Jurnal TIMES , Vol. V No 1 : 23-27 , 2016
ISSN : 2337 - 3601

MENINGKATKAN KEAMANAN DATA CLOUD COMPUTING MENGGUNAKAN ALGORITMA VIGENERE CIPHER MODIFIKASI

Zikrul Alim[1], Yunie Cancer[2]
Program Studi S2Teknik Informatika Fakultas Ilmu Komputer dan Teknologi Informasi[1,2]
Universitas Sumatera Utara[1,2]
Jalan Universitas (Pintu I) Kampus USU Medan
e-mail : zikrulalim@students.usu.ac.id[1], Yuniecancer@students.usu.ac.id[2]

Abstrak

Ketergantungan terhadap keamanan data yang disediakan oleh provider komputasi awan dirasakan belumlah cukup, hal ini karena meningkatnya kejahatan dunia maya yang merupakan ancaman terhadap keamanan data pada komputasi awan. Salah satu cara untuk meningkatkan keamanan data pada komputasi awan tersebut adalah dengan menggunakan algoritma Vigenere Cipher yang telah dimodifikasi, karena pada algoritma vigenere cipher klasik panjang kunci dapat dipecahkan dengan pengujian Kasiski. Modifikasi dilakukan dengan membangkitkan karakter kunci yang baru berdasarkan hasil enkripsi pada karakter sebelumnya. Dengan asumsi bahwa panjang kunci diketahui, dilakukan serangan dengan metode brute force untuk menganalisa tingkat keamanan data yang dienkripsikan menggunakan algoritma vigenere cipher modifikasi. Tingkat keamanan algoritma modifikasi ini akan dibandingkan dengan tingkat keamanan pada algoritma vigenere cipher klasik.

Keyword*: cloud computing, vigenere cipher, keamanan data*

1. Pendahuluan

Cara manusia bertukar informasi sejak zaman dahulu sampai dengan sekarang terus mengalami perkembangan. Dahulu orang-orang menggunakan simbol, gambar, kulit kayu yang ditulis dengan batu pada dinding goa, tulang, batu dan lainnya. Kemudian perkembangannya dilanjutkan dengan pena dan kertas yang masih digunakan sampai dengan sekarang ini [1]. Seiring dengan perkembangan zaman, disamping masih menggunakan pena dan kertas, perkembangan teknologi informasi memberikan kemajuan teknologi informasi yang salah satu kemajuan teknologi informasinya dikenal dengan istilah *cloud computing* atau sering disebut dengan komputasi awan. Pada komputasi awan data/informasi tersimpan pada suatu server yang tidak perlu diketahui keberadaannya oleh pengguna, pengguna cukup menikmati fasilitas yang disediakan oleh *provider* komputasi awan tersebut. Pengguna tidak perlu menyiapkan perangkat-perangkat *software* maupun *hardware* pendukung, tetapi cukup hanya dengan diakses dari perangkat *client* yang terkoneksi dengan jaringan internet[2].

Data yang tersimpan pada komputasi awan keamanannya akan sangat bergantung pada pengamanan oleh *provider* penyedia layanan komputasi awan tersebut. Bila pengamanannya kurang baik, akan beresiko terhadap keamanan data. Bahkan bila dirasakan cukup tetap saja beresiko karena data/informasi pengguna tersimpan bukan pada perangkat pengguna, tetapi pada *server* penyedia layanan komputasi awan.

Perkembangan komputasi awan yang begitu pesatnya seiring juga dengan meningkatnya kejahatan dunia *cyber* seperti pencurian dan pembajakan data. Hal ini berkaitan dengan semakin bertambahnya para peretas-peretas handal dari seluruh dunia yang menambah resiko terhadap keamanan data komputasi awan[3][4].

Sekaitan dengan beberapa ulasan yang telah dipaparkan, salah satu cara untuk meningkatkan kemananan data pada komputasi awan adalah dengan menggunakan kriptografi[5]. *Vigenere cipher* adalah salah satu algoritma kriptografi. *Vigenere cipher* klasik memiliki kelemahan yaitu panjang kunci yang digunakan dapat dipecahkan dengan menggunakan pengujian *Kasiski*[6][7]. Makalah ini akan membahas suatu metode untuk mengacak pesan, dimana pesan asli diacak dengan mengunakan algoritma *vigenere cipher* yang telah dimodifikasi, Sehingga diharapkan data pada komputasi awan akan lebih aman. makalah ini akan membahas dan menganalisa tingkat keamanan dengan menggunakan algoritma *vigenere cipher* yang telah dimodifikasi. Pada bagian analisa dan pembahasan dari makalah ini akan dilakukan pengujian dengan menggunakan metode *brute force* untuk melihat sejauh mana peningkatan keamanan algoritma *vigenere cipher* modifikasi.

2. Landasan Teori

Ancaman Keamanan.

Sebagian informasi hanya ditujukan untuk orang-orang ataupun kelompok tertentu, sehingga informasi tersebut harus selalu dijaga kerahasiaannya. Aspek keamanan meliputi:

1. *Interuption*
   Merupakan ancaman terhadap availability informasi, data yang ada dalam sistem komputer dirusak atau dihapus sehingga akan menyulitkan si pemilik data bila hendak dibutuhkan oleh pemiliknya.
2. *Interception*
   Merupakan ancaman terhadap secrety data dan informasi dimana data yang seharusnya bersifat rahasia (tidak boleh diketahui oleh orang lain) disadap sehingga diketahui oleh orang yang tidak berhak.
3. *Modification*
   Merupakan ancaman terhadap integrity data dan informasi, dimana data tersebut diubah atau

dimodifikasi oleh orang yang tidak berhak sehingga tidak lagi asli.

4. *Fabrication*
   Merupakan ancaman terhadap integrity data/informasi, dimana data yang asli diubah oleh penyusup dan dikirimkan kepada penerima, sehingga penerima menyangka bahwa informasi tersebut bersumber dari pengirim yang dimaksud.

Komponen Kriptografi

Kriptografi adalah ilmu yang mempelajari tentang penyandian pesan agar lebih aman ketika disampaikan kepada si penerima pesan. Beberapa komponen kriptografi:

1. Enkripsi
   Merupakan suatu cara untuk mengubah suatu pesan ke bentuk pesan yang lainnya sehingga sulit untuk dimengerti maknanya. Untuk melakukan ini menggunakan suatu algoritma tertentu.
2. Dekripsi
   Merupakan kebalikan dari enkripsi dimana pesan yang sulit untuk dimengerti diubah menggunakan suatu algoritma tertentu, sehingga menjadi pesan yang dapat dipahami maknanya.
3. Kunci
   Suatu karakter yang digunakan untuk melakukan enkripsi/dekripsi terhadap suatu pesan. Kunci terbagi menjadi kunci simetris dan kunci asimetris. Kunci simetris merupakan kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Sedangkan kunci asimetris terdiri dari kunci umum dan kunci rahasia. Kunci umum digunakan untuk proses enkripsi, kunci rahasia digunakan untuk kunci dekripsi.
4. Ciphertext
   Merupakan suatu teks yang telah melalui proses enkripsi. Teks ini tidak dipahami maknanya karena berupa karakter-karakter yang acak.
5. Plaintext
   Merupakan suatu teks yang akan dienkripsi atau telah melalui proses dekripsi. Teks ini dipahami maknanya.
6. Pesan
   Suatu data/informasi yang akan disampaikan kepada penerima melalui suatu media tertentu, seperti kurir, saluran komunikasi, dsb.
7. Kriptanalisis
   Merupakan suatu proses analisa untuk mendapatkan/memahami pesan asli terhadap pesan yang telah disandikan tanpa mengetahui kunci yang digunakan. Proses ini juga dapat menganalisa suatu kelemahan algoritma kriptografi.

Komputasi Awan

Komputasi awan yang sering dikenal dengan istilah *Cloud computing* merupakan suatu kemajuan teknologi informasi dimana informasi disimpan pada suatu server yang dapat diakses oleh pengguna (*client*) melalui jaringan internet. Informasi diakses melalui perangkat pengguna seperti smartphone, computer, tablet, dan lainnya. Komputasi awan menggabungkan teknologi komputer dengan pengembangan internet sehingga menjadi infrastruktur komplek yang abstraksi dan tersembunyi. Pengguna tidak perlu memiliki kendali terhadap infrastrukturnya, karena kemampuan teknologi ini disajikan sebagai suatu layanan (*as a service*). 5 karakteristik yang harus dipenuhi oleh komputasi awan adalah berikut ini:

1. *Resource Pooling*
   Pengguna dapat memakai secara dinamis sumber daya komputasi terkelompok yang disediakan oleh *provider* secara bersama-sama oleh sejumlah pengguna. Sumber daya termasuk dapat berupa fisik ataupun virtual yang dialokasikan secara dinamis sesuai permintaan
2. *Broad Network Access*
   Layanan yang disediakan harus dapat diakses oleh berbagai jenis perangkat melalui jaringan.
3. *Measured Service*
   Layanan yang disediakan harus dapat dimonitor oleh pengguna melalui suatu sistem pengukuran. Sumber daya yang digunakan dapat secara transparan diukur oleh pengguna untuk dijadikan dasar untuk membayar biaya penggunaan layanan.
4. *Rapid Elasticity*
   Layanan yang disediakan oleh *provider* harus dapat memenuhi kebutuhan pengguna secara dinamis sesuai kebutuhan. Pengguna dapat menurunkan dan menaikan kapasitas layanan sesuai keinginan.
5. *Self Service*
   Layanan yang disediakan harus mampu memenuhi pesanan sumber daya yang dibutuhkan dengan segera melalui suatu sistem secara otomatis.

National Institute of Standards and Technology membagi layanan cloud computing menjadi 3 jenis layanan:

1. *Software as a service (SaaS)*
   SaaS merupakan layanan *cloud computing* dimana pelanggan dapat menggunakan perangkat lunak yang disediakan oleh *provider*. Pengguna tidak perlu membeli lisensi perangkat lunak lagi, cukup dengan berlangganan dan membayar sesuai dengan permintaan. Contohnya: Facebook, Twitter, YahooMessenger, Skype, dan lainnya.
2. *Platform as a service (Paas)*
   PaaS merupakan layanan yang menyediakan hardware sehingga pengembang aplikasi tidak perlu memikirkan *operating system*, *infrastructure scalling*, *load balancing* dan lainnya. Pengembang dapat fokus pada aplikasi yang dikembangkan karena "wadah" aplikasi sudah menjadi tanggung jawab *provider*. Contohnya: Microsoft Azure.
3. *Infrastructur as a Service (IaaS)*
   IaaS merupakan layanan yang menyediakan sumber daya teknologi informasi dasar yang dapat digunakan oleh penyewa untuk menjalankan aplikasi yang dimilikinya. Model ini seperti penyedia data center yang menyewakan ruangan, tapi ini lebih ke level mikronya. Keuntungan jenis layanan ini adalah kita tidak perlu membeli komputer fisik tetapi kita dapat melakukan konfigurasi komputer virtual yang dapat diubah dengan mudah. Contohnya: Amazon EC2, Windows Azure, dsb.

Algoritma Vigenere Cipher

Algoritma *Vigenere Cipher* dipublikasikan oleh seorang kriptologis Perancis yang bernama Blaise de Vigenere pada abad 16. Algoritma ini ide dasarnya hampir sama dengan teknik substitusi pada *caesar cipher*, tetapi jumlah pergeseran hurufnya berbeda-beda untuk setiap periode beberapa huruf tertentu. Variasi jumlah pergeseran yang berbeda-beda untuk setiap periodenya akan menambah tingkat kerumitan dari pesan untuk dipecahkan.

Variasi jumlah pergeseran yang dimaksud adalah melakukan substitusi masing-masing huruf pada plainteks dengan masing-masing huruf kunci. Bila panjang kunci lebih pendek dari panjang plainteks, maka huruf kunci penggunaannya akan diulang. Misalkan kunci yang digunakan untuk melakukan enkripsi adalah k = "DIA". Maka huruf "A" digeser sejumlah 3 (karena D=3) sehingga menjadi "D". untuk huruf "B" digeser sejumlah 8 (karena I=8) sehingga menjadi J. huruf "C" digeser sejumlah 0 (karena A=0) sehingga tetap menjadi huruf "C", demikian seterusnya untuk huruf berikutnya kembali digeser sejumlah 3, karena pemakaian kunci k yang berulang.

Secara matematis algoritma untuk melakukan enkripsi pesan dirumuskan seperti persamaan 1.

$$C_i = (P_i + k_{i+1(\text{ mod } m)}) \text{ mod } 26 \qquad (1)$$

dimana $i \leq C_i < m$

keterangan: C_i = ciphertext indeks ke-i; P_i = plaintext indeks ke-i; $K_{i+1\ (\text{mod } m)}$ = karakter kunci dengan indeks i mod m; i = 0, 1, 2 dst; m = 1, 2, dst m = panjang kunci. (catatan: bila $k_{i+1\ (\text{mod } m)} = 0$, yang digunakan adalah k_m).

Sedangkan algoritma untuk melakukan dekripsi pesan dirumuskan seperti persamaan 2.

$$D_i = (C_i - k_{i+1(\text{ mod } m)}) \text{ mod } 26 \qquad (2)$$

keterangan: D_i = plaintext indeks ke-i; C_i = ciphertext indeks ke-i; $K_{i+1\ (\text{mod } m)}$ = karakter kunci dengan indeks i mod m; i = 0, 1, 2 dst; m = 1, 2, dst m = panjang kunci. (catatan: bila $k_{i+1\ (\text{mod } m)} = 0$, yang digunakan adalah k_m)

3. Metode Penelitian

Karena pemakaian kunci yang berulang, algoritmavigenere cipher klasik dapat dipecahkan melalui *Tes Kasiski* dan *koinsiden indeks*. Tes ini menganalisa jumlah panjang kunci, sehingga bila panjang kuncinya sudah didapatkan, maka dilanjutkan dengan mencoba-coba kata kunci tersebut. Penggunaan kunci yang berulang disebabkan karena panjang plaintext tidak sama dengan panjang kunci. Untuk mengatasi kelemahan ini dengan menghindari pemakaian kata kunci yang berulang. Untuk menghindari pemakaian kunci yang berulang, algoritma *Vigenere Cipher* dimodifikasi agar kunci yang digunakan tidak berulang. Modifikasi dilakukan dengan cara menukar karakter kunci setelah karakter kunci yang terakhir dengan hasil enkripsi pada karakter terakhir kunci. Demikian untuk indeks seterusnya (indeks sama dengan panjang kunci sampai dengan indeks panjang plaintext dikurangi satu), yang secara matematis dapat dirumuskan seperti pada persamaan 3.

$$C_i = (P_i + k_{i+1(\text{ mod } m)} + C_{i-1}) \text{ mod } 26 \qquad (3)$$

dimana $m \leq C_i <$ panjang plaintext

keterangan: C_{i-1} = ciphertext indeks ke i - 1. Sedangkan untuk dekripsinya digunakan algoritma yang dalam persamaan matematikanya adalah seperti persamaan 4.

$$D_i = (C_i - k_{i+1(\text{ mod } m)} - C_{i-1}) \text{ mod } 26 \qquad (4)$$

Bila hasil pengurangan $C_i - K_{i+1\ (\text{mod } m)}$ = negatif, maka jumlahkan dengan angka 26 sampai nilainya menjadi positif. Persamaan 4 digunakan untuk karakter dengan indeks selanjutnya (i ← panjang kunci s.d i ← panjang plaintext – 1). Contoh Hasil enkripsi vigenere cipher modifikasi dengan jumlah karakater 26 yang dimulai dengan karakter "A" sampai dengan "Z" sebagaimana pada tabel 1. Kata kunci yang digunakan adalah k ← "USU", setelah tabel 1, dipaparkan beberapa contoh perhitungan matematikanya.

Tabel 1 Enkripsi *vigenere cipher* modifikasi kunci k ← "USU"

Plaintext	Nomor Asli	Nomor Acak	Ciphertext
A	0	20	U
B	1	19	T
C	2	22	W
D	3	19	T
E	4	15	P
F	5	14	O
G	6	14	O
H	7	13	N
I	8	15	P
J	9	18	S
K	10	20	U
L	11	25	Z
M	12	5	F
N	13	10	K
O	14	18	S
P	15	1	B
Q	16	9	J
R	17	20	U
S	18	6	G
T	19	17	R
U	20	5	F
V	21	20	U
W	22	8	I
X	23	25	Z
Y	24	17	R
Z	25	8	I

huruf pada tabel 1 diperoleh dengan cara sebagai berikut:

$C_0 = (P_0 + k_{1 \bmod m}) \bmod 26 = (0 + 20) \bmod 26$
$= 20 \bmod 26 = 20 \Rightarrow U$

$C_1 = (P_1 + k_{2 \bmod m}) \bmod 26 = (1 + 18) \bmod 26$
$= 19 \bmod 26 = 19 \Rightarrow T$

$C_2 = (P_2 + k_{3 \bmod m}) \bmod 26 = (2 + 20) \bmod 26$
$= 22 \bmod 26 = 22 \Rightarrow W$

$C_3 = (P_3 + k_{4 \bmod m} + C_{3-1}) \bmod 26 = (3 + 20 + 22) \bmod 26$
$= 45 \bmod 26 = 19 \Rightarrow T$

$C_4 = (P_4 + k_{5 \bmod m} + C_{4-1}) \bmod 26 = (4 + 18 + 19) \bmod 26$
$= 41 \bmod 26 = 15 \Rightarrow P$

dan seterusnya.

4. Hasil Penelitian

Pada makalah ini dilakukan beberapa pengujian yang terdiri dari pengujian ke-1, enkripsi dan dekripsi dilakukan dengan menggunakan algoritma vigenere cipher klasik. Pengujian ke-2, enkripsi dan dekripsi dilakukan dengan menggunakan algoritma *vigenere cipher* modifikasi. Plaintext yang digunakan adalah "FAKULTASILMUKOMPUTER" dengan kata kunci "USU". Pengujian ke-3 dilakukan kriptanalisis dengan menggunakan metode *brute force* terhadap hasil enkripsi dari pengujian ke-1 dan ke-2.

Pengujian ke-1.

Tabel 2 Enkripsi algoritma *vigenere cipher* klasik

Input	Output	Kunci
FAKULTASILMU KOMPUTER	ZSEODNUKCFEO EGGJMNYJ	USU

Tabel 3. Dekripsi algoritma *vigenere cipher* klasik

Input	Output	Kunci
ZSEODNUKCFEO EGGJMNYJ	FAKULTASILMU KOMPUTER	USU

Pengujian ke-2

Tabel 4 Enkripsi algoritma *vigenere cipher* modifikasi

Input	Output	Kunci
FAKULTASILMU KOMPUTER	LBVPXNBLRXZP VDZFPNJJ	USU

Tabel 5 Dekripsi algoritma *vigenere cipher* modifikasi

Input	Output	Kunci
LBVPXNBLRXZP VDZFPNJJ	FAKULTASILMU KOMPUTER	USU

Pengujian ke-3
Hasil kriptanalisis pengujian ke-1.

Asumsi telah diketahui panjang kunci adalah 3

```
14006   FANULWASLLMXKOPPUWER
14007   FAMULVASKLMWKOOPUVER
14008   FALULUASJLMVKONPUUER
14009   FAKULTASILMUKOMPUTER
14010   FAJULSASHLMTKOLPUSER
14011   FAIULRASGLMSKOKPURER
14012   FAHULQASFLMRKOJPUQER
```

Gambar 1 Kriptanalisis metode *Brute Force* pada *vigenere* klasik.

Ciphertext dapat dipecahkan dengan metode *brute force* dengan urutan yang ke-14.009, kunci dimulai dari "AAA" sampai dengan "ZZZ".

Menggunakan serangan *brute force*, ciphertext akan dapat dipecahkan dengan kemungkinan yang secara matematis dapat dihitung dengan menggunakan rumus:

$$ncr = \left(\frac{26!}{1!\,(26-1)!}\right)^{l} = \left(\frac{26\ x\ 25!}{25!}\right)^{3} = (26)^3 = 17.576$$

Hasil kriptanalisis pengujian ke-2
Menggunakan panjang kunci=3

```
14006   RJEVFWHTADHYBLILXWPR
14007   RJDVFVHTZDHXBLHLXVPR
14008   RJCVFUHTYDHWBLGLXUPR
14009   RJBVFTHTXDHVBLFLXTPR
14010   RJAVFSHTWDHUBLELXSPR
14011   RJZVFRHTVDHTBLDLXRPR
14012   RJYVFQHTUDHSBLCLXQPR
```

Gambar 2 Kriptanalisis metode *Brute Force* pada *vigenere* modifikasi

Ciphertext tidak dapat dipecahkan dengan metode *brute force* dengan asumsi panjang kunci adalah 3".

Menggunakan serangan *brute force*, dengan panjang kunci sepanjang plaintext, pesan ini akan dipecahkan dengan kemungkinan yang secara matematis dapat dihitung dengan menggunakan rumus:

$$ncr = \left(\frac{26!}{1!\,(26-1)!}\right)^{l} = \left(\frac{26\ x\ 25!}{25!}\right)^{20} = (26)^{20} = 1{,}994x10^{28}$$

Bila *plaintext* semakin panjang maka kemungkinan untuk dipecahkan juga semakin sulit.

5. Kesimpulan

Analisis pada pengujian ke-3 telah menunjukkan bahwa serangan yang dilakukan dengan metode *brute force* terhadap algoritma *vigenere cipher* yang telah dimodifikasi menunjukkan peningkatan keamanan terhadap serangan dengan metode *brute force*.

6. Saran

Untuk pengembangan makalah ini lebih lanjut, modifikasi dapat dilakukan pada sistem kriptografi modern sehingga keamanan dapat lebih ditingkatkan lagi.

7. Daftar Pustaka

[1] Ariyus, D. *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*", Penerbit Andi, Yogyakarta, 2008.

[2] Budiyanto, A., *Pengantar Cloud Computing*. Komunitas Cloud Computing Indonesia, 2012.

[3] Sengupta, Nandita, Holmes & Jeffrey. 2013, *Designed of Cryptography Based Security System for Cloud Computing*. International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 2013.

[4] Buyya, R.C., Yeo, S. & Venugopa, S. *Marketoriented Cloud Computing*: *Vision, hype, and reality for delivering it services as computing utilities*, Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, IEEE CS Press, Los Alamitos, CA, USA), 2008.

[5]Kromodimoeljo, S. *Teori dan Aplikasi Kriptografi*. SPK IT Consulting, 2009.

[6] Bhateja, A & Kumar, S. *Genetic algorithm with elitism for cryptanalysis of vigenere cipher.* International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014.

[7] Stallings, W. *Cryptography and Network Security: Principles and practices.* Upper Saddle River, NJ: Prentice-Hall, 2006.