing grown from being a promising [1], Business idea to one of the fastest growing parts of the IT industry. IT organizations have express concern about security issues that exist with the widespread implementation of cloud computing. Cloud computing uses the internet as the communication media. Cloud computing provides three services are SaaS (Software as a service), PaaS (Platform as a service), IaaS (Infrastructure as a service) [6]. A cloud computing system must make a copy of all its clients' information and store it on other devices. These copies are enabling to the central server to access backup machines to retrieve the data.

Protecting privacy in cloud providers is a technical challenge. In cloud environment, this challenge is complicated by distributed nature of clouds and lack of subscriber knowledge over where the data is stored i.e. about data center and accessibility of the users. In cloud computing have problem like security of data, file systems, backups, network traffic and host security. Cryptographic encryption is certainly the best practice. Encryption techniques should also be used for data in transit. In addition authentication and integrity protection ensure that data only goes where the user wants it to go and its' not modified in transit. User authentication is often the primary basis for access control. In the cloud environment authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the internet.

II RELATED WORKS

The cloud security conations a different sort of taxonomy based on fifteen security domains and processes that need to be followed in an overall cloud deployment. The security concerns can be categorized as Traditional security, Availability and Third-party Data Control [5]. A user wants to login to a secured cloud system. To login into a system must provide a correct combination of user name and password and it should be matched with the combination stored in the database whether in plaintext from or in encrypted form.

III. ENCRYPTION TECHNIQUES

A. HYBRID ALGORITHM

A secured login user provides login credentials and then to authenticate the user system encrypts the provided password up to the number of times defined to the system. Hybrid Algorithm [2] is used to encrypt the message by which firstly the password will be encrypted by the Ceaser cipher then the encrypted result will again be encrypted by using RSA substitution algorithm and finally the result will again be encrypted by the alphabetic substation method. Then password will be sent to the server with the plain text user name and if it matches only then the user get access to the system. For generation of encryption key best encryption method by combing algorithms is used.

In this way privacy to the secured cloud is provided by which transactions can take place. Because technique behind user name and password by combining three algorithms that are RSA, Monotonic and Ceaser cipher by which security is provided. Firstly Password is encrypted by Ceaser cipher then the encrypted result is again be encrypted by using RSA algorithm and finally the result is again be encrypted by mono alphabetic substation method. Developers can benefit from this technique in order to provide security.

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.Encryption of a letter x by a shift *n* can be described mathematically as,

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

The replacement remains the same throughout the message, so the cipher is classed as a type of monoalphabetic substitution, as opposed to polyalphabetic substitution.

B. DES ALGORITHM

In cloud computing have problem like security of data, file system, backups, network traffic, and host security. A data security using encryption decryption with DES algorithm whiles us transferring it over the network. The Data Encryption Standard (DES) [4] is the name of the Federal Information Processing Standard (FIPS), which describes the Data Encryption Algorithm (DEA).DES Structure (Fig 1) has a 64-bit block size and uses a 56 bit key during execution. Its' a symmetric cryptosystem, specifically a 16-around Feistel Cipher, when used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a Message Authentication Code (MAC).It can also be used for Single user encryption, such as to store files on a hard disk in encrypted form.

In Cipher Block Chaining mode of operation of DES, each block of ECB encrypted cipher text is XORed with the next plain text block to be encrypted, thus making all the blocks dependent on all the previous blocks this means that in order to find the plaintext of a particular block, you need to know the cipher text, the key and the cipher text for the previous block. The first block to be encrypted has no previous cipher text, so the plain text is XORed with 64-bit number called the initialization vector. This mode of operation is more secure then ECB (Electronic code book) because the extra XOR step adds one more layer to the encryption process.DES exhibits the complementation property, namely that

$$E_K(P) = C \Leftrightarrow E_{\overline{K}}(\overline{P}) = \overline{C}$$

Where $\overline{x}$ is the bitwise complement of x.
E_K Denotes encryption with key K.
P And C denote plaintext and cipher text blocks respectively.

The complementation property means that the work for a brute force attack could be reduced by a factor of 2 (or a single bit) under a chosen-plaintext assumption. By definition, this property also applies also to TDES cipher.

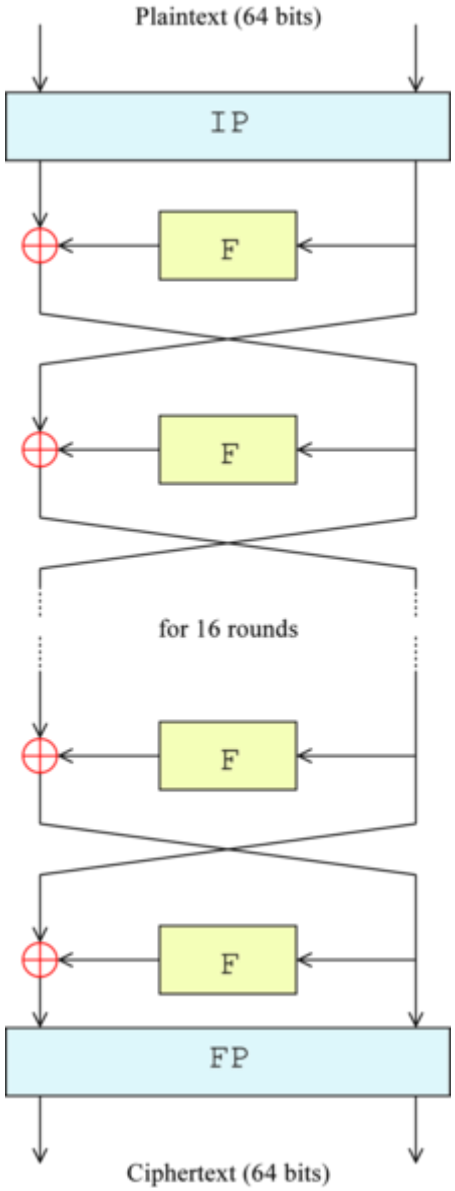

Fig1. Structure of DES

DES (Fig 1) also has four so-called *weak keys*. Encryption (*E*) and decryption (*D*) under a weak key have the same effect (see involution):

$$E_K(E_K(P)) = P \text{ or equivalently, } E_K = D_K.$$

There are also six pairs of *semi-weak keys*. Encryption with one of the pair of semiweak keys, K_1 operates identically to decryption with the other, K_2:

$$E_{K_1}(E_{K_2}(P)) = P \text{ or equivalently, } E_{K_2} = D_{K_1}.$$

C. INDENTITY BASED ENCRYPTION

Identity based Encryption (IBE) is frequent for the entities to communicate manually. To achieve the security in the communication, it is important to impose an encryption and signature schemes.IBE [3] is a form of public key cryptography in which a third party server uses a simple identifier, such as an e-mail address, to generate a public key cryptography that can be used for encrypting and decrypting electronic messages. Compared with typical public key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators. An added advantage is that a message recipient doesn't need advance preparation or specified software to read the communication. IBE depends upon the third-party IBE server that generates private keys. The only information this server stores permanently is a secret key a large random number that is exclusive to the security domain. The server uses this key to create a common set of public key parameters that are given to each user who installs the IBE software, and recipient's private keys are required.

When sender creates an encrypted message, the IBE software on his system uses three parameters to generate the public key for the message a string value, the current week number and the parameter's identity. A user who receives an IBE encrypted e-mail message but has not used the process before can request upon authentication a private key that allows him to decrypt all e-mails encrypted using his e-mail address as the public key.

An identity based signature scheme is deterministic if the signature on a message by the same user is always the same. The private key generator provides the security parameter as the input to this algorithm, generates the systems parameters and the master private key. This algorithm on input a signature on message m by the user with identity ID, parameters, checks whether signature is valid on message m by ID.

IV. CONCLUSION & FUTURE SCOPE

Among the many IT giants driven by trends in cloud computing has not doubtful. It gives almost everyone has brought good news. Provision of security to the users data on the cloud will defiantly empowers the data owner to outsource to the cloud. Data security has become the most important issue of cloud computing security. The main contribution of this paper is the new view of data security solution with encryption, which is important and can be used as reference for designing the complete security solution.

In future work, that data storage security in cloud computing, an area full of challenges and of paramount importance, are still in its infancy now, and many research problems are yet to be identified is to enhance the more security features by using other enhanced techniques of data security through cryptosystems and other technique. A best technique for securing cloud by mixture of algorithms, in this analysis fully delivers on the promise of merging the best aspects of dynamic and static testing into a tightly interwoven approach for rapidly resolving security vulnerabilities in software.

V. REFERENCES

1. Sunia Rani, Ambrish Gangal "Cloud Security with Encryption using Hybrid Algorithm" International Journal of Computer Science and Information Technologies, vol. 3(3), ISSN: 0975-9646, 2012.
2. Simarjeet Kaur "Cryptography and Encryption in Cloud Computing" VSRD International Journal of Computer Science & Information Technology- vol 2(3), ISSN: 2231-2471, 2012.
3. Neha Jain and Gurpreet Kaur "Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of Computer Science & Information Technology- vol 2(4), ISSN: 2231-2471, 2012.
4. D.H. Patil "Data Security over Cloud"International Journal of Computer Applications 2012.
5. G. Jai Arul Jose "Implementation of Data Security in cloud Computing" International Journal of P2P Network Trends and Technology – vol 1, Issue1- 2011.
6. Sriram Ramanujam "Data Security in Cloud Computing" J.Comp. & Math. Sci – vol 2(1),2011.
7. M.Rashid and F. Saeed, "Integfrating Classical Encryption with Modern Technique" International Journal of Computer Science and Network Security, Vol.10 No.5 2010.
8. http://en.kipedia.org/wiki/cloud_computing
9. http://www.cs./~crypto/historical/caesar.html
10. http://crypto.stanford.edu/ibe/
11. http://eprint.iacr.org/2010/010.pdf
12. http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation