ISSN : 1410 - 7104

Aplikasi *Credant* dan *BitLocker* untuk Sistem Keamanan Data Computer

Application of Credant and BitLocker for Computer Data Security System

Mohammad Hamdani* dan Dwi Darmi Sa'diyahti**
Program Studi Teknik Elektro, Fakultas Teknologi Industri,
Institut Sains dan Teknologi Nasional
Email: *mhamdani@istn.ac.id dan **dwidarmi@gmail.com

Abstrak---*Pada Makalah ini dibahas tentang implementasi dan pengujian sistem keamanan data menggunakan aplikasi Credant dan BitLocker untuk melindungi data/informasi pada suatu komputer dari serangan atau usaha pengambilan data oleh pihak-pihak yang tidak diinginkan. Pengujian dilakukan baik secara lokal maupun pada suatu jaringan dengan menggunakan Remote Desktop Connection. Credant mengenkripsi data pada pada level pengguna, sedangkan BitLocker mengenkripsi data pada level hardware. Sehingga kombinasi kedua sistem keamanan data ini dapat menjaga keamanan data baik dari serangan di level user maupun di level hardware. Dari hasil implementasi dan pengujian diketahui bahwa aplikasi Credant dan BitLocker mampu melindungi berbagai jenis informasi dari usaha pencurian atau akses data oleh pihak-pihak yang tidak diinginkan karena baik data maupun drive telah terenkripsi secara keseluruhan, sehingga tingkat keamanan data yang tersimpan di computer meningkat.*

Kata Kunci: *Credant, BitLocker, Algoritma Rijndael , Data Computer*

Abstract---*This Paper discribes performed the implementation and the examination of computer data security system using Credant and BitLocker, which is used to protect information/data on a computer from the hacking or stealing attempt. The examination was done both locally and through the network using Remote Desktop Connection. Credant enrypts data on user level, while BitLocker encrypts data on the volumen level. Therefore, the combination of both security system will be able to protect the data both from user level attack and hardware/volume level attack.The implementation and examination results shows that BitLocker and Credant are able to protect any type of data information from the hacking and stealing attempt because both data and drive volume are encrypted entirely. Thus, the level of data security level in the computer is increased.*

Keywords: *Credant, BitLocker, Rijndael Algorithm, Computer Data*

1. PENDAHULUAN

Meningkatnya kecanggihan teknologi selain berakibat baik dapat pula mengakibatkan timbulnya banyak tantangan baru di dalam sistem keamanan data (informasi), khususnya untuk perusahaan-perusahaan besar yang tentunya memiliki data-data penting dan rahasia.Oleh karenanya, saat ini terdapat beberapa macam pilihan sistem untuk melindungi data-data tersebut dari kemungkinan pencurian data oleh pihak-pihak yang tidak bertanggung-jawab. Salah satu solusi untuk mengatasi permasalahan keamanan data-data yang penting dan rahasia tersebut adalah dengan menggunakan metode enkripsi.

Terdapat berbagai macam metode enkripsi yang dapat diaplikasikan dan masing-masing memiliki kekurangan dan kelebihan. Seringkali data diamankan dalam proses pengiriman data. Oleh sebab itu pada makalah ini dibahas tentang level enkripsi data, tingkat keamanan data dan algoritma yang digunakan pada enkripsi *Credant* dan *Bitlocker* yang diimplementasikan pada suatu komputer client.

2. TINJAUAN PUSTAKA

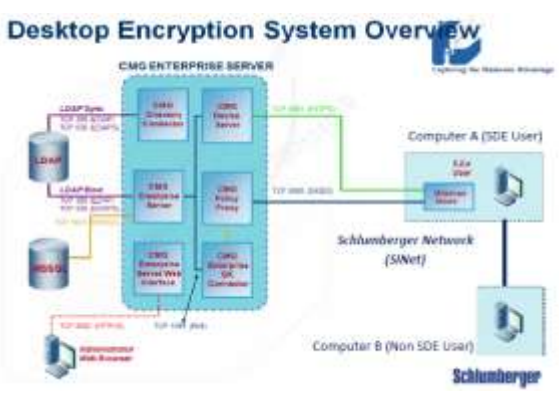
2.1 *Credant Mobile Guardian Shield*

Credant (Credant Mobile Guardian Shield) merupakan suatu aplikasi keamanan data yang berfungsi untuk memproteksi secara transparan data-data user dari akses-akses yang tidak semestinya (seperti laptop hilang, data loss/crack dan sebagainya). Credant melakukan proses enkripsi data pada level user. Sehingga secara singkat dapat dikatakan bahwa masing-masing user pada suatu komputer memiliki pola enkripsi yang berbeda-beda. Karenanya, file-file komputer yang dienkripsi menggunakan data akun sebuah user tidak akan dapat dibuka oleh user dengan login yang lain.

Aplikasi Credant yang teridiri atas dua bagian utama yaitu CMG Enterprise Server dan komputer pengguna dimana aplikasi Credant terinstal.Komputer pengguna terhubung dengan server melalui jaringan komputer Schlumberger yang disebut dengan SINet (Schlumberger Internal Network). Sistem aplikasi Credant pada kasus terlihat pada gambar 1.

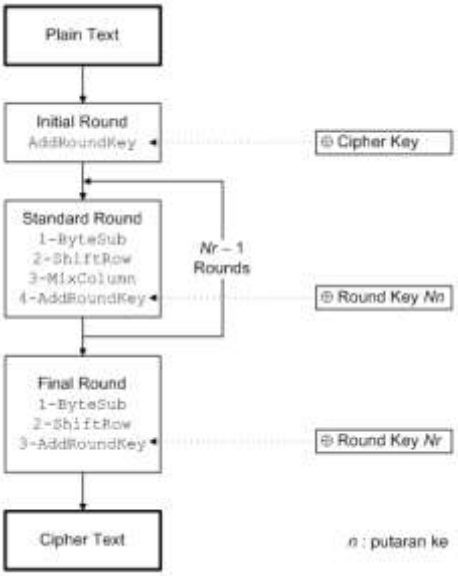
2.1.1 Algoritma Rijndael

Aplikasi Credant (versi *CMG Enterprise*) menggunakan *Algoritma Rijndael* pada proses sistem enkripsi dekripsi datanya. Algoritma Rijndael adalah algoritma yang beroperasi dalam *byte*.Algoritma ini mampu melakukan enkripsi terhadap *plaintext* sebesar 16 *byte* atau 128 *bit*.Algoritma *Rijndael* juga melakukan putaran enkripsi (*enciphering*) sebanyak 10 putaran. Garis besar Algoritma *Rijndael* adalah sebagai berikut:



Gambar 1. Sistem Aplikasi Credant pada Schlumberger Network

1. *AddRoundKey*: melakukan *XOR* antara *state* awal (plainteks) dengan *cipher key*. Tahap ini disebut juga *initial round*, terlihat pada gambar 2.



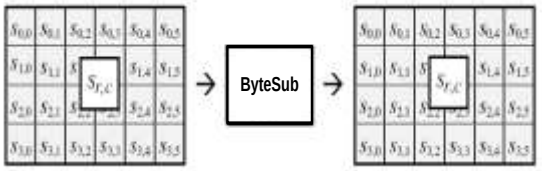
Gambar 2. Diagram Proses Enkripsi Algoritma Rijndael

2. Putaran sebanyak *Nr* – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes*: substitusi *byte* dengan menggunakan tabel substitusi (*Sbox*).

hex	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

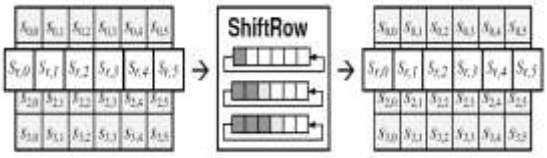
x

Gambar 3. Kotak Substitusi *(S-Box)* dalam transformasi *SubBytes*



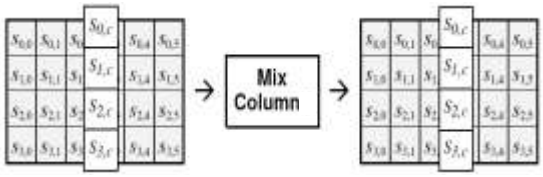
Gambar 4. Ilustrasi Transformasi *SubBytes*

   b. *ShiftRows*: pergeseran baris *array state* secara *wrapping*.



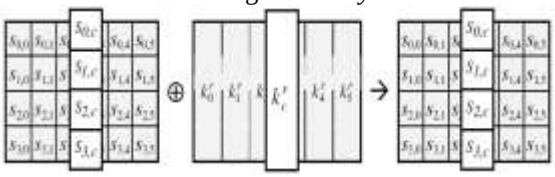
Gambar 5. Ilustrasi Transformasi *ShiftRow*

   c. *MixColumns*: mengacak data di masingmasing kolom *array state.*



Gambar 6. Ilustrasi Transformasi *MixColumn*

   d. *AddRoundKey*: melakukan XOR antara *state* sekarang *round key*.



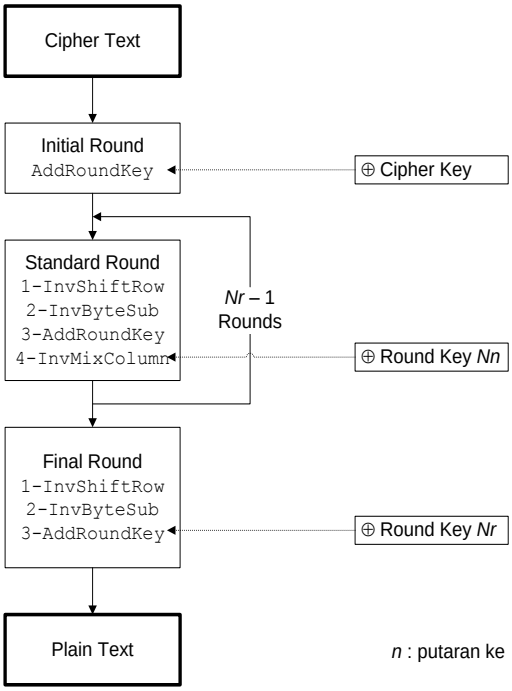
Gambar 7. Ilustrasi Transformasi *AddRoundKey*

3. *Final round*: proses untuk putaran terakhir:
   a. *SubBytes*
   b. *ShiftRows*
   c. *AddRoundKey*

Dengan 16 *byte*, maka baik blok data dan kunci yang berukuran 128-bit dapat disimpan di dalam ketiga array tersebut (128 = 16 x 8). Selama kalkulasi plainteks menjadi cipherteks, status sekarang dari data disimpan di dalam *array of byte* dua dimensi, state, yang berukuran NROWS x NCOLS. Elemen *array*state diacu sebagai $S[r,c]$, dengan $0 \le r < 4$ dan $0 \le c < Nc$ (*Nc* adalah panjang blok dibagi 32). Pada *AES*, $Nc = 128/32 = 4$.

Invers Cipher merupakan algoritma Rijndael yang digunakan untuk melakukan proses dekripsi cipherteks menjadi plainteksnya. Secara garis besar, *cipher* kebalikan yang beroperasi blok 128-bit dengan kunci 128-bit adalah sebagai berikut:

1. *AddRoundKey*: melakukan *XOR* antara *state* awal (cipherteks) dengan *cipher key*. Tahap ini disebut juga *initial round*.



Gambar 8. Diagram Proses Dekripsi Algoritma Rijndael

hex	y 0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

x

Gambar 9. Kotak Subtitusi *(S-Box)* dalam transformasi *InvSubBytes*

2. Putaran sebanyak *Nr* – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *InvShiftRow:* pergeseran baris-baris *array state* secara *wrapping*.
   b. *InvByteSub*: substitusi byte dengan menggunakan tabel substitusi kebalikan (*inverse S-box*).
   c. *AddRoundKey:* melakukan *XOR* antara *state* sekarang dengan *round key*.
   d. *InvMixColumn*: mengacak data di masing-masing kolom *array state*.
3. *Final round*: proses untuk putaran terakhir:
   a. *InvShiftRow.*
   b. *InvByteSub*.
   c. *AddRoundKey*.

Ekspansi kunci dibutuhkan utuk memenuhi kebutuhan *subkey* yang dapat mencapai ribuan bit untuk melakukan enkripsi, sementara kunci enkripsi yang disediakan hanya 128 hingga 256 bit. Total *subkey* yang diperlukan adalah Nb(Nr + 1) *word*. Jadi bila menggunakan 128 bit, maka akan dipeluas hingga menjadi 1408 bit, melalui proses yang disebut dengan *key schedule*.

Tabel 1. Jumlah Proses Berdasarkan bit blok dan kunci

Panjang Kunci (Nk) Dalam words	Ukuran Blok Data (Nb) Dalam words	Jumlah Proses (Nr)
4	4	10
6	4	12
8	4	14

Subkey sebanyak ini diperlukan karena setiap ronde membutuhkan *Nb word* ditambah satu *word subkey* untuk diawal. *Key-schedule* menghasilkan *array* linear *word[wi*] sebesar 4-*byte*, dimana *i* memiliki nilai *i<Nb(Nr + 1)*. Kriptografi yang baik menggunakan sepanjang mungkin kunci yang akan digunakan karena semakin panjang kunci, semakin lama pula waktu yang digunakan untuk melakukan proses enkripsi.

2.2 *BitLocker Drive Encryption*

BitLocker adalah sebuah fitur enkripsi full-disk yang telah tersedia dalam sistem operasi Microsoft Windows, baik versi Ultimate maupun Enterprise yang didesain untuk melindungi data dengan melakukanenkripsi terhadap keseluruhan partisi. Secara default, BitLocker Drive Encryption menggunakan algoritma *Advanced Encrypted Standart* (AES) dalam mode *Code Block Chaining* (CBC) dengan panjang kunci 128-bit, yang digabungkan dengan Elephant diffuser untuk meningkatkan keamanannya.

2.2.1 Cara Kerja *BitLocker*

Sama seperti *Credant*, BitLocker juga digunakan untuk menjaga keamanan data dengan melakukan proses enkripsi pada data yang disimpan. Namun, *BitLocker* melakukan proses enkripsi data pada level volume/drive menggunakan key storage tertentu.

Secara singkat dapat dikatakan bahwa selama user memiliki akses dan terdaftar pada sistem Active Directory tertentu, maka user dapat mengakses data pada computer tersebut menggunakan password Active Directory mereka. Pada gambar 10. terlihat Sistem Enkripsi Volume-based *BitLocker*

Gambar 10. Sistem Enkripsi Volume-based *BitLocker*

Seperti telah dikatakan sebelumnya, enkripsi data *BitLocker* dilakukan pada tingkatan volume/drive, sehingga akan terdapat suatu boot partisi bagian dari *BitLocker* sebagai lokasi penyimpanan kode enkripsi.

Partisi *BitLocker* Boot terdiri dari:

- Master Boot Record

- Windows Boot Manager
- Operating System Loader
- Boot Utilities (Unencrypted, small)

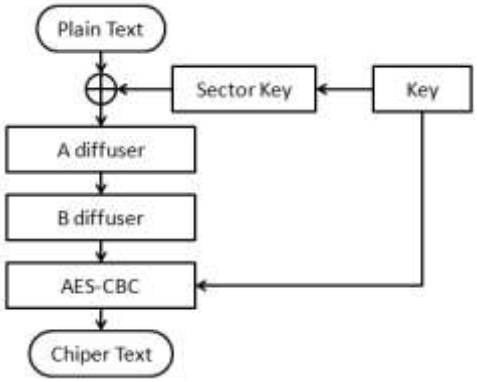
Penyimpanan Key enkripsi:

1. *SRK* (Storage Root Key) yang terdapat pada TPM
2. *SRK* mengenkripsi *VEK* (Volume Encryption Key) yang diproteksi oleh TPM/USB Key/Recovery Password

VEK disimpan di hard drive pada Boot Partition

2.2.2 Algoritma AES-CBC dan diffuser

Seperti telah dikatakan di atas, BitLocker menggunakan algoritma *Advanced Encrypted Standart* (AES) dalam mode *Code Block Chaining* (CBC) dengan panjang kunci 128-bit, yang digabungkan dengan Elephant diffuser untuk meningkatkan keamanannya. Prinsip dasar algoritma AES adalah menggunakan algoritma Rijndael. Proses enkripsi menggunakan AES-CBC dan Elephant diffuser dapat terlihat pada gambar 2.16



Gambar 11. Diagram Alir AES-CBC dengan diffuser

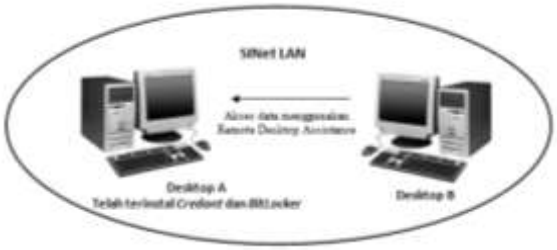
Pada gambar 2.16 terdapat 4 operasi terpisah pada setiap proses enkripsi. Dilakukan proses XOR pada plaintext dengan sector key, kemudian dilanjutkan dengan proses 2 kali *unkeyed diffuser*, dan akhirnya dienkripsi menggunakan AES pada mode CBC dengan prinsip dasar algoritma Rijndael yang telah dijelaskan sebelumnya. Komponen sector key dan AES-CBC masing-masing ditambahkan key secara independen sehingga proses ini akan lebih aman dari serangan.

3. METODA

3.1 Implementasi Sistem Keamanan Data*CREDANT* dan*BITLOCKER*

Implementasi sistem dilakukan pada komputer yang terhubung dengan studi kasus pada jaringan*Local Area Network* (LAN) Schlumberger Network (SINet). Pada kasus ini, serangan dari luar sistem computer akan disimulasikan dengan serangan dari komputer lain pada jaringan SINet yang sama.Simulasi dilakukan pada jaringan SINet karena *Credant* dan *BitLocker* yang diaplikasikan pada sistem dimaksudkan untuk menjaga keamanan data perusahaan yang tersimpan baik pada Laptop atau Desktop pegawai.Sedangkan kurang lebih 80% (6-7 jam) waktu pegawai dalam menggunakan komputer dilakukan dalam kondisi terkoneksi pada jaringan SINet.

Kedua komputer terhubung pada suatu jaringan komputer seperti terlihat pada gambar 3.1



Gambar 3.1 Pengujian implementasi enkripsi Credant dan Bitlockerpada suatu jaringan SINet LAN

Tahapan implementasi Sistem Keamanan Data menggunakan Credant dan Bitlocker ini terlihat pada gambar 3.2

Gambar 12 Diagram Alur Implementasi Sistem

3.2 Implementasi Sistem Keamanan Data *Credant*

Proses implementasi *Credant* dilakukan pada sisi client. Karena enkripsi yang dilakukan oleh *Credant* bekerja pada level user, maka dipastikan untuk login ke komputer menggunakan akun user pemilik computer dan Sebelum melakukan implementasi Credant,dipastikan bahwa data-data pada komputer belum terenkripsi.

Aplikasi CMG (Credant Mobile Guardian) Shield akan diaplikasikan bersama dengan Windows Shield, CREDActivate dan CRED2GO. Setelah sistem melakukan *restart*, akan terdapat ikon *Credant* pada *system tray* yang menunjukkan bahwa *Credant* telah berhasil diimplementasikan.

3.2.1 Proses Verifikasi

Gambar 13. Proses Verifikasi aplikasi

Proses Verifikasi aplikasi dilakukan dengan menggunankan file CredActivate.exe dan dapat dilakukan setelah proses implementasi sistem *Credant* selesai. Proses Verifikasi dilakukan untuk mengoneksikan sistem *Credant* yang telah terimplementasi di komputer ke CMG Server yang memungkinkan proses enkripsi data pada komputer dapat dimulai.

3.2.2 Proses Enkripsi Credant

Setelah proses Verifikasi selesai, maka proses enkripsi akan dimulai setelah restart. Pada sistem keamanan data Credant, pada proses inilah data dienkripsi menggunakan algoritma Rijndael. Proses enkripsi data dapat ditampilkan sehingga akan terlihat data-data apa saja yang sedang dienkripsi.

Aplikasi SDE mengenkripsi data komputer menggunakan algoritma Rijndael *(AES=Advanced Encryption Standard)*. Pada sistem enkripsi Rijndael, data *plaintext* sebelum diubah menjadi *ciphertext* telah melalui pengacakan data sebanyak *n*-kali putaran, dimana jumlah putaran ini bergantung pada tingkat kompleksitas enkripsi. Untuk ukuran blok dan panjang kunci sebesar 128 bit ditentukan 10 putaran, sedangkan untuk ukuran blok 128 bit dan panjang kunci 256 bit jumlah putaran yang ditentukan adalah 14 putaran. Masing-masing putaran terdiri dari 4 proses utama yaitu SubBytes, ShiftRows, MixColumn dan AddRoundKey. File-file dalam komputer terenkripsi menggunakan USER DCID: LDL4ZY12 (unique key untuk user) dan Machine ID: 68KALI3E (unique key untuk komputer) yang kemudian menghasilkan file chipertext.

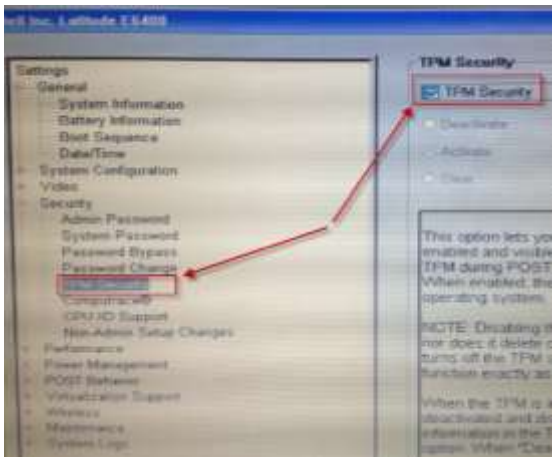
3.3 Implementasi BitLocker

BitLocker Drive Encryption yang digunakan untuk melakukan enkripsi drive adalah *BitLocker Drive Encryption* yang tersedia pada Sistem Operasi Windows.*BitLocker Drive Encryption* ini menggunakan algoritma enkripsi *Advanced Encryption Standard* (AES) pada mode *Chiper Block Chaining* (CBC) dengan 128 bit key.

3.3.1 Aktivasi BitLocker dan Konfigurasi TPM

Setelah proses aktivasi bitlocker dilakukan, sistem akan meminta untuk melakukan proses aktivasi TPM. Proses aktivasi TPM dapat dilakukan setelah komputer restart dengan memilih option "MODIFY" saat muncul pesan BIOS dan meminta persetujuan untuk mengaktifkan TPM hardware.

TPM Perlu diaktifkan karena pada komputer yang memiliki TPM, *BitLocker* menggunakan kemampuan keamanan yang ditingkatkan dari TPM untuk membantu memastikan bahwa data dapat diakses hanya jika komponen boot komputer tampak tidak berubah dan disk yang terenkripsi terletak di komputer yang sesungguhnya. Ketika pengguna mulai menjalankan sebuah sistem, TPM memeriksa integritas komponen boot awal dan data konfigurasi boot sebelum melepaskan kunci enkripsi dan memungkinkan Windows untuk mulai loading. Jika gangguan sistem terdeteksi (bisa berarti terdapat perubahan hardware atau hard disk tidak dipasang pada komputer yang benar), TPM tidak akan merilis kunci enkripsi *BitLocker* dan akan menempatkan sistem ke mode recovery. Proses aktivasi TPM terlihat pada gambar 3.4



Gambar 14. Proses aktivasi TPM

Proses enkripsi pada drive C akan berlangsung selama beberapa jam tergantung besarnya kapasitas drive. Proses enkripsi data yang sedang berjalan dapat diamati melalui progress bar enkripsi *BitLocker*.

3.3.2 Proses Enkripsi BitLocker

*BitLocker*menyimpan*recovery key* atau file kunci di *Storage Root Key* (SRK) yang terdapat pada *Trusted Platform Module* (TPM) chipset. SRK kemudian mengenkripsi *Volume Encryption Key* (VEK) yang diproteksi oleh TPM.VEK inilah yang disimpan pada hard drive di bagian Boot Patition. Sehingga, apabila potensi resiko keamanan terdeteksi, *BitLocker* akan mengunci drive dan akan meminta *recovery key* untuk mengakses sistem operasi.*BitLocker* telah diaktifkan pada Desktop A, terbukti dengan adanya ikon gembok pada kedua drive di Desktop A, seperti terlihat pada gambar 3.5

Gambar 15.*BitLocker* telah mengenkripsi Drive C dan Drive D

4. HASIL DAN PEMBAHASAN

4.1 Pengujian Ketahanan Keamanan Sistem Secara Lokal

Pengujian keamanan data pada sistem secara lokal dilakukan dalam beberapa skenario:

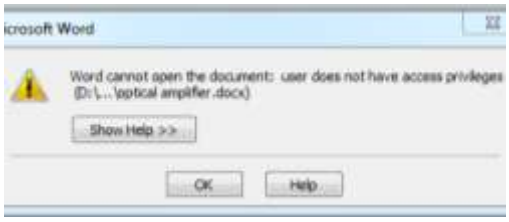
1. Komputer hilang/dicuri, login ke komputer menggunakan akun local Administrator.
2. Komputer digunakan oleh user lain (user lain dengan akun Active Directory pada domain DIR).
3. Memindahkan Hard Disk ke komputer lain untuk mengambil data di dalam Hard Disk.

4.1.1 Pengujian Keamanan Data Lokal: Komputer Hilang/Dicuri

Saat komputer hilang/dicuri, akan ada kemungkinan komputer diretas dan akun local administrator digunakan untuk login ke komputer. Pada

skenario pertama ini akan disimulasikan akses data ke Desktop A menggunakan akun local administrator: "slbadmin".Ketika data/file pada Desktop A coba diakses dengan menggunakan login akun "slbadmin", muncul pesan error seperti pada gambar 16. dan gambar 17.

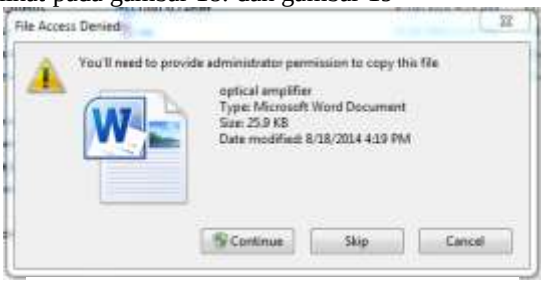
Gambar 16. File Microsoft PowerPoint tidak dapat diakses



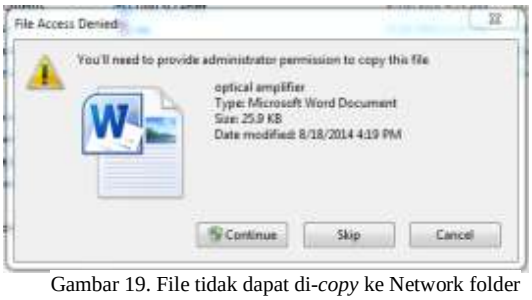
Gambar 17. File Microsoft Word tidak dapat diakses

Dengan tampilnya pesan error saat data/file pada Desktop A diakses menggunakan akun login local administrator, dapat dikatakan bahwa data/file **terproteksi**dari akses yang tidak diingin-kan.Dengan demikian Data/file telah **aman.**

Selanjutnya, data/file coba di-*copy* ke external hard disk dan ke network folder \\srv011jksm, hasilnya terlihat pada gambar 18. dan gambar 19



Gambar 18. File tidak dapat di-*copy* ke external hard disk



Gambar 19. File tidak dapat di-*copy* ke Network folder

Dari gambar 18. dan gambar 19. terlihat bahwa pesan error muncul, sistem **menolak** request *copy* data ke external hard disk dan ke network folder menggunakan login yang tidak diinginkan.Data/file **aman.**Dapat dikatakan bahwa data/file yang tersimpan di sistem **terproteksi** dari serangan local dengan login menggunakan akun local administrator.

4.1.2 Pengujian Keamanan Data Lokal: Akses data dilakukan oleh User Lain

Pengujian kedua dilakukan untuk skenario saat ada user lain yang memiliki akun pada Active Directory yang sama, namun ingin mencoba mengakses data menggunakan login akun user yang lain.

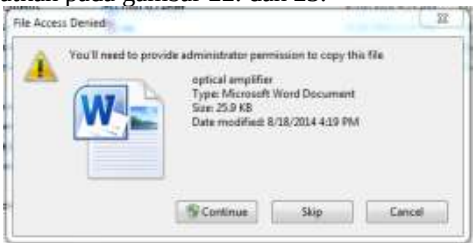
Pada simulasi ini, akun yang digunakan untuk login ke komputer adalah: "AHidayat3". Ketika data/file pada Desktop A coba diakses dengan menggunakan login "AHidayat3", muncul pesan error seperti pada gambar 20. dan gambar 21.

Gambar 20. File PDF tidak dapat diakses

Gambar 21. File Microsoft Word tidak dapat diakses

Dengan tampilnya pesan error saat data/file pada Desktop A diakses menggunakan login akun "AHidayat3", dapat dikatakan bahwa data/file **terproteksi** dari akses yang tidak diinginkan.Data/file **aman.**

Selanjutnya, data/file coba di-*copy* ke external hard disk dan ke network folder \\srv011jksm, hasilnya diperlihatkan pada gambar 22. dan 23.



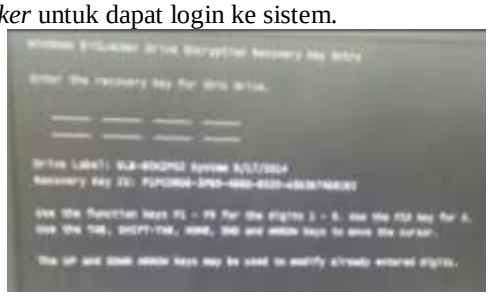
Gambar 22. File tidak dapat di-*copy* ke external hard disk

Gambar 23. File tidak dapat di-*copy* ke Network folder

Terlihat bahwa pesan error muncul, sistem **menolak** request *copy* data ke external hard disk maupun network folder menggunakan login yang tidak diinginkan.Data/file **aman.**Dengan demikian dapatdikatakan bahwa data/file yang tersimpan di sistem **terproteksi** dari serangan local dengan login menggunakan akun user lain.

4.1.3 Pengujian Keamanan Data Lokal: Hard Disk Dipindahkan ke Komputer Lain

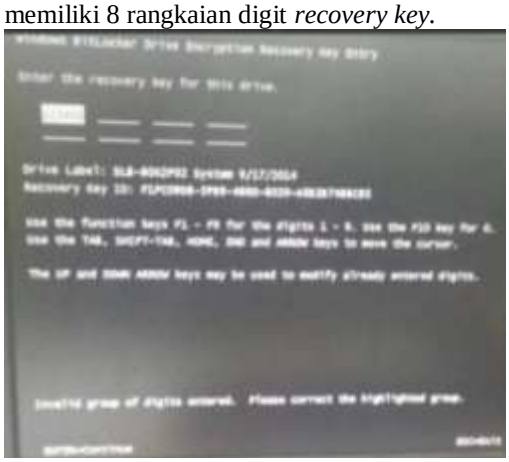
Pengujian selanjutnya adalah untuk mengamati ketahanan sistem dalam proteksi data/file dari serangan di level hardware. Pada pengujian ini, disimulasikan apabila hard disk dari komputer diambil dan dihubungkan ke komputer lain sebagai *secondaryhard drive*. Setelah dicoba untuk memindahkan hard disk ke PC lain, maka pada proses *booting up* Desktop B terhenti dan muncul layar hitam dimana pengguna harus memiliki 8 rangkaian digit (48 digit angka) *recovery key BitLocker* untuk dapat login ke sistem.



Gambar 24. Tampilan yang muncul di layar Desktop B saat *booting up* dengan Hard Drive Desktop A yang terproteksi dengan *BitLocker*

Apabila *recovery key* yang dimasukkan tidak sesuai, maka akan muncul peringatan bahwa digit yang dimasukkan salah dan diminta untuk mengubah digit tersebut: "*Invalid group of digits entered. Please correct the highlighted group"*

Dengan demikian, dapat dikatakan bahwa data/file pada Hard Disk Desktop A **terproteksi** dari kemungkinan pengambilan data dengan mengambil dan memasang Hard Disk ke komputer lain (Desktop B). Data-data dalam hard disk hanya dapat dibuka apabila user memiliki 8 rangkaian digit *recovery key.*



Gambar 25. Rangkaian *recovery key* yang dimasukkan salah

4.2 Pengujian Ketahanan Keamanan Sistem Dalam Jaringan Komputer

Pengujian keamanan data dalam suatu sistem jaringan komputer dilakukan setelah menghubungkan kedua desktop pada suatu jaringan komputer Local Area Network: Schlumberger Network. Pengujian ini dilakukan dalam 2 skenario:

1. Akses komputer menggunakan Windows Remote Desktop Assistance saat account "DSadiyahti" masih login ke Desktop A.
2. Akses komputer menggunakan Windows Remote Desktop Assistance saat account "DSadiyahti" telah logout dari Desktop A.

4.2.1 Akses Data Komputer Saat Account Pengguna Masih Login

Keamanan data di komputer tidak hanya rentan terhadap akses saat komputer berpindah tangan.Bisa juga terjadi saat-saat dimana terdapat percobaan akses komputer yang terhubung di jaringan.Pada skenario pertama, disimulasikan Desktop A dan Desktop B terhubung dalam jaringan LAN Schlumberger Network (SINet). User "DSadiyahti" masih login ke Desktop A. Pengguna Desktop B berusaha login ke Desktop A untuk mengambil data menggunakan Remote Desktop Connection dengan Nama komputer Desktop A: JKTSD11-DWI dan User name akun local administrator: JKTSD11-DWI\slbadmin.

Setelah melanjutkan proses uji, diketahui bahwa muncul pesan Credant yang memperlihatkan bahwa user lain telah melakukan login, dan login
Ditolak, hal ini terlihat pada gambar 26.. Kemudian, setelah beberapa detik, muncul pesan lanjutan bahwa sesi Remote Desktop Connection telah berakhir, terlihat pada gambar 27.

Gambar 26. Akses ditolak oleh *Credant*

Gambar 27.Sesi Remote Desktop Connection berakhir secara otomatis

Dengan demikian, dapat dikatakan bahwa data/file di Desktop A**aman** dari usaha pengambilan data menggunakan Remote Desktop Connection saat pengguna Desktop A masih melakukan login.

4.2.2 Akses Data Komputer Saat Account Pengguna Telah Logout

Pengujian selanjutnya adalah percobaan akses data Desktop A saat pengguna tidak melakukan login (pengguna Desktop A telah logoff dari sistem).Seperti pada pengujian sebelumnya, pada Desktop B, Windows Remote Desktop Connection dibuka dan dilanjutkan dengan memasukkan nama komputer Desktop A: JKTSD11-DWI dan User name akun local administrator: JKTSD11-DWI\slbadmin, lalu click Connect.

Diketahui bahwa user Desktop B berhasil masuk ke sistem Desktop A menggunakan Remote Desktop Connection.Namun, meski user Desktop B dapat masuk ke sistem Desktop A, namun saat dicoba untuk akses data/file, error muncul, usaha akses data ditolak karena data terenkripsi oleh *Credant*, hal ini terlihat pada gambar 28. dan gambar 29.

Gambar 28. File Microsoft Word tidak dapat diakses

Gambar 29. File PDF tidak dapat diakses

Dengan demikian, dapat dikatakan bahwa data/file di Desktop A**aman** dari usaha pengambilan data menggunakan Remote Desktop Connection saat pengguna Desktop A telah logoff dari sistem.

Hasil dari pengujian sistem keamanan data di Desktop A di level user menunjukkan bahwa data/file pada sistem yang terinstal *Credant* **aman dari serangan secara lokal pada level user.** Data user tidak dapat diakses apabila komputer digunakan oleh akun local administrator atau akun lain (baik yang terdaftar di Active Directory yang sama maupun tidak).

Sebelum komputer terenkripsi dengan *Credant*, data pada komputer dapat diakses oleh siapa saja (oleh akun user apapun, baik akun administrator maupun akun user lain dalam satu domain yang sama). Namun, setelah komputer terproteksi dengan *Credant* data yang tersimpan pada komputer hanya dapat diakses oleh user yang memiliki USER DCID: LDL4ZYI2. Pengguna komputer lain (baik menggunakan local administrator maupun akun lain) tidak dapat mengakses data karena data telah terenkripsi oleh unique USER ID: LDL4ZYI2. Dapat dikatakan bahwa tingkat keamanan data telah meningkat dari yang sebelumnya dapat diakses semua akun tanpa terkecuali, kini data hanya dapat diakses oleh akun user tertentu yang memiliki USER ID yang sama dengan yang digunakan dalam proses enkripsi.

Sedangkan hasil pengujian sistem keamanan Desktop A pada sisi hardware dapat diamati dengan munculnya jendela *recovery key* saat hard disk berusaha dipindahkan ke komputer lain. Hal ini membuktikan bahwa Desktop A**aman dari serangan secara lokal pada level drive (hardware)**.

Dengan demikian dapat dikatakan bahwa sistem komputer dengan enkripsi *Credant*dan *Bitlocker***aman dari serangan secara lokal pada level user dan level Drive (hardware).** Saat peretas berusaha mengambil data dengan login sebagai user lain, peretas tidak akan dapat mengakses data karena data-data dalam komputer telah terenkripsi menggunakan unique USER ID melalui implementa
si*Credant.* Selain itu, usaha untuk mengambil data dengan memindahkan hard disk pun akan gagal karena hard disk telah terenkripsi/ terkunci sepenuhnya oleh BitLocker.

4.3.2 Hasil Data Pengujian Keamanan Data Terhadap Serangan di Jaringan Komputer

Hasil pengujian keamanan sistem terhadap usaha akses data/file di Desktop A menggunakan Remote Desktop Connection, baik saat user Desktop A masih melakukan login maupun saat user telah logoff, **tidak berhasil** karena data/file dalam sistem telah terenkripsi. Ini membuktikan bahwa sistem aman dari serangan menggunakan Remote Desktop Encryption.

5. SIMPULAN

Implementasi Credant dan BitLocker pada suatu komputer, data/informasi yang tersimpan menjadi lebih aman dari serangan/usaha akses data yang tidak diinginkan secara langsung maupun melalui jaringan baik di level user maupun hardware, karena data telah terenkripsi menggunakan Credant pada level user dan hard disk telah terenkripsi seluruhnya menggunakan BitLocker.

Credant mampu memberikan keamanan data dari serangan lokal, baik serangan menggunakan akun local administrator maupun akun lain yang terdaftar dalam Active Directory yang sama, karena data tenenkripsi dengan algoritma rijndael menggunakan user ID yang telah ditentukan, serta mampu memberikan keamanan data dari serangan pada jaringan dengan menggunakan Remote Desktop Connection,

baik saat pengguna masih login maupun setelah pengguna logout dari komputer.

BitLocker adalah sebuah fitur enkripsi full-disk yang melindungi data pada level hardware dengan melakukan enkripsi terhadap keseluruhan partisi hard drive, serta mampu memproteksi data/informasi pada komputer dari usaha pengambilan data dengan pencurian hard disk, karena saat hard drive dipindahkan ke komputer lain, data tidak akan dapat diakses kecuali tersedia *recovery key*.

DAFTAR PUSTAKA

Dang, Anh, 2010. *SDE FAQ and Technical Data*. April,. (online) melalui http://www.hub.slb.com/sde

Felix, Fidens.2010.*Dasar Kriptografi*, (online) melalui http://ikc.depsos.go.id/umum/fidens-dasarkriptografi.php, (diakses November 2014).

Hasan, Rusydi.2013.*Mengenal Algoritma DES*, (online) melalui http://pustaka.unpad.ac.id/wp-content/uploads/2009/06/enkripsi_dan_dekripsi_data_dengan_algoritma_3_des.pdf (diakses Oktober 2014).

IEEE.(2011).IEEE P1619/D20Draft Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices.New York, USA.

Kromodimoeljo, Sentot.2009.Teori dan Aplikasi Kriptografi.SPK IT Consulting, Jakarta.

Kwang, H. Lee.*Basic Encryption and Decryption.Department of Electical Engineering & Computer Science*, KAIST.

Pfleeger, Charles P.2010. *Security in Computing Second Edition. Prentice-Hall International. Inc*, New Jersey.

Rinaldi Munir.2006.*Kriptografi*.Informatika Bandung, Bandung.

Stallings, William.2011.*Cryptography and Network Security : Principles and Practice (5th Edition), Prentice Hall, United States of America.*

Vanstone.1996.*Handbook of Applied Cryptography*.CRC Press, USA.A. Menezes, P. van Oorschot, S.