SECURING THE DATA IN THE CLOUD USING TWO FISH ALGORITHM

[1]P Dileep Kumar Reddy
Lecturer, CSE Department,
JNTUA College of Engineering, Anantapuram, Andhra Pradesh, India

Abstract--In 2016 Perez et.al proposed an data driven access control scheme for self-ensured information that can keep running in entrusted CSPs. Their plan is helpless against Man-in-Middle assault and uses more mind boggling encryption strategies. So this paper introduces an answer in which security is centered on ensuring the client information paying little mind to the cloud specialist co-op that holds it. The arrangement in this paper exploits encryption of information to be transferred to cloud utilizing Two Fish Algorithm.

Keywords-- Cloud Computing, Man-in-Middle attack, Two Fish Algorithm.

I. INTRODUCTION

Security and protection are the noteworthy factors in the execution of cloud for securing data. It is basic to ensure the data respectability, security and affirmation for the cloud advantage. Therefore, a couple of expert focuses are using various methodologies and instrument that depend on the nature, sort and size of data.

Sharing data among various affiliations is the key favored point of view of Cloud Computing. Nevertheless, this favored point of view itself speaks to a danger to data. To avoid this potential danger to the data, it is critical to secure data chronicles.

This paper is the investigation of information security and talks about around Two Fish encryption calculation that protected information put away on mists. Two Fish is piece figure calculation and is secure against cryptanalytic assaults. It is adaptable, which implies it can be actualized on various workplace effectively, its key readiness is capable which implies setup time of key is less and this calculation is straightforward and to utilize it.

Section 2 shows the sorts of dangers and some capable data security techniques hold all through the world to data in cloud. In Section 3 we survey perez.et.al plan and its issues. Section 4 depicts the proposed outline and its Security examination is displayed in section 5. The last segment contains the conclusion.

II. THREATS AND SECURITY STRESSES IN CLOUD PROCESSING

A couple of threats and security concerns are connected with cloud computing and its data. Regardless this construction assesses, the limit out in the open cloud and multi inhabitance which are identified with the information security in cloud computing [2].

Capacity in Public Cloud

The security stress in cloud computing is securing data in an open cloud. Cloud united storerooms, which can be a drawing in center for software engineers. Limit assets and convoluted structures that are mix of rigging. Programming use can likewise cause introduction information if a slight burst happens in the comprehensive group cloud [4].

Remembering the true objective to keep up a vital separation from such dangers, it is continually endorsed to have a private cloud if workable for incredible degree sensitive data**.**

Multi tenancy

Shared or multi tenure is besides considered as one of the honest to goodness hazard to information in cloud computing [3]. Since various customers are using the same shared figuring resources like CPU, Storage and memory et cetera it is hazard to a customer's and additionally various customers.

In such circumstances there is reliably a danger of private data flood together to various customers. Multi occupancy can be especially unsafe in light of the way that blame in the structure can engage another customer or software engineers to get to every last single other information [5]. These sorts of issues can be managed via deliberately approving the customers previously they can approach the data. A couple of check frameworks are being utilized to avoid multi tenure issues in cloud computing [6].

III. REVIEW OF PEREZ ET.AL. SCHEME

In this area, we audit the Perez.et.al.[1] plot. This plan is made out of 6 stages to be specific setup stage, key era stage, encryption stage, re-key era stage, re-encryption stage and unscrambling stage. A personality based intermediary Re-encryption (IBPRE) approach has been utilized by perez. It consolidates both Identity-based encryption (IBE) and Proxy re-encryption (PRE), enabling an intermediary to interpret a cipher ext encryption under a client's personality into another cipher text under client's character. For approval reason Role Based access control (RBAC) was utilized as a part of this plan which takes more intricate work to approve the client to scramble the record and also to unscramble it. The stages were portrayed each as takes after:

Setup Phase

It states the cryptographic scheme. Takes the contribution from the client open parameters p and security parameter k and yields both the Master mystery key msk and an arrangement of open parameters p that is utilized as contribution for the rest capacities.

Key Generation Phase

Creates secret keys. It takes contribution as msk and a personality idœ and yields the mystery key skœ relating to that character.

Encryption Phase

Encrypts information. It takes an information a character idœ and a plain content m, and yields the encryption of m under determined personality cœ.

Re-key Generation Phase

Produces Re-encryption keys. It takes as information the source and target characters idœ and idβ and in addition the secret key of the source personality skœ and yields the Re-encryption key rkœ→β that empowers to re-scramble from idœ to idβ.

Re-Encryption Phase

Re-encodes information. It takes as info a cipher text cœ under character idœ and a Re-encryption key rkœ→β and yields the re-scrambled figure content cœ under personality idœ.

Decryption Phase

Decrypts information. It takes as info a figure content cœ and its relating mystery key skœ; and yields the plain content m coming about of unscrambling cœ.

Problems in marin perez model

The Perez.et.al proposed scheme does not give a protected confirmation process which may prompts a security threat. In the event that user id and secret word of a client were hacked then there is conceivable shot of taking the information from client's cloud account. The algorithm Identity-based proxy re-encryption (IBPRE) that perez group used to scramble information doesn't give end-to-end confirmation to getting to information, even the mind boggling encryption philosophies and the decoding strategy turns out to be more asset complex which prompts Man-in-Middle attack.

To address these issues in Martin Perez display, we propose another model that defeats existing framework demonstrate issues. The proposed demonstrate utilizes Two Fish Algorithm to encrypt the information which performs more effectively than existing framework algorithm.

IV. PROPOSED MODEL FOR AUTHENTICATION AND ENCRYPTION PROCESS

Proposed model contains Two Fish Algorithm where it will be used for the encryption as well as for the decryption process [7]. The entire procedure will be discussed as follows:

Two Fish Building Block

Feistel Networks – the major building square is the F work:

- A key-subordinate mapping of an information string onto a yield string.
- An F work is dependably non-direct and potentially non-surjective

$$F : \{0,1\}^{n/2} \times \{0,1\}^{N} \mapsto \{0,1\}^{n/2}$$

- Where n is the piece size of the Feistel Network, and F is a capacity taking n/2 bits of the square and N bits of a key as info, and delivering a yield of length n/2 bits

Two Fish Round Description

- The two words on the left are utilized as contribution to the g capacities after the turn by 8 bits of one of them
- The g work comprises of four far reaching key-subordinate S-boxes, trailed by a direct blending venture in view of a MDS network
- The aftereffects of the two g capacities are consolidated utilizing a Pseudo-Hadamard Transform (PHT), and two catchphrases are included
- One of the words on the privilege is pivoted by 1 bit and afterward them two are XORed in to the outcomes on the left
- The left and right parts are then swapped for the following round
- After 16 adjusts, the swap of the last round is turned around, and the four words are XORed with four more watchwords to create the cipher text.

Proposed Scheme

The design shows how the Two Fish Algorithm endeavors to affirm customer and to scramble data in the Cloud. This proposed plot contains 2 stages which are key era stage and Data transmission stage.

Key Generation Phase

Domain Authority produces an arbitrary key PK in view of clients and information proprietor's parameters and id that were taken at the enlistment stage. Space expert sends those created key to their separate character individual

Data transmission Phase

Data transmission phase contains two phases. They are encryption phase and decryption phase.

- ***Encryption Phase***

Data owner scrambles the record m utilizing information proprietor's personality idœ private key PK and transfers it to the cloud. The key that was utilized to encode the record is just used to unscramble that scrambled document Cœ.

$$(m, PK, id_{œ}) \rightarrow C_{œ}$$

- ***Decryption Phase***

Data Owner encoded record Cœ that is transferred to cloud gets unscrambled, when client demonstrates character. The client demands key to decode the encrypted document to the area specialist. Space expert sends key PK alongside character of the data owner idœ to decrypts the document.

$$(C_{œ}, PK, id_{œ}) \rightarrow m$$

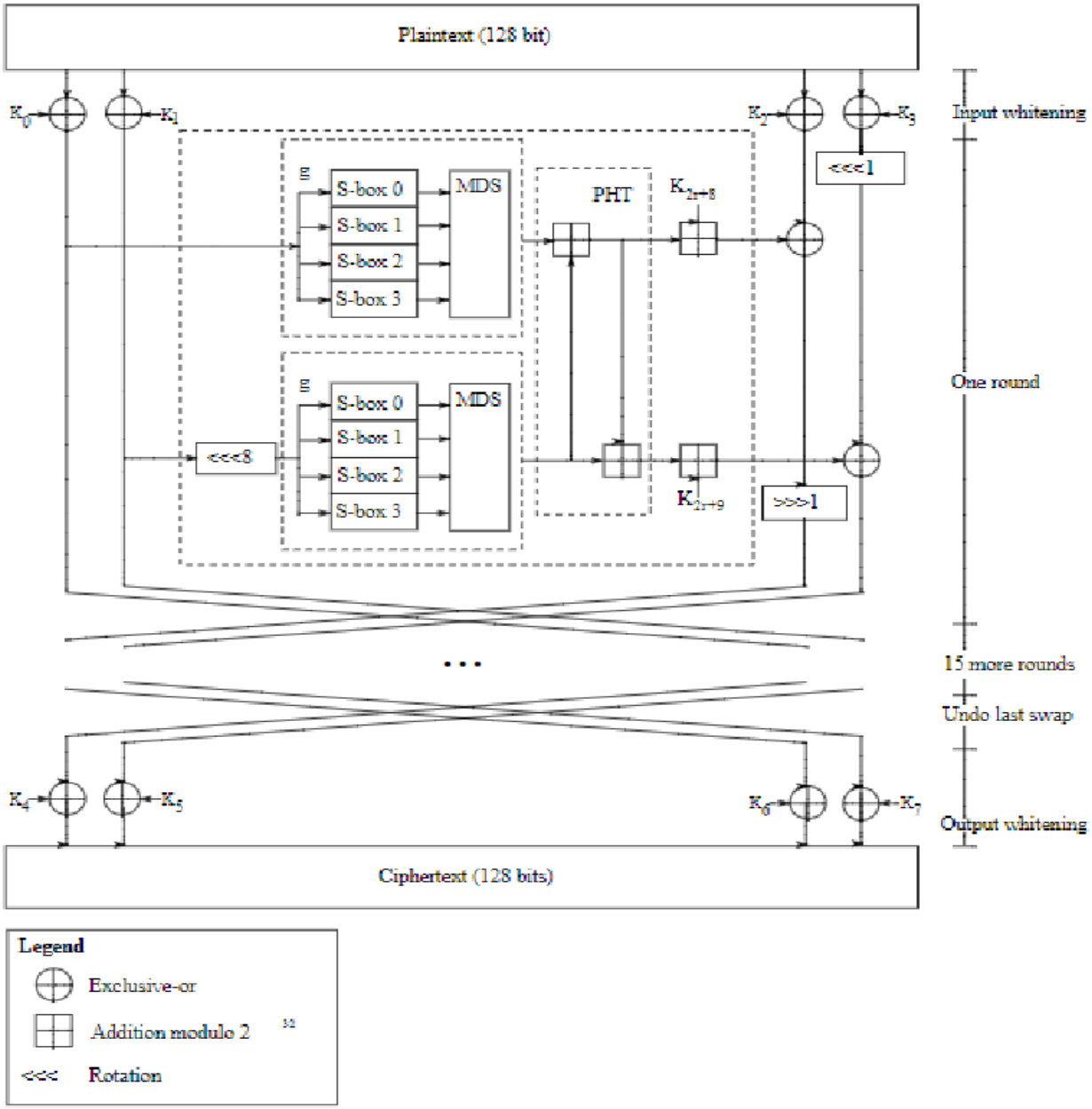

Figure 1: Flow of Mechanism of Proposed System

V. PERFORMANCE ANALYSIS AND SECURITY ANALYSIS

In this section, we show that our scheme works more efficient than Perez scheme.

Performance Analysis

Time taken by various phases in both the schemes is given in Table: 1

Phases	**Perez et.al Scheme**	**Our Scheme**
User setup	178	122
Key Generation	29	19
Encryption	29	17
Decryption	247	23
Total	**489**	**181**

Table 1: Comparison of Two Schemes

The comparisons of two schemes were showed below using a graph which shows performance of both schemes in milliseconds. See Fig:2

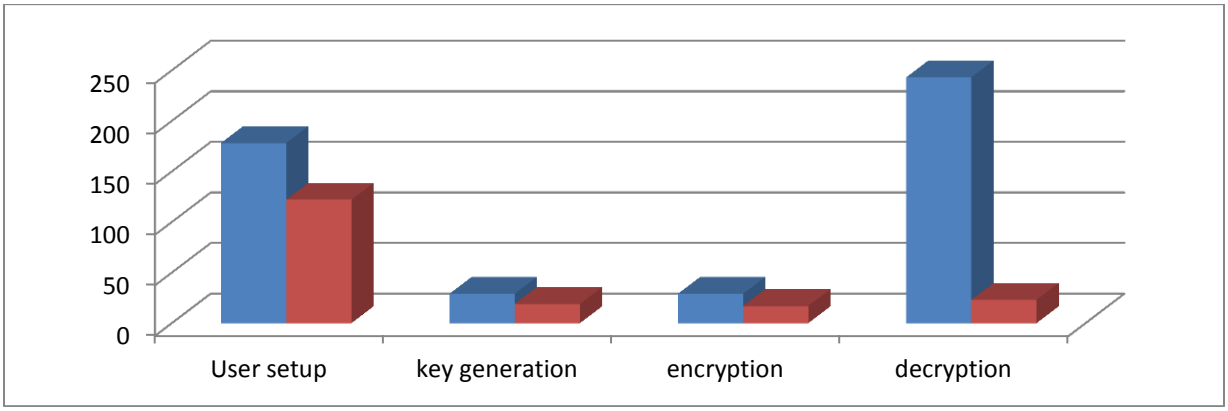

Figure 2: Graph comparing both schemes

Defend Man-in the Middle Attack

This scheme defends the man-in-the middle attack as for every round the key gets changed and even the size of the key will not be predicable to the person who is in the middle.

VI. CONCLUSION

The risk of security is an earnest concern, where some secret information is secured in cloud. It is basic to judge the customer approval suitably to expel data from the cloud. In case we use single factor to endorse the customer it may break downs the entire data security then positively some additional counter measure should be taken while laying out he illustrate.

We have formed a model that thrashings all security issues to secure data in the cloud. In any case, the Two Fish calculation security is ensured just in case it is precisely executed and extraordinary key organization is used.

VII. REFERENCES

[1] Juan M. Marin Perez gregorio Martinez Perez Antonio F. Skarmea Gomez "SecRBAC: Secure data in the Clouds" IEEE Transactions , DOI 10.1109/TC.2016.2553668.

[2] P. S. Wooley, "Identifying Cloud Computing Security Risks," *Contin. Educ.*, vol. 1277, no. February, 2011.

[3] F. Sabahi, "Virtualization-level security in cloud computing," *2011 IEEE 3rd Int. Conf. Commun. Softw. Networks*, pp. 250–254, 2011.

[4] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," *Security*, no. February, pp. 1–14, 2013.

[5] A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," *4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc.*, pp. 121–128, 2012.

[6] T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy," p. 299, 2009.

[7] P. Dileep Kumar Reddy, R. Praveen Sam, C. Shoba Bindu "Optimal Blowfish Algorithm based Technique for Data Security in Cloud" Int. J. Business Intelligence and Data Mining, Vol. 11, No. 2, 2016**.** Pp.171–189**.** DOI: 10.1504/IJBIDM.2016.10001484