Cloud Security : Blockchain Access Control

Ariq Radhitama Ariasatya, 18217017, Sistem Teknologi Informasi

Makalah Keamanan Informasi

***Abstract*—Dalam era globalisasi ini teknologi *cloud* sudah banyak digunakan dalam berbagai proses bisnis di dunia. Penyimpanan data di *cloud* dapat mempermudah pengaksesan jarak jauh, pengambilan keputusan, pengurangan biaya untuk penyimpanan data dan distribusi data. Dengan banyaknya penggunaan *cloud, cloud security* merupakan salah satu isu terpenting dalam bidang *cloud computing.* Salah satu solusi untuk mengatasi masalah *cloud security*, adalah menggunakan *blockchain access control.* Dengan menggunakan alamat akun dari *node* pada *blockchain* sebagai identitas, dan mendefinisikan kembali izin mengakses data pada *cloud*, yang lalu dienkripsi dan disimpan pada *blockchain*.**

Keywords*—makalah, keamanan informasi, *cloud security, blockchain, security, access control.

1. Pendahuluan

1.1. Latar Belakang

Pada era globalisasi ini, teknologi dan internet sudah digunakan pada hampir semua kegiatan yang dilakukan oleh manusia. Beberapa aktivitas bahkan tidak bisa dilakukan tanpa bantuan teknologi. Dengan teknologi yang mempermudah segala aktivitas manusia, tidak mengejutkan jika perusahaan dan industri juga menggunakan berbagai macam teknologi untuk mengefisiensikan proses bisnis mereka. Peran manusia pun sudah ada yang tergantikan oleh teknologi karena jika menggunakan teknologi, biaya yang dikeluarkan dapat berkurang, mengurangi kemungkinan kesalahan yang terjadi, dan dapat mempercepat proses juga. Tidak mengejutkan jika dalam beberapa tahun lagi, peran manusia tidak diperlukan dalam menjalankan proses bisnis.

Dalam penggunaan teknologi tersebut, tentu terdapat data yang harus disimpan, seperti identitas pengguna, informasi perusahaan, dll. Untuk skala individu, menggunakan media penyimpanan lokal seperti *hard disk* biasanya sudah cukup, tetapi untuk skala perusahaan atau industri, dengan banyaknya data yang disimpan dan diolah, penggunaan media penyimpanan lokal akan meningkatkan biaya yang diperlukan secara signifikan. Seiring berkembangnya teknologi, datanglah teknologi *cloud computing.*

Cloud computing adalah salah satu platform komputasi terdistribusi yang paling cepat berkembang di perusahaan, industri, akademik, dan komunitas penelitian saat ini [1]. *Cloud computing*, sebagai model komputasi yang lumayan baru juga bisa menyediakan pengguna dengan layanan yang selalu ada, mengurangi biaya dari penyimpanan dan komputasi, dan meningkatkan kemudahaan penggunaan, karena dari itu semakin banyak bisnis dan individu yang menyimpan data dalam sebuah *cloud* [2]. Jaringan merupakan bagian terpenting dalam *cloud computing* dengan menyediakan layanan berkualitas, seperti memastikan batasan waktu [3], dan tanpanya, *cloud computing* tidak dapat mengintegrasi berbagai sumber daya komputasi dan penyimpanan [2].

Pentingnya jaringan dalam sebuah *cloud computing*, menarik orang yang ingin menyerang jaringan *cloud* dengan berbagai cara, seperti akses ilegal, pemasukan kode berbahaya, menguping, dan mengirim paket tidak valid [4]. Serangan tersebut akan berdampak terhadap aplikasi pengguna dan sumber daya *cloud* dan akan menunda waktu eksekusi proses dari keseluruhan aplikasi *cloud computing* [5]. Salah satu contohnya, pada laporan kejadian pada bulan September 2017 oleh HIPAA Journal [6] menunjukkan bahwa 76,81% dari informasi kesehatan dengan jumlah 363,364 catatan telah tersebar.

Access Control merupakan salah satu area fokus untuk keamanan *cloud computing*, dan merupakan salah satu teknologi utama untuk keamanan *cloud* [7]. Tujuan penggunaan *access control* adalah untuk mencegah sumber daya yang disimpan dalam *cloud* untuk diakses atau dicuri oleh pengguna ilegal. Pada makalah ini, akan dibahas penggunaan *blockchain access control* dalam mengamankan data pada sebuah *cloud* agar tidak dieksploitasi oleh pengguna ilegal.

1.2. Dasar Teori

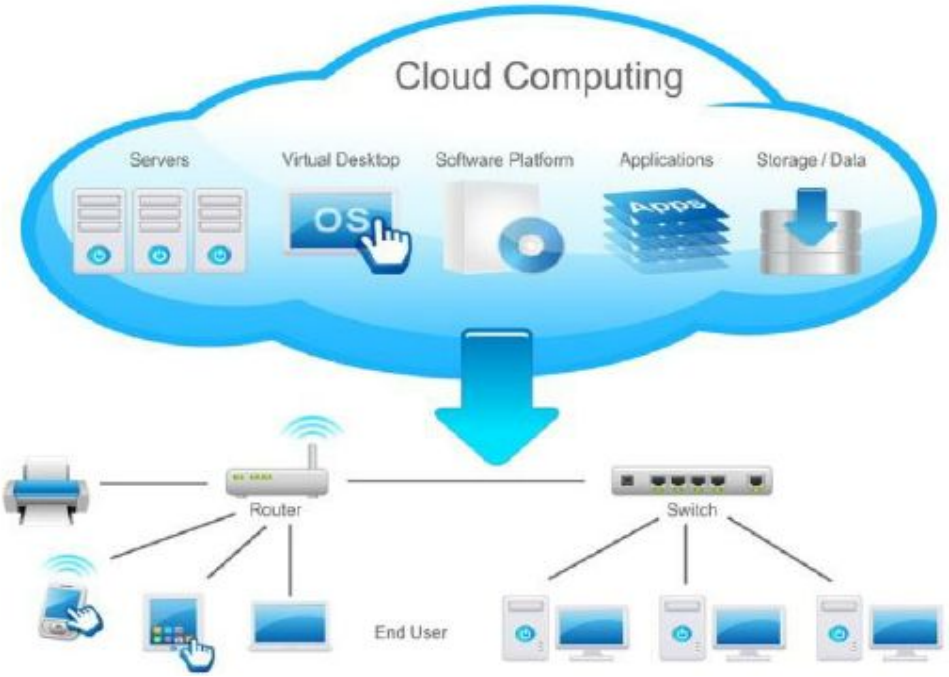
1.2.1. *Cloud Computing*

Cloud computing, adalah sebuah model yang memungkingkan akses jaringan di manapun, dan sesuai kebutuhan untuk mengakses kumpulan sumber daya komputasi yang dapat digunakan bersama dan dikonfigurasi seperti jaringan, server, media penyimpanan, aplikasi dan layanan, yang dapat digunakan dengan usaha minim [2]. Teknologi ini menjadikan internet sebagai pusat server dalam mengelola data, sehingga pengguna dapat menjalankan program atau aplikasi tanpa harus menginstall aplikasi tersebut. Karena tidak perlu menginstall, maka media penyimpanan data dari pengguna juga disimpan secara *virtual* dan tidak membebani media penyimpanan lokal pengguna.

Beberapa manfaat dari penggunaan *cloud computing*, adalah media penyimpanan terpusat pada server, sehingga memudahkan pengguna untuk menyimpan dan mengaksesnya, dan tidak perlu menyediakan media penyimpanan lagi. Lalu keamanan data, dimana beberapa penyedia *cloud*

computing sudah menyediakan jaminan data sehingga data tidak mudah *corrupt* atau rusak. *Cloud computing* juga lebih murah dan tahan lama, karena tidak memerlukan media penyimpanan lokal seperti *hard disk*.

Terdapat juga beberapa model dari *cloud computing*, pertama adalah *private cloud*, dimana infrastruktur tersebut hanya dapat digunakan oleh sebuah organisasi yang terdiri dari beberapa pengguna, seperti unit bisnis. Kedua adalah *community cloud*, dimana infrastruktur disediakan kepada sebuah komunitas, yang anggota dari komunitas tersebut memiliki tujuan sama. Ketiga adalah *public cloud*, dimana infrastruktur dapat digunakan oleh publik, contohnya adalah *social media.* Yang keempat dan terakhir adalah *hybrid cloud* yang merupakan gabungan dari dua atau lebih infrastruktur *cloud* [2].



Gambar 1. Proses *cloud computing*

sumber :
https://www.researchgate.net/figure/Cloud-computing-architecture-process_fig1_267921329

1.2.2. *Access Control*

Access control adalah sebuah proses dimana sebuah administrator dari sebuah objek, memberi hak akses kepada pengguna untuk mengakses informasi yang terdapat pada ACL (*access control list)*. Pengguna hanya dapat mengakses data dimana dia diberikan izin dan juga sebaliknya, dimana data hanya dapat diakses oleh pengguna yang memiliki izin akses data tersebut.

Access control memiliki beberapa prinsip, yang pertama adalah *principle of least privilege,* dimana jika tidak ada konfigurasi untuk pengguna secara spesifik, maka pengguna seharusnya tidak dapat mengakses informasi tersebut. Kedua adalah *separation of duties*, yaitu memisahkan *area access* untuk mengurangi modifikasi data yang tidak sah pada informasi. Yang terakhir adalah *need to know*, yaitu perinsip dimana pengguna hanya diberikan akses untuk informasi yang mereka butuhkan saja [8].

1.2.3. *Blockchain*

Blockchain adalah serangkaian catatan data yang dikelola oleh sekelompok komputer yang tidak dimiliki oleh satu entitas, dimana masing-masing blok data tersebut diamankan dan terhubung satu sama lain menggunakan prinsip kriptografi. Jaringan pada *blockchain* tidak memiliki otoritas pusat, dimana informasi di dalamnya terbuka untuk siapa saja dan dapat dilihat siapa saja.

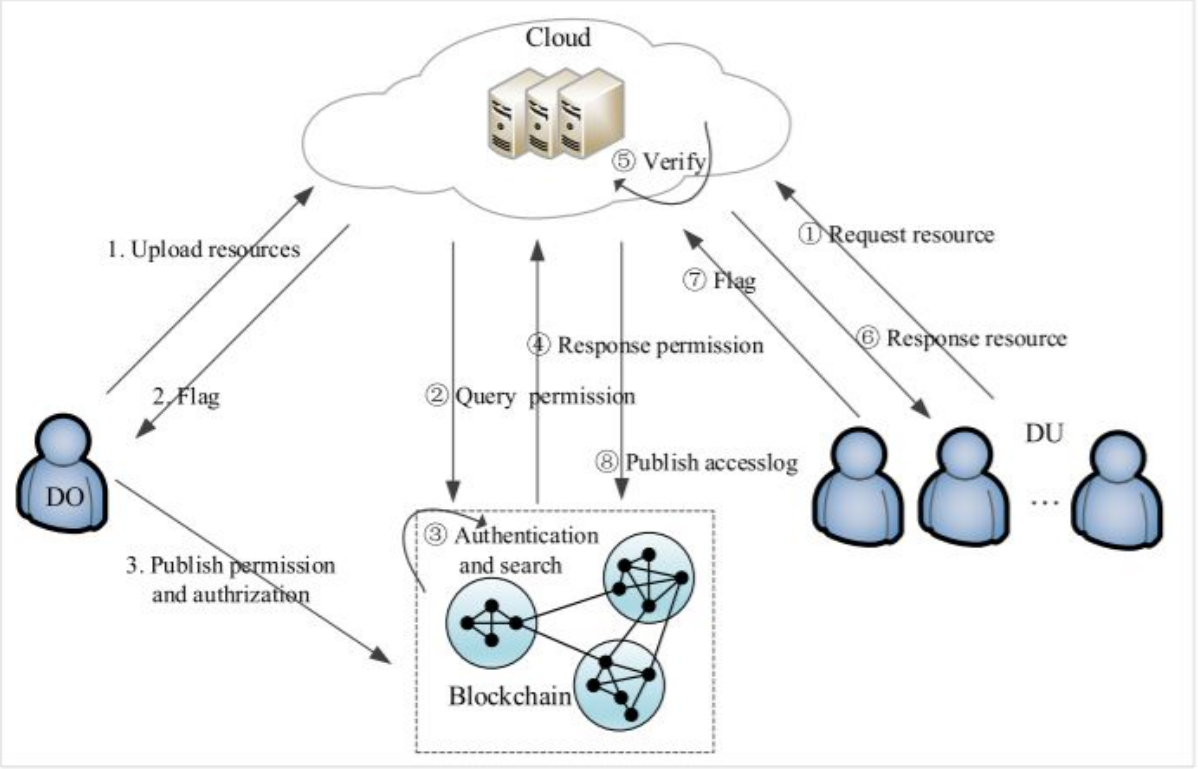
Blockchain memiliki tiga sifat utama, yang pertama adalah desentralisasi, dimana informasi tidak disimpan pada sebuah entitas tunggal, hal ini memberi keamanan lebih karena data tidak tersimpan pada satu tempat, dan mempercepat interaksi karena tidak perlu melalui pihak ketiga. Kedua adalah transparansi, dimana seluruh transaksi yang terjadi pada *blockchain* dapat dilihat, hal ini meningkatkan tingkat akuntabilitas dari proses yang dilakukan. Yang terakhir kekal, dimana jika sesuatu sudah masuk ke *blockchain,* hal itu tidak dapat dirusak *blockchain menggunakan* algoritma hash, dimana tiap blok pada *blockchain* menyimpan hash *pointer*

yang menunjuk blok sebelum dan setelahnya, sehingga jika ada data yang diubah, terlihat oleh blok sebelum dan sesudahnya [9].

2. Pembahasan

Berdasarkan latar belakang dan permasalahan diatas, diharapkan pembaca tau pentingnya keamanan dari data yang disimpan dalam *cloud.* Untuk dari itu, demi mengatasi permasalahan tersebut, dapat digunakan *blockchain access control*, yang memiliki dua karakteristik umum sebagai berikut:

- **Lebih dari satu pusat**. diperlukan beberapa pusat untuk menyimpan identitas pengguna, informasi hak akses, dsb, agar tidak terkumpul pada satu pusat penyimpanan.
- ***System administrator* (SA) terpercaya.** dalam penggunaannya, diperlukan seorang SA untuk mengelola hak pengaksesan data.



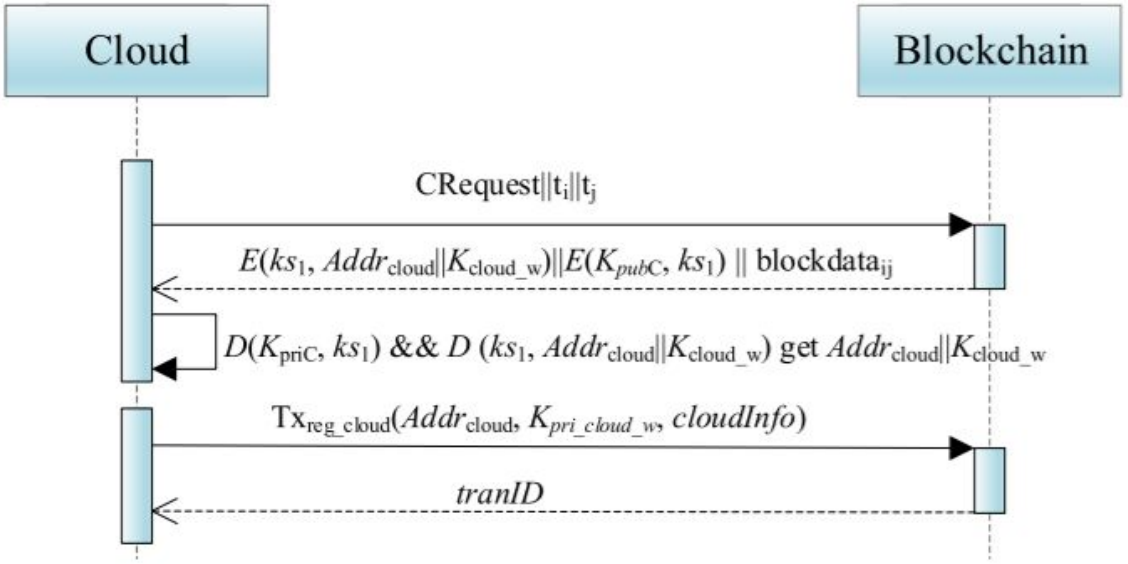
Gambar 2. Model sistem *blockchain access control* [10]

Gambar 2 menjelaskan alur kerja *blockchain access control,* dimana pertama *Data Owner* (DO) mengunggah sebuah data menuju *cloud*, yang lalu diberi response berupa *flag*, menandakan data sudah diterima. Lalu DO akan Mengunggah izin akses dan otorisasi ke *blockchain.* Ketika ada *Data User* (DU) yang ingin menggunakan data, ia akan meminta data ke *cloud*, dimana akan dicek apakah DU tersebut memiliki izin akses dengan dilakukan pengecekan pada *blockchain*. Setelah menemukan izin dari DU tersebut, akan memberikan *response* terhadap *cloud* berupa izin akses milik DU tersebut, yang kemudian akan diverifikasi oleh *cloud* dan memberikan *response* ke DU berupa data jika memang memiliki hak akses, atau notifikasi bahwa DU tidak memiliki hak akses terhadap data tersebut. Lalu DU akan memberi *flag* kepada *cloud* menandakan bahwa dia sudah mendapatkan *response,* lalu *cloud* mengunggah informasi pengakses ke *blockchain.*

2.1. *Initialization*

Pada tahap ini, terdapat registrasi dari *cloud*, DO & DU, dan publikasi data.

1) Registrasi *Cloud*



Gambar 3. Workflow registrasi *cloud* [10]

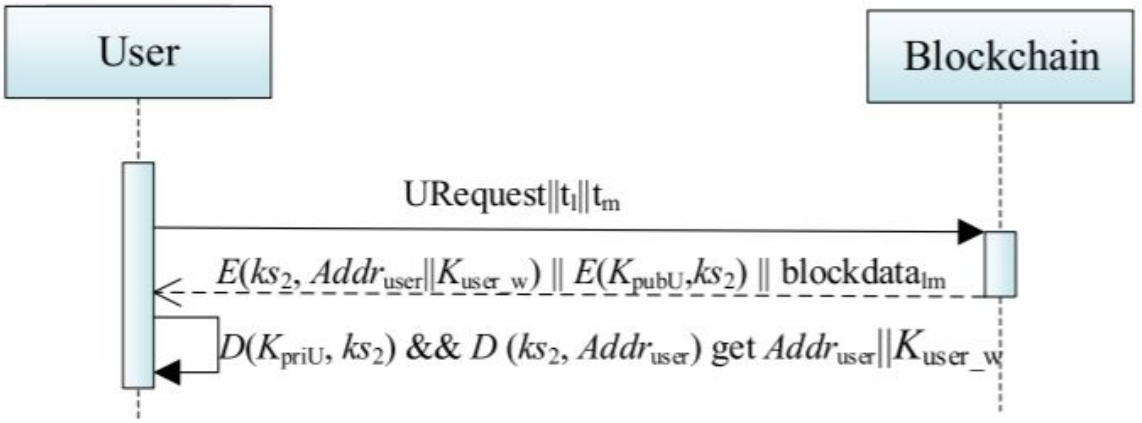
Pada tahap ini, *cloud* melakukan registrasi ke *blockchain* untuk dapat menggunakan *node* dari *blockchain.* Seperti yang terlihat pada gambar 3, proses ini terbagi menjadi tiga langkah.

a. *Cloud* mengirim *request* untuk registrasi pada *blockchain* (CRequest).

b. *Blockchain* memanggil fungsi untuk menghasilkan *public & private key* dari *cloud*. Lalu menggunakan sebuah fungsi dengan input *public key* dari *cloud,* untuk menghasilkan *address* dari *cloud. address* tersebut lalu di enkripsi, lalu dikirim kembali ke *cloud*, yang lalu akan di dekripsi untuk mendapatkan *address*.

c. Lalu dengan menggunakan sebuah algoritma, dengan input berupa *address, private key,* dan informasi dari *cloud, blockchain* akan menyimpannya beserta waktu penyimpanan. *Transaction* ID dari proses tersebut lalu dikembalikan kepada *cloud.*

2) Registrasi Pengguna



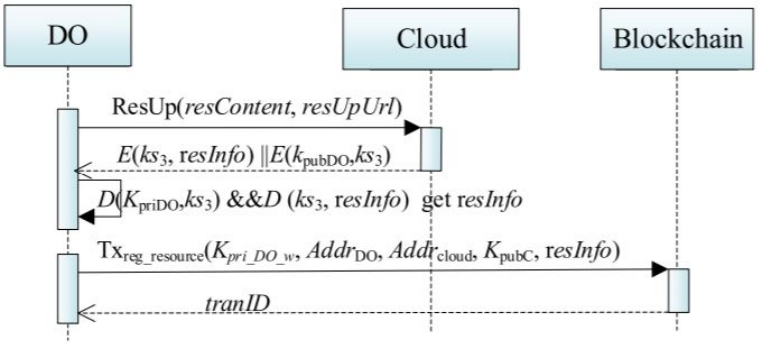
Gambar 4. Workflow registrasi user[10]

Pada tahap ini, pengguna melakukan registrasi ke *blockchain* untuk dapat menggunakan *blockchain.* Seperti yang terlihat pada gambar 4, proses pendaftaran DU dan DO sama, maka dijadikan satu, proses ini terbagi menjadi dua langkah.

a. Pengguna mengirim *request* untuk registrasi pada *blockchain* (URequest).

b. *Blockchain* memanggil fungsi untuk menghasilkan *public & private key* dari pengguna. Lalu menggunakan sebuah fungsi dengan input *public key* dari pengguna, untuk menghasilkan *address* dari pengguna. *address* tersebut lalu di enkripsi, lalu dikirim kembali kepada pengguna yang lalu akan di dekripsi untuk mendapatkan *address*.

3) Pengunggahan Data



Gambar 5. Workflow pengunggahan data[10]

Pada tahap ini, DO mengunggah data ke *cloud* dan *metadata* ke *blockchain.* Seperti yang dapat dilihat pada gambar 5, terdapat tiga langkah,

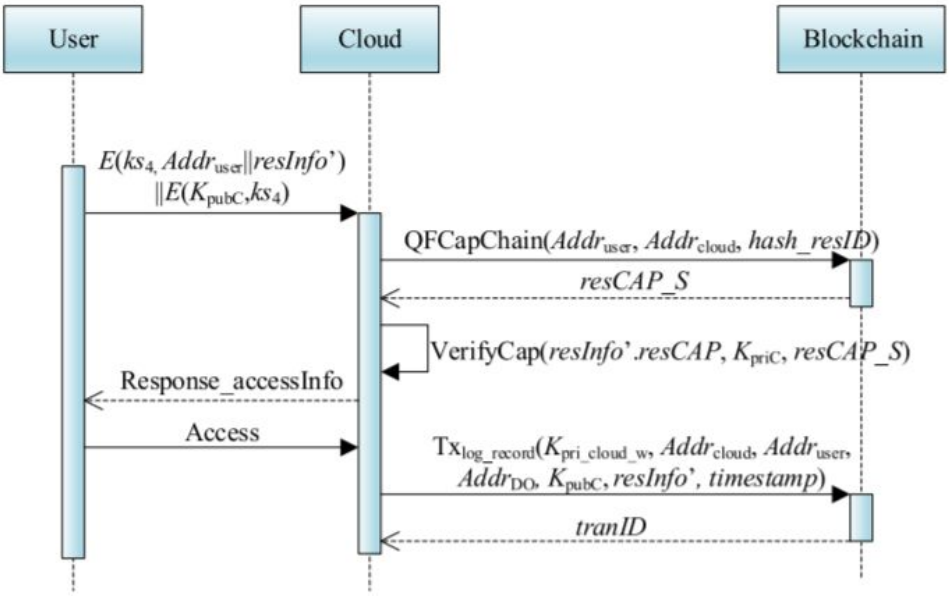
a. DO mengunggah data ke *cloud* yang berisi konten dan urlnya. (ResUp)

b. Menggunakan *public key* milik DO, *cloud* mengenkripsi informasi dari data dan mengembalikannya ke DO, yang lalu akan di dekripsi untuk mendapat informasi data.

c. Menggunakan suatu algoritma, mengunggah informasi data menuju *blockchain.* Dimana pertama mengkonfigurasi *blockchain* dengan memilih *access node*, lalu membuat identitas unik menggunakan hash, lalu izin akses di enkripsi, mengambil timestamp, dan mengembalikan *transaction ID* yang berisi hasil hash, enkripsi dan timestamp ke DO.

2.2. *Access Control*

Bagian ini menjelaskan ketika pengguna mengakses data pada *cloud*, dan *cloud* menentukan apakah pengguna tersebut memiliki akses data berdasarkan izin yang disimpan di *blockchain.* Jika DU memiliki akses, maka *cloud* akan memberikan datanya dan menyimpan catatan akses di *blockchain.*



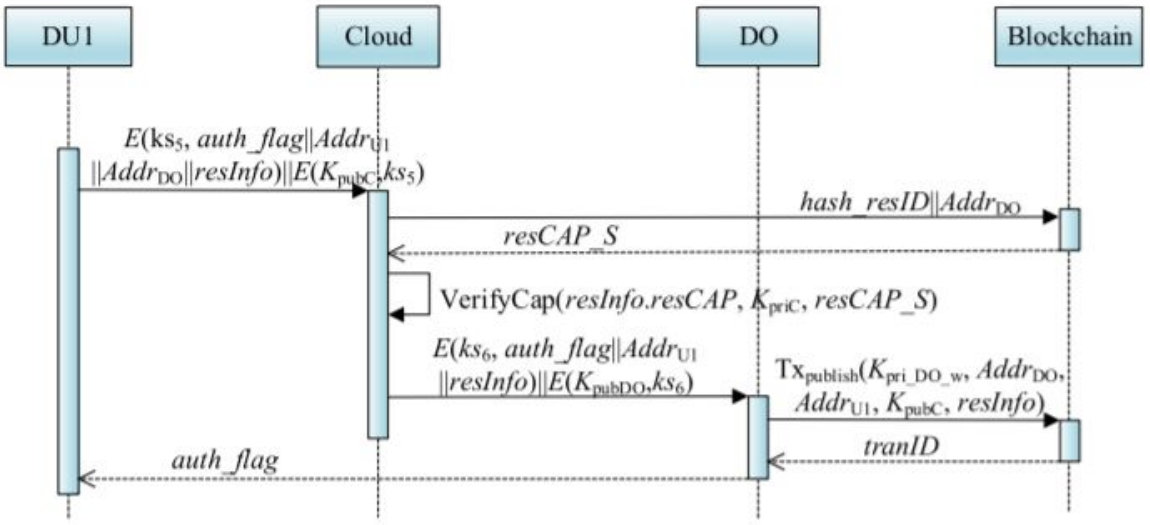
Gambar 6. Workflow *access control*[10]

Pada tahap ini, seperti yang dapat dilihat pada gambar 6 terdiri dari enam langkah yang perlu dilakukan.

a. Pengguna mengirim *request* ke *cloud* yang berisi data apa yang ingin diakses.
b. *Cloud* mendekripsi untuk mendapatkan *address* dari user, data apa yang diakses, lalu dengan fungsi hash, mendapatkan id dari dari data yang ingin diakses. Lalu memanggil fungsi untuk mendapatkan informasi mengenai izin akses dari file tersebut dari *blockchain.*
c. *Blockchain* mengembalikan informasi mengenai izin akses file.
d. *Cloud* melakukan verifikasi, jika pengguna data yang didapat dari hasil dekripsi sesuai dengan yang dikembalikan *blockchain*, maka pengguna dapat mengakses data tersebut.
e. *Cloud* mengembalikan *response* yang bertipe boolean, jika *true* maka pengguna dapat mengakses data tersebut.
f. *Cloud* mengunggah catatan pengaksesan data tersebut ke *blockchain.*

2.3. *Authorization*

Bagian ini menjelaskan ketika DO ingin memberikan akses data kepada DU agar dapat mengakses data yang di unggah oleh DO.



Gambar 7. Workflow *authorization*[10]

Pada tahap ini, seperti yang dapat dilihat pada gambar 7 terdiri dari tujuh langkah yang perlu dilakukan.

a. DU mengirim *request* izin mengakses data ke *cloud*, *cloud* mendekripsi untuk mendapatkan *address* DU, *address* DO, dan informasi data.
b. *Cloud* memanggil fungsi dengan hash dari informasi data, untuk mendapat informasi izin akses data tersebut dari *blockchain.*
c. *Blockchain* mengembalikan informasi izin akses data.
d. *Cloud* memverifikasi apakah benar data tersebut milik DO, dilihat dari *address* DO, dan apakah permintaan akses oleh DU tidak melanggar peraturan akses data yang ditentukan sebelumnya. Jika melanggar salah satu peraturan sebelumnya, maka proses dibatalkan, jika tidak lanjut ke langkah berikutnya.
e. *Cloud* mengirimkan permintaan izin akses dari DU ke DO
f. DO memanggil fungsi untuk mengunggah otorisasi ke *blockchain*, yang menandakan *address* DU dapat mengakses data yang diminta.
g. DO memberikan *response* ke DU bahwa data sudah bisa diakses.

Dengan melihat workflow dari *blockchain access control* diatas, kita dapat mengevaluasi keamanan dari framework ini, framework ini memastikan keamanan data karena transmisi informasi antara DO, DU, *cloud*, dan *blockchain* selalu di enkripsi, informasi mengenai izin mengakses juga di enkripsi dan disimpan pada *blockchain*. Ketika ada DU yang ingin mengakses data baru pun, ia harus meminta dulu ke *cloud* yang kemudian memastikan apakah izin tersebut legal dan pemilik datanya benar, jika iya baru diteruskan ke DO, yang memutuskan apakah DU boleh mengakses atau tidak. Setiap pengguna pun harus memberikan *public key*-nya, sehingga lebih terverifikasi dan terpercaya. Data yang dikirim pun dipastikan sampai ke tangan yang tepat, karena memerlukan *private key* dari penerima untuk mendekripsikan data tersebut.

3. Kesimpulan

Berdasarkan analisis dan pembahasan diatas, *cloud computing* sudah menjadi salah satu teknologi yang paling banyak digunakan pada zaman ini, karena itu keamanan data yang disimpan pada *cloud* merupakan salah satu aspek terpenting. Banyak perusahaan dan industri yang menyimpan data perusahaan mereka pada sebuah layanan *cloud,* jika mudah dibobol, maka data perusahaan tersebut mudah dieksploitasi.

Terdapat berbagai cara untuk meningkatkan keamanan dalam penggunaan *cloud,* salah satunya adalah menggunakan *blockchain access control*, dengan menggunakan *access control*, dan menyimpan *access control* tersebut pada sebuah *blockchain* sehingga tidak dapat diubah oleh pihak luar. Harapannya dengan penerapan teknologi ini, penggunaan *cloud* menjadi lebih aman.

REFERENSI

[1] A. Baldwin, D. Pym, and S. Shiu, ‘‘Enterprise information risk management: Dealing with cloud computing,’’ in Privacy Security for Cloud Computing. London, U.K.: Springer, 2013, pp. 257–291.

[2] P. Mell and T. Grance, ‘‘The NIST definition of cloud computing,’’ Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. Special Publication 800-145, 2011.

[3] S. Choy, B. Wong, G. Simon, and C. Rosenberg, ‘‘The brewing storm in cloud gaming: A measurement study on cloud to end-user latency,’’ in Proc. 11th Annu. Workshop Netw. Syst. Support Games, 2012, p. 2.

[4] S. R. Hassan, J. Bourgeois, V. Sunderam, and X. Li, ‘‘Detection of distributed attacks in hybrid & public cloud networks,’’ in Proc. 8th Int. Conf. Semantics, Knowl. Grids (SKG), 2012, pp. 9–15.

[5] S. Khan et al., "Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis," in IEEE Access, vol. 4, pp. 9800-9820, 2016.

[6] H. Journal, ‘‘Summary of September 2017 healthcare data breaches,’’ HIPAA J., Oct. 2017. [Online]. Available: https://www.hipaajournal.com/september-2017-healthcare- data-breaches/

[7] Cloud Security Alliance, Security Guidance V4.0. Accessed: Apr. 16, 2020. [Online]. Available: https://c-csa.cn/i/file/20171225/ 2017122523220533533.pdf

[8] R. S. Sandhu and P. Samarati, "Access control: principle and practice," in IEEE Communications Magazine, vol. 32, no. 9, pp. 40-48, Sept. 1994.

[9] B. Lucas and R. V. Páez, "Consensus Algorithm for a Private Blockchain," 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 2019, pp. 264-271.

[10] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao and K. Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud," in IEEE Access, vol. 8, pp. 70604-70615, 2020.