

Peningkatan Keamanan dengan Implementasi *Secure Multy Computation* pada Absensi Mahasiswa Menggunakan Metode *Shamir Secret Share*

Dimas Pangestu Restu Putra¹, Maman Abdurohman², Aji Gautama Putrada³

^{1,2,3}Fakultas Informatika, Universitas Telkom, Bandung
¹dimasprp@students.telkomuniversity.ac.id, ²abdurohman@telkomuniversity.ac.id, ³
ajigp@telkomuniversity.ac.id

Abstrak

Penggunaan perangkat RFID sebagai absensi kehadiran mahasiswa masih rentan terhadap rekayasa absensi. Sehingga mahasiswa dapat menyalahgunakannya seperti melakukan spoofing atau merekayasa pada absensi tersebut, dengan kata lain RFID dapat dikatakan tidak aman jika tidak meningkatkan keamanan dalam RFID tersebut. Keamanan yang telah dilakukan dengan penerapan implementasi *Secure Multiparty Computation* menggunakan metode *Shamir Secret Share*. Berbagi rahasia pada metode Shamir menggunakan perhitungan interpolasi linear, untuk menentukan nilai yang berada diantara dua persamaan berbasis linear dimana nilai setiap RFID memiliki dua titik koordinat yang berbeda untuk menentukan titik temu antar keduanya. Telah ditentukan nilai X sebagai nilai rahasia Dosen dan nilai Y sebagai nilai rahasia mahasiswa. Bahwa nilai X tersebut telah ditentukan nilainya untuk memperoleh share rahasia nilai Y tersebut. Pemanfaatan seperti ini dapat membuat kamanan pada RFID tersebut lebih aman dengan sistem keamanan tambahan.

Kata kunci : *Interpolasi linear, RFID, Secure MultyParty Computation, Shamir Secret Share.*

Abstract

The use of RFID devices as student absent turns out that it is still vulnerable to attack commonly called attendance engineering. So that students can misuse if students can abuse it like spoofing or manipulating the attendance, it can be said RFID is not safe if it does not improve security in the RFID. The security that has been done with the application of the implementation of the Secure Multi-Party Computation used the Shamir Secret Share. Secret shared on Shamir method uses a calculation by linear interpolation, to determine the value of which is between two values based linear equation where each RFID has two different coordinate points to define the common ground. Rated X for secret share values lecturers and the Y value as the value of the secret of the student, which is where the value of X has been determined that the calculation is to obtain secret share student (Y). Utilization like this can make it a more secure RFID security system with the added security.

Keywords: *Linear Interpolation, RFID, Secure Multy-Party Computation, Shamir Secret Share*

1. Pendahuluan

Latar Belakang

Teknologi bidang IoT dalam satu dekade terakhir semakin berkembang. Hal ini karena teknologi IoT dipercaya dapat mempermudah berbagai kegiatan sehari-hari [1][2]. Salah satu teknologi yang marak dikembangkan saat ini adalah RFID. RFID merupakan teknologi yang telah ada sejak 50 tahun terakhir, dan telah digunakan diberbagai organisasi industri seperti perkantoran, perkuliahan dan berbagai macam perusahaan lainnya[2][3]. Pada sistem keamanan RFID ini digunakan untuk berbagai macam hal, seperti absensi data kehadiran, serta keamanan ruangan yang dipasang RFID pada pintu.

Kasus yang akan dibahas kali ini mengenai sistem absensi pada absensi perkuliahan. Kehadiran di kelas adalah kondisi utama bagi mahasiswa untuk mendapatkan hasil akademik yang baik[4]. Dalam kasus ini penggunaan absensi dengan RFID cukup efektif dan efisien. Karena secara unik dapat mengidentifikasi seseorang berdasarkan tag yang dimasukkan [4]. Setiap mahasiswa memiliki RFID yang telah diberikan oleh kampus untuk melakukan tag absensi di kelas, dengan menggunakan kode unik yang menyimpan identitas mahasiswa itu sendiri dengan menggunakan uid yang membedakan mahasiswa satu dengan yang lainnya. Namun penggunaan RFID ini hanya sebatas penyimpanan uid sehingga RFID tersebut dikatakan masih belum aman, karena pada kasus lain RFID dapat dikloning pada sistem RFID anonim, dengan menyamakan uid pada RFID lainnya [5].

Pada tugas akhir ini akan mengambil suatu kasus absensi di Universitas Telkom yang telah menggunakan kartu RFID sebagai absensi, akan tetapi absensi tersebut tidak cukup aman. Seperti mahasiswa melakukan tap yang tidak dibatasi oleh waktu, sehingga mahasiswa dapat melakukan absensi sebelum dosen pengampu hadir di