T – 5

Manajemen Kunci Pada Mekanisme Akses Kontrol Sistem Ujian *Online* Program Penerimaan Mahasiswa Baru Menggunakan *Untrusted Public Cloud*

Caesario Oktanto Kisty, Taufik Shokhiful Azhar

Sekolah Tinggi Sandi Negara
caesarioriorio.kisty@gmail.com

***Abstrak*—**Cloud computing merupakan teknologi yang sumber daya komputasinya (storage, CPU, memory, network broadband, dsb) disediakan oleh penyedia layanan untuk memenuhi kebutuhan banyak pelanggannya. Selain itu pengguna dapat menggunakan layanan cloud computing dengan berbagai jenis perangkat, seperti laptop, tablet, smartphone, dsb. Cloud computing dapat diterapkan pada sistem ujian online program penerimaan mahasiswa baru menggunakan untrusted public cloud. Seringkali pada program penerimaan mahasiswa baru, ujian diselenggarakan secara terpusat. Hal ini menyebabkan kendala bagi peserta ujian yang berada jauh dari tempat pelaksanaan. Dengan sistem ujian online ini, peserta tidak harus berada di tempat pelaksanaan ujian. Peserta dapat mengerjakan ujian dimana saja dan mengunggahnya di cloud. Penggunaan untrusted public cloud juga merupakan keuntungan bagi pihak panitia penyelenggara ujian dibandingkan dengan membuat website, karena layanan untrusted public cloud dapat digunakan secara gratis. Namun, karena untrusted public cloud merupakan layanan yang tidak memiliki pengamanan terhadap data penggunanya karena siapapun dapat mengunduh data yang diunggah oleh pengguna. Oleh karena itu, pada makalah ini akan diajukan sebuah mekanisme akses kontrol berbasis enkripsi asimetris untuk sistem ujian online pada untrusted public cloud beserta manajemen kuncinya. Akses kontrol ini menggunakan public key, private key, dan group key untuk melindungi data pengguna yang diunggah di cloud agar tidak dapat dilihat oleh orang yang tidak berhak. Dengan mekanisme tersebut, diharapkan sistem ujian online dapat mempermudah peserta maupun penyelenggara ujian dan tetap terjamin keamanannya.

Kata kunci: Akses Kontrol, Cloud Computing, Group Key, Public Key.

I. PENDAHULUAN

Pada era perkembangan teknologi seperti saat ini, teknologi *cloud computing* semakin menjadi populer karena layanannya yang menawarkan pengguna untuk memiliki sumber daya komputer yang tak terbatas, dimana mereka dapat menggunakan sumber tersebut sebanyak mungkin yang mereka mau tanpa harus memikirkan bagaimana cara menyediakan sumber tersebut. Menurut NIST, terdapat empat buah *deployment model* dari *cloud computing*, yaitu *private cloud*, *public cloud*, *community cloud*, dan *hybrid cloud*[1]. *Public cloud* merupakan infrastuktur *cloud* yang tersedia bagi masyarakat umum[1], sehingga banyak pengguna dapat mengakses data yang terletak pada situs milik *cloud service provider* (CSP)[2]. Hal itu akan memberikan kerawanan pada kerahasiaan data pengguna, karena CSP tidak menyediakan layanan kerahasiaan didalamnya[3].

Untuk mengatasi masalah pada paragraf diatas, *provider* atau pemilik data dapat menerapkan mekanisme akses kontrol untuk menjamin kerahasiaan data pada *cloud*. Data yang berada di *cloud* hanya dapat diakses oleh entitas yang diberikan hak akses dari pemilik data. Mekanisme akses kontrol ini dapat dibentuk dengan berbasis enkripsi asimetris, dengan menggunakan manajemen kunci yang efisien secara komputasi.

Setiap tahun perguruan tinggi di Indonesia mengadakan program penerimaan mahasiswa baru. Biasanya calon mahasiswa baru harus melewati beberapa tahap seleksi untuk menjadi mahasiswa di suatu perguruan tinggi. Salah satu tahap seleksi yang harus dihadapi adalah ujian akademik, dimana calon mahasiswa akan mengerjakan soal yang nilainya akan dijadikan parameter bagi penyelenggara untuk menentukan siapa saja yang lulus seleksi pada tahap tersebut. Beberapa perguruan tinggi mengadakan tahap seleksi ini secara terpusat, sehingga calon mahasiswa yang berada jauh dari tempat pelaksanaan harus datang ke tempat pelaksanaan. Misal, penyelenggaraan ujian akademik suatu perguruan tinggi berada

di Jakarta, maka calon mahasiswa yang berada di Aceh atau Papua akan membutuhkan biaya transportasi yang cukup besar. Oleh sebab itu, sistem ujian online dapat menjadi solusi agar mempermudah pelaksanaan ujian. Untuk mengefisiensikan sumber daya yang dimiliki, penyelenggara ujian dapat menggunakan layanan *cloud computing*. Jika dibandingkan dengan membuat website atau menyewa suatu server, dari sisi ekonomi layanan *untrusted public cloud* lebih menguntungkan karena dapat digunakan secara gratis. Namun dari sisi keamanan perlu dilengkapi dengan mekanisme akses kontrol dan manajemen kunci yang efisien. Pada makalah ini akan diajukan sebuah mekanisme akses kontrol berbasis *public key encryption* untuk sistem ujian online pada *untrusted public cloud* beserta manajemen kuncinya. Akses kontrol ini menggunakan *public key*, *private key*, dan *group key* untuk melindungi data pengguna yang diunggah di *cloud* agar tidak dapat dilihat oleh orang yang tidak berhak. Tujuan dari makalah ini adalah untuk mengenalkan manajemen kunci, khususnya pada mekanisme akses kontrol berbasis *public key* encryption pada *public cloud* computing. Manfaat dari makalah ini diharapkan dapat menjadi referensi ilmiah dan inovasi baru dalam penyelenggaraan program mahasiswa baru. Dengan mekanisme tersebut, diharapkan sistem ujian online dapat mempermudah peserta maupun penyelenggara ujian dan tetap terjamin keamanannya.

II. DASAR TEORI

A. *Cloud Computing*

Berdasarkan *The* NIST *definition of cloud computing*, terdapat lima karakteristik, tiga model layanan, dan empat *deployment model* pada *cloud computing*.

Sistem disebut *cloud computing* jika memiliki lima karakteristik seperti dibawah ini:

1) *On-demand self service*
   Pengguna *cloud* dapat mengatur sendiri layanan yang ingin digunakan secara otomatis tanpa harus membutuhkan interaksi dengan *cloud service provider*.
2) *Broad network access*
   Kapabilitas layanan yang tersedia di jaringan dapat diakses melalui berbagai jenis perangkat, seperti *handphone*, tablet, laptop, *workstations*, dsb.
3) *Resource pooling*
   Untuk memenuhi kebutuhan banyak pelanggan dengan model *multi-tenant*, sumber daya komputasi (*storage, CPU, memory, network bandwidth*, dsb.) disediakan oleh *cloud service provider*.
4) *Rapid elasticity*
   Kapabilitas layanan dapat dipakai oleh *cloud consumer* secara dinamis berdasarkan kebutuhan.
5) *Measured service*
   Sistem *cloud* dapat di monitor secara otomatis, sehingga pengguna dapat melihat *resources* komputasi yang telah dipakai.

Jenis layanan *cloud computing* dibagi menjadi tiga sebagai berikut:

1) *Software as a service (SaaS)*
   Cloud consumer dapat menggunakan *software* (perangkat lunak) yang telah disediakan oleh *cloud service provider*.
2) *Platform as a service (PaaS)*
   Cloud consumer dapat menggunakan sistem operasi berserta aplikasinya yang disediakan oleh *cloud service provider*.
3) *Infrastucture as a service (IaaS)*
   Cloud consumer dapat menyewa infrastuktur IT (unit komputasi, *storage*, *memory*, *network*, dsb) yang telah disediakan oleh *cloud service provider*.

Terdapat empat *deployment model* dari *cloud computing*, yaitu:

1) *Private cloud*
   Layanan *cloud computing* yang disediakan untuk memenuhi kebutuhan internal dari organisasi/perusahaan.
2) *Community cloud*
   Layanan *cloud computing* yang disediakan eksklusif untuk komunitas tertentu.
3) *Public cloud*
   Layanan *cloud computing* yang disediakan untuk masyarakat umum. Pengguna dapat langsung mendaftar atau memakai layanan yang ada.
4) *Hybrid cloud*

Layanan *cloud computing* yang merupakan gabungan *public cloud* dan *private cloud*, yang diimplementasikan oleh suatu organisasi atau perusahaan.

B. Group Communication

Group communication adalah komunikasi antara seseorang dengan suatu kelompok (grup). Terdapat tiga teknik *group communication*: *multicast* yaitu mengirimkan informasi ke sekumpulan komputer yang tergabung dalam satu grup, *unicast* yaitu informasi dikirimkan dari satu titik ke titik yang lain, dan *broadcast* yaitu mengirimkan infoemasi ke seluruh titik yang ada di jaringan.

C. Skema Akses Kontrol untuk Group Communication pada Cloud Computing

Untuk membatasi pengguna yang tidak memiliki hak untuk mengakses data, maka dibutuhkan sebuah skema akses kontrol. Pada makalah ini diajukan sebuah skema akses kontrol untuk *group communication* pada *cloud computing* yang selanjutnya disebut dengan *group access control*. Pada skema ini tidak sembarang pengguna *cloud service* dapat mengakses data yang berada di *cloud*. Karena data yang berada di *cloud* dienkripsi oleh pemilik data dengan suatu kunci. Sehingga hanya pengguna yang memiliki akses saja yang dapat mendekripsi data tersebut, sehingga kerahasiaan data tersebut dapat terjaga. Kunci untuk mengenkripsi data dibangkitkan secara dinamis untuk setiap *session* komunikasi menggunakan manajemen kunci yang efektif. Kunci dibagikan kepada pengguna yang sah agar pengguna dapat mengakses data yang tersimpan di *cloud*. Ketika struktur grup berbentuk dinamis, maka setiap adanya pengguna yang masuk atau keluar dari grup, kunci harus selalu diperbarui. Namun yang dibahas pada makalah ini sedikit berbeda, karena pada sistem ujian *online* yang dibahas pada makalah ini hanya menggunakan satu kali *session* komunikasi, sehingga tidak perlu memperbarui kunci. Pemilik data membangkitkan *private key* untuk dibagikan kepada pengguna yang sah. Berdasarkan *private key* tersebut, dapat dihitung *public key* yang digunakan oleh pemilik data untuk mengenkripsi data yang akan disimpan di *cloud*.

D. Skema Group Key Management

Skema manajemen kunci terdiri dari proses pembangkitan, pendistribusian, pemeliharaan, dan pemulihan kunci. Tipe manajemen kunci dibagi menjadi dua yaitu terpusat dan terdistribusi. Skema tersebut mendukung untuk komunikasi *multicast*. Pada skema terpusat diperlukan sebuah *trusted third party* untuk mengontrol aktivitas manajemen grup, meliputi pendaftaran pengguna, pembangkitan kunci, pendistribusian kunci, dan manajemen grup. Skema manajemen kunci yang dibahas pada makalah ini yaitu skema manajemen kunci terpusat yang mengatur pemilik data dan pengguna *cloud*.

Skema *group key management* yang digunakan pada makalah ini menggunakan parameter *public key*, *private key*, *group key*, dan *hash value*. Pemilik data akan membangkitkan dua pasang *public key* dan *private key* (($K_{pub(1)}$, $K_{priv(1)}$) dan ($K_{pub(2)}$, $K_{priv(2)}$)). Pengguna *cloud* yang hendak bergabung dengan grup terlebih dahulu melakukan pendaftaran kepada pemilik data menggunakan mekanisme tertentu. Setelah menjadi anggota grup, pengguna mendapatkan *group key* ($K_{priv(1)}$, $K_{pub(2)}$) yang merupakan parameter kunci yang dimiliki setiap anggota grup. Pemilik data mengunggah dokumen yang dienkripsi menggunakan $K_{pub(1)}$, dan *hash value* dari dokumen. Tujuan dari enkripsi dokumen untuk menjaga kerahasiaan dokumen, sedangkan *hash value* digunakan untuk memastikan keaslian dokumen. Pengguna akan mengunduh dokumen terenkripsi dan mendekripsi dokumen menggunakan $K_{priv(1)}$ serta memverifikasi keaslian dokumen dengan *hash value*. Apabila pengguna hendak mengirimkan dokumen kepada pemilik data, dokumen dienkripsi menggunakan $K_{pub(2)}$ dan di unggah ke *cloud*. Pemilik data akan mengunduh dokumen yang terenkripsi dan mendekripsi dokumen tersebut menggunakan $K_{priv(2)}$. Skema ini diajukan untuk sistem ujian *online* dengan *untrusted public cloud*, dimana komunikasi akan berlangsung hanya pada hari pelaksanaan ujian. Oleh sebab itu, tidak diberikan proses pemulihan kunci pada skema ini.

III. PEMBAHASAN

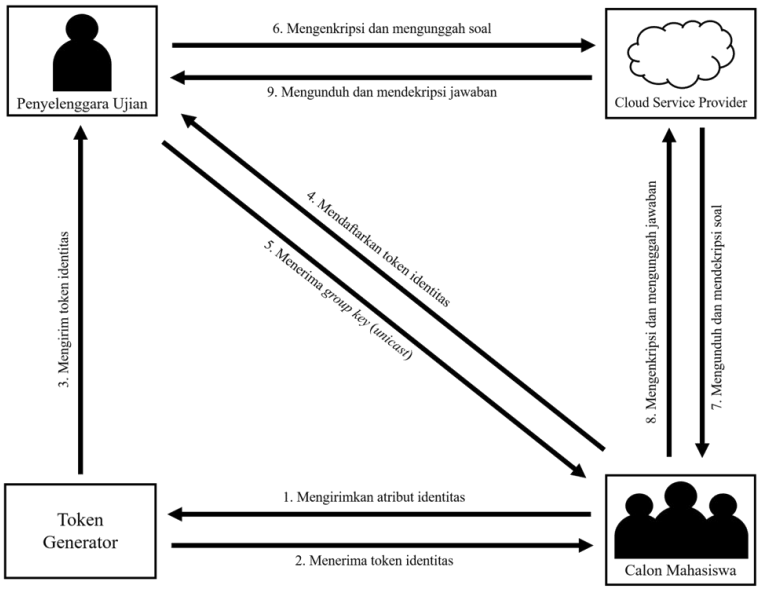
Skema manajemen kunci yang dibahas dalam makalah ini meliputi beberapa komponen antara lain:

1) Penyelenggara ujian sebagai pemilik data
2) *Cloud Service Provider*(CSP)
3) *Token generator* (pembangkit token)
4) Calon mahasiswa yang merupakan pendaftar di suatu perguruan tinggi

Penyelenggara ujian adalah orang yang mengunggah soal ujian pada *public cloud* untuk diakses oleh calon mahasiswa. Sebuah CSP mengoperasikan *server* untuk memelihara data yang diunggah oleh penyelenggara ujian. Pembangkit token digunakan untuk membangkitkan sebuah token yang berasal dari atribut identitas calon mahasiswa, dimana token identitas tersebut digunakan oleh calon mahasiswa untuk

mendapatkan *group key* dari penyelenggara ujian. Calon mahasiswa meupakan pendaftar di suatu perguruan tinggi yang mengikuti ujian *online* penerimaan mahasiswa baru menggunakan *cloud*.

Skema sistem ujian *online* ini diawali dengan proses pendaftaran calon mahasiswa pada suatu perguruan tinggi. Calon mahasiswa mengirimkan atribut identitasnya kepada pembangkit token untuk mendapatkan token. Setelah calon mahasiswa mengkonfirmasi telah mendapatkan token, maka pembangkit token akan mengirimkannya ke penyelenggara ujian. Pada saat pendaftaran ulang, calon mahasiswa akan mendaftarkan token identitasnya untuk mendapatkan *group key* yang digunakan saat pelaksanaan ujian. Ketika pelaksanaan ujian, penyelenggara ujian akan mengunggah soal ujian yang terenkripsi di *cloud*. Calon mahasiswa mengunduh soal ujian dari *cloud* dan mendekripsi soal ujian tersebut menggunakan *group key*. Setelah menjawab soal ujian, jawaban soal dienkripsi menggunakan *group key* dan diunggah di *cloud*. Selanjutnya jawaban akan diunduh oleh penyelenggara ujian untuk diperiksa hasil ujian setiap calon mahasiswa.



GAMBAR 1. ALUR SISTEM AKSES KONTROL BERBASIS PUBLIC KEY ENCRYPTION

Proses tersebut dapat dikelompokan menjadi tiga modul. Antara lain:

A. Modul Perlindungan Privasi

Modul ini dibuat agar privasi setiap calon mahasiswa dapat terlindungi. Setiap calon mahasiswa harus memiliki atribut identitas untuk mendapatkan token identitas. Atribut identitas ini tidak boleh diketahui oleh siapapun, karena jika orang lain mengetahui atribut identitas maka dia dapat mengakses data calon mahasiswa yang bersangkutan. Perlindungan data dilakukan dengan melindungi atribut identitas menggunakan token. Ada dua tahap, yaitu pengeluaran token identitas dan pendaftaran token identitas.

1) Tahap pengeluaran token

Calon mahasiswa mengirimkan atribut identitasnya ke *token generator*. Kemudian calon mahasiswa akan mendapatkan token identitas.

2) Tahap pendaftaran token

Calon mahasiswa mendaftarkan token identitasnya kepada penyelenggara ujian agar dapat mengakses soal yang disimpan oleh CSP. Dengan mendaftarkan token identitas, calon mahasiswa akan mendapatkan *group key*.

B. Modul Manajemen Kunci

Skema manajemen kunci yang diajukan dalam makalah ini terdiri dari tiga tahap yaitu pembangkitan *public key* dan *private key*, pendistribusian kunci, dan penghapusan kunci.

1) Tahap pembangkitan *Public Key* dan *Private Key*

2) Penyelenggara ujian membangkitkan dua pasang *public key*dan *private key* (($K_{pub(1)}$, $K_{priv(1)}$) dan ($K_{pub(2)}$, $K_{priv(2)}$)). Ketika calon mahasiswa mendaftarkan token identitasnya, penyelenggara ujian akan memberikan *group key* ($K_{priv(1)}$, $K_{pub(2)}$) kepada calon mahasiswa.

3) Tahap pendistribusian kunci

Untuk mendapatkan *group key*, calon mahasiswa harus mendaftarkan token identitasnya. Token identitas didapatkan dengan membangkitkan *token generator* menggunakan atribut identitas. Pendistribusian *group key* dilakukan secara *unicast*, yaitu ketika calon mahasiswa mendaftarkan token identitasnya.

4) Tahap penghapusan kunci

Ketika pelaksanaan ujian *online* selesai, maka seluruh kunci yang digunakan tidak lagi digunakan. Jika pada tahun berikutnya dilaksanakan ujian *online* kembali, maka penyelenggara ujian harus membangkitkan ulang *public key* dan *private key*.

C. *Modul Manajemen Dokumen*

Setiap dokumen yang diunggah ke *cloud* harus terenkripsi. Penyelenggara ujian mengenkripsi soal ujian menggunakan $K_{pub(1)}$, serta menghitung *hash value* dari soal ujian. Soal ujian diunggah ke *cloud* beserta *hash value*-nya. Calon mahasiswa mengunduh soal ujian yang berada di *cloud* dan didekripsi menggunakan $K_{priv(1)}$, serta memverifikasi keasliannya berdasarkan *hash value*. Setelah soal ujian selesai dikerjakan, calon mahasiswa mengenkripsi jawaban ujian menggunakan $K_{pub(2)}$. Penyelenggara ujian akan mengunduh setiaap jawaban milik calon mahasiswa dengan didekripsi terlebih dahulu menggunakan $K_{priv(2)}$. Setelah itu jawaban diperiksa oleh penyelenggara ujian.

IV. SIMPULAN DAN SARAN

A. *Simpulan*

Penerapan *public key encryption* pada skema akses kontrol sistem ujian *online* pada *untrusted public cloud* antara lain:

1) Penyelenggara ujian membangkitkan 2 pasang *public key* dan *private key*
2) Penyelenggara ujian membagikan *group key* kepada calon mahasiswa

Dengan skema *group key management* yang telah dibahas pada bagian pembahasan, pelaksanaan ujian penerimaan mahasiswa baru dapat diselenggarakan secara *online*. Penyelenggara ujian tidak perlu menyiapkan tempat ujian dan calon mahasiswa tidak perlu datang ke tempat pelaksanaan ujian. Soal ujian yang diunggah ke *cloud* dapat terjamin kerahasiaan dan keasliannya. Begitupun juga pada jawaban dari setiap calon mahasiswa dapat terjaga kerahasiaannya, karena setiap calon mahasiswa tidak dapat melihat jawaban dari calon mahasiswa lainnya. Sehingga dapat mencegah terjadinya "pencontekan" jawaban milik calon mahasiswa lain. Jadi, sistem ujian *online* ini dapat mempermudah bagi pihak penyelenggara ujian maupun calon mahasiswa, serta tetap terjaga keamanannya.

B. *Saran*

1) Perlu dilakukan penelitian lebih lanjut mengenai tingkat keamanan pada skema akses kontrol sistem ujian *online* pada *untrusted public cloud*.
2) Perlu dilakukan penelitian lebih lanjut mengenai pemilihan algoritma *public key encryption* dan *hash function* pada skema akses kontrol sistem ujian *online* pada *untrusted public cloud*.
3) Perlu dilakukan penelitian lebih lanjut mengenai bagaimana cara memastikan bahwa jawaban yang dikerjakan calon mahasiswa memang dikerjakan oleh calon mahasiswa, atau dengan kata lain tidak menggunakan jasa orang lain.

DAFTAR PUSTAKA

[1] NIST."The NIST Definition of Cloud Computing".Special publication 800-145.

[2] Alex Budiyanto. 2012." Pengantar Cloud Computing". Cloud Indonesia.

[3] Cloud Security Alliance. 2010. "Top Threats to Cloud Computing".

[4] Yacine Challal, Hamida Seba. 2005. “Group Key Management Protocols : A Novel Taxonomy”. International Journal of Information Technology.

[5] M. Al Fikri, Caesario. O. K., Hendrik Maulana. “Manajemen kunci pada mekanisme akses kontrol komunikasi grup pada untrusted public cloud”.unpubulished.