A New Method for Symmetric Key Encryption using Plaintext Key Pair Split (Pi,Ki) Algorithm

Agrim Aggarwal[1] Sanchit Singhal[2]
[1,2]Maharaja Agrasen Institute of Technology Delhi, India

Abstract— Cloud Computing is the new-generation architecture of the IT enterprise, and IT applications. Cloud storage lets users to remotely store their data and use cloud applications, services without the requirement of local hardware and software, anytime and anywhere, i.e. on-demand. In cloud, the data is transferred between the server and the client, and high transmission speeds is an important aspect in networking. As with the advent of any new technology, its security and efficiency is considered, cloud security is the current big-thing in IT Industry all across the world. This research paper provides a method for hiding, protecting and securing the data without affecting the network layers; from unauthorized access to the server. In comparison to traditional solutions, where IT services are under physical, logical and personnel controls, in Cloud Computing the application software and data is moved to large data centres, where the management of software, services and data may not be secure and private, thus posing many new security challenges which have not been well understood. In this paper we compare and survey different security issues to cloud and different cryptographic algorithms adoptable for better security in the cloud. Cryptography is defined as the science and study of secret writing, that concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only intended people can see the real message. We propose the design and implementation of a new symmetric key algorithm. The algorithm functions by encrypting the plaintext file, using the password of the file as key. The plaintext and key are split in equal numbers and shift cipher is applied to each block of the plaintext. This new algorithm can be considered as a hybrid approach to its precursors. Most of the existing and proposed algorithms encounter problems such as lack of robustness, privacy concerns and addition of time to packet delay to maintain the security on the communication channel between the terminals. In this paper, the security features were enhanced and upgraded to maintain high security on communication channels by increasing the difficulty for attacker to recognize, understand a pattern and speed of the encryption/decryption scheme.

Keywords: Cloud Computing, Symmetric Key Encryption, Plaintext Key Pair Split (Pi,Ki) Algorithm

I. INTRODUCTION

Cloud computing is defined as set of resources or services offered through the internet to users on their demand by cloud providers. Cloud Computing conveys everything as a service over internet based on the user demand. As each and every organization is moving its data to the cloud, meaning it uses the storage service provided by the cloud service provider. Thus is a need to protect that data against unauthorized access, modification or denial of services etc. Security concerns of data include three points: Availability, Confidentiality, and Integrity. Confidentiality of data in the cloud is maintained through the use of cryptography. Cryptography, is considered combination of three types of algorithms.

They are:

1) Asymmetric-Key Algorithms
2) Symmetric-Key Algorithms
3) Hashing Algorithms

Data cryptography essentially is scrambling content of the data, such as image, video, audio, text and so forth to make the data unreadable, illegible, meaningless and untraceable during transmission or storage. The purpose of cryptography is to protect the data from invaders and provide security. The process of conversion of encrypted data back to the original data is Decryption, restoring the original data. For cloud storage both symmetric-key (secret-key) and asymmetric-key (public-key) algorithms could be used to for implementation of cryptography. For large databases, asymmetric-key (public-key) algorithm's performance is slower in comparison to symmetric-key (secret key) algorithms. In this paper, we propose a new symmetric cryptographic algorithm that splits the plaintext and the key in equal numbers and applies the split key on corresponding split plaintext. Here the number of splits is determined by a random number generating algorithm. The input to crypto algorithm is a file (the plaintext) and password (the key).

II. SPLITTED PLAIN-TEXT KEY PAIR (PI, KI) ALGORITHM

The algorithm uses a password to encrypt the file with a unique number that creates an encrypted text file. The same password is used to decrypt the file, enabling maximum security. The algorithm in detail:

The plaintext for algorithm is a file that contains some text information and the key is the password of the file. The algorithm computes a random number from the given password to generate a key. The number of letters and ASCII value of the key determines number of splits of key and the plaintext. The key and the plaintext are split equally. Let plaintext (P) be split into [p1,p2, p3...pn] and let key (K) be split into [k1,k2,k3...kn.] The pairs (p1,k1), (p2,k2), (p3,k3)...(pn,kn) undergo encryption. For a pair (pi,ki) referred to as split plaintext key pair, (pi) is encrypted by the key (ki).

The algorithm uses shift cipher to create the cipher text. Shift cipher is applied on each split plaintext key pair to get corresponding cipher text. These cipher texts are then combined to get the final cipher text. Figure 1 shows the flowchart on encryption side.

III. K-NEAREST NEIGHBOR CLASSIFIER (KNN)

Encryption is done as in the following steps:

1) Step 1 - Start
2) Step 2 - Accept file name and password

3) Step 3 - Generate unique random number from the password, which becomes the key
4) Step 4 - Split plaintext and the key into n splits
5) Step 5 - Encrypt the first split of the plaintext (p1) with the first split of the key (k1), second split of plaintext (p2) with second split of key (k2) and so on
6) Step 6 - Combine splits to get the cipher text
7) Step 7 - Stop

IV. FLOWCHART FOR ENCRYPTION

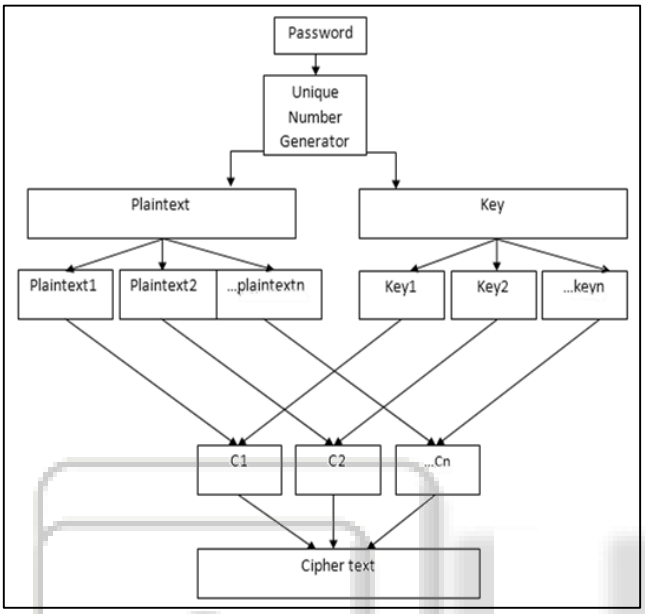

Fig. 1: Split Plaintext Key-Pair Algorithm – Encryption

V. INTRUDER DETECTION PROCEDURE

The unique random number is generated from key. Each character of password is converted to ASCII. Depending on number of characters of key and the ASCII value of each character a unique number "n" is generated. This unique number "n" represents the number of splits on the plaintext and key. Figure 2 illustrates the uniqueness of the random number generator for 50 trials. For each trial the password is entered and a random number is generated.

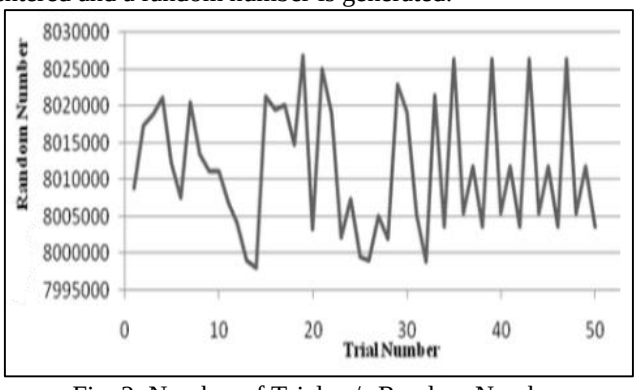

Fig. 2: Number of Trials v/s Random Number

VI. DECRYPTION

By applying Unique Number Generator, password of the file (symmetric key) is divided to get the number of splits. The key and cipher text are then split accordingly. The split key is applied on corresponding split cipher text (i.e. i^{th} key split is applied on i^{th} cipher text) for decryption. Combine the plaintext splits to complete the decryption process as shown in Figure 3.

VII. FLOWCHART FOR DECRYPTION

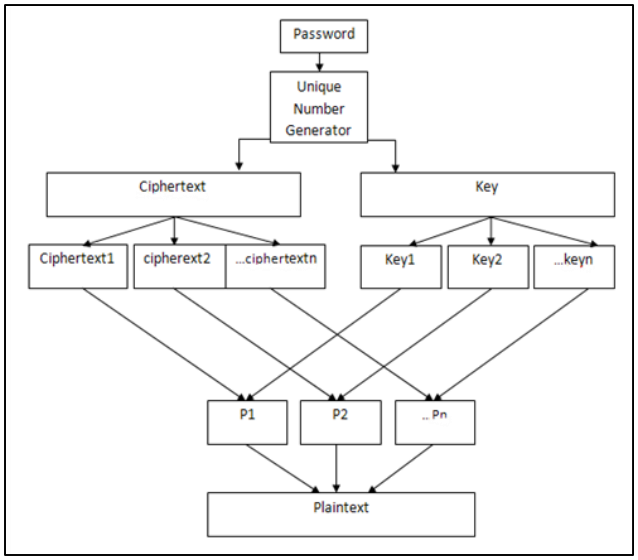

Fig. 3: Split Plaintext Key-Pair Algorithm – Decryption

ACKNOWLEDGMENT

It gives me immense pleasure to express my deepest sense of gratitude and sincere thanks to my highly respected and esteemed guide Ms. Vanadana Choudhary (Assistant Professor, IT), MAIT Delhi, for her valuable guidance, encouragement and help for completing this work. Her useful suggestions for this whole work and co-operative behaviour are sincerely acknowledged. I am also grateful to my project coordinator, Mr. Varun Goel for his constant support and guidance. Also, I wish to express indebtedness to my parents and my family members whose blessings and support have always helped me to face the challenges ahead.

REFERENCES

[1] William Stallings, "Cryptography and Network Security" 4th Edition. Pearson Education Inc, Upper Saddle River, New Jersey, 2006.
[2] Christopher Paar, Jan Pelzl, Bart Preneel,"Understanding Cryptography- A Textbook for Students and Practitioners", Springer, Berlin Heidelberg 2010.
[3] Aruljothi, S. Venkatesulu, M.R. Nicole, "Symmetric Key Cryptosystem Based on Randomized Block Cipher", Future Information Technology (FutureTech), 2010 5th International Conference

