TUGAS MAKALAH

II3230 KEAMANAN INFORMASI

"Symmetric Balanced Incomplete Block Design for Group Data Sharing in Cloud Computing"

Disusun Oleh:

Naradita Kunti Nabila 18217034

Program Studi Sistem dan Teknologi Informasi

Sekolah Teknik Elektro dan Informatika - Institut Teknologi Bandung

Jl. Ganesha 10, Bandung 4013

DAFTAR ISI

ABSTRAK

Pada saat ini, penggunaan teknologi komputasi awan sebagai platform untuk melakukan penyimpanan data serta berbagi data dalam suatu kelompok tertentu sudah banyak dikenal dan diminati oleh masyarakat luas. Hal ini dikarenakan rendahnya konsumsi energi yang digunakan serta adanya penyediaan sumber daya komputasi dan penyimpanan tidak terbatas yang dapat dibagikan. Namun, kelebihan ini justru dapat menimbulkan masalah baru di kalangan pengguna, yaitu masalah keamanan dan privasi data. Data pengguna yang disimpan dalam sistem penyimpanan cloud menyebabkan pengguna tidak dapat mengontrol keamanan data untuk memastikan kerahasiaan dan integritas. Salah satu solusi yang dapat diterapkan untuk mengatasi masalah tersebut adalah dengan menerapkan protokol berbasis desain blok yang menggunakan sistem manajemen key agreement, yang dinamakan Symmetric Balanced Incomplete Block Design (SBIBD). Pada makalah ini akan dibahas apa itu SBIBD serta bagaimana protokol ini dapat mengatasi masalah keamanan dan privasi pada penggunaan teknologi komputasi awan.

BAB I
PENDAHULUAN

1.1. Latar Belakang

Pada era saat ini, kebutuhan masyarakat untuk dapat berbagi data di dalam suatu kelompok agar dapat mempermudah kolaborasi dalam melakukan suatu pekerjaan semakin tinggi. Salah satu teknologi yang dapat memenuhi kebutuhan tersebut adalah cloud computing. Menurut National Institute of Standards and Technology (NIST), cloud computing adalah suatu model komputasi yang memberikan kemudahan dan kenyamanan dalam mengakses dan mengkonfigurasi sumber daya komputasi yang sesuai dengan permintaan dan cepat dirilis tanpa adanya banyak interaksi dengan penyedia layanan. [1] Seiring berjalannya waktu, teknologi ini semakin diminati oleh sebagian besar masyarakat karena rendahnya konsumsi energi, tersedianya sumber daya komputasi, dan penyimpanan tidak terbatas yang dapat dibagikan.

Salah satu layanan unggulan yang biasanya disediakan oleh penyedia layanan cloud computing adalah layanan penyimpanan cloud yang memungkinkan berbagi data dalam suatu kelompok. Layanan ini memungkinkan seluruh anggota kelompok dapat berbagi data di dalam grup secara bebas sehingga dapat meningkatkan efisiensi kerja. Beberapa karakteristik yang biasanya berlaku dalam penggunaan layanan ini adalah jumlah anggota kelompok yang bersifat dinamis, kerahasiaan data outsourcing harus dijaga, serta mendukung metode multi-pemilik dan properti toleran kesalahan untuk mengatasi adanya serangan kunci yang berbeda. [6] Untuk mendukung karakteristik tersebut sehingga penggunaan layanan dapat berbagi data dalam kelompok secara aman, diperlukan suatu protokol yang memiliki spesifikasi seperti berikut.

1) Pembuatan kunci konferensi umum dilakukan di saluran publik
2) Protokol menyediakan berbagi data yang mengikuti pola banyak-ke-banyak
3) Protokol didasarkan pada model desentralisasi dimana data outsourcing dikontrol oleh semua pemilik data dalam suatu kelompok

Protokol yang memenuhi spesifikasi tersebut adalah protokol key agreement berbasis desain blok SBIBD yang mendukung banyak anggota kelompok dan dilengkapi dengan layanan autentikasi dan properti toleransi kesalahan. [3]

1.2. Rumusan Masalah

Berikut ini merupakan rumusan masalah yang akan dibahas dalam makalah ini.

1. Apa itu *Symmetric Balanced Incomplete Block Design* (SBIBD)?
2. Apa saja masalah yang dihadapi dalam *group data sharing* pada *cloud computing*?
3. Bagaimana cara untuk mengimplementasikan SBIBD untuk menyelesaikan permasalahan pada *group data sharing* di lingkungan *cloud computing*?

1.3. Tujuan

Penulisan makalah ini memiliki beberapa tujuan sebagai berikut.

1. Mengetahui definisi dari *Symmetric Balanced Incomplete Block Design* (SBIBD)
2. Mengetahui masalah yang dihadapi dalam *group data sharing* pada *cloud computing*
3. Mengetahui bagaimana mengimplementasikan SBIBD untuk menyelesaikan permasalahan pada *group data sharing* di lingkungan *cloud computing*

1.4. Metodologi

Pada makalah ini, penulis menggunakan metode analisis terhadap data dari kajian pustaka. Makalah akan dibagi menjadi tiga bagian utama, yaitu :

1. Pendahuluan, berisi penjelasan singkat mengenai isi makalah dan penulisannya. Bagian ini terdiri dari latar belakang, rumusan masalah, tujuan, dan metodologi.
2. Pembahasan, merupakan inti makalah yang membahas rumusan masalah yang telah didefinisikan pada bagian pendahuluan. Pada makalah ini, bagian ini terdiri dari *Symmetric Balanced Incomplete Block Design* (SBIBD), masalah dalam *group data*

sharing pada *cloud computing,* serta cara mengimplementasikan SBIBD dalam *group data sharing* di lingkungan *cloud computing.*

3. Penutup, merupakan bagian penyelesaian makalah. Bagian ini terdiri dari kesimpulan dan saran.

BAB II
PEMBAHASAN

2.1. *Symmetric Balanced Incomplete Block Design* (SBIBD)

Dalam ilmu matematika kombinatorial, desain blok adalah satu set bersama-sama dengan keluarga himpunan bagian yang anggotanya dipilih untuk memenuhi beberapa set properti yang dianggap berguna untuk aplikasi tertentu. [2] Dalam perkembangannya, desain blok ini memiliki jenis - jenis yang sangat beragam menyesuaikan dengan kebutuhan dalam pengaplikasiannya, seperti dalam desain eksperimental, geometri terbatas, kimia fisik, pengujian perangkat lunak, kriptografi, dan geometri aljabar. Terdapat beberapa parameter yang dapat menentukan jenis dari blok desain, yaitu :

- v = jumlah varietas,
- b = jumlah blok,
- r = jumlah blok yang mengandung poin tertentu,
- k = jumlah poin dalam satu blok, dan
- λ = jumlah blok yang mengandung dua poin tertentu yang sama.

Sehingga desain blok ini sering dilambangkan dengan (v, b, r, k, λ) desain. Pada *Symmetric Balanced Incomplete Block Design,* atau yang biasa disebut dengan SBIBD, terdapat beberapa karakteristik yang mendefinisikan jenis blok desain ini. Beberapa karakteristik tersebut diantaranya adalah sebagai berikut.

- ❑ Tidak lengkap (*incomplete*).

  Maksud dari karakteristik ini adalah tidak ada satupun blok yang memiliki semua elemen himpunan, sehingga $v > k$.

- ❑ Seimbang (*balanced*)

  Maksud dari karakteristik ini adalah pembagian banyaknya satu elemen (varietas) yang menempati sejumlah blok sama rata, sehingga setiap elemen (varietas) x terkandung dalam sejumlah r blok.

- Simetris (*symmetric*)

  Karakteristik ini berlaku jika jumlah varietas dengan jumlah blok adalah sama, sehingga v = b.

Sehingga, karakteristik ini membentuk beberapa persamaan yang mencirikan dari desain blok SBIBD ini, yaitu:

$$\lambda(v - 1) = r(k - 1); \qquad b = v; \qquad r = k$$

Dengan demikian, desain blok SBIBD biasa juga direpresentasikan dengan (v, k, λ) desain. [2]

2.2. Masalah dalam *Group Data Sharing* pada *Cloud Computing*

Dalam mekanisme berbagi data di dalam suatu kelompok terdapat dua hal penting yang perlu diperhatikan, yaitu metode berbagi data dan sistem manajemen kunci. Dari sisi metode berbagi data, terdapat dua cara yaitu pola satu-ke-banyak dan pola banyak-ke banyak. Pola satu-ke-banyak mengacu pada skenario dimana satu klien mengotorisasi akses data kelompok ke banyak klien. Sedangkan, pola banyak-ke-banyak mengacu pada skenario dimana banyak klien dapat mengotorisasi data kelompok kepada banyak klien lainnya dalam waktu bersamaan. Pola banyak-ke-banyak dinilai lebih efektif dan efisien karena semua pengguna dalam grup dapat dengan bebas menyimpan, membaca, dan menghapus data mereka yang tersimpan di penyimpanan *cloud.* [4]

Sedangkan, dari sisi sistem manajemen kunci terdapat dua jenis, yaitu *key distributed* dan *key agreement.* Pada sistem *key distributed,* pembuatan dan distribusi kunci dilakukan sepenuhnya oleh pengontrol pusat. Sedangkan pada sistem *key agreement,* semua anggota dalam kelompok secara adil berkontribusi, bernegosiasi, dan menentukan kunci konferensi bersama - sama. Dalam lingkungan komputasi awan, *key agreement* dinilai lebih baik karena pembagian beban kerja yang lebih baik.. [4] Namun kemudahan yang diberikan dari cara berbagi data dan sistem manajemen kunci tersebut, justru membuat aktivitas ini sangat rentan terhadap masalah keamanan informasi. Berikut ini merupakan masalah - masalah yang biasanya terjadi dalam aktivitas berbagi data dalam suatu kelompok pada lingkungan komputasi awan.

1. Penyerang dari luar kelompok mencoba untuk mengungkapkan kunci konferensi umum untuk mendekripsi data yang di-*outsource*, yang bisa jadi penyerang eksternal atau *server cloud* itu sendiri.

2. Anggota yang dicabut hak aksesnya dapat memanfaatkan *server cloud* untuk menyimpan data yang di-*outsource* tanpa izin dari manajer grup.

3. Anggota jahat dapat menghasilkan sub kunci yang berbeda dan mengirimkan pesan yang berbeda ke anggota yang berbeda selama proses pembuatan kunci, sehingga kunci terakhir yang dihitung oleh anggota berbeda.

4. Penyerang eksternal atau anggota yang dicabut dapat memalsukan tanda tangan yang sah dari anggota kelompok yang sah.

2.3. Implementasi SBIBD dalam *Group Data Sharing* pada *Cloud Computing*

Untuk mengatasi masalah yang telah disebutkan pada poin sebelumnya, maka diperlukan suatu desain yang dapat memenuhi beberapa aspek berikut ini.

1. Perubahan dinamis pada entitas anggota grup

   Adanya anggota grup yang masuk dan keluar grup secara dinamis, membuat skema harus menjamin anggota yang baru masuk dapat mengakses data sebelumnya, dan anggota yang sudah keluar grup tidak dapat memperoleh data grup tersebut.

2. Kerahasiaan data

   Data *outsourcing* tidak dapat dilihat oleh *server cloud* dan anggota ilegal.

3. Anonimitas

   Hal ini didukung oleh fakta bahwa sebagian besar pengguna lebih menyukai berbagi data secara anonim.

4. Ketertelusuran

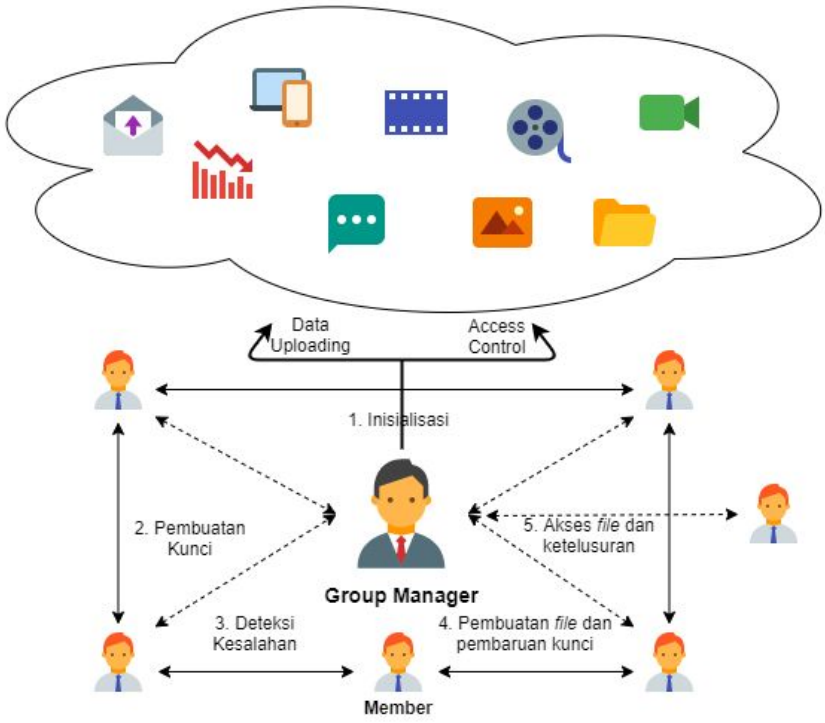
   Aspek ini diperlukan untuk menyelesaikan suatu perselisihan di dalam grup dengan menemukan pemilik data yang bersangkutan.

5. Properti toleransi kesalahan

   Aspek ini menjamin anggota grup yang berwenang masih memiliki akses untuk mendapatkan kunci konferensi umum secara efektif.

Oleh karena itu, perlu diterapkan protokol *key agreement* berbasis desain blok yang menggunakan struktur SBIBD untuk memenuhi aspek - aspek tersebut dengan beban komputasi yang relatif kecil dan mendukung sistem komunikasi yang kompleks. [6]

Berikut ini merupakan desain dari sistem *group data sharing* pada *cloud computing* yang mengimplementasikan SBIBD.



Gambar 1. Model Sistem *Cloud Computing*

Pada model sistem ini, terdapat tiga entitas utama, yaitu:

a) *Cloud*

Entitas ini memiliki peran dalam menyediakan layanan penyimpanan dan berbagi data yang efisien dan nyaman bagi pengguna. Entitas ini dapat membaca data yang tersimpan, namun tidak dapat menambah, menghapus, atau memodifikasi data tersebut. *Cloud* adalah pihak semi-tepercaya dalam skema tersebut.

b) Manajer grup

Entitas ini bertanggung jawab dalam menghasilkan parameter sistem, mengelola anggota grup, termasuk mengunggah data terenkripsi anggota, mengesahkan anggota kelompok, dan mengungkapkan identitas asli anggota, serta mendeteksi toleransi kesalahan. Manajer grup dalam skema ini adalah pihak ketiga yang sepenuhnya terpercaya untuk *cloud* dan anggota grup.

c) Anggota

Entitas ini terdiri dari serangkaian pengguna berdasarkan model komunikasi SBIBD. Dalam skema tersebut, anggota adalah orang-orang dengan minat yang sama dan ingin berbagi data di lingkungan komputasi awan.

Skema yang diusulkan untuk menyelesaikan permasalahan yang telah didefinisikan pada poin sebelumnya, terdiri dari lima tahapan, yaitu

1. Inisialisasi

Proses ini dilakukan oleh manajer grup dan memiliki tiga sub-tahapan, yaitu:

a) Inisiasi parameter

Setelah dilakukan beberapa proses [6], parameter ini disimpan sebagai kunci utama.

b) Pendaftaran anggota

Setiap anggota grup mendaftarkan diri ke manajer grup dengan ID-nya. Kemudian, manajer grup memetakan informasi identitas anggota dan menghitung beberapa operasi untuk mendapatkan kunci rahasia dari anggota tersebut.

Selanjutnya, informasi identitas anggota tersebut ditambahkan ke dalam daftar anggota grup yang dimiliki oleh manajer grup.

c) Konstruksi SBIBD

Setelah pendaftaran, manajer grup bertanggung jawab untuk membangun struktur SBIBD sesuai dengan jumlah anggota grup.

2. Pembuatan Kunci

Dalam pembuatan kunci, terkadang diperlukan sejumlah relawan terpercaya untuk membantu anggota kelompok menghasilkan *key agreement.*

3. Deteksi Kesalahan

Pada proses ini, manajer grup perlu memastikan bahwa setiap anggota hanya menghasilkan sub-kunci yang unik sehingga kesepakatan tidak akan ditunda atau dihancurkan oleh pelaku jahat.

4. Pembuatan *file* dan Pembaruan Kunci

Proses ini memiliki tiga sub-tahapan, yaitu:

a) Pembuatan *file*

Proses yang perlu dilakukan untuk mengunggah data *file* ke dalam penyimpanan *cloud* adalah sebagai berikut.

- Anggota mengenkripsi data *file* dengan algoritma enkripsi simetris dan kunci konferensi umum. Kemudian, anggota grup mengirimkan data terenkripsi ke manajer grup
- Manajer grup memverifikasi validitas anggota melalui *VerSign()* dan *VerRevo().* Setelah verifikasi berhasil, manajer grup mendapatkan kunci publik dan kunci pribadi melalui beberapa perhitungan enkripsi.
- Setelah itu, manajer grup mengenkripsi ulang pesan terenkripsi dan mengunggah *file* ke *cloud* beserta tanda tangan grup.

b) Pencabutan anggota

Pencabutan anggota dilakukan oleh manajer grup yang bertugas mengelola RL. Selain itu, anggota yang telah dicabut hak aksesnya tidak dapat diverifikasi untuk mengakses *cloud.*

c) Pembaruan utama

Pembaruan kunci dibagi menjadi dua bagian, yaitu pembaruan untuk kunci konferensi umum di antara anggota grup dan pembaruan kunci pribadi manajer grup. Kunci konferensi umum dapat diperbarui dalam periode waktu tertentu, sedangkan kunci pribadi manajer grup harus diperbarui setiap saat setelah jumlah anggota grup diubah.

5. Akses *File* dan Ketelusuran

Proses ini memiliki dua sub-tahapan, yaitu:

a) Akses *file*

Proses yang perlu dilakukan untuk mendapatkan data yang disimpan di *cloud* adalah sebagai berikut.

- Anggota mengirimkan permintaan data ke manajer grup
- Manajer grup mengirim informasi otorisasi ke *cloud* setelah verifikasi berhasil
- Setelah menerima informasi otorisasi dari manajer grup, *cloud* menghitung *per* [6] dan memberikan respon berupa data yang diminta dan *per* kepada anggota
- Setelah menerima data dari *cloud,* anggota dapat memperoleh kunci rahasia enkripsi ulang dari manajer grup menggunakan kunci rahasia miliknya.
- Anggota yang berwenang dapat memperoleh data grup yang dibutuhkan.

b) Ketelusuran

Manajer grup dapat melacak identitas sebenarnya dari pemilik data ketika terjadi perselisihan dengan cara memverifikasi kebenaran tanda tangan dan pencabutan

yang berhasil, lalu mencari daftar pengguna grup untuk mengungkap identitas sebenarnya dari pemilik data.

BAB III
PENUTUP

3.1. Kesimpulan

Dari pembahasan yang telah dijelaskan pada bab sebelumnya, dapat diambil beberapa kesimpulan sebagai berikut.

- *Symmetric Balanced Incomplete Block Design* (SBIBD) adalah salah satu jenis desain blok yang memiliki karakteristik tidak lengkap, seimbang, dan simetris, sehingga membertuk beberapa persamaan yang diantaranya adalah $\lambda(v-1) = r(k-1)$; $b = v$; $r = k$, dan biasanya direpresentasikan dengan (v, k, λ) desain.

- Masalah - masalah yang biasanya dihadapi dalam *group data sharing* pada *cloud computing* diantaranya adalah pengungkapan kunci konferensi umum oleh anggota ilegal, pemanfaatan *server cloud* untuk menyimpan data yang di-*outsource* tanpa izin dari manajer grup, anggota jahat yang dapat menghasilkan sub kunci yang berbeda dan mengirimkan pesan yang berbeda ke anggota yang berbeda selama proses pembuatan kunci, dan pemalsuan tanda tangan yang sah dari anggota kelompok yang sah.

- Cara mengimplementasikan SBIBD dalam *group data sharing* di lingkungan *cloud computing* terdiri dari 5 tahapan, yaitu inisiasi, pembuatan kunci, deteksi kesalahan, pembuatan *file* dan pembaruan kunci, dan akses *file* dan ketelusuran.

3.2. Saran

Seiring perkembangan teknologi yang mempermudah kehidupan manusia, akan ada kemungkinan munculnya masalah - masalah baru di bidang keamanan informasi, terutama di lingkungan komputasi awan. Sehingga, diharapkan makalah ini dapat terus dikembangkan untuk menghasilkan skema - skema baru yang dapat mengatasi masalah - masalah keamanan informasi yang lebih efektif dan efisien.

REFERENSI

[1] Mell, Peter and G. Timothy. "The NIST Definition of Cloud Computing. Special Publication 800-145." *Gaithersburg: National Institute of Standards and Technology* (2011).

[2] J. Shen, S. Moh and I. Chung, "Identity-Based Key Agreement Protocol Employing A Symmetric Balanced Incomplete Block Design," in Journal of Communications and Networks, vol. 14, no. 6, pp. 682-691, Dec. 2012.

[3] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing* (2017).

[4] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing*

[5] A. Sun, G. Gao, T. Ji and X. Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform," *2018 Sixth International Conference on Advanced Cloud and Big Data (CBD)*, Lanzhou, 2018, pp. 197-201.

[6] J. Shen, T. Zhou, X. Chen, J. Li and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912-925, April 2018.