Analisis Penerapan Skema Pembagian Rahasia Bai untuk Keamanan Lokasi

Nando Rusrin Pratama / 13517148
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517148@std.stei.itb.ac.id

***Abstrak*— Skema pembagian rahasia adalah suatu metode penyebaran data ke sekumpulan pihak sehingga data hanya dapat direkonstruksi oleh sebagian dari kumpulan tersebut. Kegunaan dari skema pembagian rahasia adalah untuk memperketat keamanan dari sebuah data yang dianggap penting. Aplikasi-aplikasi *secret sharing* dapat diterapkan dalam berbagai bidang antara lain perjanjian Byzantine, E-voting, manajemen kata sandi di keaman jaringan, kriptografi ambang, penyembunyian informasi, keamanan transaksi daring hingga keamanan lokasi. Pada makalah ini akan dibahas mengenai analisis suatu skema pembagian rahasia yaitu skema Bai. Selain itu, akan dibahas juga mengenai analisis skema pembagian rahasia Bai untuk keamanan lokasi.**

Kata Kunci*— *Skema pembagian rahasia; skema Bai; skema ambang; dealer; participant; keamanan lokasi.

I. PENDAHULUAN

Skema pembagian rahasia merupakan salah satu cara yang efektif untuk mendistribusikan sebuah pesan rahasia ke sekumpulan pihak tertentu, yang dimana setiap pihak memegang sebuah bagian dari pesan rahasia. Salah satu skema pembagian rahasia yang dikenal adalah skema pembagian rahasia Shamir. Skema Shamir membagi sebuah pesan rahasia ke dalam beberapa bagian, lalu membagikan setiap bagian unik dari pesan rahasia kepada sejumlah partisipan.

Skema pembagian rahasia yang diusulkan oleh Shamir (1979) memanfaatkan konsep matematika bahwa polinomial berderajat k-1 dapat didefinisikan jika diketahui sejumlah k titik yang melewati polinomial tersebut. Skema ini dapat kita modifikasi untuk mempermudah pembaruan bagian. Pembaruan bagian adalah proses mengubah seluruh bagian tanpa mengubah data asli untuk meminimalisasi kemungkinan bocornya pesan rahasia jika ada bagian yang dicuri. Ide pembaruan bagian pertama kali dicetuskan oleh Ostrovsky & Yung (1991). Pembaruan bagian dilakukan dengan melakukan konstruksi ulang pesan rahasia dan pembagian ulang bagian. Lalu, Herzberg dkk., (1995) mengajukan sebuah ide untuk pembaruan bagian yang lebih baik yang diberi nama pembagian rahasia proaktif. Pada pembagian rahasia proaktif, pembaruan bagian tidak membutuhkan proses rekonstruksi pesan rahasia sehingga keamanan pesan rahasia lebih terjamin.

Salah satu aplikasi dari skema pembagian rahasia yang dapat ditingkatkan keamanannya lewat pembaruan bagian dengan pembagian rahasia proaktif adalah lokasi. Hal ini dikarenakan aplikasi yang menangani lokasi harus dapat menangani proses pengiriman bagian. Untuk itu, aplikasi tidak dapat digunkan untuk menangani proses pembangkitan bagian dan rekonstruksi pesan rahasia saja. Hal ini dikarenakan jika bagian dikirim secara manual dapat berpotensi menyebabkan kebocoran bagian jika cara pengiriman yang dipilih tidak aman.

Dalam makalah ini, akan dibahas mengenai aplikasi penanganan proses pengiriman bagian sehingga keamanan bagian dapat lebih terjamin. Analisis akan dilakukan dengan mempertimbangkan pengiriman bagian menggunakan sistem terdistribusi, yaitu sistem yang berjalan pada suatu jaringan sehingga setiap komponen dapat saling berhubungan dengan komponen lain walaupun terletak pada lokasi yang berbeda. Oleh karena itu, perlu dibahas mengenai skema pembagian lokasi rahasia yang mampu mendukung layanan pembagian rahasia proaktif, yaitu skema Bai.

II. DASAR TEORI

A. Skema Pembagian Rahasia Shamir

Shamir (1979) mengembangkan gagasan untuk teknik berbagi rahasia berbasis ambang batas dengan $k \leq n$. Teknik untuk membangun fungsi urutan polinomial $(k-1)$ adalah,

$$f(x) = d_0 + d_1x + d_2x^2 + \cdots + d_{k-1}x^{k-1} \pmod p,$$

dimana nilai d_0 adalah pesan rahasia dan p adalah bilangan prima. Bagian rahasia adalah pasangan nilai (x_i, y_i) dimana

$$y_i = f(x_i),\ 1 \leq i \leq n \text{ dan } 0 < x_1 < x_2 \cdots < x_n \leq p-1.$$

Fungsi polinomial $f(x)$ dihancurkan setiap P_i mendapatkan pasangan nilai baru (x_i, y_i) sehingga tidak ada bagian yang mengetahui d_0 sebelumnya. Jika hanya $(k-1)$ bagian rahasia atau kurang yang tersedia, maka tidak dapat digunakan untuk menemukan pesan rahasia d_0. Sedangkan, jika k atau lebih bagian rahasia yang tersedia, maka kita dapat membuat k persamaan $y_i = f(x_i)$ dengan k parameter d_i. Lalu, solusi unik d_0 dapat diselesaikan. Selain itu, ada formula lain yang sering

digunakan adalah interpolasi Lagrange (Shamir, 1979) untuk mendapatkan pesan rahasia d_0 yaitu

$$d_0 = \sum_{i=0}^{k} \left(\prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-x_j}{x_i - x_j} \right) y_i \pmod p$$

dimana (x_i, y_j) adalah bagian k untuk $1 \leq i \leq k$. Formula ini sudah cukup bagus karena mengetahui (k − 1) persamaan tidak dapat menyebabkan didapatkan pesan rahasia.

B. Skema Pembagian Rahasia Proaktif Herzberg

Salah satu cara untuk menghindari serangan dari pihak lain adalah dengan melakukan perbaruan bagian rahasia secara berkala. Herzberg et al. (1995) mengembangkan sebuah skema pembagian rahasia proaktif dari skema Shamir. Setelah inisialisasi pada skema Shamir, pada awal setiap periode waktu, semua bagian dapat memicu fase pembaruan di mana bagian melakukan protokol pembaruan bagian. Bagian yang dihitung pada periode t dilambangkan dengan menggunakan skrip t, yaitu, $(x_i, f^t(x_i))$, $t = 0, 1, ...$ dengan pesan rahasia d_0 pada waktu $(t - 1)$ adalah

$$d_0 = f^{(t-1)}(0).$$

Algoritma ini akan membangun $(k – 1)$ fungsi polinomial acak baru pada setiap fase pembaruan sebagai berikut.

$$\delta(x) = a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \pmod p,$$

dimana $\delta(0) = 0$ sehingga $f'(0) = f^{(t-1)}(0) + \delta(0) = d_0 + 0 = d_0$.

Protokol pembaruan bagian Herzberg untuk setiap bagian P_i, $i \in A$, pada awal periode waktu t adalah sebagai berikut:

1. P_i memilih $k - 1$ angka acak dari Z_p untuk $m = 1, 2, ..., (k - 1)$. Angka-angka ini menentukan fungsi polinomail $\delta_i(x) = a_{i1}x + a_{i2}x^2 + \cdots + a_{i(k-1)}x^{k-1} \pmod p$ pada Z_p.
2. Untuk semua bagian P_j, P_i secara rahasia mengirim $u_{ij} = \delta_i(x_j)$ ke P_j .
3. Setelah mendekripsi u_{ji}, $\forall j \in \{1, 2,...,n\}$ P_i melakukan pembaruan bagian dengan formula

   $$f'(x_i) = f^{-1}(x_i) + u_{1i} + u_{2i} + \cdots + u_{ni} \pmod p,$$

4. P_i menghapus semua bagian kecuali bagian rahasia sekarang $y'_i = f'(x_i)$.

Fungsi $\delta(x)$ tidak memiliki nilai yang konstan, sehingga setiap bagian rahasia k atau lebih masih dapat menghitung d_0 dengan menggabungkan bagian baru mereka. Namun, kombinasi k bagian yang menggunakan bagian rahasia sebelumnya dan saat ini tidak dapat digunakan untuk merekonstruksi pesan rahasia. Untuk itu, pesan rahasia itu terlindungi dari pembobolan oleh musuh pasif.

C. Skema Pembagian Rahasia Projeksi Matriks Bai

Bai (2006) mengembangkan skema pembagian rahasia baru menggunakan metode projeksi matriks. Berikut penjelasan mengenai skema projeksi matriks Bai.

Misalkan A adalah matriks $m \times k$ dengan *rank* sebanyak k $(m \geq k > 0)$, dan

$$S = A(A\ A) - 1A\ \backslash,$$

dimana S' adalah matriks transpose. Matriks S adalah matriks proyeksi $m \times m$ dari matriks A.

Kita juga dapat menghitung vektor v_i menggunakan k linear bebas $k \times 1$ vektor x_i,

$$v_i = Ax_i,$$

dimana $1 \leq i \leq k$. Lalu, $m \times 1$ vektor v_i dapat dimasukkan ke

$$B = [\ v_1\ v_2\ ...v_k\ ].$$

Proyeksi matriks A sama dengan proyeksi matriks B. Dapat ditbuktikan melalui teorema berikut.

Teori 2.1 (Teori Invariansi): Untuk matriks $m \times k$ A dari *rank* k $(m \geq k > 0)$ dan matriks $m \times k$ B = $[v_1\ v_2\ ...\ v_k]$ di mana $v_i = Ax_i$ untuk $i = 1, 2, ..., k$ dan x_is adalah vektor $k \times 1$ bebas linear. Proyeksi matriks A adalah sama dengan matriks B, atau $S = A\ (A\ A) - 1A = B\ (B\ B) - 1B$.

III. Pemodelan Masalah dan Solusi

Terdapat sebuah lokasi rahasia yang terbagi menjadi tiga bagian rahasia yang harus dapat dikirim oleh sistem, yaitu dengan penyebaran bagian, rekonstruksi pesan rahasia, dan pembaruan bagian. Pada bab ini akan dijelaskan mengenai solusi dari cara kerja dari setiap operasi pada sistem.

A. Metode Penyebaran Bagian

Penyebaran bagian adalah operasi yang wajib dilakukan setelah skema pembagian rahasia dibuat oleh pemimpin. Pembuatan skema dilakukan dengan memberikan nama skema, menentukan nilai ambang (k), jumlah partisipan (n), dan daftar calon partisipan. Calon partisipan adalah calon anggota yang ingin berada di bawah kepemimpinan pemimpin. Calon partisipan pada akhirnya bisa saja tidak menjadi partisipan karena terdapat verifikasi persetujuan calon partisipan sebelum bagian lokasi disebarkan. Penyebaran bagian lokasi hanya dapat dilakukan apabila semua calon partisipan setuju untuk menjadi partisipan.

Proses verifikasi dilakukan dengan mengirimkan permintaan untuk menjadi partisipan ke setiap calon. Lalu, jawaban dari setiap calon akan dikirimkan ke pemimpin untuk dilihat. Pengiriman permintaan dan jawaban dilakukan melalui antrian pesan.

Berikut langkah-langkah dari metode penyebaran bagian antara lain.

1. Pemimpin membuat skema pembagian rahasia baru dengan memberikan masukan nama skema, nilai ambang (k), jumlah partisipan (n), dan daftar calon partisipan. Lalu, proses verifikasi dimulai dengan dikirimkannya permintaan menjadi partisipan ke seluruh calon.
2. Calon partisipan menjawab permintaan dari pemimpin dengan jawaban ya atau tidak berdasarkan

kepercayaan calon partisipan terhadap pemimpin. Jawaban ini dikirimkan ke pemimpin.

3. Pemimpin melihat jawaban dari setiap calon.
4. Langkah ini bergantung pada jawaban para calon partisipan. Jika terdapat minimal satu calon yang menolak permintaan, operasi penyebaran bagian dianggap gagal. Seluruh calon partisipan akan mendapatkan pemberitahuan mengenai hal ini dan operasi selesai. Jika seluruh calon menyetujui, mereka resmi menjadi partisipan. Sekarang, pemimpin dapat melakukan pembangkitan bagian rahasia dengan memberi masukan lokasi rahasia yang ia inginkan. Kemudian, aplikasi akan mengirimkan seluruh bagian yang telah dibangkitkan ke para partisipan.
5. Para partisipan menerima bagian yang dikirimkan.

B. Metode Rekonstruksi Pesan Rahasia

Metode rekonstruksi pesan rahasia dapat dilakukan baik oleh pemimpin ataupun partisipan. Pihak yang ingin melakukan rekonstruksi disebut penggagas rekonstruksi. Untuk melakukan rekonstruksi, penggagas rekonstruksi membutuhkan bagian-bagian lokasi dari para partisipan hingga jumlah minimal nilai ambang (k). Para partisipan tidak boleh begitu saja mengirimkan bagian lokasi tanpa proses verifikasi atau persetujuan.

Persetujuan dilakukan dengan pengiriman permintaan bagian lokasi dari penggagas ke para partisipan. Partisipan dapat menyetujui dengan mengirimkan bagian lokasi miliknya atau mengirimkan jawaban tidak. Jika ada partisipan yang menjawab tidak, operasi akan tetap dilanjutkan karena rekonstruksi tidak membutuhkan semua bagian (jika nilai ambang kurang dari jumlah partisipant). Konsekuensinya, pesan error dapat muncul saat penggagas melakukan rekonstruksi apabila jumlah bagian lokasi yang dimasukkan kurang dari nilai ambang.

Berikut langkah-langkah operasi rekonstruksi secret adalah:

1. Terdapat pemimpin atau partisipan yang berperan sebagai penggagas rekonstruksi. Bertugas mengirimkan permintaan rekonstruksi ke seluruh partisipan.
2. Partisipan menerima permintaan rekonstruksi. Lalu, menyetujui atau menolak permintaan berdasarkan kepercayaannya terhadap penggagas rekonstruksi.
3. Langkah ini bergantung pada aksi partisipan pada langkah 2. Jika menolak, penggagas akan menerima notifikasi penolakan dan tidak akan ada lagi langkah berikutnya. Jika menyetujui, maka partisipan harus mengunggah bagian lokasi miliknya ke aplikasi. Lalu, aplikasi akan mengirimkan bagian lokasi ke penggagas rekonstruksi.
4. Penggagas menerima bagian lokasi dari partisipan.
5. Penggagas melakukan rekonstruksi pesan rahasia dengan mengunggah bagian-bagina yang telah diterima.

C. Metode Pembaruan Bagian

Operasi pembaruan bagian diawali oleh pemimpin atau salah satu partisipan. Disini, pemimpin atau partisipan tersebut disebut sebagai penggagas pembaruan. Penggagas akan meminta para partisipan untuk memperbarui bagian mereka. Para partisipan tidak boleh begitu saja menyetujui permintaan penggagas. Hal ini dikarenakan bisa saja partisipan tidak lagi percaya pada penggagas atau mereka yakin bahwa akun penggagas telah diambil alih oleh pihak lain yang berbahaya. Oleh karena itu, harus ada mekanisme yang dapat memastikan pembaruan bagian hanya akan dilakukan apabila seluruh partisipan menyetujui. Semua partisipan harus menyetujui karena pembaruan bagian adalah operasi yang melibatkan seluruh partisipan. Jika salah satu partisipan tidak setuju, operasi dianggap gagal.

Jika proses verifikasi berhasil, para partisipan dapat memulai proses pembaruan bagian dengan skema pembagian rahasia proaktif Bai. Berikut langkah-langkah dari metode pembaruan bagian antara lain.

1. Setiap partisipan membangkitkan subbagian lokasi sejumlah banyaknya partisiopan (n). Subbagian dibangkitkan secara otomatis oleh aplikasi. Kemudian, aplikasi mengirimkan subbagian-subbagian tersebut ke seluruh partisipan.

2. Participant menerima subbagian-subbagian dari para partisipan lain.

3. Setelah semua partisipan telah selesai mengirimkan subbagian, setiap partisipan dapat memulai proses pembaruan bagian. Proses ini dilakukan dengan mengunggah bagian lama serta semua subbagian yang telah diterima ke aplikasi. Aplikasi akan membangkitkan bagian lokasi baru yang dapat diunduh partisipan. Lalu, participant harus menghapus bagian lokasi lamanya.

IV. ANALISIS SOLUSI

Setelah melakukan pengujian keamanan lokasi pada skema pembagian rahasia Shamir dan Asmuth-Bloom didapatkan hasil analisis sebagai berikut.

Skema	Bai	Shamir	Asmuth-Bloom
Teknik	Matriks proyeksi	Polinomial	CRT
Proaktif	Iya	Tidak	Tidak
Ambang	Iya	Iya	Iya
Pesan Rahasia	Mudah	-	-
Penambahan Bagian	Mudah	Mudah	-

Dari analisis, kita dapatkan jika skema pembagian rahasia Bai adalah proaktif, lolos kriptografi ambang, pesan rahasia nya mudah, dan penambahan bagian nya juga mudah.

KESIMPULAN

Skema berbagi rahasia setelah dilakukan evaluasi, keamanannya sudah sangat bagus. Dapat dikatakan bahwa tidak ada satu bagian pun yang akan mengungkapkan informasi. Lalu, ketepatan rekonstruksi pesan rahasia juga dapat dipulihkan tanpa ada perubahan dari aslinya. Kemudian, kompleksitas perhitungan dan persyaratan penyimpanan juga mudah dan aman. Aman dalam artian, tidak ada satu pun pihak yang dapat membocorkan informasi dan k-1 bagian tidak dapat mengungkapkan pesan rahasianya, tetapi skema ini tidak aman terhadap penipu. Adapun ketepatan rekonstruksi akan jelek, jika ada satu atau lebih bagian yang palsu, maka pesan rahasia mungkin tidak direkonstruksi dengan benar oleh bagian k. Kompleksitas perhitungan interpolasi adalah O (nlog2n).

Skema yang berbeda diperkenalkan oleh banyak peneliti dengan mengambil faktor-faktor yang ada sehingga dapat dilakukan peningkatan skema Shamir. Salah satunya adalah skema pembagian rahasia Bai yang dapat menjamin keamanan lokasi dengan sangat bagus dan mudah.

REFERENSI

[1] Asmuth, C. and J. Bloom, 1983. A modular approach to key safeguarding. IEEE Trans. Inf. Theory, 29: 208-210.

[2] Bai, L., 2006. A strong ramp secret sharing scheme using matrix projection. Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks, June 26-29, 2006, Buffalo-Niagara Falls, USA., pp: 652-656.

[3] Bai & Zou (2009). A Proactive Secret Sharing Scheme in Matrix Projection Method. International Journal of Security and Networks, Vol. 4, No. 4

[4] Herzberg, A., Jarecki, S., Krawczyk, H. and Yung, M. (1995) 'Proactive secret sharing or: how to cope with perpetual leakage', in Don Coppersmith (Ed.): Advances in Cryptology – Crypto '95, August, Santa Barbara, CA, pp.339–352.

[5] Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613.

[6] Silverstone, Daniel (2006). Libgfshare – A Secret Sharing Library. http://www.digital-scurf.org/software/libgfshare.

[7] Tompa, M. and H. Woll, 1988. How to share a secret with cheaters. J. Cryptol., 1: 133-138.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung , 7 Mei 2020

Nando Rusrin Pratama