PENERAPAN METODE 3DES PADA KEAMANAN FILE DOKUMEN "BILL OF MATERIAL" PT WE TECH INDONESIA MENGGUNAKAN PHP

Tri Wahyana [1)],Tri Masruroh[2)]
[1)]Program Studi Manajemen Informatika, Universitas Panca Sakti Bekasi
email : triwahyana4330@gmail.com
[2)]Program Studi Teknik Informatika, Universitas Panca Sakti Bekasi
E-mail : trimasruroh.tm@gmail.com

ABSTRAKSI

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data atau informasi. Terdapat banyak sekali ancaman – ancaman dari luar, maupun ancaman dari dalam yang mengancam keamanan data. Pada PT We Tech Indonesia memiliki data yang sangat penting sehingga tidak semua diijinkan mengakses. Data terebut adalah *file Bill Of Material* yang digunakan untuk proses manufakture ICT fixture. Saat ini proses akses file melalui *share* folder tanpa ada kemanannya sehingga penulis melakukan penelitian untuk meningkatkan keamanan *file* tersebut dengan cara kriptografi *file Bill of material* menggunakan metode 3DES dengan mode operasi CBC. Pengimplementasian sistem sudah dibagi untuk beberapa bagian yaitu admin, member, pimpinan dan *guest.* Keseluruhan kinerja user saling berkesinambungan sehingga aksesnya dapat termonitor. Pengujian dengan menggunakan *black box testing* Dari hasil pengujian tersebut maka dapat disimpulkan bahwa sistem ini layak untuk digunakan.

Kata kunci : Kriptografi , 3DES , Keamanan Data, CBC, Bill Of Material

1. PENDAHULUAN

Menghadapi era Revolusi Industri 4.0 masyarakat harus dapat memahami dinamika yang muncul dan mempersiapkan diri untuk perubahan yang akan terjadi ke depannya. Salah satu contoh perubahan drastis yang terjadi sekarang adalah ketergantungan kita terhadap teknologi internet. Internet menjadi sarana untuk berkomunikasi dan memenuhi beragam kebutuhan sehari-hari. Namun, perlu diingat bahwa akhir-akhir ini marak terjadi serangan *cyber* serta adanya penyalahgunaan data. Mewujudkan kesadaran akan keamanan *cyber* dapat dimulai dari diri sendiri. Hal yang paling sederhana adalah dengan memahami pemanfaatan *Internet of Things* di sekitar untuk menjamin keamanan dari data dan privasi di dunia maya. Contohnya adalah dengan secara rutin mengganti kata sandi akun email dan media sosial serta memanfaatkan *software* yang resmi.

Kriptografi merupakan salah satu ilmu pengkodean pesan yang digunakan untuk meningkatkan keamanan dalam pengiriman pesan atau komunikasi data. Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi dalam pengiriman pesan penting dan rahasia. Pengiriman pesan penting dan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim, dan hal-hal yang merugikan lainnya.

Salah satu metode kriptografi adalah metode algoritma *Triple Data Encryption Standard* (3DES). Metode algoritma 3DES merupakan pengembangan dari metode algoritma *Data Encryption Standard* (DES). Dengan menggunakan metode algoritma 3DES, kata kunci akan dienkripsi terlebih dahulu pada saat disimpan dan kemudian didekripsi pada saat proses verifikasi.

PT. We Tech Indonesia merupakan salah satu perusahaan asing di Indonesia yang bergerak di bidang *manufaktur*. Dalam proses pembuatannya yaitu mengolah data untuk *Computer Numerical Control* (CNC) dan program dimana dalam proses program tersebut membutuhkan *Bill Of Material* yang berisi spesifikasi komponen yang data tersebut sangat rahasia. Saat ini file *Bill Of Material* belum ada keamanan sehingga ketika menerima file bisa diakses oleh siapa saja. Hal ini dapat berdampak pada kebocoran *file*, yang tentunya menguntungkan bagi pihak kompetitor.

Dalam penelitian ini sistem yang akan dibangun adalah mengubah dokumen dalam bentuk yang tidak dapat dikenali agar kerahasiaannya dapat terjaga dan monitoring akses file. Oleh karena itu salah satu metode yang digunakan untuk mengamankan dokumen ialah metode enkripsi dan dekripsi.

2. LANDASAN TEORI

2.1 kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian *modern* kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adlah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

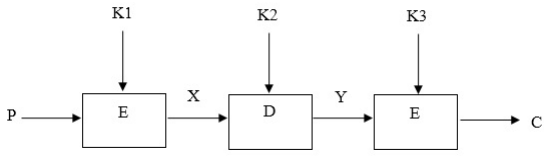
Sistem Kripdtografi terdiri dari 5 bagian yaitu (Rifki Sadikin, 2012:15)

1. *Plaintext* : pesan atau data dalam bentuk aslinya yang dapat terbaca. *Plaintext* adalah masukan bagi algoritma enkripsi. Untuk selanjutnya digunakan istilah *text* asli sebagai padanan kata *plaintext*.

2. *Secret key* : *secret key* yang juga merupakan masukan bagi algoritma enkripsi merupakan nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi. Untuk selanjutnya digunakan istilah kunci rahasia sebagai padanan kata *secret key*.
3. *Ciphertext* : *ciphertext* adalah keluaran algoritma enkripsi. *Ciphertext* dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan ciphertext yang terlihat acak. Untuk selanjutnya digunakan istilah *text* sandi sebagai penanda kata *ciphertext*.
4. Algoritma enkripsi : algoritma enkripsi memiliki dua masukan yaitu teks sandi dan kunci rahasia. Algoritma enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan teks sandi.
5. Algoritma dekripsi : algoritma dekripsi memiliki dua masukan yaitu teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai algoritma dekripsi sama dengan kunci rahasia yang dipakai algoritma enkripsi.

2.2 Metode 3 DES

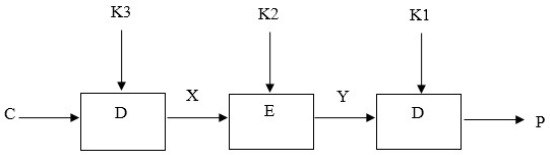
3DES merupakan algoritma pengembangan dari algoritma DES. algoritma 3DES menggunakan *cipher Data Encryption Standard* (DES) tiga kali untuk mengenkripsi datanya. Dibawah ini adalah skema 3DES dengan 3 kunci:



Gambar 2.1. Skema Enkripsi 3DES

Proses Enkripsi 3DES adalah sebagai berikut :
1. Enkripsi blok *plaintext* menggunakan DES tunggal dengan kunci K1.
2. Dekripsi *output* dari langkah 1 menggunakan DES tunggal dengan kunci K2.
3. Enkripsi *output* langkah 2 menggunakan DES tunggal dengan kunci K3.

Output dari langkah 3 adalah *ciphertext*.



Gambar 2.2. Skema Enkripsi 3DES

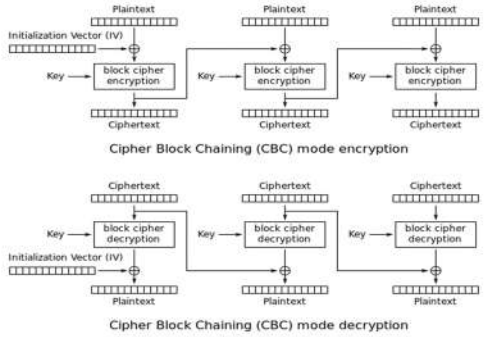
Proses Dekripsi 3DES adalah sebagai berikut :
1. Dekripsi blok *plaintext* menggunakan DES tunggal dengan kunci K3.
2. Enkripsi *output* dari langkah 1 menggunakan DES tunggal dengan kunci K2.
3. Dekripsi *output* langkah 2 menggunakan DES tunggal dengan kunci K1.

Output dari langkah 3 adalah *plaintext*.

2.3 Mode Operasi CBC

Mode operasi yang dapat diterapkan pada algoritma kriptografi penyandi blok Triple DES salah satunya adalah *Cipher Block Chaining* (CBC). Caranya, blok *plainteks* yang *current* di-XOR-kan terlebih dahulu dengan blok *cipherteks* hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan mode CBC, setiap blok *cipherteks* bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya.

Dekripsi dilakukan dengan memasukkan blok *cipherteks* yang *current* ke fungsi dekripsi, kemudia meng-XOR-kan hasilnya dengan blok *cipherteks* sebelumnya. Dalam hal ini, blok *cipherteks* sebelumnya berfungsi sebagai umpan maju maju *(feedforward)* pada akhir proses dekripsi.



Gambar 2.3. Skema Enkripsi Dan Dekripsi Dengan Mode CBC

2.4 File Bill Of Material

Bill of materials (BOM) berisi daftar komponen yang nilainya akan digunakan untuk proses produksi. Agar efektif, BOM perlu mencakup tidak hanya bahan baku tetapi juga sub-rakitan, subkomponen, dan bagian serta jumlah masing-masing yang tepat.Format yang tepat untuk BOM akan bervariasi tergantung pada sifat produk yang diproduksi, tetapi itu adalah khas untuk dua jenis BOM yang berbeda untuk dikaitkan dengan masing-masing produk, satu digunakan untuk tahap rekayasa ketika suatu produk pertama kali dikembangkan, dan tipe BOM lain yang digunakan saat produk diluncurkan untuk produksi massal untuk dikirim ke pelanggan.

2.5 Pengujian Software

Pengujian *software* sangat diperlukan untuk memastikan *software*/aplikasi yang sudah/sedang dibuat dapat berjalan sesuai dengan fungsionalitas yang diharapkan. Pengembang atau penguji *software* harus menyiapkan sesi khusus untuk menguji program yang sudah dibuat agar kesalahan ataupun kekurangan dapat dideteksi sejak awal dan dikoreksi secepatnya. Pengujian atau testing sendiri merupakan elemen kritis dari jaminan kualitas perangkat lunak dan merupakan bagian yang tidak terpisah dari siklus hidup

pengembangan *software* seperti halnya analisis, desain, dan pengkodean. (Shi, 2010).
Black-Box Testing merupakan pengujian yang berfokus pada spesifikasi fungsional dari perangkat lunak, tester dapat mendefinisikan kumpulan kondisi *input* dan melakukan pengetesan pada spesifikasi fungsional program. (Khan, 2011).

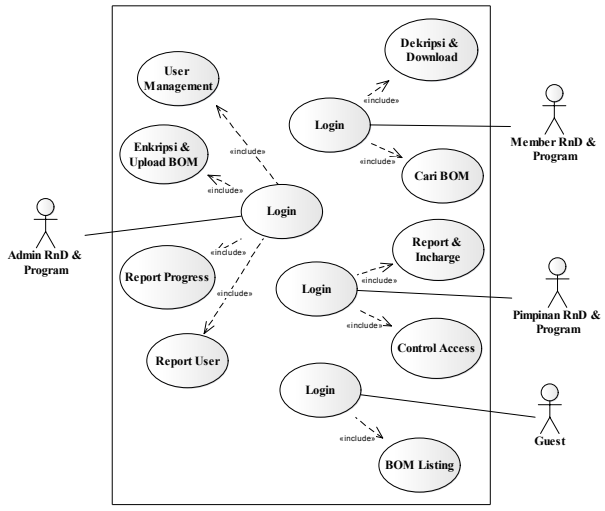
3. RANCANGAN SISTEM DAN APLIKASI

Sistem yang dibangun merupakan suatu sistem yang memproses enkripsi dan dekripsi file dokumen dengan ekstansi txt. Pada sistemi ini terdapat satu *user* yaitu admin yang melakukan enkripsi dan dekripsi. Member hanya bisa melakukan proses dekripsi dan pimpinan dapat melakukan monitoring terhadap akses file. Sistem ini berbasis *web base* yang dibangun dengan Bahasa PHP dengan menggunakan algoritma Triple DES.

3.1 Use Case Diagram

Dalam tahap perancangan digunakan *use case diagram* untuk menggambarkan fungsionalitas sistem yang dilakukan oleh pengguna. Pengguna dapat melakukan beberapa proses saat memulai menggunakan sistem. *Use case diagram* sistem ditunjukan pada Gambar 4. Proses yang dilakukan pengguna adalah:

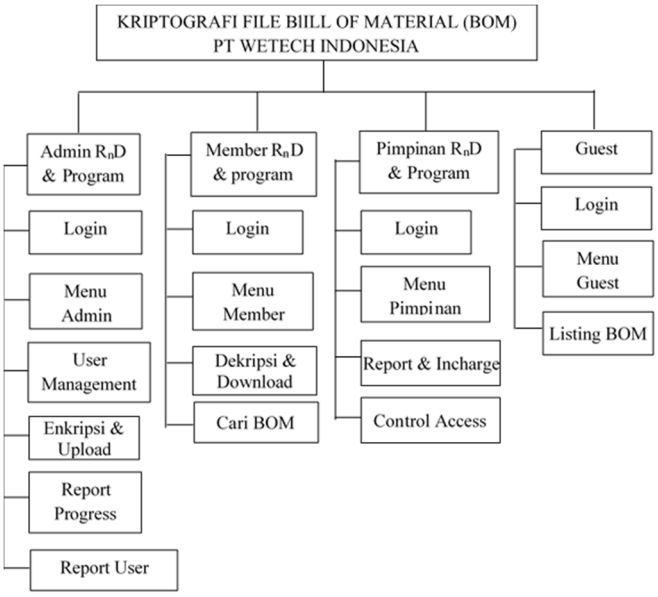
1. Untuk mengkses dan menggunakan sistem pertama yang harus dilakukan oleh admin, member & pimpinan R_nD & Program adalah login ke sistem keamanannya.
2. Admin R_nD & Program memasukkan *password* untuk masuk ke sistem keamanan kemudian upload *file Bill Of Material* (BOM) yang berbentuk teks untuk selanjutnya dilakukan proses enkripsi file. Admin juga dapat menambah *user* atau pengguna baru serta dapat membaca *report* akses *file Bill Of Material* (BOM).
3. Member R_nD & Program memasukkan *password* untuk masuk ke sistem keamanan kemudian pilih menu *download* & dekripsi *file* untuk mengambil *file Bill Of Material* (BOM) yang dibutuhkan.
4. Pimpinan R_nD & Program Program memasukkan *password* untuk masuk ke sistem keamanan kemudian menampilkan *report* akses *file Bill Of Material* (BOM).
5. Guest memasukkan username & password yang sudah ditentukan oleh sistem, kemudian dapat melihat daftar *file Bill Of Material* (BOM) yang sudah terenkripsi.



Gambar 3.1. Use Case Diagram Sistem Usulan

3.2 Rancangan Antar Muka Sistem

Rancangan antar muka sistem merupakan tampilan program yang akan dibuat pada sistem. Berikut struktur menu-menu yang akan dirancang pada Penerapan Metode 3DES pada Keamanan File Dokumen *Bill of Material* (BOM) PT We Tech indonesia.

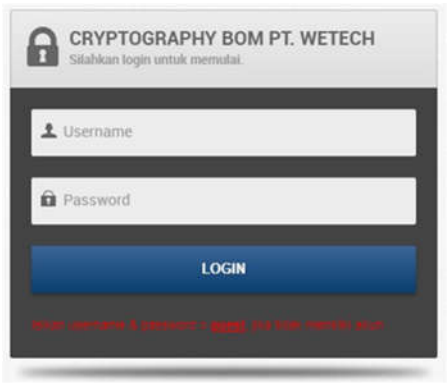


Gambar 3.2. Rancangan Antar Muka Sistem

4. HASIL DAN PEMBAHASAN

4.1 Halaman Login

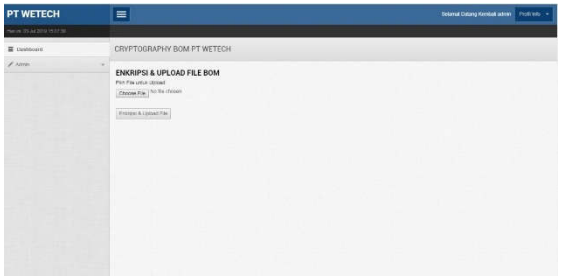
Halaman ini merupakan halaman login untuk masuk ke masing-masing bagian . pengisian untuk *username* & *password* , *button* masuk untuk proses ke halaman selanjutnya.



Gambar 4.1. Halaman Login

4.2 Halaman untuk Enkripsi & Upload

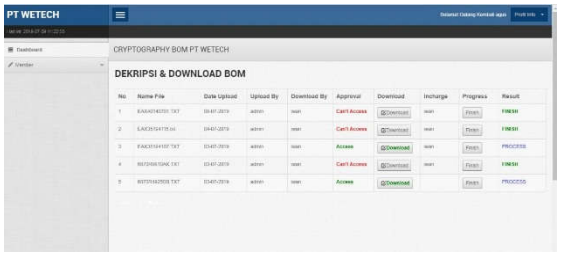
Menu Enkripsi & Upload adalah halaman untuk enkripsi & upload file Bill Of Material. Terdapat 2 button yaitu button choose file untukmemilih file BOM yang akan dienkripsi & upload. Button enkripsi & upload untuk proses enkripsi & upload setelah memilih file.



Gambar 4.2. Tampilan Menu Enkripsi & Upload

4.3 Halaman untuk Dekripsi & Download

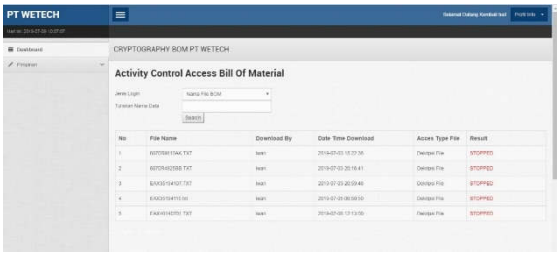
Menu Dekripsi & Download BOM adalah halaman untuk dekripsi & download file BOM yang dibutuhkan serta konfirmasi finish jika project yang menggunakan file BOM tersebut selesai dikerjakan.



Gambar 4.3. Tampilan Menu Dekripsi & Download

4.4 Halaman Report

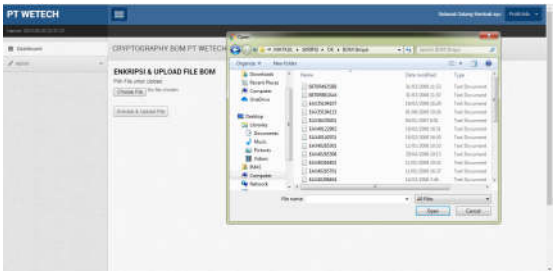
Menu Control Access BOM berisi data berupa nama file, download by, date time download, access type file dan result. Dapat melakukan pencarian data langsung berdasarkan nama file dan siapa yang mendownload.



Gambar 4.4. Tampilan Menu Control Access BOM

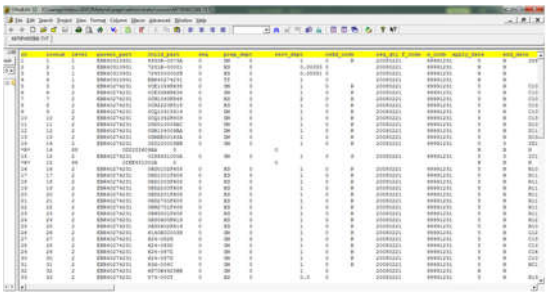
4.5 Pengujian Enkripsi Dokumen

Untuk melakukan enkripsi *file bill of material*, maka pengguna harus masuk ke menu Enkripsi & Upload. kemudian akan tampil pencarian dokumen yang ingin di enkripsi. Tampilan pencarian dokumen yang ingin dienkripsi dapat dilihat pada gambar 10.



Gambar 4.5. Pencarian Dokumen

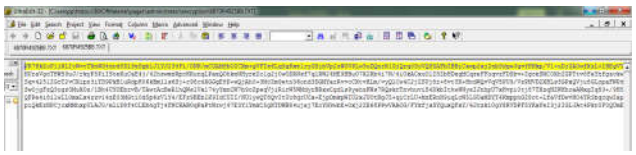
Dalam pengujian enkripsi, dokumen yang dipilih dapat dilihat pada gambar 14 yang merupakan dokumen berekstensi txt yang berisikan komponen penting untuk pembuatan produk.



Gambar 4.6. File Asli "6870R4925BB.TXT"

4.6 Pengujian Dekripsi Dokumen

Dalam pengujian dekripsi, dokumen yang akan dipilih ialah dokumen berekstensi txt yang telah terenkripsi berisikan kalimat yang tidak dapat dikenali. Hasil dari proses dekripsi dapat dilihat pada gambar 12.



Gambar 4.7. File Enkripsi "6870R4925BB.TXT"

4.7 Pengujian Black Box Testing pada Sistem

pengujian sistem dilakukan untuk mengetahui apakah sistem yang dibuat sudah bekerja sesuian dengan fungsinya atau belum.

Tabel 4.1. Hasil Pengujian Black Box Testing Login Admin R_nD & Program

No	Skenario pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Username dan Password tidak diisi kemudian klik tombol Login	Username: (kosong) Password: (kosong)	Sistem akan menolak dan menampilkan pesan "Maaf, username atau password salah"	Sesuai harapan	Valid
2	Mengetikkan Username, dan password tidak diisi atau kosong kemudian klik tombol Login	Username: ayu Password: (kosong)	Sistem akan menolak dan menampilkan pesan "Maaf, username atau password salah"	Sesuai harapan	Valid
3	Mengetikkan Password, dan username tidak diisi atau kosong kemudian klik tombol Login	Username: (kosong) Password: ayu	Sistem akan menolak dan menampilkan pesan "Maaf, username atau password salah"	Sesuai harapan	Valid
4	Mengetikkan Username dan/atau password tidak sesuai, kemudian klik tombol Login	Username: adm Password: adm123	Sistem akan menolak dan menampilkan pesan "Maaf, username atau password salah"	Sesuai harapan	Valid
5	Mengetikkan Username dan password yang sesuai, kemudian klik tombol Login	Username: ayu Password: ayu	Sistem menerima akses login dan kemudian menampilkan halaman utama Admin	Sesuai harapan	Valid

Tabel 4.2. Hasil Pengujian Black Box Testing Menu Enkripsi & Upload

No	Skenario pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Memilih file dengan menekan button choose file, lakukan enkripsi dan upload file dengan menekan button enkripsi & upload	Mengklik enkripsi & upload tanpa memilih file yang akan diproses	Sistem menampilkan pesan "no file specified"	Sesuai harapan	Valid
2	Memilih file dengan menekan button choose file, lakukan enkripsi dan upload file dengan menekan button enkripsi & upload	Memilih file yang akan diproses dan klik button enkripsi & upload	Sistem menampilkan informasi tentang file yang diproses	Sesuai harapan	Valid

Tabel 4.3. Hasil Pengujian Black Box Testing Menu Dekripsi & Download BOM

No	Skenario pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Menekan button download	klik button download pada kolom download	Sistem dapat melakukan download file dekripsi	Sesuai harapan	Valid
2	Menekan button finish	Klik button finish pada kolom progress	Sistem akan menampilkan "finish" pada kolom result	Sesuai harapan	Valid

Tabel 4.4. Hasil Pengujian Black Box Testing Menu Utama Pimpinan R_nD & Program

No	Skenario pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Menekan button masuk	Klik button masuk pada Report & Incharge BOM	Sistem menampilkan halaman menu Report & Incharge BOM	Sesuai harapan	Valid
2	Menekan button masuk	Klik button masuk pada Control Access BOM	Sistem menampilkan halaman menu Control Access BOM	Sesuai harapan	Valid

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil penelitian dan implementasi Metode 3DES *(3-Data Encryption Standard)* pada keamanan *file bill of material*, dapat diperoleh kesimpulan berdasarkan hasil implementasi dan pengujian yang dilakukan penulis selama proses pengerjaan skripsi sebagai berikut :

1. Algoritma Kriptografi 3DES *(3-Data Encryption Standard)* dapat diimplementasikan pada *file Bill Of Material* dengan melakukan enkripsi dan dekripsi isi file sehingga file tersebut tidak bisa diakses oleh orang yang tidak memiliki kepentingan.
2. Sistem yg dibuat dapat melakukan monitoring proses akses *file Bill Of Material* sehingga seluruh aktivitas pemakaian *file Bill Of Material* pada PT We Tech terkontrol.

5.2 Saran

Dalam pembuatan sistem kriptografi pada penelitian ini masih terdapat kekurangan sehingga perlu disempurnakan untuk hasil yang lebih baik lagi. Saran yang dapat diberikan penulis untuk melakukan penyempuraan penelitian ini adalah sebagai berikut :

1. Sistem ini dikembangkan dengan metode kriptografi lain, yang mempunyai spesifikasi keamanan lebih tinggi tanpa merusak integritas file tersebut.
2. Sistem kriptografi yang dibuat bisa diintegrasikan dengan sistem lain yang ada di tempat penelitian.

DAFTAR PUSTAKA

Gravell, H., & Rees, R. (2004). *Microeconomics* (3rd ed.). Harlow: Pearson Education Limited.

Khan, Mohd Ehmer, 2011, Different Approach to Blackbox Testing Technique for Finding Error, International Journal of Software Engineering & Applications (IJSEA), Vol.2, No.4, October 2011

Kristanto, A. (2018). *Perancangan Sistem Informasi dan Aplikasi.* Yogyakarta: Penerbit Gavamedia.

MF, M. (2018). *Buku Sakti Pemrograman Web seri PHP*. Bandung: Informatika Bndung.

Mukhtar, H. (2018). *Kriptografi untuk keamana Data.* Yogyakarta: CV Budi Utama.

Nurcholish, A. (2018). *Membangun Database Arsip Persuratan Menggunakan Pemrograman PHP dan MySQL.* Sukabumi: CV Jejak.

Raharjo, B. (2018). *Belajar Otodidak Framework Codeigniter.* Bandung : Informatika Bandung.

S, R., & Salahudin, M. (2015). *Rekayasa Perangkat Lunak.* Bandung: Informatika.

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: CV Andi Offset.

Samuelson, P., & Nordhaus, W. (2005). *Economics* (18th ed.). New York: Mc-Graw Hill.

Shi, Mingtao, 2010, Software Functional Testing from the Perspective of Business Practice Computer and Information Science, www.ccssenet.org/cis

Suprapto, F. (2018). *Rekayasa Peragkat Lunak.* Jakarta: Lentera Ilmu Cendekia.

Widodo, P. P., & Herlawati. (2011). *Menggunakan UML.* Bandung: Informatika Bandung.

Winarto, E., & Zaky, A. (2014). *24 Jam Belajar PHP*. Semarang: PT Elex Media Komputindo.