Analisis Penggunaan Protokol Kerberos pada Cloud storage untuk Meningkatkan Keamanan Otentikasi

Analysis of The Use of Kerberos protocol on The Cloud Storage to Increase Authentication Security

Ardian Septa Nugraha[1], Fazmah Arif Yulianto[2], Gandeva Bayu Satrya[3]

[1]Prodi S1 Teknik Informatika, Telkom Informatics School, Universitas Telkom
[1]ardian.septa.nugraha@gmail.com , [2]fazmaharif@telkomuniversity.ac.id, [3]gandeva.bayu.s@gmail.com

Abstrak

Penggunaan cloud computing merupakan generasi lanjut (next-generation) dari teknologi informasi pada saat ini. Cloud computing merupakan teknologi berbasiskan Internet, dimana user dapat berbagi sumber daya diantara penyedia jasa layanan berbasiskan cloud. Cloud computing diharuskan membuat kualitas layanan yang tinggi dan ketersediaan (availablity) yang tinggi, sehingga user dapat mengaksesnya dimana pun, kapan pun, dan menggunakan platform apapun. Hal ini membuat pengguna banyak mempercayakan data-datanya kepada penyedia layanan cloud computing. Contohnya cloud storage, yakni media penyimpanan berbasiskan Internet, sehingga user tidak perlu membeli perangkat keras storage (harddisk, flashdisk, SD Card, dll) dan user juga hanya perlu mengunggahnya ke cloud. Namun aspek keamanan menjadi nomor satu untuk urusan layanan cloud ini, karena pada sudut pandang user, layanan cloud ini bisa dipandang sebagai layanan publik dimana semua orang bisa mengakses layanan penyedia jasa cloud ini dan hanya dipisahkan dengan username & password masing-masing. Tujuan dari tugas akhir ini adalah fokus mengimplementasikan protokol Kerberos untuk penjaminan keamanan otentikasi cloud storage dan untuk mengukur Average Service Time, CPU usage, dan Memory usage.

Kata Kunci: Cloud computing, Kerberos, Keamanan, Otentikasi

Abstract

The use of cloud computing is a next-generation (next-generation) of information technology at the moment. Cloud computing is Internet-based technology, where users can share resources among the cloud-based service providers. Cloud computing is required to make a high quality of service and availability is high, so the user can access them anywhere, anytime, and using any platform. This makes a lot of users entrust their data to the cloud computing service providers. For example, cloud storage, the Internet-based storage media, so the user does not need to purchase hardware storage (hard drive, flash, SD Card, etc.) and also the user only needs to upload them to the cloud. However, security is the number one aspect of the cloud services business, because the user standpoint, cloud services can be regarded as a public service in which everyone can access the cloud service provider and only separated by a username and password, respectively. The purpose of this thesis is focusing implement the Kerberos protocol to guarantee the security of the cloud and to measure the Services Average Time, CPU usage, and Memory usage.

Keywords: Cloud computing, Kerberos, Security, Authentication

1. Pendahuluan

Keamanan cloud computing menjadi isu utama saat ini. Menurut Forbes, 69% dari perusahaan enterprise mengeluarkan dana untuk belanja untuk layanan cloud computing, bertambah pada tahun 2013 hingga tahun 2014 [9]. Lalu menurut laporan Akamai, pada kuarter kedua tahun 201, Indonesia menempati urutan pertama di dunia, pada serangan DDoS (Distributed Denial of Service), diikuti oleh China dan Amerika Serikat. Serangan dari Indonesia naik sebanyak 38% jika dibandingkan dengan pada kuarter pertama tahun 2013 dan umumnya serangan dari Indonesia mayoritas menyerang port 80 dan 443, yaitu HTTP dan HTTPS. Maka dari itu perlu dilakukan riset lebih mendalam dengan mengimplementasikan protokol Kerberos dalam layanan cloud computing ini.. Penggunaan protokol Kerberos sendiri dipilih karena memiliki tiga security object, yaitu Ticket, Authenticator, dan Session Key [11]. Diharapkan dengan adanya tugas akhir ini, layanan cloud computing kedepannya bisa aman mulai dari proses otentikasi login, pengiriman data, hingga proses end session atau logout. Tujuan dari Tugas Akhir ini adalah untuk meninjau dua aspek, yaitu aspek efektivitas dan aspek efisiensi. Aspek efektivitas dilihat dari segi keamanan yang menyatakan bahwa protokol Kerberos bisa digunakan sebagai otentikasi tambahan,

apabila terjadi pencurian identitas pengguna cloud storage yang dalam hal ini adalah cookie. Sedangkan aspek efisiensi diukur berdasarkan parameter Average Service Time, CPU usage, dan Memory usage.

2. Dasar Teori

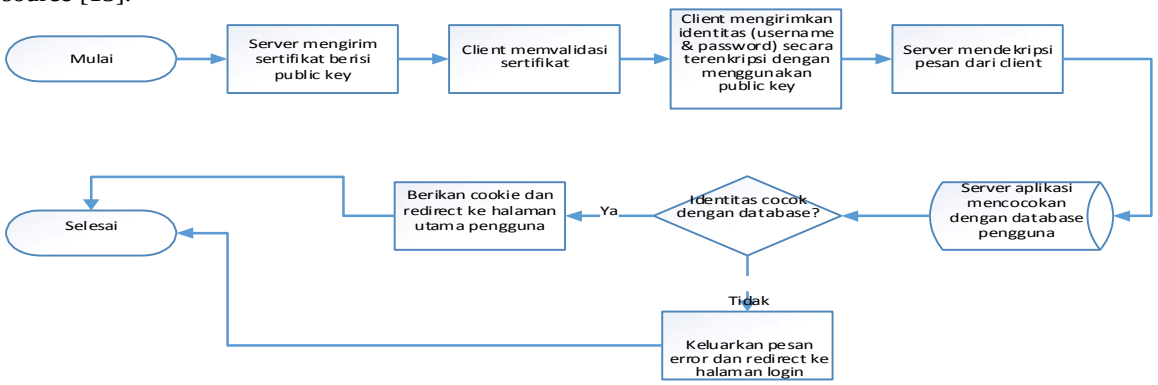
2.1 Cloud Computing

Cloud computing mengacu kepada perangkat keras, sistem perangkat lunak, dan aplikasi yang ditujukan sebagai layanan yang berbasiskan Internet. Ketika sebuah cloud dibuat tersedia dalam bentuk pay-as-you-go kepada publik umum, maka kita menyebutnya sebagai public cloud. Bentuk private cloud juga digunakan ketika infrastruktur cloud dioperasikan hanya oleh untuk sebuah bisnis atau organisasi. Sebuah komposisi dari dua tipe (privat dan publik) disebut sebagai hybrid cloud, dimana sebuah layanan cloud privat dapat menangani layanan yang memiliki availibility tinggi dengan menaikkan skala sistemnya dengan menetapkan resources eksternal dari sebuah public cloud ketika ada perubahan secara cepat dari workload atau kerusakan perangkat keras.
Secara umum, penyedia layanan cloud membagi ke dalam tiga kategori, yaitu :
1. Infrastruktur sebagai layanan / Infrastructure as a Service (IaaS) : menawarkan akses berbasis web untuk penyimpanan dan daya komputasi. Konsumen tidak perlu mengelola atau mengendalikan infrastruktur awan yang mendasari tetapi memiliki kontrol atas sistem operasi , penyimpanan, dan disebarkan aplikasi.
2. Platform sebagai layanan / Platform as a Service (PaaS) : memberikan pengembang alat untuk membangun dan host web aplikasi (misalnya Google Cloud Platform).
3. Software sebagai layanan / Software as a Service (SaaS): aplikasi yang dapat diakses dari berbagai klien perangkat melalui antarmuka klien tipis seperti browser web.

Selanjutnya, cloud computing menawarkan banyak keuntungan untuk vendor, seperti infrastruktur mudah dikelola karena pusat data memiliki hardware homogen dan perangkat lunak sistem. Selain itu, mereka berada di bawah kendali tunggal, entitas yang berpengetahuan (knowledgeable) [3].

2.2 OwnCloud

OwnCloud adalah layanan cloud computing yang termasuk dalam kategori IaaS yang dalam hal ini menyediakan layanan file storage. OwnCloud memberikan akses secara universal melalui antar muka web atau WebDAV. Lalu menyediakan juga platform untuk memudahkan melihat dan sinkronisasi kontak, kalender, dan bookmark di semua perangkat dan memungkinkan untuk melakukan pengeditan secara langsung melalui web. Untuk instalasi memiliki persyaratan server minimal, tidak perlu izin khusus dan cepat. OwnCloud dapat diperpanjang melalui API yang powerful untuk aplikasi dan plugin [13].
OwnCloud dimulai oleh seorang keynote yaitu Frank Karlitschek pada Camp KDE'10 dimana dia berbicara tentang kebutuhan dari layanan komputasi awan yang dapat dikendalikan oleh penggunanya secara gratis dan open source [13].

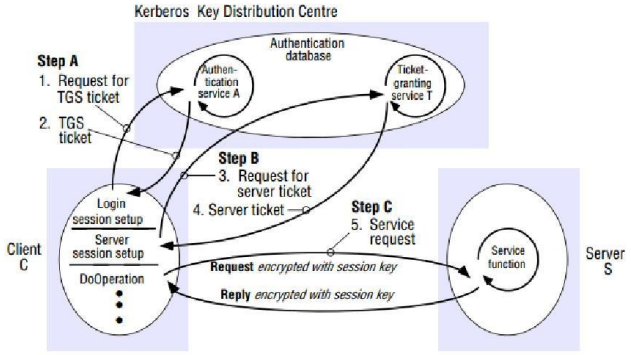


Gambar 1 Proses otentikasi dengan menggunakan HTTPS pada OwnCloud

OwnCloud dibuat untuk menutupi kekurangan yang ada dalam penyedia cloud storage saat ini seperti Dropbox, Google Drive, Swift, dan lain-lain. Kekurangan yang ada penyedia cloud storage diatas adalah tidak adanya kontrol dari bagian IT jika cloud storage digunakan pada skala perusahaan, pengelolaan tidak terlihat langsung, kebijakan kerahasiaan data bergantung pada negara dimana cloud provider tersebut berada [14]. Pada gambar 1 adalah gambaran umum proses otentikasi bawaan OwnCloud dengan menggunakan HTTPS.

2.3 Protokol Kerberos

Kerberos dikembangkan di MIT pada tahun 1980 [Steiner et al. 1988] untuk menyediakan berbagai otentikasi dan keamanan fasilitas untuk digunakan dalam jaringan komputer kampus di MIT dan intranet lainnya. Hal ini telah mengalami beberapa revisi dan perangkat tambahan dalam terang pengalaman dan umpan balik dari organisasi pengguna. Kerberos versi 5 [Neuman dan Ts'o 1994], yang kami jelaskan di sini, adalah standar Internet (lihat RFC 4120 [Neuman et al. 2005]) dan digunakan oleh banyak perusahaan dan organisasi. Source code untuk implementasi Kerberos tersedia fromMIT [web.mit.edu], melainkan termasuk dalam OSF Distributed Computing Environment (DCE) [OSF 1997] dan sebagai default layanan otentikasi di Microsoft Windows [www.microsoft.com]. Ekstensi dimasukkan untuk menggabungkan penggunaan certificates public key untuk awal otentikasi principal (Langkah A pada Gambar 1) [Neuman et al.1999] [2].



Gambar 2 Proses otentikas protokol Kerberos [2]

Protokol Kerberos memiliki delapan unsur dalam penggunaannya yaitu :

1. Principal : setiap pengguna, komputer, dan layanan yang diberikan oleh server harus didefinisikan sebagai Kerberos Prinsipal.
2. Instances : digunakan untuk layanan principal dan principal administratif khusus.
3. Realms : alam unik kontrol yang disediakan oleh instalasi Kerberos. Anggap saja sebagai domain atau kelompok host dan pengguna milik. Konvensi menentukan alam harus dalam huruf besar. Secara default, ubuntu akan menggunakan domain DNS dikonversi ke huruf besar (EXAMPLE.COM) sebagai kerajaan.
4. Key Distribution Center : (KDC) terdiri dari tiga bagian, database dari semua principal, server otentikasi, dan server tiket granting. Untuk setiap realm harus ada setidaknya satu KDC.
5. Ticket Granting Ticket : dikeluarkan oleh Authentication Server (AS), Ticket Granting Ticket (TGT) dienkripsi menggunakan kata kunci pengguna yang hanya diketahui pengguna dan KDC.
6. Ticket Granting Server : (TGS) mengeluarkan tiket layanan kepada klien atas permintaan.
7. Tickets : mengkonfirmasi identitas kedua principal. Salah satu principal menjadi pengguna dan lainnya adalah layanan yang diminta oleh pengguna. Ticket menetapkan kunci enkripsi yang digunakan untuk komunikasi yang aman selama sesi dikonfirmasi.
8. Keytab Files : adalah file diekstrak dari database principal KDC dan mengandung kunci enkripsi untuk layanan atau host.

Untuk menempatkan delapan unsur Kerberos, sebuah realm paling tidak memiliki sebuah KDC, disarankan lebih dari satu untuk keperluan reduncancy, yang berisi sebuah database dari principal. Ketika pengguna login ke sebuah workstation yang telah dikonfigurasi dengan mekanisme otentikasi Kerberos, KDC akan mengeluarkan sebuah Ticket Granting Ticket (TGT). Jika pengguna memberikan mandat (credential) yang sesuai, maka pengguna terotentikasi dan dapat meminta tiket untuk layanan yang kerberized dari Ticket Granting Server (TGS). Tiket layanan memperbolehkan pengguna untuk mengotentikasi layanan tanpa harus memasukan username dan password. [15]

2.4 Paramater Pengujian

Parameter uji yang dilakukan dalam penelitian ini ada tiga buah yaitu Average Service Time, CPU usage dan Memory usage.

2.4.1 Efektivitas

Dalam Tugas Akhir ini yang dimaksud efektivitas adalah penggunaan protokol Kerberos dapat menangani masalah yang disebutkan dalam bab 1.2. Artinya bahwa kegunaan protokol tambahan akan berlaku efektif.

2.4.2 Efisiensi

2.4.2.1 Average Service Time

Average Service Time adalah waktu layanan dari pertama client memberikan request login sampai server membalas request dari client tersebut dan dinyatakan logged-in oleh server. Dirumuskan sebagai berikut :

$$= \frac{(\quad)}{} \quad (1)$$

Dalam Tugas Akhir ini jumlah request dari seratus pengguna dalam waktu kurang dari satu menit dan diukur dari sisi pengguna dalam bentuk satuan milisecond (ms).

2.4.2.2 CPU Usage

CPU (Central Processing Unit) usage atau CPU Time adalah metode untuk mengukur kuantitas penggunaan CPU, khususnya metode untuk mengukur kuantitas penggunaan CPU yang mampu mendapatkan jumlah kredibel penggunaan CPU tanpa mengubah algoritma dalam rangka untuk beradaptasi dengan sistem operasi, misalnya, MS-windows System, atau memerlukan kode yang rumit. Metode ini menggunakan berbagai algoritma yang disediakan oleh sistem operasi pada nama registri menyimpan kuantitas penggunaan CPU di dalam sistem. Dengan demikian penemuan ini dapat mengukur kuantitas penggunaan CPU dengan mudah tanpa menurunkan kinerja dari sistem operasi [16].

$$\text{Idle Ticks} = \text{Sum (across sampling interval) [Second Timer Read} - \text{Initial Timer Read]} \quad (2)$$

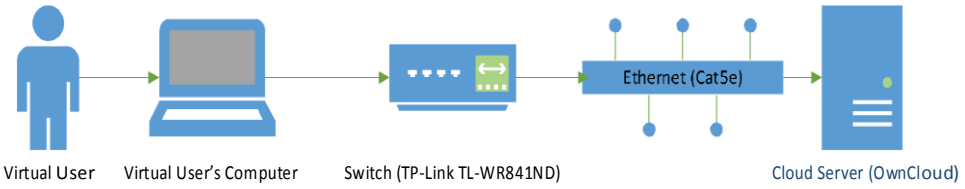
$$\text{CPU Idle}(\%) = \text{Idle Ticks} \times \frac{()}{()} \times 100\% \quad (3)$$

Pada persamaan 2.3 dapat dilihat CPU idle dalam bentuk satuan persen, maka yang akan dihitung pada Tugas Akhir ini adalah penggunaan CPU yang merupakan hasil pengurangan dari 100% dikurangi dengan CPU idle dalam bentuk satuan persen diukur dari sisi server.

2.4.2.3 Memory Usage

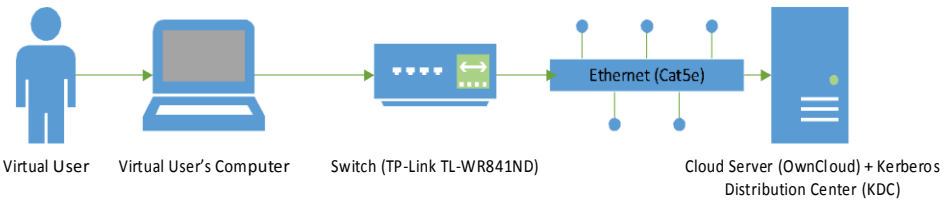
Memory usage adalah pengunaan memori yang disediakan oleh RAM (Random Access Memory). Dalam Tugas Akhir ini yang dimaksudkan Memory usage adalah penggunaan memori yang diakibatkan oleh penggunaan cloud. Diukur dari sisi server dalam bentuk satuan kilobytes (KB).

3. Gambaran Umum Perangkat Lunak



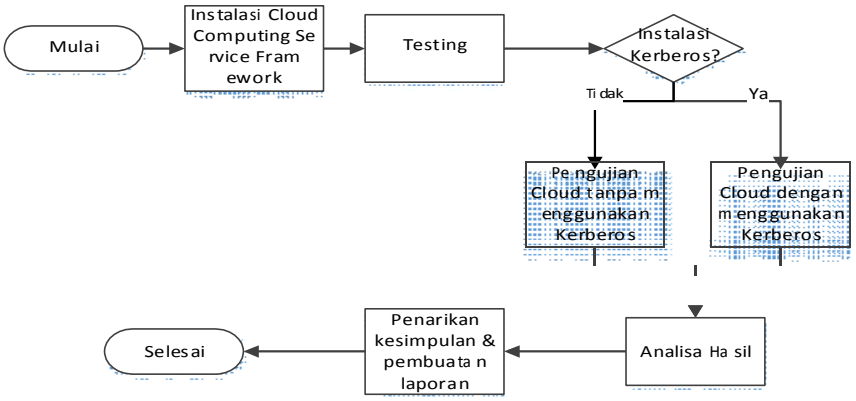
Gambar 3 Arsitektur jaringan pada kondisi awal

Rancangan umum sistem terdiri atas dua arsitektur jaringan yang berbeda. Pada Gambar 3 merupakan arsitektur jaringan pada kondisi awal dimana sebelum terpasang Kerberos Distribution Center (KDC).



Gambar 4 Arsitektur jaringan ketika sudah implementasi Kerberos

Pada Gambar 4, terdapat diagram alir atau flowchart yang menggambarkan langkah-langkah untuk melakukan penelitian ini yang ditujukan untuk penyusunan tugas akhir.



Gambar 1 Diagram alir langkah-langkah penelitian tugas akhir

4. Skenario Pengujian

Dalam perancangan pengujian ini terdapat empat perancangan uji yang akan diterapkan pada penelitian ini. Skenario uji akan dikategorikan ke dalam dua, yakni untuk meninjau efektivitas dan mengukur efisiensi. Skenario ujinya adalah sebagai berikut :

4.1 Skenario 1

Pada skenario uji satu ditujukan untuk meninjau efektivitas keamanan bawaan pada cloud storage OwnCloud. Dimana terdapat suatu kejadian pencurian cookie milik pengguna OwnCloud yang diambil oleh penyerang. Lalu penyerang menggunakan cookie tersebut untuk mengakses layanan cloud storage OwnCloud melalui web browser.

4.2 Skenario 2

Skenario pengujian ini ditujukan untuk mengukur performasi atau efiesiensi pada satu client yang melakukan proses login. Parameter Average Service Time, CPU usage & Memory usage diambil dari data-data yang direkam pada server dan client, sesuai dengan aturan pada bab 2.4. Dilakukan testing terhadap sistem cloud storage OwnCloud dengan menggunakan virtual user sebanyak seribu user dalam waktu lima detik secara bersamaan.

4.3 Skenario 3

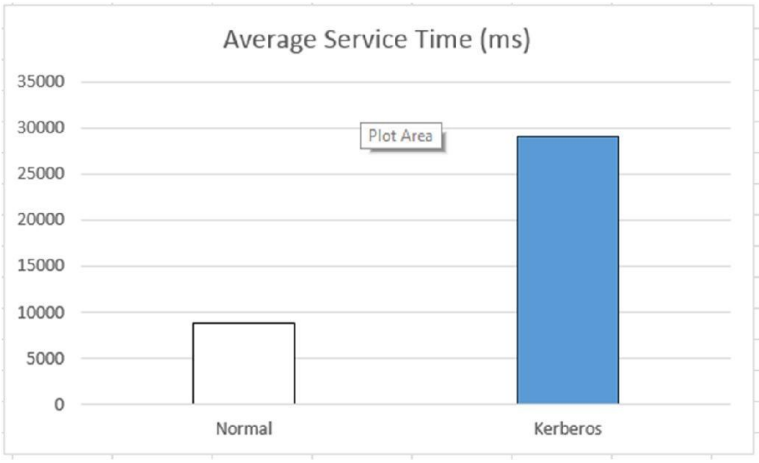
Pada skenario uji satu ditujukan untuk meninjau efektivitas keamanan bawaan pada cloud storage OwnCloud. Dimana terdapat suatu kejadian pencurian cookie milik pengguna OwnCloud yang diambil oleh penyerang. Lalu penyerang menggunakan cookie tersebut untuk mengakses layanan cloud storage OwnCloud melalui web browser. Pengujian ini akan membuktikan bahwa setelah penggunaan protokol Kerberos, maka penyerang yang memiliki cookie tidak akan bisa lagi mengakses layanan cloud storage OwnCloud.

4.4 Skenario 4

Skenario pengujian ini ditujukan untuk mengukur performasi atau efiesiensi pada satu client yang melakukan proses login. Setelah penggunaan protokol Kerberos pada server OwnCloud dilakukan pengukuran terhadap parameter Average Service Time, CPU usage & Memory usage diambil dari data-data yang direkam pada server dan client, sesuai dengan aturan pada bab 2.4. Dilakukan testing terhadap sistem cloud storage OwnCloud dengan menggunakan virtual user sebanyak seribu user dalam waktu lima detik secara bersamaan.

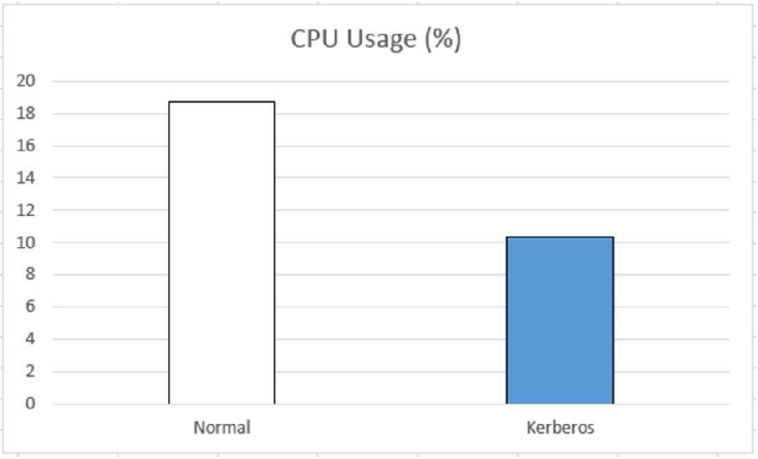
4.5 Analisis Hasil Pengujian

Hasil data pengujian pada skenario 2 dan skenario 4 akan dibandingkan untuk melihat secara jelas perbandingan antar pengujian.



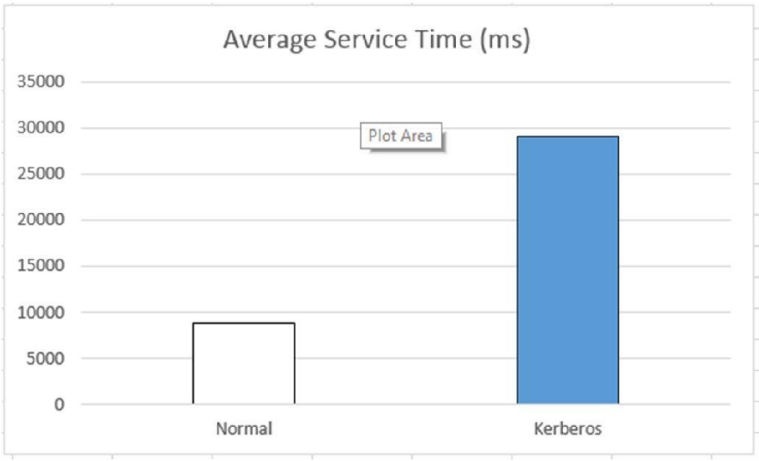
Gambar 7 Grafik perbandingan Average Service Time

Pada gambar 7, grafik menunjukkan bahwa Average Service Time atau waktu layanan rata-rata yang diberikan oleh OwnCloud setelah penggunaan protokol Kerberos jauh lebih lama jika dibandingkan dengan sebelum menggunakan protokol Kerberos. Pada kondisi awal menunjukkan nilai rata-rata waktu layanan sebesar 8906,16 milisecond dan kondisi setelah penggunaan protokol Kerberos menjadi 29015,66 milisecond. Average Service Time setelah penggunaan protokol Kerberos naik menjadi lebih dari tiga kali lipat dibandingan kondisi awal. Hal ini dikarenakan penggunaan protokol Kerberos yang menambahkan service dan proses tambahan pada sistem operasi server untuk otentikasi.



Gambar 8 Grafik perbandingan CPU usage

Pada gambar 8 menunjukkan grafik perbandingan penggunaan CPU atau CPU usage. Dari hasil sepuluh kali pengujian pada skenario 2 dan skenario 4 menunjukkan bahwa penggunaan CPU pada kondisi layanan OwnCloud sebelum penggunaan protokol Kerberos lebih tinggi daripada setelah penggunaan protokol Kerberos. Nilai rata-rata pada kondisi awal sebesar 18,7085% sedangkan setelah menggunakan protokol Kerberos menjadi sebesar 10,3478%. Setelah penggunaan protokol Kerberos, penggunaan CPU turun menjadi setengah jika dibandingkan dengan kondisi awal. Hal ini dikarenakan ketika penggunaan protokol Kerberos untuk proses otentikasi dikerjakan secara serial oleh sistem operasi server. Ketika pengguna ingin melakukan otentikasi pada layanan cloud storage maka ia diharuskan untuk melakukan otentikasi melalui protokol Kerberos terlebih dahulu, setelah itu dapat melakukan otentikasi melalui layanan OwnCloud



Gambar 9 Grafik perbandingan Memory usage

Pada gambar 9 menunjukkan grafik perbandingan penggunaan memori atau memory usage. Dari hasil sepuluh kali pengujian pada skenario 2 dan skenario 4 menunjukkan bahwa penggunaan memori pada kondisi layanan OwnCloud sebelum penggunaan protokol Kerberos lebih rendah daripada setelah penggunaan protokol Kerberos. Nilai rata-rata pada kondisi awal sebesar 18,7085% sedangkan setelah menggunakan protokol Kerberos menjadi sebesar 10,3478%. Setelah penggunaan protokol Kerberos, penggunaan CPU turun menjadi setengah jika dibandingkan dengan kondisi awal. Hal ini disebabkan karena sistem operasi server menjalankan service tambahan yaitu protokol Kerberos yang tentunya membutuhkan ruang dalam memori.

5. Kesimpulan

Berdasarkan hasil pengujian dan analisis penggunaan protokol Kerberos pada layanan cloud computing OwnCloud, dapat disimpulkan sebagai berikut :

1. Masalah pencurian cookie dapat diatasi dengan salah satunya menggunakan protokol Kerberos melalui modul Apache mod_auth_kerb.
2. Average Service Time atau waktu layanan rata-rata dengan menggunakan protokol Kerberos jauh lebih lama jika dibandingkan dengan tidak menggunakan.
3. Penggunaan CPU atau CPU usage pada komputer server lebih rendah jika menggunakan protokol Kerberos.
4. Penggunaan memori atau memory usage pada komputer server jauh lebih besar jika menggunakan protokol Kerberos.

6.Saran

Saran untuk pengembangan Tugas Akhir selanjutnya sebagai berikut :

1. Komputer server Kerberos Distribution Center diletakkan terpisah dengan server layanan OwnCloud.
2. Penggunaan protokol Kerberos sebaiknya menggunakan sistem tiket agar pengguna dapat mengakses berbagai macam layanan melalui mekanisme otentikasi Single Sign-On yang sebenarnya.

Daftar Pustaka

[1]. Coulouris, George. et al., 2012, Distributed Systems : Fifth Edition, Boston, Addison-Wesley.
[2]. Antonopoulos, N. , and L. Gillam (editor), 2010, Cloud Computing :Principles,Systems and Applications, Springer-Verlag London Limited.
[3]. Cole, Dr. Eric, et al, 2005, Network Security Bible, Indianapolis, Wiley Publishing Inc.
[4]. Peterson, Larry L., Bruce S. Davie, 2007, Computer Networks A System Approach, San Francisco, Morgan Kaufmann Publisher.
[5]. Mao, Wenbo, 2003, Modern Cryptography : Theory and Practice, New Jersey, Prentice Hall PTR.
[6]. Shaikh, Farhan Bashir, Sajjad Haider, 2011, Security Threats in Cloud Computing, Abu Dhabi, 6th International Conference on Internet Technology and Secured Transactions, diunduh dari ieeexplore.ieee.org pada 30 Oktober 2013.
[7]. Kulkarni, G.; Gambhir, J.; Patil, T.; Dongare, A., A security aspects in cloud computing, Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on , vol., no., pp.547,550, 22-24 June 2012.

[8]. Subashini, S., V. Kavitha, 2011, A Survey on Security Issues in Service Delivery Models of Cloud Computing, diunduh dari sciencedirect.com pada 30 Oktober 2013.
[9]. Colombus, Louis, http://www.forbes.com/sites/louiscolumbus/2013/09/04/predicting-enterprise-cloud-computing-growth/, Forbes. November 2013.
[10]. Hojabri, K.V. Rao, Innovation in cloud computing : Implementation of Kerberos version5 in cloud computing in order to enhance the security issues. Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.452,456, 21-22 Feb. 2013.
[11]. Linn, J., Juni 1996, The Kerberos Version 5 GSS-API Mechanism, IETF, RFC 1964, diakses 1 Desember 2013.
[12]. Kurose, James F., Keith W. Ross, 2009, Computer Networking A Top-Down Approach Fifth Edition, Addison-Wesley.
[13]. OwnCloud Inc. http://owncloud.org/about/, diakses 9 Juni 2014.
[14]. OwnCloud Architecture Overview, OwnCloud Inc.
[15]. Ubuntu. https://help.ubuntu.com/14.04/serverguide/kerberos.htmldiakses9Juni2014.
[16]. Sang Ho Lee, Jang Keun Oh. US Patent No. US6804630 B2. http://www.google.com/patents/US6804630, diakses 9 Juni 2014.