Manajemen Kunci Pada Mekanisme Akses Kontrol Komunikasi Grup Pada *Untrusted Public Cloud*

Muhamad Al Fikri[1)],Caesario Oktanto Kisty[2)], Hendrik Maulana[3)]
[1,2,3]Sekolah Tinggi Sandi Negara
Jalan Raya Haji Usa, Desa Putat Nutug, Bogor, Bogor, 16330
Telp : (0251) 8541742/8541754, Fax : (0251) 8541720
E-mail : malfikri87@gmail.com[1)] , caesarioriorio.kisty@gmail.com[2)] , maulana.hendrikk@gmail.com[3)]

Abstrak

Cloud computing merupakan teknologi yang memungkinkan penggunanya untuk menghemat biaya komputasi. Dengan menggunakan cloud computing, pengguna tidak perlu lagi memikirkan lisensi software, sistem operasi, bahkan dapat menggunakan komputer virtual yang disediakan oleh cloud service provider.Beberapa perusahaan teknologi informasi seperti Google dan Microsoft telah menyediakan layanan cloud computing. Harga yang harus dibayar untuk mendapatkan layanan ini pun beragam, mulai dari gratis hingga berbayar per bulan. Namun, untuk layanan gratis yaitu untrusted public cloud, sama sekali tidak ada pengamanan terhadap data penggunanya karena data yang diunggah oleh pengguna dapat diunduh oleh siapapun. Oleh karena itu, dalam penelitian ini diajukan sebuah mekanisme akses kontrol berbasis enkripsi asimetris untuk komunikasi grup pada untrusted public cloud beserta manajemen kuncinya secara efektif. Akses kontrol ini menggunakan beberapa kunci, yaitu public key, private key, dan group key. Penerapan akses kontrol ini dapat melindungi data pengguna yang disimpan di cloud agar tidak diunduh oleh orang yang tidak berhak.

Kata kunci: Cloud Computing, Group Communication, Akses Kontrol

Abstract

Cloud computing is a technology that allows users to save on the computation cost. By using cloud computing, users no longer need to think about software license and operating systems Users can even use a virtual computer which is provided by the cloud service provider.Some information technology companies such as Google and Microsoft has been providing cloud computing services. The price paid to obtain these services also varied, ranging from free to paid per month. However, there is absolutely no security for user's data in the untrusted public cloud which is a free service. The uploaded data by the user can be downloaded by anyone. Therefore, this research proposed an access control mechanism based on asymmetric encryption for group communications on untrusted public cloud along with effective key management. Access control using multiple keys, namely public key, private key, and the key group. The application of access control can protect user's data stored in the cloud so that the data can not be downloaded by unauthorized party.

Key Word: Cloud Computing, Group Communication, Access Control

1. PENDAHULUAN

Dewasa ini cloud computing (komputasi awan) digunakan oleh banyak organisasi besar maupun kecil, baik secara langsung maupun tidak langsung. Sebuah cloud services (layanan awan) memungkinkan pengguna untuk berbagi data dalam cara yang mudah serta ekonomis. Cloud services dapat dibagi menjadi tiga kategori yaitu Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS).

Sama dengan cloud services, cloud computing juga dibagi menjadi beberapa jenis yaitu public cloud, private cloud, hybrid cloud, dan community cloud. Di dalam public cloud, layanannya dikontrol oleh pemilik data dan cloud service provider (CSP). Google adalah salah satu contoh public cloud provider. Layanan cloud dapat disediakan untuk pengguna dengan gratis, pay-per-user, atau pay per usage. Pada public cloud, banyak pengguna dapat mengakses data yang terletak pada situs milik CSP (Alex Budiyanto,2012). Hal inilah yang menyebabkan kerawanan, karena CSP tidak menyediakan layanan kerahasiaan data dari penggunanya (Cloud Security Alliance, 2012). Masalah keamanan dan privasi data menjadi hal yang sangat dipertimbangkan pengguna apalagi dengan skala yang besar seperti perusahaan atau organisasi.

Untuk menjamin kerahasiaan data yang tersimpan di cloud, dibutuhkan mekanisme akses kontrol yang diterapkan oleh provider. Pada makalah ini, sebuah skema akses kontrol berbasis public key encryption digunakan untuk menyimpan data pada untrusted public cloud. Sehingga data hanya bisa diakses oleh pengguna yang memiliki hak akses dari pemilik data. Akses diberikan untuk pengguna berdasarkan atribut identitasnya. Atribut ini disimpan di cloud ketika pengguna melakukan registrasi. Identitas pengguna kemudian diproteksi untuk menjamin privasi dan keamanan dari data dan pengguna. Pada skema ini, pengguna dapat mendekripsi data jika dan hanya jika atribut identitas pengguna memenuhi kebijakan akses kontrol dari pemilik data. Selain itu, pemilik data dan CSP tidak mengetahui mengenai atribut identitas dari pengguna. Dengan demikian, menyembunyikan atribut identitas berarti melindungi privasi dari data yang diakses oleh tiap pengguna. Untuk menerapkan mekanisme akses kontrol tersebut, diperlukan manajemen kunci yang efisien secara komputasi yang diajukan dalam makalah ini.

2. LANDASAN TEORI

a. *Cloud Computing*[1]

Cloud computing adalah sistem yang memiliki karakteristik berikut:

1) *Resource Pooling*
   Sumber daya komputasi (*storage*, CPU, *memory*, *network bandwidth*, dan lain sebagainya) yang dikumpulkan oleh penyedia layanan (*service provider*) untuk memenuhi kebutuhan banyak pelanggan (*service costumer*).
2) *Broad Network Access*
   Kapabilitas layanan dari tersedia lewat jaringan dan bisa diakses oleh berbagai jenis perangkat seperti *smartphone, tablet, laptop, workstation*, dan sebagainya.
3) *Measured Service*
   Tersedia layanan untuk mengoptimasi dan memonitor layanan yang dipakai secara otomatis.
4) *Rapid Elasticity*
   Kapabilitas dari layanan bisa dipakai oleh pengguna secara dinamis berdasarkan kebutuhan.
5) *Self Service*
   Pengguna bisa mengkonfigurasi secara mandiri layanan yang ingin dipakai melalui sebuah sistem, tanpa perlu interaksi manusia dengan pihak *provider*.

Ada beberapa jenis *cloud computing* yaitu :

1) *Public Cloud*
   Adalah layanan *cloud computing* yang disediakan untuk masyarakat umum. Pengguna bisa langsung mendaftar ataupun menggunakan layanan yang ada. Layanan ini ada yang gratis maupun berbayar. Contohnya yaitu *Google Mail, Sales Force*.
2) *Private Cloud*
   Private cloud disediakan untuk memenuhi kebutuhan internal dari organisasi / perusahaan.
3) *Hybrid Cloud*
   Gabungan dari layanan *public cloud* dan *private cloud* yang diimplementasikan oleh suatu organisasi / perusahaan. Pengguna dapat memilih jalur mana yang akan dilewati, bisa *public* atau *private*.
4) *Community Cloud*
   Layanan ini dibangun khusus untuk komunitas tertentu, yang penggunanya berasal dari organisasi yang mempunyai urusan yang sama.

b. *Group Communication*[3]

Group communication merupakan komunikasi antara seseorang dengan kelompok orang (grup). Teknik *group communication* ada tiga, yaitu *multicast, unicast,* dan *broadcast*. Teknik *multicast* yaitu informasi dikirimkan ke sekumpulan komputer yang tergabung dalam sebuah grup tertentu, yang disebut *multicast group*. Teknik *unicast* mengirimkan informasi dari satu titik, dan memiliki tujuan hanya satu titik lain. Teknik *broadcast* mengirimkan informasi dari satu titik ke seluruh titik yang ada di jaringan.

c. Skema akses kontrol untuk Group Communication pada Cloud Computing[5]

Mekanisme akses kontrol membatasi pengguna yang tidak berhak untuk mengakses data. Terdapat banyak pengembangan dari akses kontrol berbasis mekanisme keamanan untuk jaringan kabel dan nirkabel.

Group access control dapat dibuat dengan mengenkripsi data (dokumen) menggunakan kunci dengan ukuran yang cocok. Kunci ini dibangkitkan secara dinamis untuk setiap *session* komunikasi. Pembangkitan kunci ini menggunakan skema manajemen kunci yang efektif, sehingga *Session Key* (SK) atau *Group Key* (GK) dapat dibagi ke seluruh pengguna yang sah dari grup tersebut untuk mengakses data yang tersimpan di *cloud server*. Pembagian kunci ini penting ketika struktur grup berbentuk dinamis, yaitu apabila ada pengguna yang baru bergabung atau meninggalkan grup, secara otomatis grup akan menyesuaikan bentuknya. Kunci enkripsi yang

digunakan harus selalu diperbarui untuk mencegah pengguna yang baru masuk atau yang meninggalkan grup masih dapat mengakses data setelah melakukan hal tersebut. Skema *group key management* telah banyak dibahas dan dikembangkan, namun yang diajukan di makalah ini sedikit berbeda, yaitu *key server* di skema ini tidak membangkitkan kunci. Sebagai gantinya, pemilik data membangkitkan *private key* untuk setiap pengguna. Berdasarkan *private key* tersebut, dapat dihitung *public key* yang digunakan sebagai *group key*. Setelah membangkitkan *group key*, pemilik data mengenkripsi datanya menggunakan *group key* dan menyimpannya di *cloud*.

d. **Skema *Group Key Management*[4]**

Proses dari pembangkitan, pendistribusian, dan pemeliharaan kunci merupakan bagian dari skema manajemen kunci. Ada dua tipe manajemen kunci yaitu terpusat dan terdistribusi. Kedua skema ini mendukung untuk komunikasi *multicast*. Pada skema terpusat, sebuah *trusted third party* diperlukan untuk mengendalikan aktivitas manajemen grup. Aktivitas ini meliputi pendaftaran pengguna, pembangkitan kunci, pendistribusian kunci, dan manajemen grup. Sedangkan pada skema terdistribusi, kunci dikomputasi dan dipelihara dengan melibatkan seluruh anggota grup. Skema terdistribusi dibagi menjadi dua yaitu terdistribusi penuh dan terdistribusi sebagian. Pada skema terdistribusi penuh, pengguna berperan dalam pembangkitan dan pendistribusian kunci, yang membantu untuk menjaga keamanan dan keanggotaan grup. Dalam skema terdistribusi sebagian, baik pengguna dan *group controller*, terlibat dalam pembangkitan, pemeliharaan kunci. Skema manajemen kunci yang dibahas dalam makalah ini yaitu sebuah skema manajemen kunci terpusat yang beroperasi di antara pemilik data dan pengguna *cloud*.

Pembangkitan dan distribusi kunci akan lebih sulit ketika pesannya didistribusikan ke sebuah grup pengguna dari *cloud server*, karena pengguna mungkin bisa bergabung atau meninggalkan grup secara dinamis. Oleh karena itu kunci harus selalu diperbarui. Setelah anggota grup baru bergabung atau keluar dari grup, pemilik data membangkitkan *group key* baru dan mendistribusikannya ke semua anggota grup. Sebagai hasilnya, parameter akses kontrol pun berubah.

Setelah mengubah parameter akses kontrol, pemilik data menyebarkan parameter ini ke seluruh anggota grup dari pengguna *cloud* dan setiap pengguna *cloud* menghitung *group key* baru. Pengguna lama yang keluar dari grup maupun pengguna baru tidak dapat menemukan *group key* ini karena *private key* miliknya tidak digunakan saat nilai *group key* baru didistribusikan ke pengguna yang masih di dalam grup.

3. PEMBAHASAN

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

a. Pemilik data
b. *Cloud Service Provider* (CSP)
c. *Token generator* (pembangkit token)
d. Pengguna

Pemilik data adalah orang yang menempatkan dokumen asli pada *public cloud* untuk diakses oleh pengguna *cloud*. Sebuah CSP mengoperasikan *server* untuk memelihara data yang disimpan oleh pemilik data. Pembangkit token digunakan untuk membangkitkan sebuah token, yang diberikan kepada setiap pengguna *cloud* untuk mendapatkan kunci rahasia dari pemilik data. Pengguna merupakan orang atau aplikasi yang ingin mengakses data melalui CSP.

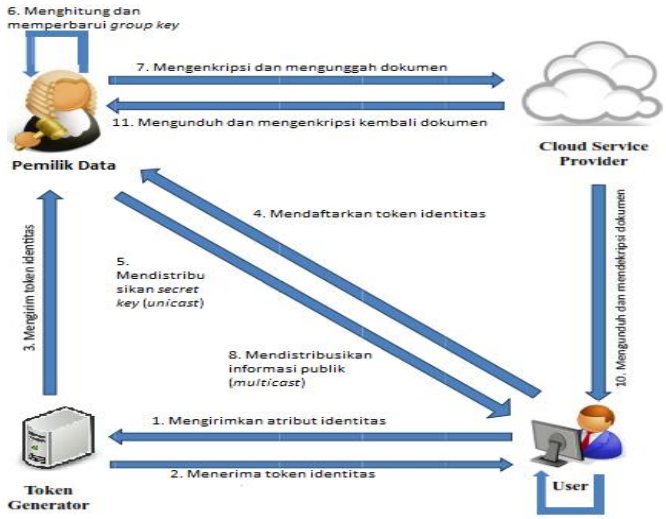
Mula-mula setiap pengguna *cloud* harus mengirimkan atribut identitasnya kepada pembangkit token untuk mendapatkan token. Setelah token dibangkitkan, pembangkit token membangkitkan token baru kepada user dan mengirimkannya ke pemilik data untuk memverifikasinya. Proses verifikasi dilakukan setelah pembangkit token memberikan token ke pengguna, setelah pengguna mengkonfirmasi bahwa token telah diterima, pembangkit token lalu mengirimkan token tadi ke pemilik data.

Pengguna mendaftarkan token identitasnya ke pemilik data untuk mendapatkan kunci rahasia. Pemilik data memberikan kunci rahasia berdasarkan token identitasnya. Setelah menyediakan kunci rahasia, pemilik data menghitung *group key* untuk setiap grup berdasarkan nilai kunci rahasia mereka. Kemudian, pemilik data mengenkripsi dokumen dan mengunggahnya ke *cloud provider* melalui CSP. Setiap pengguna *cloud* dapat menurunkan *group key* menggunakan kunci rahasia mereka dan dapat menggunakan nilai turunan dari *group key* ini untuk mendekripsi dokumen yang disimpan di *cloud*. Ketika keanggotaan grup berubah, pemilik data harus mengganti nilai *group key*. Pemilik data dapat juga mengganti nilai *group key* secara berkala. Sebagai contoh ketika seorang anggota keluar dari grup atau bergabung dengan grup, pemilik data mengunduh dokumen yang diunggah tadi dari *cloud service provider* dan mengenkripsi kembali dokumen dengan nilai *group key* yang baru, kemudian menggunggah hasilnya ke *cloud*. Proses tersebut dapat dikelompokkan menjadi tiga modul, antara lain :

a. Modul perlindungan privasi

b. Modul manajemen kunci
c. Modul manajemen dokumen

Gambar 1. Alur Sistem Akses Kontrol Berbasis *Public Key Encryption*

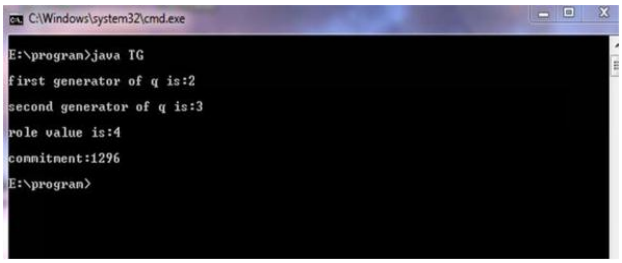


a. Modul perlindungan privasi

Modul ini didesain untuk melindungi privasi setiap pengguna *cloud*. Setiap pengguna harus mempunyai atribut identitasnya masing-masing. Atribut identitas ini tidak boleh diketahui oleh pemilik data maupun pengguna lain. Dengan tujuan melindungi privasi, maka atribut identitas ini harus dilindungi, karena ketika orang lain mengetahui atribut identitas ini, maka dia dapat mengakses data pengguna. Perlindungan data dilakukan dengan melindungi atribut identitas ini. Caranya yaitu dengan menggunakan token. Ada dua tahap, yaitu pengeluaran token identitas, dan pendaftaran token identitas.

1) Tahap pengeluaran token
Pada tahap ini, setipa pengguna mengirimkan atribut identitasnya ke *token generator*. Kemudian *token generator* akan mengirimkan token identitas ke pengguna setelah menerima atribut identitas pengguna tersebut.

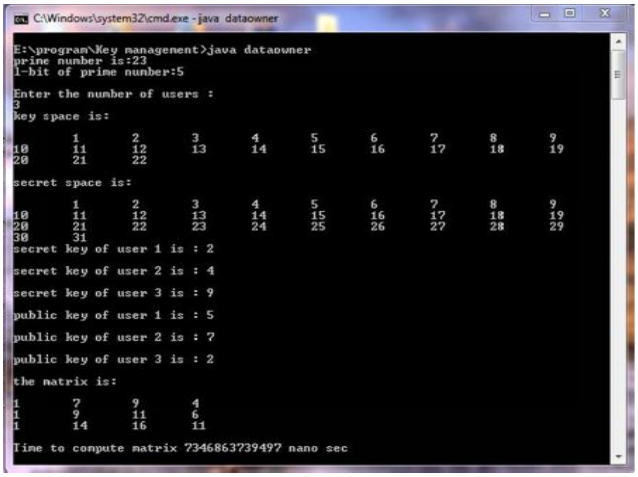
2) Tahap pendaftaran token
Pengguna mendaftarkan token identitasnya kepada pemilik data supaya pengguna dapat mengakses dokumen yang disimpan oleh CSP. Dalam tahap pendaftaran, pengguna memberikan token identitasnya ke pemilik data kemudian menerima nilai kunci rahasia.



Gambar 2. Proses pembangkitan dan pendaftaran token

b. Modul manajemen kunci

Dalam manajemen kunci grup, skema enkripsi kunci simetris digunakan untuk melindungi data. Skema manajemen kunci grup dapat dibagi menjadi dua jenis yaitu statis dan dinamis. Dalam sebuah skema manajemen kunci grup dinamis, *group key* selalu diperbarui ketika keanggotaan grup berubah. Proses memperbarui kunci ini (disebut *rekeying*) membutuhkan komputasi tambahan. Skema yang digunakan pada makalah ini yaitu *multicast dynamic group key management*. Keuntungan menggunakan skema manajemen kunci grup yaitu pembaruan kunci hanya perlu mengganti *public key* saja, *private key* sama sekali tidak terpengaruh dengan pembaruan tersebut. Skema manajemen kunci yang diajukan dalam makalah ini terdiri dari lima tahap yaitu inisialisasi, pembangkitan *private key* dan *public key*, komputasi kunci, penurunan kunci, dan pembaruan kunci.



Gambar 3. Proses manajemen kunci

1) Tahap inisialisasi

Pemilik data membangkitkan *l*-bit bilangan prima *q* untuk mendefinisikan grup F_q dan fungsi hash H(). Kemudian pemilik data menghitung *key space* KS=F_q dan *secret space* SS={1,2,3,.....,2^l-1}.

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

Pemilik data membangkitkan *private key* s_i secara acak untuk setiap pengguna. *Private key* hanya diketahui oleh pemilik data dan pengguna yang bersesuaian. Kemudian pemilik data membangkitkan *public key* z_i dari *secret space* (SS) dan menginformasikannya ke seluruh pengguna.

3) Tahap komputasi kunci

Pemilik data memilih *group key* secara acak dari *key space* (KS) dan menghitung informasi publik menggunakan nilai *private key* setiap pengguna dan *public key*, lalu pemilik data mengirimkan informasi publik tersebut ke semua pengguna. Informasi publik merupakan *group key* yang dienkripsi dengan *public key* pengguna.

4) Tahap penurunan kunci

Setiap pengguna *cloud* menurunkan *group key* menggunakan *private key* dan informasi publik yang diterima dari pemilik data. Pengguna dapat menggunakan *group key* ini untuk mendekripsi dokumen yang disimpan di *cloud*.

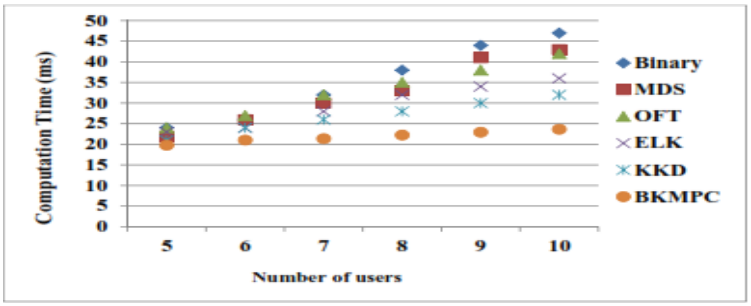
5) Tahap pembaruan kunci

Ketika ada anggota bergabung atau meninggalkan grup, sebuah *group key* baru harus dibangkitkan dan didistribusikan kepada pengguna *cloud*.

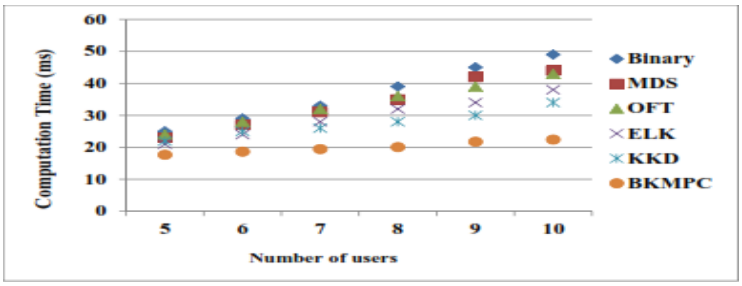
c. Modul manajemen dokumen

Manajemen dokumen dilakukan oleh pemilik data. Pemilik data mengenkripsi seluruh dokumen yang dapat diakses oleh grup menggunakan *group key*. Pemilik data mengunggah dokumen terenkripsi ke *cloud*. Jika pengguna ingin melihat dokumen tersebut, pengguna harus mengunduh dokumen dari *cloud*. Setelah pengguna mendapat dokumen tersebut, pengguna harus menurunkan *group key* untuk mendekripsi dokumen menggunakan informasi publik dan *public key* yang diterima dari pemilik data. Pengguna kemudian mendekripsi dokumen menggunakan *group key* yang sudah diturunkan. Ketika ada anggota bergabung atau meninggalkan grup, pemilik data harus mengunggah kembali setiap dokumen yang terenkripsi dengan *group key* baru.

Dari uji coba komputasi yang dilakukan, didapatkan bahwa ketika jumlah *user* 10 orang, maka dibutuhkan 24.49 ms untuk menghitung *group key* baru dan membutuhkan 22.45 ms untuk menurunkan *group key* tersebut.
Dengan menerapkan teknik manajemen kunci ini pada *untrusted public cloud*, maka privasi dari pengguna layanan *cloud* akan terjamin dan proses komputasi kunci yang dilakukan menjadi lebih cepat apabila dibandingkan dengan teknik manajemen kunci lainnya, seperti tampak pada gambar di bawah ini.



Gambar 4. Waktu komputasi *group key*



Gambar 5. Waktu komputasi penurunan *group key*

4. SIMPULAN DAN SARAN

a. Simpulan

Berdasarkan hasil analisis yang dilakukan, maka diperoleh simpulan sebagai berikut :

1) Penerapan enkripsi asimetris pada skema akses kontrol komunikasi grup pada *untrusted public cloud* antara lain :

a. *Public* key, *private key*, dan *group key* dibangkitkan oleh pemilik data.
b. *Public key* dan *private key* dibagikan ke tiap pengguna *cloud*.
c. *Group key* dibagikan ke pengguna dengan terlebih dahulu dienkripsi menggunakan *public key* pengguna.
d. Pengguna menurunkan *group key* menggunakan *private key*.
e. *Group key* inilah yang digunakan untuk mendekripsi dokumen yang tersimpan di *cloud*.

2) Komputasi yang dilakukan cepat, karena hanya setiap *user* hanya menghitung satu perkalian vektor setiap perhitungan *group key*.
3) Manajemen kunci pada penerapan enkripsi asimetris pada skema akses kontrol komunikasi grup pada *untrusted public cloud* antara lain :

a. Pembangkitan kunci
b. Penyebaran kunci
c. Penggunaan kunci
d. Perubahan kunci

b. Saran

Setelah melakukan analisis, maka saran yang diberikan penulis sebagai berikut:

1) Perlu dilakukan penelitian lebih lanjut mengenai aspek keamanan pada skema akses kontrol komunikasi grup pada untrusted public cloud.
2) Perlu dikaji lebih lanjut mengenai manajemen kunci pasca operasional pada penerapan enkripsi asimetris skema akses kontrol komunikasi grup pada *untrusted public cloud.*

5. DAFTAR RUJUKAN

[1] Alex Budiyanto. 2012. Pengantar *Cloud Computing*. Cloud Indonesia.
[2] Alliance, Cloud Security. 2010. Top Threats to Cloud Computing.
[3] Khazan, Roger I. 2006. Securing Group Communication of Dynamic Groups in Dynamic Network-Centric Environments. MIT Lincoln Laboratory.
[4] NIST. 2013. Cryptographic Key Management Issues and Challenges in Cloud Services.
[5] Onankuju, Bibin K. 2013. Access Control in Cloud Computing. Manipal University of Technology : India.
[6] Challal, Yacine. 2005. Group Key Management Protocols : A Novel Taxonomy. International Journal of Information Technology.