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

Dimas Pangestu Restu Putra[1], Maman Abdurohman[2], Aji Gautama Putrada[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]dimasprp@students.telkomuniversity.ac.id, [2]abdurohman@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 kemanan 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 witg 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

kelas atau melakukan absensi ketika pembelajaran telah usai akan tetapi waktu pembelajaran tersebut belum selesai sesuai dengan waktu yang telah diberikan. Oleh karena itu perlu adanya peningkatan keamanan dan kewaspadaan terhadap penyimpanan data-data pada user RFID [5]. Upaya peningkatan kemanan yang dilakukan dengan menggandakan keamanan pada pengguna RFID [6]. Sistem yang dimakasud dengan menggandakan keamanan ini dengan menambahkan kode dengan peimplementasian *Secure Multy-Computation* yang melakukan kolerasi sederhana dengan menggunakan pola tag [6]. Tag tersebut menyimpan data yang akan diproses dengan metode *Shamir Secret Shared*. peningkatan keamanan ini guna pencegahan terhadap rekayasa absensi.

Topik dan Batasannya

Pada latar belakang tersebut terdapat beberapa permasalahan yang telah disebutkan yang pertama adalah mengenai implementasi *Secure Multy-Party Computation*, dengan membuat pola dengan metode *Shamir Secret Shared*. Metode tersebut digunakan dengan tujuan menentukan titik satu dengan titik lainnya. Pada permasalahan kedua pada metode ini melakukan bagaimana cara bertemu dengan titik satu dengan titik lainnya dalam suatu garis lurus yang membuat titik temu.

Pada perumusahan masalah diatas diberikan batasan-batasan untuk mempermudah pengimpementasikannya dengan menentukan satu titik secret pada RFID dosen tersebut. Batasan kedua menggunakan perhitungan operasi linear karena pada pengujian tersebut hanya terdapat dua user yaitu satu dosen dan satu mahasiswa. Batasan ketiga, dalam perhitungan interpolasi linear diketahui beberapa titik yaitu $(x1, y1)(x2, y2)$ nilai x, yang dimana nilai x1 < x < x2. Batasan yang ketiga dengan mengkonversikan batasan waktu pada tag dosen tersebut dengan waktu yang telah ditentukan.

Tujuan

1. Melakukan pola *Secure Multi Computation* dengan menggunakan skema tag dosen terlebih dahulu.
2. Mendapatkan hasil Share Secret tersebut menggunakan perhitungan interpolasi linear.

Organisasi Tulisan

Urutan penulisan laporan selanjutnya adalah bagian 2 menjelaskan tentang studi yang terkait dengan penelitian ini. Pada bagian ke 3 dijelaskan detil sistem yang dibangun menggunakan *Secure Multy Computation* beserta Metode *Shamir Secret Share*. Pada bagian ke 4 berisi tentang hasil pengujian dan analisis hasil pengujian. Pada bagian ke 5 berisi tentang kesimpulan dan saran pengembangan untuk penelitian selanjutnya.

2. Studi Terkait

2.1 RFID

RFID merupakan salah satu teknik pengidentifikasi secara otomatis. Sistem otomatis ini terdiri dari microchip yang terdapat didalem tag RFID yang berfungsi untuk membaca data pada tag RFID tersebut [7]. RFID merupakan elektronik yang aman dengan pengidentifikasi teknologi nirkabel berdasarkan sistem resonan [7][8]. Setiap tag pada RFID tersebut menyimpan Uid dan memiliki memori untuk menyimpan Uid masing-masing pada tiap tag tersebut. Penggunaan tag RFID tersebut dengan menempelkan pada sensor yang biasa dinamakan Rc522 atau RFID Reader. RFID memiliki bagian yaitu :

a. RFID Reader yang berfungsi sebagai alat yang digunakan untuk membaca Tag RFID melalui gelombang radio. Gelombang radio yang dipancarkan melaui antena yang berfungsi mentransmisikan gelombang [8]. Pada tag RFID karakteristik tag baca pada jangkauan maksimum yang harus diperhitungkan [9]. Gambar no 1 adalah RFID Reader.

Gambar 1. RFID Reader