Jurnal Sistem Informasi (JSI), VOL .9, NO.2, Oktober 2017
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

Komputasi Paralel GPU Dengan Teknologi Nvdia Cuda Untuk Enkripsi Berkas Pdf Menggunakan Algoritma RC4 DAN MD5

Al Farissi, Samatra Marwa Hany, Rifkie Primartha
Teknik Informatika, Universitas Sriwijaya Palembang, Indonesia
alfarissi@gmail.com, osiriskuno@gmail, rifkie77@gmail.com

Abstract

One way to secure files on storage media is by cryptographic techniques.The content of PDF files sometimes Contains with important information. therefore information security becomes a priority at this time. In this research, PDF files will be encrypted with MD5-RC4 technique. This combination makes information more secure and protected from information disclosure. This research implement parallel computing using GPU and CPU that make a performance of process run faster. When Nvidia released CUDA, GPU Become a strong power as an efficient accelerator for complex computations. Therefore, the GPU with CUDA and the comparision between CUDA and CPU will be discussed in this study.

Keywords: *PDF, Enkripsi,CUDA,MD5,RC4.*

Abstrak

Salah satu cara pengamanan berkas di dalam media penyimpanan yaitu dengan cara teknik kriptografi. Berkas PDF merupakan salah satu tipe berkas yang sering digunakan untuk menyimpan informasi. Oleh karena itu keamanan informasi menjadi prioritas saat ini. Dalam penelitian ini berkas PDF akan dienkripsi dengan teknik MD5-RC4. Kombinasi ini membuat informasi lebih aman dan terlindungi dari pencurian informasi. Selain itu, pada penelitian ini menerapkan komputasi paralel dengan menggunakan GPU dan CPU agar proses berjalan lebih cepat. GPU menjadi kekuatan yang kuat sebagai akselerator yang efisien untuk perhitungan kompleks. Oleh karena itu, GPU dengan CUDA serta perbandingan kecepatan antara CUDA dan CPU akan dibahas dalam penelitian ini.

Kata kunci: *PDF, Enkripsi,CUDA,MD5,RC4.*

1. PENDAHULUAN

Pada saat ini GPU hanya digunakan dalam dunia permainan komputer dan multimedia, hal ini disebabkan oleh anggapan mengenai performa CPU lebih baik dibandingkan dengan GPU. Namun, kemampuan GPU tidak dapat diabaikan karena GPU memiliki inti lebih banyak dibandingkan CPU. Oleh karena itu, proses komputasi secara paralel dengan menggunakan CPU dan GPU memiliki performa yang lebih baik dari pada hanya menggunakan CPU saja. Menggunakan CPU dan GPU dalam membuat perangkat lunak, akan membuat perangkat lunak yang dibuat memiliki kecepatan yang lebih baik daripada program komputer yang hanya menggunakan CPU. Saat ini GPU telah berada pada titik di mana banyak aplikasi dunia nyata yang mudah diimplementasikan dan lebih cepat dari pada sistem multi-inti milik CPU. Arsitektur komputasi masa depan akan menggunakan sistem hibrida dengan GPU paralel-inti yang bekerja bersama-sama dengan CPU multi-inti

Banyak orang menyimpan dan bertukar informasi penting atau rahasia dalam berkas PDF, itu membuat informasi tersebut harus dilindungi. Untuk melindungi informasi tersebut, berkas PDF tersebut akan di enkripsi dengan menggunakan algoritma MD5 dan RC4. Sedangkan untuk meningkatkan kecepatan pada proses enkripsi, CPU akan di bantu GPU berasiktektur CUDA yang dibuat oleh NVIDIA sehingga proses kecepatannya kan lebih baik. Pada penelitian ini GPU yang di pakai adalah NVIDIA Gforce GT640.

2. METODOLOGI

Message-Digest algorithm 5 (MD5) adalah fungsi hash kriptografi yang banyak digunakan dalam memproses pesan, pesan yang telah di proses dengan menggunakan algoritma MD5 memiliki ukuran yang tetap yaitu 128 bit. Pesan masukan dibagi menjadi beberapa blok 512-bit, dan melalui proses lima langkah berikut[4]:

1. menambahkan bit padding,
2. menambahkan panjang,
3. menginisialisasi buffer MD5,
4. memproses pesan dalam blok
5. output 16-*word*.

Dalam algoritma utama MD5, sebuah *state* 128-bit yang dibagi menjadi empat *word* 32-bit. Kemudian keempat *word* tersebut dinotasikan menjadi a, b, c dan d, diinisialisasi ke konstanta tertentu. Blok pesan 512 bit dioperasikan satu demi satu bersamaan dengan modifikasi *state*. Pengolahan setiap blok pesan berisi empat putaran. Setiap putaran terdiri dari 16 operasi serupa yang didasarkan pada fungsi non-linear F, penambahan modular dan rotasi kiri[4]. Fungsi F dalam setiap rondenya di perlihatkan pada Tabel 1.

Tabel 1. Fungsi F pada setiap ronde.

Ronde	Fungsi F
1	(b AND c) OR ((NOT b) AND d)
2	(d AND b) OR ((NOT d) AND c)
3	b XOR c XOR d
4	C XOR (b OR (NOT d))

Masukan algoritma enkripsi RC4 merupakan sebuah byte, kemudian dilakukan operasi XOR dengan sebuah byte kunci, dan mengahasilkan sebuah byte sandi. Ada 2 Algoritma yang terdapat pada RC4:

1. Algoritma Penjadwalan Kunci (KSA).
2. Algortima Pembangkit Kunci (PRGA).

Sistem sandi RC4 menggunakan state, yaitu larik byte berukuran 256 yang termutasi, dan tercampur oleh kunci. Kunci merupakan larik byte berukuran 256 byte. Sebelum melakukan enkripsi, dan dekripsi, sistem sandi RC4 melakukan inisialisasi terhadapat *state* dengan menggunakan algoritma penjadwalan. Algoritma penjadwalan kunci dapat dilihat pada Gambar 1.

```
Prosedur penjadwalan kunci
{
   For i=0 to 255 do
      S[i]=i;
      K[i]=key[I mod keylen];
J=0;
   For i=0 to 255 do
      J=(j+S[i]+K[i] mod 256;
      Swap (S[i].S[j]);
}
```

Gambar 1. Algortima penjadwalan kunci (KSA)

Setelah *state S* terinisialisasi oleh penjadwalan kunci setiap byte pada teks asli dikenakan operasi XOR dengan kunci byte untuk menghasilkan *byte* pada teks sandi. Kunci *byte* yang digunakan pada enkripsi dibangkitkan dengan memanfaatkan *state* S. Algoritma pembangkit kunci dapat di lihat pada Gambar.2.

```
Prosedur penjadwalan kunci
{
  i,j=0;
  while(true)
       i=(j+1) mod 256;
       j=(j+S[i]) mod 256;
       Swap(S[i],S[j]);
       t=(S[i]+S[j]) mod 256;
       streamteks=S[t];
}
```

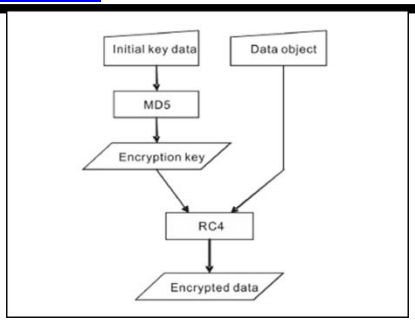
Gambar 2. Algoritma pembangkit kunci

Algoritma RC4 membuat penggunaan swapping byte yang tinggi dalam array permutasi 256-byte "S". Untuk membuat proses lebih cepat, susunan permutasi "S" harus ditempatkan ke dalam memori bersama.[2]

MD5-RC4

Penelitian ini menggunakan algoritma MD5 dan RC4. Kriptosistem menggunakan algoritma message-digest MD5 untuk mengenkripsi data kunci awal. Data kunci awal diperoleh dengan menambahkan kunci enkripsi asal ke nomor objek dan nomor generasi pada objek data [1]. Nilai keluaran dari data kunci hash digunakan sebagai kunci enkripsi untuk perhitungan RC4. Kemudian objek data beserta kunci enkripsi yang dihasilkan dilewatkan ke fungsi RC4 yang panjang kunci 128, output adalah data terenkripsi yang sesuai [2]. Gambar 3 menunjukkan alur enkripsi berkas PDF.

Jurnal Sistem Informasi (JSI), VOL .9, NO.2, Oktober 2017
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com



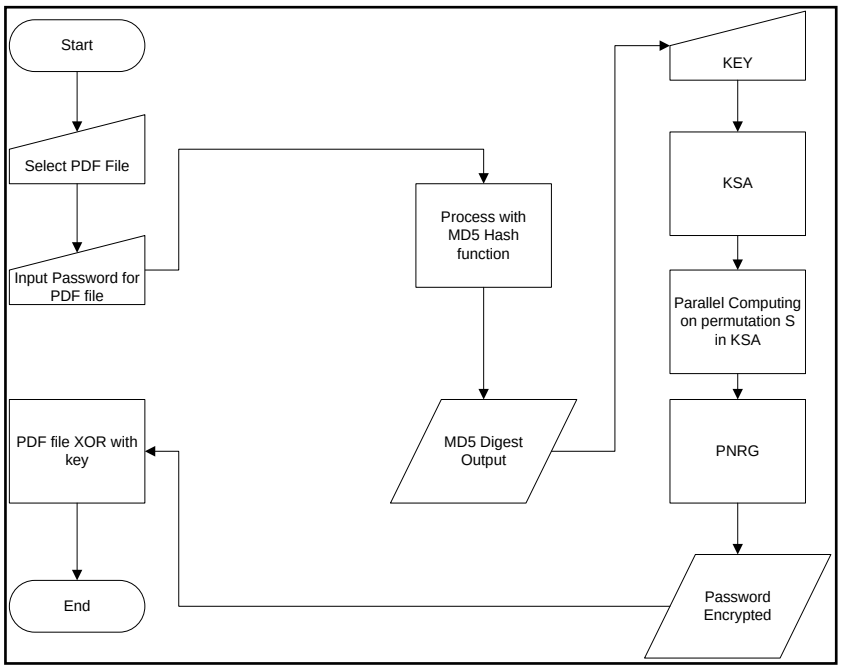
Gambar 3. Proses Enkripsi MD5-RC4 [2].

GPU

Kinerja dan potensi GPU menawarkan banyak harapan untuk sistem komputasi masa depan, namun model arsitektur dan pemrograman GPU sangat berbeda. Pada penelitian ini GPU yang di gunakan adalah GPU dengan platform CUDA[3]. *Compute Unified Device Architecture* (CUDA) adalah platform komputasi paralel dan model pemrograman yang dikembangkan oleh NVIDIA dan diimplementasikan oleh unit pemrosesan grafis (GPU)[3].

CUDA memiliki beberapa kelebihan dibanding perhitungan general purpose pada GPU (GPGPU) dengan menggunakan API grafis:

i. *Scattered reads* - kode bisa dibaca dari alamat yang sewenang-wenang di memori.
ii. *Shared memory* - CUDA menampilkan area memori bersama yang cepat (hingga 48KB per Multi-Processor) yang dapat dibagi di antara benang. Ini bisa digunakan sebagai cache yang dikelola pengguna, memungkinkan bandwidth lebih tinggi daripada yang mungkin dilakukan dengan menggunakan pencarian tekstur.[5]
iii. Download dan pembacaan ulang lebih cepat ke dan dari GPU.
iv. Dukungan penuh untuk operasi integer dan bitwise, termasuk pencarian tekstur integer.



Gambar 4. Diagram Alur Perangkat Lunak

Gambar 4. Diatas menjelaskan alur enkripsi berkas di mana berkas PDF dan kunci yang di input akan di proses menggunakan algortima MD5, setelah kunci di proses menggunakan kunci MD5 maka kunci akan di proses kembali menggunakan algoritma RC4, penjadwalan kunci pada rc4 dilakukan secara paralel dan dilanjutkan dengan algoritma pembangkit kunci yang ada pada RC4, setelah melalui algoritma RC4 kunci akan melalui proses XOR dengan berkas.

3. HASIL DAN IMPLEMENTASI

Pengujian di lakukan dengan mengenkripsi 30 berkas PDF dengan menggunakan kunci yang sama. Berkas tersebut di enkripsi dengan dua cara, Pertama menggunakan hanya CPU dan kedua menggunakan CPU dan GPU. Keluaran dari perangkat lunak yang hanya menggunakan CPU dan yang menggunakan CPU dan GPU memilki ukuran berkas yang sama dengan keadaan sebelum terenkripsi.

Tabel 2. Pengujian Berkas

NO	NAMA *FILE*	MASUKAN	SIZE	OUTPUT
1	11.pdf	kunci,PDF	75KB	*PDF*
2	16_MD5.pdf	kunci,PDF	746KB	*PDF*
3	98-500-1-PB.pdf	kunci,PDF	760KB	*PDF*
4	189-349-1-PB.pdf	kunci,PDF	414KB	*PDF*
5	1574-3509-1-SM.pdf	kunci,PDF	67KB	*PDF*
6	18052-20587-1-PB.pdf	kunci,PDF	308KB	*PDF*
7	00563518.pdf	kunci,PDF	527KB	*PDF*
8	01625328.pdf	kunci,PDF	405KB	*PDF*
9	04439099.pdf	kunci,PDF	344KB	*PDF*
10	05276924.pdf	kunci,PDF	1085KB	*PDF*
11	06018677.pdf	kunci,PDF	388KB	*PDF*
12	7407040060_m.pdf	kunci,PDF	350KB	*PDF*
13	A9-access-best-practices.pdf	kunci,PDF	1229KB	*PDF*
14	A421-424-Wahyu-Indah.pdf	kunci,PDF	214KB	*PDF*
15	(AES).pdf	kunci,PDF	275KB	*PDF*
16	aes_ref.pdf	kunci,PDF	259KB	*PDF*
17	aes_usr.pdf	kunci,PDF	265KB	*PDF*
18	amikom_yog_kripto.pdf	kunci,PDF	185KB	*PDF*
19	Artikel_50401408.pdf	kunci,PDF	1734KB	*PDF*
20	artikel_lengkap.pdf	kunci,PDF	700KB	*PDF*
21	asmhandout_2.pdf	kunci,PDF	5999KB	*PDF*
22	aspek_Pedagogi.pdf	kunci,PDF	224KB	*PDF*
23	bulletn4.pdf	kunci,PDF	230KB	*PDF*
24	C03+-+String.pdf	kunci,PDF	84.6KB	*PDF*
25	C0428022313.pdf	kunci,PDF	194KB	*PDF*

26	ch3-preview.pdf	kunci,PDF	198KB	*PDF*
27	chap1.pdf	kunci,PDF	291KB	*PDF*
28	crypto.pdf	kunci,PDF	578KB	*PDF*
29	a.pdf	kunci,PDF	166KB	*PDF*
30	Hash1.pdf	kunci,PDF	3366KB	*PDF*

Total *size* enkripsi tanpa menggunakan GPU pada kasus uji ini adalah 21660.60 KB dengan rata-rata *size* 722.20 KB/Berkas. Tidak ada perubahan ukuran terhadap Berkas yang telah terenkripsi. Berkas yang telah terenkripsi akan menampilkan pesan *file corrupt*. Untuk mengukur kecepatan perangkat lunak, maka perangkat lunak di bandingkan dengan perangkat lunak yang hanya menggunakan CPU dalam pemrosesannya.

Tabel 3. Perbandingan Waktu

NO	NAMA *FILE*	WAKTU (cpu)	WAKTU (gpu)	*SIZE*
1	11.pdf	0.388 detik	0.234 detik	75KB
2	16_MD5.pdf	3.972 detik	2.278 detik	746KB
3	98-500-1-PB.pdf	3.949 detik	4.009 detik	760KB
4	189-349-1-PB.pdf	2.235 detik	1.295 detik	414KB
5	1574-3509-1-SM.pdf	0.416 detik	0.218 detik	67KB
6	18052-20587-1-PB.pdf	1.603 detik	0.967 detik	308KB
7	00563518.pdf	2.747 detik	1.608 detik	527KB
8	01625328.pdf	2.115 detik	1.232 detik	405kb
9	04439099.pdf	1.791 detik	1.045 detik	344KB
10	05276924.pdf	5.635 detik	3.182 detik	1085KB
11	06018677.pdf	2.047 detik	1.194 detik	388KB
12	7407040060_m.pdf	1.825 detik	1.079 detik	350KB
13	A9-access-best-practices.pdf	6.737 detik	4.241 detik	1229KB
14	A421-424-Wahyu-Indah.pdf	1.129 detik	0.714 detik	214KB
15	(AES).pdf	1.464 detik	0.868 detik	275KB
16	aes_ref.pdf	1.385 detik	0.826 detik	259KB
17	aes_usr.pdf	1.399detik	0.834 detik	265KB
18	amikom_yog_kripto.pdf	0.967detik	0.606 detik	185KB
19	Artikel_50401408.pdf	8.969 detik	5.198 detik	1734KB
20	artikel_lengkap.pdf	3.713 detik	2.112 detik	700KB
21	asmhandout_2.pdf	3.120 detik	1.896 detik	5999KB
22	aspek_Pedagogi.pdf	1.248 detik	0.751 detik	224KB
23	bulletn4.pdf	1.186 detik	0.653 detik	230KB
24	C03+-+String.pdf	0.468 detik	0.293 detik	84.6KB
25	C0428022313.pdf	1.061 detik	0.623 detik	194KB
26	ch3-preview.pdf	1.029 detik	0.758 detik	198KB
27	chap1.pdf	1.544 detik	0.954 detik	291KB

28	crypto.pdf	3.027 detik	1.770 detik	578KB
29	a.pdf	0.953 detik	0.610 detik	1.66KB
30	Hash1.pdf	17.30 detik	10.252 detik	3366KB

Pada hasil uji kasus kecepatan rata-rata enkripsi perangkat lunak tanpa menggunakan GPU adalah 251.65 KB/detik, sedangkan untuk yang menggunakan GPU adalah 429.45 KB/detik atau 1.71 kali lebih cepat di bandingkan CPU.

4. KESIMPULAN

Berdasarkan hasil pengujian disimpulkan bahwa perangkat lunak dengan menggunakan pemerosesan paralel GPU dan CPU memiliki kecepatan hampir dua kali lipat dibandingkan dengan perangkat lunak yang hanya mengunakan pemrosesan komputasi dengan CPU saja. Perbedaan kecepatan ini di karenakan GPU yang memiliki inti yang lebih banyak di bandingkan dengan CPU, sehingga proses komputasi perangkat lunak yang menggunakan GPU dan CPU lebih cepat dibandingkan perangkat lunak yang hanya menggunakan CPU saja. Selain itu, pembagian proses dimana algoritma enkripsi RC4 yang dilakukan oleh GPU, sedangkan proses *checksum* yang dilakukan oleh MD5 dilakukan oleh CPU membuat kinerja perangkat lunak lebih efektif.

DAFTAR PUSTAKA

[1] Adobe Systems Incorporated.*Portabel document format version 1.7*. 2006.
[2] Changxin, L. Hongwei, W. Shifeng, C. Xiaochao, L. and Donghui, G.Efficient implementation for MD5-RC4 encryption using GPU with CUDA. *In Proceedings of the Anti-counterfeiting, Security, and Identification in Communication. 3rd International Conference on. 2009; 167-170.*
[3] Owens, Jhon D. Houston, M. Luebke, D. Green, S. Stone, J. E. and Phillips, J. C. GPU Computing. *Proceedings of the IEEE,* 96 (5)**,** 2008; 879-899.
[4] R. Rivest, The MD5 Message-Digest Algorithm, RFC 1321, April 1992
[5] Silberstein, M. Schuster, A. Geiger, D. Patney, A; Owens, John D. (2008). *Efficient computation of sum-products on GPUs through software-managed cache*. Proceedings of the 22nd annual international conference on Supercomputing –ICS. 2008; 309–318.
[6] William, S.Cryptography and *Network Security Principles and Practices*. Fourth edition. Prentice Hall.2005.