Implementasi Zero-Knowledge untuk menjaga privasi pada Aplikasi Crowdsensing: Studi kasus Sistem SmartParking = Zero-Knowledge implementation on Crowdsensing Application to protect privacy: Case study of SmartParking System

Gregorius Aprisunnea, author

Abstrak

Aplikasi crowdsensing adalah aplikasi yang mampu membantu dalam pengumpulan data secara bersama-sama yang dilakukan oleh banyak partisipan sekaligus. Di dalam aplikasi crowdsensing yang membutuhkan penyimpanan atau pemrosesan data pengguna, priva- si pengguna dapat dipertanyakan keamanannya. Pada penelitian ini diimplementasikan pemanfaatan metode kriptografis bernama zero-knowledge pada aplikasi crowdsensing bernama SmartParking. SmartParking adalah sistem crowdsensing yang memungkinkan pengguna untuk mengetahui ketersediaan tempat parkir pada lokasi tertentu dan juga ber- partisipasi dalam menentukan ketersediaan suatu tempat parkir. Sistem SmartParking tidak menyimpan data pengguna pada server dan implementasi zero-knowledge dilakuk- an dengan mengintegrasikan protokol privacy preserving yang dirancang khusus untuk SmartParking. Protokol tersebut memastikan bahwa data pengguna yang diproses di dalam sistem SmartParking tidak diketahui oleh backend SmartParking. Akan tetapi, kebenaran atas pengetahuan akan data tersebut tetap dapat diverifikasi di dalam sistem SmartParking. Pada akhir penelitian dihasilkan produk berupa sistem SmartParking yang telah mengimplementasikan empat dari lima sub-protokol utama pada protokol privacy preserving.

.....Crowdsensing application is an application that helps in collecting massive data be- tween many participants. In a crowdsensing application that needs to store or process user information, user privacy might be intruded. This research implements a cryptogra- phic method called zero-knowledge in a crowdsensing application called SmartParking. SmartParking is a crowdsensing system that helps in providing parking availability in many different places. Through SmartParking, user can know the availability of parking spots inside a certain location and also participate to decide the availability of a certain parking spot. SmartParking system is designed to not store user data inside its backend server. Zero-knowledge implementation in SmartParking is done by integrating a privacy preserving protocol specially made for SmartParking. The protocol will make sure that user information that is processed by SmartParking system is not known by SmartPar- king’s backend. However, the knowledge of knowing that certain information can still be verified. At the end of this research, a new SmartParking system that has implemen- ted four of the five sub-protocols in the privacy preserving protocol for SmartParking is produced.