Analisis Perbandingan Skema Pembagian Rahasia Untuk Struktur Akses dan Struktur Terlarang Berdasarkan Graf

Retno Indah, author

Abstrak

Keamanan data terhadap informasi rahasia (secret) smerupakan hal yang sangat penting, sehingga tidak setiap orang berhak mengakses informasi rahasia tersebut. Oleh karena itu diperlukan suatu metode yang dapat digunakan untuk mengatur siapa saja yang berhak mengakses rahasia tersebut. Salah satu metode yang dapat digunakan adalah skema pembagian rahasia. Skema pembagian rahasia adalah suatu metode untuk membagikan potongan-potongan rahasia kepada partisipan sedemikian sehingga hanya subhimpunan-subhimpunan dari himpunan partisipan yang memenuhi kualifikasi tertentu yang dapat merekonstruksi rahasia.
Dalam skema pembagian rahasia terdapat skema yang berdasarkan Struktur Akses dan Struktur Terlarang. Struktur Akses adalah kumpulan dari subhimpunan-subhimpunan partisipan yang dapat merekonstruksi rahasia. Sedangkan Struktur Terlarang adalah kumpulan dari subhimpunan-subhimpunan partisipan yang tidak dapat merekonstruksi rahasia.
Dalam tulisan ini dibandingkan dua jenis skema tersebut yang berbentuk graf, dilihat dari cara membangun share dan information ratenya. Berdasarkan graf yang digunakan, tahapan konstruksi pada skema dengan Struktur Akses lebih sederhana jika dibandingkan dengan skema dengan Struktur Terlarang. Berdasarkan konstruksi skema maka dapat disimpulkan kedua skema tersebut bukan skema yang saling komplemen meskipun representasi grafnya saling komplemen.
.....Data security of confidential information is something that is very important, so not everyone has access to such confidential information. Therefore we need a method that can be used to regulate anyone who has access the secret. One method that can be used is a secret sharing scheme. Secret sharing scheme is a method to distribute pieces of the secret to the participants such that only qualified subsets of the participants that can reconstruct the secret.
In secret sharing schemes are schemes based on Access Structure and Prohibited Structure. Access Structure is a collection of subsets of participants that can reconstruct the secret. While the Prohibited Structure is a collection of subsets of participants who can not reconstruct the secret.
In this paper we compare two types of such schemes based on graphs, and we see from the process of building the share and from the information rate. Based on the graph is used, the stages of construction on the scheme with access structure is simpler than the scheme with access structure. The two schemes are not complement to each other, even the graph representations are complement each other.