International Journal of e-Collaboration
Volume 16 • Issue 1 • January-March 2020

Secure and Effective Key Management Using Secret Sharing Schemes in Cloud Computing

Shahin Fatima, Integral University, India

Shish Ahmad, Integral University, India

ABSTRACT

Security is a crucial problem in Cloud computing. Storing and accessing the data in the Cloud is very popular nowadays but the security of data is still lagging behind. Secret sharing schemes are widely used to improve the security of data. In this article, a threshold secret sharing scheme using Newton divided difference interpolating polynomial (TSSNIP) is proposed in a distributed Cloud environment to enhance security of keys used for encryption. The proposed method uses a Newton divided difference interpolating polynomial for key splitting and key reconstruction. A threshold value is used to reconstruct the shares in secret sharing schemes. The proposed work made use of dynamic and random threshold generation method to ensure security of key. The experimental output shows reduced execution time, better security, efficiency, and robustness in the proposed scheme. Furthermore, the proposed scheme also outperformed other secret sharing schemes.

KEYWORDS

Cloud Computing, Encryption, Interpolating Polynomial, Newton Divided Difference, Privacy, Security, Shamir Secret Sharing, Threshold Generation

DOI: 10.4018/IJeC.2020010101

INTRODUCTION

The development of cloud computing led many people to store their data on the cloud. Cloud computing is relatively less expensive and easier for data storage which makes it progressively popular. However, leakage of data sensitive information can be a significant threat. When the users upload their data on the cloud, they lose control of their information to resource providers. Encryption is the basic method used for preventing the resource providers to retrieve plaintext data. If the keys used for encryption is hacked, then the whole data is lost. So, the main question is how to protect the keys used for encryption process? Secret-sharing schemes (SSS) are used to alleviate the risk of key management. Adi-Shamir (Shamir, 1979) and George -Blakeley (Blakeley, 1979) proposed the idea of Secret-sharing schemes SSS" s. In secret sharing schemes the data is partitioned into several shares and stored on different resource providers. A threshold value is calculated to retrieve the original data. In order to reconstruct the original secret, the number of data shares must be smaller than threshold value. Shamir' Secret-sharing schemes-SSS uses Lagrange Interpolating-Polynomial and geometry is used in Blakeley's SS. Different types of secret-sharing are proposed by various researchers.

In the given paper a threshold Secret-sharing scheme is proposed using Newton divided difference Interpolating Polynomial. The proposed method is made secure by using dynamic threshold generation. The paper comprises of the introduction of cloud computing followed by types of secret sharing schemes and LaGrange interpolating polynomial. Next, the problem statement is discussed and the proposed algorithm Threshold Secret-Sharing using Newton divided difference Interpolating Polynomial (TSSNIP) is described. Furthermore, the paper also discusses the experimental results of the proposed TSSNIP method and also compares the proposed method with existing methods. Finally, the paper highlights the conclusion with future work.

SYSTEM DESIGN

This section gives the detail of various Secret-Sharing Scheme's.

Secret Sharing Scheme

Adi-Shamir & George-Blakeley (Shamir, 1979; Blakely, 1979) developed Secret-Sharing Scheme's. The Shamir- Secret-sharing schemes makes use of polynomial interpolation. Shamir (k, n) threshold scheme states that 'k'-points are required to create a polynomial of [k-1] degree. In this scheme Lagrange' Interpolating polynomial is used. The Secret is partitioned into several shares(n) and minimum k threshold value is required to re-assemble the original secret data. Each user will have a share of secret. To re assemble the secret data, a sufficient number of shares should be collected. This sufficient number of shares are determined by threshold value k. If users can have k number of shares, they can re-assemble the secret data. The Secret-Sharing Schemes (SSS) can also be used to secure the data in 'multi-clouds' (Muhil et al., 2015). The encrypted data is stored on multiple clouds.

Definition

The given method is called 'k-n' threshold scheme. The algorithm partitions the data into n number of shares share1, share2, -----, share n such that:

1. Collecting k pieces of share will retrieve the original data;
2. Collecting k-1 or lesser pieces of share will not be sufficient to re-assemble the original data;
3. Collecting k=n pieces of share will retrieve the original data.

The aim of Shamir-SSS is to define that (k) points are necessary to describe a polynomial of degree k-1 i.e., a line is constructed using 2 points and a parabola is constructed using 3 points.