Jurnal SimanteC

Vol. 4, No. 1 Juni 2014 ISSN 2088-2130

PENERAPAN AES UNTUK OTENTIKASI AKSES CLOUD COMPUTING

Imamah[1)], Arif Djunaidy[2)], Muchammad Husni[3)]

[1,2,3)]Teknik Informatika, Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
email : [1)]i2munix@gmail.com

ABSTRAK

Otentikasi merupakan salah satu bagian penting dari proses pengamanan data, yang bertujuan untuk membatasi tingkatan hak akses pengguna. Cloud Computing merupakan model komputasi yang mengalihkan sumber daya seperti daya komputasi, penyimpanan, jaringan dan perangkat lunak menjadi layanan di internet. Kehilangan data akibat kebocoran hak akses atau mekanisme otentikasi yang lemah diduga sebagai resiko dan ancaman paling rentan pada cloud computing. Penelitian ini mengajukan sebuah metode pengamanan untuk otentikasi hak akses menggunakan AES (Advance Encryption Standard). Password yang merupakan metode pengamanan hak akses akan dienkripsi menggunakan AES kemudian diuji coba dalam sebuah server PC yang telah diintalasi eyeOS (server private cloud). Hasil percobaan dengan menambahkan enkripsi AES untuk enkripsi password menggunakan data uji Rockyou menghasilkan skor 0.97 lebih kuat dibandingkan metode MD5 dengan selisih waktu komputasi 0.0004 mikro-detik lebih lambat. Hasil percobaan dengan menggunakan data uji MySpace menghasilkan skor 1.24 lebih kuat dibandingkan dengan metode MD5 dengan selisih waktu komputasi 0,0011 mikro-detik lebih lambat. Berdasarkan hasil penelitian menunjukkan bahwa sistem otentikasi yang dikembangkan dalam penelitian ini layak untuk diaplikasikan dalam lingkungan cloud computing.

Kata Kunci: AES (*advanced encryption standard)*, Biometrik tanda tangan *offline* ,*Cloud computing*, manajemen otentikasi,.
.

ABSTRACT

Authentication is one important part of the process of data security, which aims to restrict user access levels. Cloud Computing is a computational model that diverts resources such as computing power, storage, networking and software as a service on the internet. Data loss due to leakage permissions or weak authentication mechanism thought to be most vulnerable to the risks and threats to cloud computing. This study proposed a method for authentication security permissions using AES (Advanced Encryption Standard). Password is a method for securing rights access will be encrypted using the AES then tested in a server PC that has installation with eyeOS (private cloud server) . The experimental results by adding AES encryption for encrypting passwords using RockYou generate test data score 0.97 is stronger than MD5 method with a computing time 0.0004 microseconds slower . The experimental results using MySpace generate test data resulted in a score 1.24 stronger than MD5 method with computing time 0.0011 microseconds slower . Based on the results of the study indicate that the authentication system developed in this study feasible to be applied in a cloud computing environment .

Keyword: *AES (advanced encryption standard), Biometric offline signature, Cloud computing, management authentication.*

PENDAHULUAN

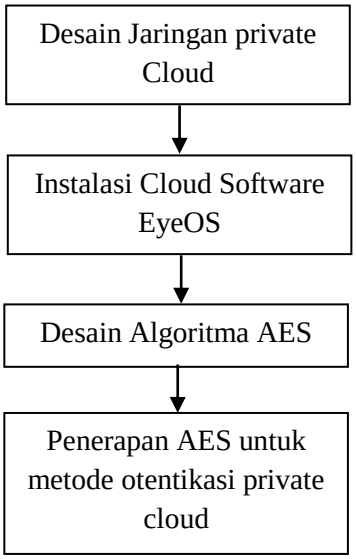
Cloud Computing merupakan model komputasi yang mengalihkan sumber daya seperti daya komputasi, penyimpanan, jaringan dan perangkat lunak menjadi layanan di internet. Cloud computing membagi layanannya menjadi tiga yaitu, SAAS (*software as a service*), PAAS (*platform as a service*), IAAS (*Infrastructure as a service*)[1]. Berdasarkan survey dari PEW *Research Institute*, hampir 69% penduduk amerika menggunakan layanan dari *cloud computing*. Perusahaan besar di India seperti Ashok Ley-Land, Tata Elxi, Bharti, Infosys, Asian Paints, Maruti dan kurang lebih 1500 perusahaan lainnya juga telah memanfaatkan layanan *cloud computing* [2]. Bertambahnya peminat teknologi cloud disebabkan beberapa keuntungan, diantaranya adalah :

a. Lebih efisien karena menggunakan anggaran yang rendah untuk sumber daya.
b. Membuat operasional dan manajemen lebih mudah, karena sistem pribadi atau sistem perusahaan yang terkoneksi dalam suatu cloud dapat dimonitor dan diatur dengan mudah.
c. Mudah dalam hal skalabilitas.

Namun akhir-akhir ini, banyak berita, jurnal ataupun media publikasi lainnya yang memperingatkan tentang resiko dan ancaman keamanan dari cloud computing. Kehilangan data akibat kebocoran hak akses atau mekanisme otentikasi yang lemah diduga sebagai resiko dan ancaman paling rentan pada *cloud computing* ([1][3][4]). Manajemen antar-muka merupakan fitur yang harus ada pada cloud computing, dengan tujuan untuk memudahkan pengguna mengakses layanan yang tersedia baginya. Akses yang tidak terotorisasi pada manajemen antar-muka merupakan salah satu celah kebocoran pada *cloud computing* [3][5]. Diharapkan dengan penelitian ini, dapat ditemukan algoritma kriptografi yang paling tepat untuk enkripsi password sehingga salah satu masalah keamanan otentikasi hak akses pada cloud computing dapat teratasi.

METODE OTENTIKASI PADA PRIVATE CLOUD DAN ENKRIPSI AES

Tahapan proses dalam penelitian ini ditunjukkan pada gambar 1.



Gambar 1.Diagram alir sistem.

Manajemen Otentikasi

Manajemen otentikasi digunakan untuk membatasi tingkatan akses pada suatu sistem. Otentikasi melibatkan proses identifikasi. Identifikasi merupakan proses untuk menunjukkan identitas pengguna pada sistem, sedangkan otentikasi adalah proses validasi terhadap keabsahan pengguna. Otentikasi biasanya berupa sesuatu yang diketahui (contoh: *password*), sesuatu yang dimiliki (contoh: *smart card*), dan sesuatu yang melekat pada pengguna (contoh: biometrik)[6]. Password bersifat sangat rahasia dan umumnya digunakan untuk otentikasi. Dalam penggunaaannya *password* seringkali dipadukan dengan *username* dan

digunakan untuk melindungi data, system dan jaringan. *Password* terdiri dari beberapa macam, salah satunya adalah PIN. PIN terdiri dari 4-6 digit angka, biasanya digunakan untuk otentikasi ATM (Anjungan Tunai Mandiri)[7]. Pada umumnya password dienkripsi dengan menggunakan algoritma kriptografi terlebih dahulu sebelum disimpan pada *database* [8]. Algoritma kriptografi yang populer adalah *one way function*, seperti MD5 atau SHA-1. Pada penelitian ini akan digunakan algortima kriptografi AES untuk mengetahui tingkat keamanan dibandingkan dengan algoritma MD5..

Private Cloud

Private cloud dibangun, dioperasikan, dan dikelola oleh sebuah organisasi untuk keperluan internal. *Private cloud* banyak digunakan oleh masyarakat umum, perusahaan swasta, hingga organisasi pemerintah di seluruh dunia untuk mengeksploitasi manfaat *cloud* seperti fleksibilitas, pengurangan biaya, kecepatan dan sebagainya. Pada penelitian ini *private cloud* dibangun dengan menggunakan sistem operasi Ubuntu 12.04 serta perangkat lunak eyeOS. eyeOS merupakan cloud computing yang menyediakan layanan *software as a service* (SAAS). Hal ini berarti bahwa layanan yang akan disediakan oleh *private cloud* berbasis aplikasi. Perbedaan aplikasi pada layanan *cloud* dengan aplikasi pada umumnya adalah pada proses instalasinya. Layanan *cloud* menyediakan aplikasi tanpa perlu proses instalasi, dan dapat digunakan secara bersama-sama. Layanan cloud pada *private cloud* yang akan dibangun menyerupai layanan yang disediakan oleh server google, yaitu googledoc. Aplikasi pengolah dokumen, presentasi dan spreadsheet atau lembar kerja mirip seperti layanan googledoc juga disediakan oleh eyeOS. eyeOS pada penelitian ini dijalankan pada satu komputer server. Untuk membangun server private cloud ini ada beberapa komponen yang perlu diperhatikan untuk kebutuhan perangkat kerasnya. Spesifikasi minimum yang diperlukan untuk membangun private *Cloud Server* adalah sebagai berikut:

a Processor : Intel EMT64 atau AMD Phenom II X4945.
b Memory : 512 MB DDR3.
c Harddisk : 500GB SATA.
d Operating System : Ubuntu 12.04
e Cloud Software : eyeOS

Langkah awal yang harus dilakukan adalah konfigurasi jaringan, server cloud pada penelitian adalah AMD 64 bit yang memiliki 2 buah NIC (Network Interface Card). Namun karena LAN yang digunakan dalam penelitian ini telah dibangun atau memanfaatkan LAN di lingkungan Fakultas Teknik Informatika ITS, sehingga hanya satu NIC yang dibutuhkan. Alamat LAN pada penelitian adalah 10.151.13.0/24. Sedangkan Ip Address yang digunakan sebagai server private cloud adalah 10.151.13.101.

Enkripsi AES

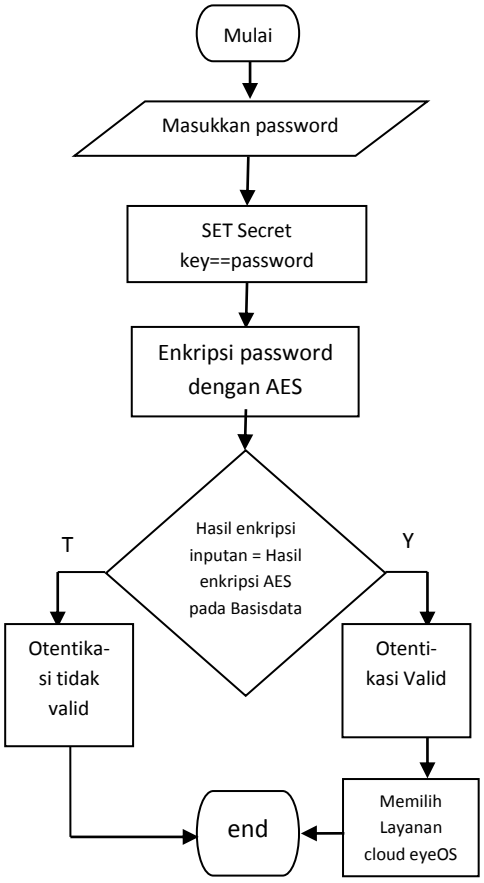
AES adalah Algoritma kriptografi bernama Rijndael yang didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia. Mereka merupakan pemenang kontes algoritma kriptografi pengganti DES yang diadakan oleh NIST (*National Institutes of Standards and Technology*) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan *Advanced Encryption Standard* (AES).
Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002. Pada 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik.
AES ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaimana block cipher pada umumnya. Jenis AES terbagi 3, yaitu :

a AES-128
b AES-192
c AES-256

Pengelompokkan jenis AES ini adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tiap-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya round yang dipakai. AES-128 menggunakan 10 round, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 round. AES memiliki ukuran block yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. AES tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan.ES merupakan algoritma kriptografi yang didesain untuk beroperasi pada blok pesan 128 bit menggunakan tiga variasi blok kunci dengan panjang 128 bit, 192 bit, atau 256 bit. Khusus untuk penelitian ini, pengkajian akan dibatasi pada blok pesan 128 bit dengan ukuran blok kunci 128 bit. Empat proses utama algoritma terdiri atas satu proses permutasi (ShiftRows) dan tiga proses subtitusi (SubBytes, MixColumns, dan AddRoundKey).

Struktur algoritma secara umum cukup sederhana, dengan proses enkripsi maupun dekripsi diawali proses *AddRoundKey*, diikuti sembilan round yang masing-masing tersusun atas empat proses, dan diakhiri round kesepuluh yang terdiri atas tiga proses. Proses *AddRoundKey* membentuk Vernam cipher, sedangkan tiga proses lainnya menciptakan proses pengacakan dan penggabungan secara tak linear [9].

Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi *ciphertext*. *secret key* dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES ini. Pada penelitian ini, secret key dibuat berdasarkan password yang telah diinputkan oleh pengguna, sehingga alur dari sistem enkripsi digambarkan pada gambar 2.



Gambar 2. Rancangan metode otentikasi

HASIL UJI COBA DAN PEMBAHASAN

Setelah tahapan pembuatan aplikasi atau implementasi algoritma selesai, maka tahapan penelitian dilanjutkan dengan melakukan suatu uji coba terhadap aplikasi yang telah dibuat untuk kemudian melakukan analisis dari

hasil uji coba yang telah dilakukan tersebut.

Data Uji

Data yang digunakan dalam penelitian ini adalah data yang diambil dari RockYou dan MySpace.

Tabel 1.Data Uji Rockyou dan Myspace

RockYou	**123456**	**12345**	**123456789**
MySpace	password1	abc123	fuckyou

Skenario Uji Coba

Pada penelitian ini, uji coba dilakukan dengan membandingkan password yang telah dienkripsi MD5 dengan password yang dienkripsi AES. Tujuan dari penelitian ini untuk mengetahui waktu komputasi rata-rata dan skor dari kedua metode. Selanjutnya akan dianalisis pengaruh metode terhadap waktu komputasi dan tingkat kekuatan passwor yang telah dienkripsi.

Hasil Uji Coba

Berdasarkan hasil pengujian yang dilakukan terhadap data uji, didapatkan hasil perbandingan waktu komputasi dan perbandingan skor atau tingkat kekuatan password terenkripsi sebagai berikut.

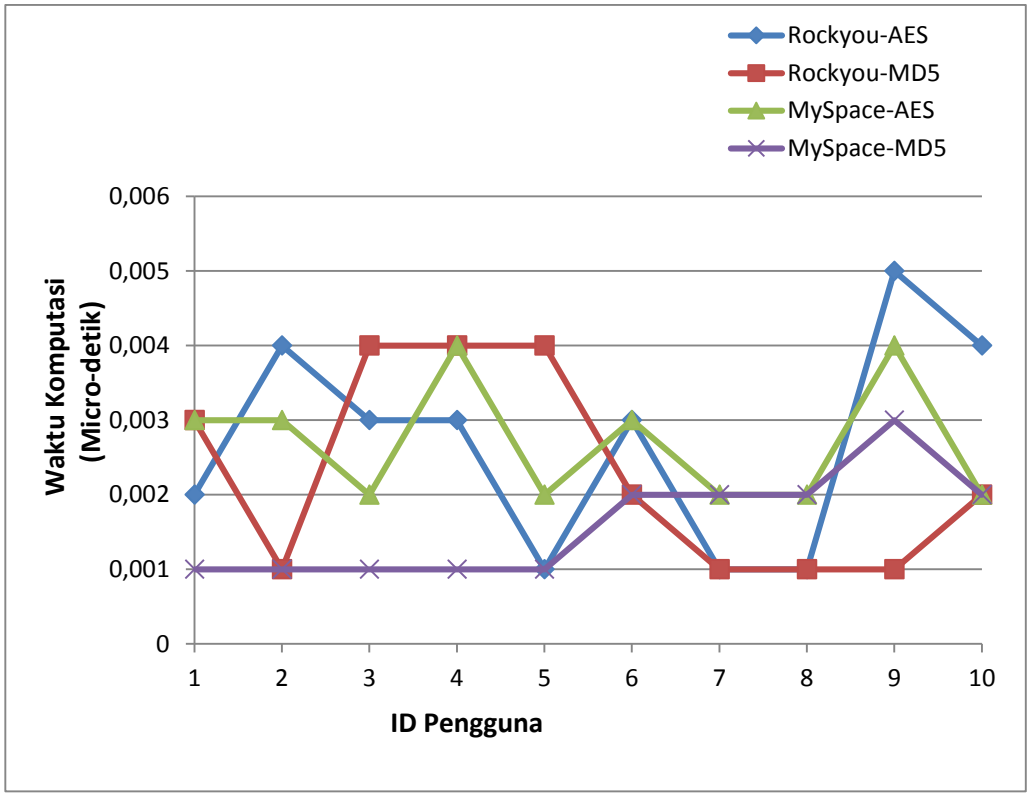
Perbandingan Waktu Kom-putasi

Hasil perbandingan waktu komputasi dengan menggunakan data uji Rockyou dan MySpace ditunjukkan pada tabel 2.

Tabel 2. Hasil perbandingan waktu komputasi data uji rockyou dan myspace dengan MD5 dan AES yang diterapkan pada private cloud menggunakan eyeOS.

ID Pengguna	Rockyou (MD5)	Rockyou (AES)	MySpace (MD5)	MySpace (AES)
1	0.003	0.002	0.001	0.003
2	0.001	0.004	0.001	0.003
3	0.004	0.003	0.001	0.002
4	0.004	0.003	0.001	0.004
5	0.004	0.001	0.001	0.002
6	0.002	0.003	0.002	0.003
7	0.001	0.001	0.002	0.002
8	0.001	0.001	0.002	0.002
9	0.001	0.005	0.003	0.004
10	0.002	0.004	0.002	0.002
Rata-rata	**0.0023**	**0.0027**	**0.0016**	**0.0027**

Berdasarkan hasil pengujian penerapan metode MD5 dan AES pada private cloud yang dibangun menggunakan cloud software eyeOS didapatkan waktu komputasi metode AES saat menggunakan data uji Rockyou 0.0004 kali lebih lambat dibandingkan dengan menggunakan metode MD5. Pada data uji Myspace, metode AES memiliki waktu komputasi 0.0011 kali lebih lambat dibandingkan dengan menggunakan metode MD5. Hasil pengujian digambarkan dengan grafik pada gambar 3. Waktu komputasi yang didapatkan menunjukkan bahwa penerapan AES sebagai algoritma enkripsi dapat dilakukan tanpa berpengaruh pada waktu komputasi dari server cloud.



Gambar 3. Hasil pengujian data uji Rockyou dan MySpace dengan menggunakan AES dan MD5 pada private cloud server menggunakan eyeOS.

Metode MD5 memiliki waktu komputasi yang lebih cepat dibandingkan dengan metode AES. Namun MD5 merupakan algoritma enkripsi yang bersifat *one way*, artinya algoritma ini tidak dapat dideskripsikan kembali. Keahlian pada kriptoanalis terus berkembang, walaupun tidak dapat didekripsi namun MD5 tidak dinilai lebih aman dibandingkan dengan algoritma AES yang menurut National Standard of Information Technology (NIST) merupakan standart enkripsi[7]. Berdasarkan hasil uji coba penerapan AES dan MD5 pada lingkungan private cloud yang dibangun dengan menggunakan eyeOS, didapatkan hasil waktu komputasi dari metode AES sebagai algoritma enkripsi dari password membutuhkan waktu yang tidak lama, sehingga metode ini dapat diterapkan pada lingkungan cloud computing yang membutuhkan kecepatan akses.

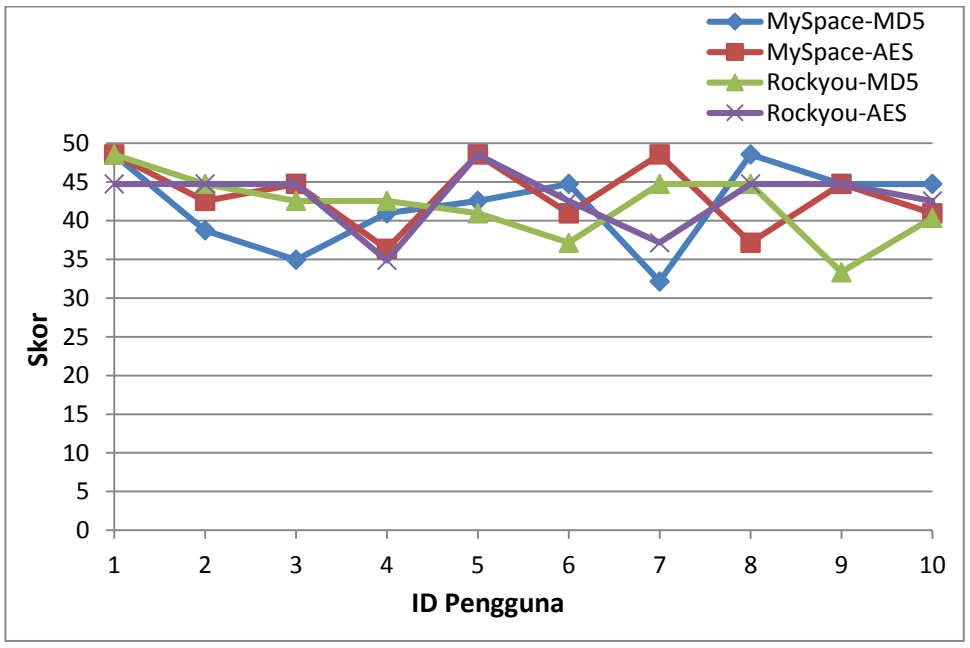
Perbandingan skor

Untuk mengetahui tingkat kekuatan atau skor dari metode yang diusulkan, maka dilakukan pengujian dengan menggunakan aplikasi passwordmeter [10]. Passwordmeter merupakan aplikasi yang dapat memberikan skor terhadap tingkat kekuatan sebuah password yang didasarkan pada kompleksitas dan panjang karakter dari password yang dimasukkan. Aplikasi ini dapat diakses secara online melalui www.yetanotherpassword-meter.com. Hasil dari penelitian dengan menggunakan passwordmeter ditunjukkan pada tabel 3.

Tabel 3. Hasil perbandingan skor data uji rockyou dan myspace dengan MD5 dan AES.

ID Pengguna	Rockyou (MD5)	Rockyou (AES)	MySpace (MD5)	MySpace (AES)
1	48.56	44.76	48.56	48.56
2	44.76	44.76	38.76	42.56
3	42.56	44.76	34.96	44.76
4	42.56	34.86	40.96	36.36
5	40.96	48.56	42.56	48.56
6	37.16	42.56	44.76	40.96
7	44.76	37.16	32.16	48.56
8	44.76	44.76	48.56	37.16
9	33.36	44.76	44.76	44.76
10	40.36	42.56	44.76	40.96
Rata-rata	**41.98**	**42.95**	**42.08**	**43.32**

Berdasarkan hasil pengujian tingkat kekuatan atau skor dari data uji didapatkan bahwa skor metode AES saat menggunakan data uji Rockyou 0.97 kali lebih kuat dibandingkan dengan menggunakan metode MD5. Pada data uji Myspace, metode AES memiliki skor 1.24 kali lebih kuat dibandingkan dengan menggunakan metode MD5. Hasil pengujian digambarkan dengan grafik 4. Berdasarkan hasil tersebut dapat disimpulkan bahwa metode enkripsi AES menghasilkan skor lebih kuat dibandingkan dengan menggunakan metode enkripsi MD5. Perbedaan waktu komputasi pada percobaan sebelumnya yang hanya beberapa mikro-detik dapat diabaikan dengan melihat tingkat proteksi yang dihasilkan oleh AES.



Gambar 4. Hasil perbandingan skor data uji Myspace dan Rockyou dengan menggunakan metode MD5 dan AES.

SIMPULAN

Pada penelitian ini penggunaan metode AES untuk enkripsi password menggunakan data uji rockyou telah menghasilkan skor 0.97 lebih kuat walaupun waktu komputasi 0.0004 lebih lambat dibandingkan metode MD5, sedangkan dengan menggunakan data uji MySpace menghasilkan skor 1.24 lebih kuat dengan waktu komputasi 0,0011 lebih lambat dibandingkan dengan metode MD5. Pada penelitian selanjutnya, dapat dicoba untuk menggabungkan atau memodifikasi S-Box AES untuk meningkatkan keamanan dari otentikasi.

DAFTAR PUSTAKA

[1] Haoyong Lv, Yin Hu, (2011), Analysis and research about cloud computing security protect policy, ISIE, pp. 214-216.

[2] Kaufman L.M, (2009) , Data security in the world of cloud computing, Security & Privacy, IEEE vol 7, pp 61-64.

[3] Grobauer B, Walloschek T, Stocker E, (2010), Understanding cloud computing vulnerabilities, Security & Privacy, IEEE vol 9 pp 50-57.

[4] Ziyuan Wang, (2011), Security and privacy issues within the Cloud Computing, International Conference on Computational and Information Sciences, IEEE.networks, Communications in Nonlinear Science and Numerical Simulation, 16: 3746–3759, 2011.

[5] Prasad P, Ojha B, Shahi RR, Lal R, Vaish A, Goel U. (2011). 3 Dimensional security in cloud computing, Computer Research and Development (ICCRD), Vol 3, pp. 198-201.

[6] Jain AK, Flynn P, Ross AA, (2008), Handbook of Biometrics, Springer, New York.

[7] Karen Scarfone , Murugiah Souppaya, (2009), Guide to Enterprise Password Management (Draft), Computer Security Division Information Technology Laboratory National Institute of Standards and Technology , Gaithersburg, MD 20899-8930 .

[8] Munir, R, (2006), Kriptografi, Informatika, Bandung.

[9] William Stallings, (2003), Cryptography and Network Security: Principles and Practice, Prentice Hall, New Jersey.

[10] Blasé, at all, (2012), How Does Your Password Measure Up?The Effect of Strength Meters on Password Creation, Carnegie Mellon University.