OPEN ACCESS
CENTIVE 2019
ISBN: 978-602-53004-0-0

Conference on Electrical Engineering, Telematics, Industrial Technology, and Creative Media 2019

Keamanan Data Modern Di Dalam Penyimpanan Awan Menggunakan THAMKS-VOD

Rio Darmawan [#1], Jenal Abidin [#2], Jerry Lasama [#3], Aditya Wijayanto [#4]

 # Fakultas Teknologi Industri dan Informatika, Institut Teknologi Telkom Purwokerto
Jl. DI Panjaitan No 128 Purwokerto 53147 Indonesia

[1] 18102283@ittelkom-pwt.ac.id
[2] 18102270@ittelkom-pwt.ac.id
[3] 18202018@ittelkom-pwt.ac.id
[4] aditya.wijayanto@ittelkom-pwt.ac.id

Abstrak

Cloud computing adalah jenis teknologi informasi baru yang pengguna dapat menikmati berbagai layanan *cloud* dari sumber daya komputasi yang telah dikonfigurasikan. Dibandingkan dengan penyimpanan cadangan tradisional, penyimpanan awan adalah pilihan yang lebih ekonomis, karena pusat data jarak jauh yang dikelola oleh suatu perusahaan sehingga pengguna tidak perlu melakukan pemeliharaan, yang dapat menghemat waktu dan uang pada rangkaian layanan *cloud*. Dalam beberapa tahun terakhir, semakin banyak serangan berbahaya pada sistem penyimpanan *cloud* dari kebocoran data juga sering terjadi. Keamanan penyimpanan *cloud* menyangkut keamanan data pengguna. Tujuan dari makalah ini adalah untuk merumuskan keamanan data penyimpanan cloud dan kebijakan keamanan yang sesuai yang digabungkan dengan hasil penelitian akademis yang ada dengan menganalisis risiko keamanan data pengguna dan mendekati subjek teknologi keamanan yang relevan, yang didasarkan pada karakteristik struktural sistem penyimpanan *cloud*.

Kata kunci: Komputasi Awan, Penyimpanan Awan, Security Police, Keamanan Data

I. PENDAHULUAN

Komputasi awan merupakan teknologi yang sedang berkembang pesat di era Industri 4.0. Komputasi awan ini menjadi terkenal, karena menyediakan layanan sesuai permintaan dan nyaman dari sumber daya komputasi gabungan dari sumber daya bersama. Oleh karena itu, semakin banyak perusahaan dan individu lebih memilih untuk mengalihkan penyimpanan data mereka ke server cloud. Terlepas dari keuntungan ekonomi dan teknis yang luar biasa, masalah keamanan dan privasi yang tidak dapat diprediksi, menjadi masalah paling berpengaruh yang menghambat adopsi penyimpanan data yang tersebar luas di infrastruktur cloud publik. Untuk sistem berbagi file, seperti skenario multi-pengguna, pemberian hak pencarian yang halus adalah fungsi yang diinginkan bagi pemilik data untuk membagikan data pribadi mereka dengan pengguna resmi lainnya.

Namun, sebagian besar sistem yang tersedia, mengharuskan pengguna untuk melakukan sejumlah besar operasi pemasangan bilinear kompleks. Perhitungan yang kewalahan ini menjadi beban berat bagi terminal

pengguna, yang sangat serius untuk perangkat yang dibatasi energi. Metode dekripsi outsourcing memungkinkan pengguna untuk memulihkan pesan dengan dekripsi sangat ringan. Namun, server cloud mungkin mengembalikan informasi yang salah-dekripsi salah karena serangan jahat atau malfunction system. Dengan demikian, ini adalah masalah penting untuk menjamin kebenaran dari dekripsi dan enkripsi kunci publik dengan sistem pencarian kata kunci (PEKS).

Entitas yang berwenang dapat secara ilegal membocorkan kunci rahasia mereka pihak ketiga untuk mendapatkan untung [4]. misalkan seorang pengguna menemukan sebuah kode kunci yang sesuai, ia mencoba mencari tahu apa rahasia perusahaan yang ia tempati. perilaku tercela seperti itu secara serius mengancam keberlangsungan perusahaan. bahkan lebih buruk lagi jika, data yang ia dapatkan mengandung data yang sangat penting bagi perusahaan, dan disalahgunakan untuk kepentingan pribadi. Kebocoran kunci rahasia yang disengaja secara serius merusak fondasi kontrol akses resmi dan perlindungan privasi data. Dengan demikian, sangat penting untuk mengidentifikasi pengguna jahat atau bahkan membuktikannya di pengadilan. Dalam sistem kontrol akses berbasis atribut, kunci rahasia pengguna dikaitkan dengan sekumpulan atribut daripada identitas individu. Sebagai otoritas pencarian dan dekripsi dapat dibagikan oleh satu set pengguna yang memiliki set atribut yang sama, sulit untuk melacak pemilik kunci asli [5], [6]. Memberikan keterlacakan [7] ke sistem otorisasi pencarian berbutir halus sangat penting dan tidak dipertimbangkan dalam sistem enkripsi yang dapat dicari sebelumnya [2], [3], [4],[10].

Lebih penting lagi, dalam definisi asli skema PEKS [4], key generation centre (KGC) menghasilkan semua kunci rahasia yang berada di dalam sistem, yang pasti mengarah pada masalah escrow kunci. Yaitu, KGC mengetahui semua kunci rahasia pengguna dan dengan demikian dapat dengan tidak hati-hati mencari dan mendekripsi file yang dienkripsi, yang secara nyata mengancam keamanan data dan privasi. Selain itu, masalah kunci escrow membawa masalah lain ketika kemampuan penelusuran direalisasikan dalam PEKS. Jika kunci rahasia ditemukan untuk dijual dan identitas pemilik kunci (yaitu, pelacak) tidak dikenal, pelapor dapat mengklaim bahwa kunci rahasia tersebut bocor oleh KGC. Tidak ada metode teknis untuk membedakan siapa penjahat yang asli jika masalah kunci escrow tidak diselesaikan.

II. METODE PENELITIAN

Kami melakukan resensi pada penelitian sebelumnya, yaitu: *escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption* (EF-TAMKSVOD), yang memiliki kelebihan sebagai berikut:

1) *Flexible Authorized Keyword Search* EF-TAMKSVOD mencapai otorisasi akses data sangat halus dan mendukung untuk pencarian subset kata kunci. Dalam fase enkripsi, kumpulan kata kunci KW diekstraksi dari sebuah file, dan KW serta file dienkripsi. Kebijakan akses juga diberlakukan untuk mendefinisikan tipe pengguna yang diotorisasi. Dalam fase pencarian, pengguna data menentukan kata kunci yang mengatur KW0 dan menghasilkan pintu jebakan. TKW0 menggunakan kunci rahasianya. Pada fase pengujian, jika atribut yang dikaitkan dengan kunci rahasia pengguna memenuhi kebijakan akses file dan KW0 (tertanam di pintu jebakan) adalah subset dari KW (tertanam dalam ciphertext), file yang sesuai dianggap sebagai file yang cocok dan dikembalikan ke pengguna data. Urutan kata kunci di KW0 dapat diubah secara sengaja, dan yang penting adalah tidak memengaruhi hasil pencarian.
2) *White-box Traceability of Abused Secret Key* Penelusuran penjahat dapat dibagi menjadi dua penelusuran yaitu kotak putih dan kotak hitam. Jika pengguna yang berwenang membocorkan atau menjual kunci rahasianya, penelusuran kotak putih mampu mengidentifikasi siapa yang membocorkan kunci tersebut. Persepsi keterlambatan kotak hitam adalah persepsi yang salah, di mana kebocoran pengguna yang jahat adalah peralatan pencarian dan dekripsi alih-alih kunci rahasia. EF-TAMKS-VOD mencapai keterlacakan kotak putih. Setiap pelanggan yang membocorkan kunci rahasia ke pihak ketiga secara sengaja atau tidak sengaja dapat dilacak. Selain itu, keterlacakan EFTAMKS-VOD tidak membawa komputasi tambahan dan overhead transmisi.
3) *Flexible System Extension* EF-TAMKS-VOD mendukung ekstensi sistem yang fleksibel, yang mengakomodasi jumlah atribut yang fleksibel. Atribut tidak tetap dalam fase inisialisasi sistem dan ukuran set atribut tidak terbatas pada ikatan polinomial, sehingga atribut baru dapat ditambahkan ke sistem kapan saja. Selain itu, ukuran parameter publik tidak bertambah dengan jumlah atribut. Tidak peduli berapa banyak atribut yang didukung dalam sistem, tidak ada komunikasi tambahan atau biaya penyimpanan

yang dibawa ke EF-TAMKS-VOD. Fitur ini diinginkan untuk sistem cloud karena volume penggunanya yang semakin meningkat.

4) *Efficient Verifiable Decryption* EF-TAMKS-VOD mengadopsi beberapa mekanisme dekripsi yang di-outsource untuk mewujudkan dekripsi yang efisien. Sebagian besar perhitungan dekripsi di-outsource ke server cloud, dan pengguna data dapat menyelesaikan dekripsi akhir dengan perhitungan yang sangat ringan. Terlebih lagi, kebenaran dari perhitungan dekripsi parsial komputer ini dapat diverifikasi oleh pengguna.
5) *Key Escrow Free* Untuk mengurangi kepercayaan pada KGC, protokol pembuatan kunci interaktif dirancang untuk memecahkan masalah pada kunci escrow. EF-TAMKS-VOD mengambil proses interaksi yang ada di antara KGC dan server cloud sehingga tidak satupun dari mereka yang mampu secara mandiri menghasilkan seluruh kunci rahasia pengguna, di mana algoritma enkripsi homomorfik ringan digunakan. Dengan demikian, kunci rahasia pengguna tidak di-escrow ke entitas mana pun dan EF-TAMKS-VOD adalah kunci gratis escrow.
6) *Efficient User Revocation* Setelah pengguna diidentifikasi sebagai penjahat melalui algoritma penelusuran, EF-TAMKS-VOD mencabut pengguna jahat ini dari grup yang berwenang. mekanisme pencabutan EF-TAMKS-VOD memiliki efisiensi yang jauh lebih baik [9].

III. HASIL PENELITIAN

Untuk mengevaluasi kinerja, skema di [2], [3], [4], [5], [9] dan EF-TAMKS-VOD disimulasikan menggunakan laptop dengan spesifikasi CPU: Intel core i5 CPU pada 2.5GHz; memori fisik: DDR3 8GB. Parameter kurva elips tipe A dipilih untuk pengujian. Ini memberikan kekuatan keamanan log disk terpisah 1024-bit yang setara dengan urutan grup 160-bit. Paring bertipe A dibangun pada kurva 2 = 3 + dibawah untuk beberapa prime = 3 (4). Di dalam hasil eksperimen, kami menggunakan parameter = 87807107996633125224377819847540498158068199414208211028653399266475630880222957078625179422662221423155858769582317459277713367317481324925129998224791, yang disediakan di library PBC [8]. Algoritma inti dieksekusi pada eksperimen ini dan biaya overhead dari skema pengiriman di [2], [3], [4], [5] dan EFTAMKS-VOD. Menurut parameter yang dipilih dalam percobaan, kami miliki $|Z_p|$ = 160bits, $|G|$ = 1024bits, dan $|G_t|$ = 1024 bits. Angka pada l1 pada keyword ditetapkan menjadi 5 untuk melakukan testnya.

IV. PEMBAHASAN

Dalam bab ini, kami menggambarkan konstruksi pondasi TAMKS-VOD dan kebenaran sistem dianalisis dalam Bagian C dalam Bahan Tambahan. Diasumsikan bahwa peminjam dan KGC dapat menggunakan pengguna.

A. *System Initialization*

Misalkan G adalah grup bilinear dari orde utama p dan g menjadi generator G. Misalkan e: $G \times G \rightarrow G_t$ menjadi peta bilinear. Definisi fungsi : $\{0,1\}^* \rightarrow K$, $H: \{0,1\}^* \rightarrow G$ dan $H': \{0,1\}^* \rightarrow Z_{*p}$.

Gambar. 1. Inisialisasi Sistem dan Registrasi Pengguna

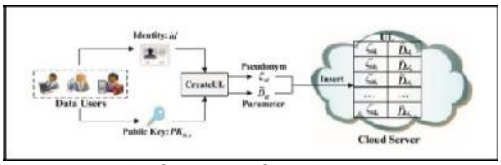
B. *Registrasi Pengguna*

Ketika seorang pengguna berlaku untuk bergabung dengan sistem TAMKS-VOD, KGC memberikan atribut set S kepada pengguna sesuai dengan identitasnya. Kemudian, KGC menjalankan algoritma pembuatan kunci untuk menghasilkan kunci publik/rahasia bagi pengguna. Registrasi pengguna baru diilustrasikan pada Gambar 1.

KeyGen (MSK,id,S) → *(Pkid,Skid,S)*. KGC memilih elemen acak *t, 0, Xid, D4* ∈ *R* Z*Z*p dan computer $S_{id} = SEnck_1(id)$, $\delta = SEnck_2(\zeta id||\theta), D_1 = g^{\frac{a}{\alpha+\delta}} g^{\beta t}, D'1 = \delta, D_2 = g^t, D'2 = g^{\lambda t}, D3, x = H(x)^{(\lambda+\delta)}$ t(∀x ∈ S),Y_{id}. Dan kunci rahasia penggunanya adalah $PK_{id},S = Y_{id}$ dan $SK_{id},S = (D_1, D'_1, D_2, D'_2\{D_3,x\}x \in S, D_4, X_{id})$

C. *Membuat List User*

Dalam TAMKS-VOD, file yang dienkripsi oleh pemilik data dapat dicari oleh banyak pengguna data. Daftar pengguna ditentukan oleh pemilik data bersama dengan parameter penting yang digunakan dalam fase pencarian fi le. Daftar pengguna disimpan oleh server cloud.



Gambar. 2. Membuat List User

D. *Membuat File Enkripsi dan Kata Kunci Index*

Sebelum file M diunggah ke server cloud, pemilik data memproses file dengan langkah-langkah berikut. (1) Pemilik data mengekstrak kata kunci yang mengatur KW dari fi le M, di mana KW = {kw1, ⋯, kwl1}. (2)Ini mengenkripsi pesan M dengan kunci rahasia kSE menggunakan algoritma enkripsi simetris aman kriptografi, di mana kSE = h (Y) dan Y adalah elemen yang dipilih secara acak dari G_{*t}. File ciphertext dilambangkan sebagai C_m. (3) Hasilkan kunci verifikasi V_{km} yang dapat digunakan untuk memverifikasi hasil komputasi outsourcing. (4) Anggota grup Y ∈ G_{*t} dan set kata kunci yang dipilih KW dienkripsi untuk mengamankan indeks. (5) File yang dienkripsi dan indeks aman dikirim ke server cloud untuk penyimpanan. Perhatikan bahwa kebijakan akses yang ditentukan oleh pemilik data dimasukkan ke dalam ciphertext dalam algoritma ini.

V. PENUTUP

A. *Kesimpulan*

Penerapan akses kontrol dan bantuan kata kunci adalah masalah penting dalam kerangka penyimpanan terdistribusi yang aman. Dalam makalah ini, kami menandai pandangan dunia lain dari kerangka kerja enkripsi yang dapat diakses, dan mengusulkan pengembangan yang solid. Ini mendukung tampilan subset catchphrases yang dapat diadaptasi, dan menangani masalah kunci escrow di tengah metode usia kunci. Client yang terindikasi sebagai penjahat yang menggerakkan kunci misteri untuk mendapatkan sebuah keuntungan dapat diikuti. Aktivitas decoding setengah dikirim kembali ke server cloud dan hasil dari setengah dekode dapat dikonfirmasi oleh informasi *client*. Penyelidikan investigasi menunjukkan produktivitasnya dalam perhitungan dan overhead kapasitas. Hasil pengujian menunjukkan bahwa *overhead* perhitungan di terminal *client* berkurang secara serempak, yang secara signifikan menghemat vitalitas untuk gadget yang memaksa aset *client.*

B. *Saran*

Berdasarkan penelitian ini, semakin berkembangnya *cloud computing* harus diiringi dengan berkembangnya sistem keamanan yang ada. Agar para pengguna tidak ragu dalam menggunakan teknologi yang sedang berkembang ini.

DAFTAR PUSTAKA

[1] W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, “Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud,” IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198.

[2] K. Liang, W. Susilo, “Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 9, pp. 1981-1992.

[3] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in: EUROCRYPT, 2004, pp. 506-522.

[4] J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, “White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes,” IEEE Transactions on Information Forensics and Secu-rity, 2015, vol. 10, no. 6, pp. 1274-1288.

[5] Z. Liu, Z. Cao, D.S. Wong, "Traceable CP-ABE: how to trace decryption devices found in the wild," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 1, pp. 55-68.
[6] B. Chor, A. Fiat, and M. Naor. "Tracing traitors". In: CRYPTO, Springer, 1994, pp. 257-270.J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes," IEEE Transactions on Information Forensics and Secu-rity, 2015, vol. 10, no. 6, pp. 1274-1288.
[7] B. Lynn. "The Stanford Pairing Based Crypto Library." [Online]. Available: http://crypto.stanford.edu/pbc, accessed May 7, 2014.
[8] C. Wang, N. Cao, J. Li, K. Ren, W. Lou. "Secure positioned catchphrase seek over scrambled cloud data"[C]//IEEE 30th International Meeting on Distributed Computing Systems (ICDCS), IEEE, 2010: 253-262.
[9] P. Xu, H. Jin, Q. Wu and W. Wang, "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Gusssing Attack," IEEE Transactions on Computers, 2013, vol. 62, no. 11, 2266-2277
[10] B. Zhang, F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, 2011, vol. 34, no. 1, pp. 262-267.