PENGAWALAN SISTEM KESELAMATAN PENGURUSAN MAKLUMAT PESAKIT MENGGUNAKAN TEKNIK PIAWAIAN PENYULITAN TERKEHADAPAN (AES)

NURUL RAIHANAH HAZMAN
RAVIE CHANDREN MUNIYANDI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Dewasa ini, pengkomputeran di atas talian merupakan suatu yang penting bagi memudahkan suatu pengurusan maklumat. Hal ini kerana, maklumat dapat diurus dengan baik dan mudah untuk dicapai. Sebagai contoh, pengurusan maklumat pesakit di pusat-pusat perubatan. Namun, pada masa yang sama terdapat risiko dari segi privasi dan keselamatan ke atas maklumat peribadi pesakit. Objektif kajian ini adalah untuk membangunkan satu pengawalan sistem keselamatan pengurusan maklumat pesakit menggunakan teknik Piawaian Penyulitan Terkehadapan (AES) yang bertujuan bagi melindungi maklumat pesakit daripada dicerobohi atau hilang. PHP dan JavaScript merupakan bahasa pengaturcaraan yang paling utama dalam membangunkan sistem ini. Segala maklumat pesakit yang telah disulit akan disimpan dalam pangkalan data yang diuruskan oleh kakitangan perubatan.

1 PENGENALAN

Pada era yang serba canggih dengan kedatangan teknologi telefon pintar ini, industri kesihatan juga tidak ketinggalan untuk bersaing seiring dengan permintaan teknologi oleh rakyat sekeliling. Sistem pengurusan maklumat merupakan satu platform penting untuk menyimpan, mengurus dan mengakses data. Semua maklumat kesihatan dan rekod peribadi akan disimpan rapi untuk digunakan oleh pengguna dengan selamat. Keselamatan sesuatu maklumat dan rekod kesihatan seseorang pesakit seperti maklumat kebenaran pembedahan atau kehendak pesakit mengenai pendermaan organ untuk orang lain adalah sangat dilindungi dan sulit. Hal ini amat penting untuk memberi kepercayaan kepada pesakit agar mereka berasa selamat untuk berkongsi maklumat kesihatan. Seterusnya, dapat memudahkan pihak kesihatan berurusan bersama pesakit.

Namun, laporan Symantec menunjukkan bahawa industri kesihatan menyumbang 36% daripada jumlah pelanggaran kes keselamatan pada tahun 2013 dan industri kesihatan perlu bertanggungjawab terhadap peratusan yang terbesar kepada pelanggaran kes

pendedahan data kesihatan pesakit (Symantec, 2013). Organisasi yang bertanggungjawab seharusnya mengambil pengajaran dan iktibar daripada kejadian tersebut agar kejadian pendedahan data kesihatan pesakit tidak berlaku lagi. Ini adalah disebabkan oleh sistem pengawalan data kesihatan pesakit yang longgar dan tidak menggunakan teknik penyulitan yang betul.

Ancaman dalam dunia siber adalah tanpa batas dan tidak nyata, sistem keselamatan menggunakan teknik Piawaian Penyulitan Terkehadapan (AES) merupakan salah satu penyelesaian bagi semua sektor yang memerlukan fungsi penyulitan termasuk industri kesihatan masa kini.

2 PENYATAAN MASALAH

Untuk membangunkan sebuah sistem yang berkesan, masalah sistem tersebut perlu dikenal pasti dan dikaji. Antara penyataan masalah bagi sistem keselamatan maklumat pesakit ini ialah kurang pengawalan bagi hak akses masuk terhadap sistem. Hal ini menyebabkan individu yang tidak bertanggungjawab dan tidak berdaftar mampu akses masuk seterusnya menyalahgunakan dengan mendedahkan maklumat rekod kesihatan oleh pesakit berdaftar tanpa kebenaran pihak berkuasa.

Selain itu, kurang pengawalan keselamatan bagi menjaga dan menyimpan maklumat rekod pesakit. Penggodam yang licik boleh menggodam data dengan menukar data pesakit atau merosakkan sistem klinikal, mengetahui masalah pengurusan data jangka panjang dan campur tangan kerajaan terhadap hal-hal kesihatan dari organisasi kesihatan swasta.

3 OBJEKTIF KAJIAN

Objektif bagi projek ini adalah untuk membangunkan satu pengawalan sistem keselamatan pengurusan maklumat pesakit menggunakan teknik Piawaian Penyulitan Terkehadapan (AES) yang bertujuan bagi melindungi maklumat pesakit daripada dicerobohi atau hilang.

Kertas ini membincang tentang projek pembangunan untuk membuat pengujian terhadap sistem keselamatan pengurusan maklumat pesakit untuk melihat keupayaan fungsi algorithma AES ini. Seterusnya, kertas ini juga menjelaskan bagaimana algorithma AES beroperasi terhadap sistem keselamatan pengurusan maklumat pesakit.

4 METOD KAJIAN

Penggunaan model pembangunan yang sesuai penting untuk memastikan perjalanan projek berjalan dengan lancar dan menjamin hasil kerja yang berkualiti. Model sistem keselamatan data pesakit menggunakan teknik AES yang digunakan ialah Model Air Terjun melibatkan beberapa fasa pembangunan dan ditambah dengan penggunaan perisian dan perkakasan yang bersesuaian. Fasa pembangunan termasuk fasa perancangan, analisis, reka bentuk, pengujian dan dokumentasi. Model ini penting untuk memastikan perjalanan projek lancar dan teratur. Rajah 1 menunjukkan model pembangunan yang diguna untuk membina proses sistem keselamatan data pesakit menggunakan teknik AES.

4.1 Fasa Perancangan

Fasa ini melibatkan proses pengenalpastian masalah, objektif, persoalan kajian dan menentukan skop. Langkah seterusnya adalah kajian susastera yang melibatkan pengumpulan, pencarian dan pembacaan jurnal dan kajian lepas bagi menjana idea dan inspirasi. Contoh topik-topik yang berkaitan yang dikaji terutama berkaitan dengan konsep reka bentuk sistem sistem keselamatan data pesakit yang sedia ada dan proses serta fungsi algorithma AES beroperasi. Penggunaan internet untuk mencapai maklumat berkaitan dan pencarian bahan di Perpustakaan Tun Seri Lanang Universiti Kebangsaan Malaysia dilakukan. Maklumat dikumpul, distruktur dan disintesis dan dipersembah secara kritis dan kreatif dalam fasa analisis.

4.2 Fasa Analisis

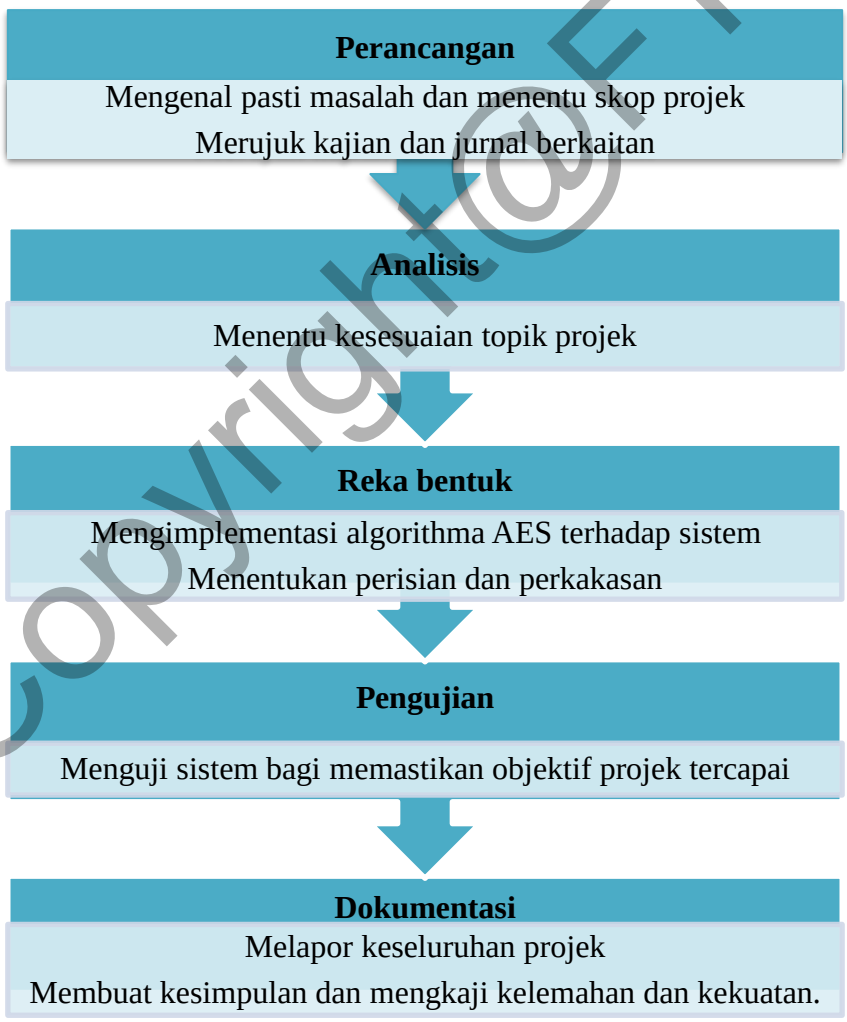
Fasa ini melibatkan analisis dan tafsiran maklumat yang dikumpul dalam fasa perancangan. Analisis tentang kesesuaian topik dan menilai kepentingan dan manfaat untuk menjalankan kajian ini dilakukan. Selain daripada itu, analisis tentang perkakasan dan perisian juga

dijalankan untuk memastikan perkakasan dan persisian yang sedia ada sesuai untuk membangunkan projek ini.

4.3 Fasa Reka Bentuk

Fasa ini merupakan fasa yang penting dalam keseluruhan projek. Fasa ini melibatkan proses penting, iaitu mereka bentuk , membangun dan mengimplementasi algorithma AES terhadap sistem keselamatan data pesakit . Pembangunan sistem keselamatan data pesakit dibangun dengan menggunakan perisian *Hypertext Preprocessor*(PHP). Maklumat pesakit akan disimpan ke dalam pangkalan data PhpMy Admin.

Bagi menghasilkan algorithma AES, bahasa pengaturcaraan JavaScript telah digunakan. Seterusnya, algorithma AES akan diimplemetasi ke dalam sistem yang telah dibangun bagi menghasilkan sistem yang lengkap dan baik.



Rajah 1 Model Pembangunan Sistem Keselamatan Data Pesakit Menggunakan Teknik AES.

4.4 Fasa Pengujian

Fasa ini bertujuan menguji fungsi – fungsi sistem yang dibangunkan dan fungsi algorithma AES dapat berfungsi dengan baik. Selain itu, proses pengujian juga bertujuan untuk mengenal pasti sebarang ralat. Fasa ini juga bertujuan untuk menghasilkan sistem yang mampu memenuhi objektif dan menepati skop yang telah ditetapkan. Sekiranya gagal mencapai objektif projek, penyelarasan perlu dijalankan atau mengimbas kembali fasa analisis bagi membuat penambahbaikan kajian yang mendalam. Fasa ini bermula dari perancangan ujian, mereka bentuk kes-kes ujian, bersedia untuk pelaksanaan dan menilai status sehingga penutupan ujian. Aktiviti dalam proses pengujiaan terbahagi kepada langkah-langkah berikut.

1. Perancangan dan Kawalan

Perancangan dan kawalan mempunyai tugas-tugas utama seperti:

a. Untuk menentukan skop, risiko dan mengenal pasti objektif pengujian.
b. Untuk menentukan pendekatan pengujian.
c. Melaksanakan dasar pengujian atau strategi pengujian.
d. Untuk mengetahui sumber pengujian yang diperlukan seperti persekitaran pengujian, komputer dan lain-lain.

2. Analisis dan Reka Bentuk

Analisis pengujian dan pengujian reka bentuk mempunyai tugas-tugas utama seperti:

a. Untuk mengkaji asas kajian.
b. Untuk mengenal pasti keadaan pengujian.
c. Untuk mereka bentuk pengujian.
d. Untuk menilai kebolehujian keperluan dan sistem.
e. Untuk mereka bentuk persekitaran pengujian dan mengenal pasti perkakasan yang diperlukan.

3. Melaksana dan Pelaksanaan

Melaksana ujian mempunyai tugas utama seperti berikut:

a. Membangunkan dan mengutamakan kes-kes ujian dengan menggunakan sebarang teknik dan mewujudkan data untuk ujian tersebut.
b. Membuat set ujian daripada kes-kes ujian untuk pelaksanaan ujian yang cekap.
c. Melaksana dan mengesahkan persekitarannya.

Antara fungsi yang akan duji adalah berdasarkan Jadual 1

ID Fungsi	Butiran fungsi Sistem
F001	Log Masuk
F002	Daftar Pengguna Baru
F003	Memuat Naik Maklumat Pesakit
F004	Penyulitan/Penyahsulitan Maklumat

Jadual 1

5 HASIL KAJIAN

Bahagian ini membincangkan hasil daripada proses pembangunan sistem. Bagi pembangunan antara muka pengguna dari segi kebolehgunaan fungsi Daftar Masuk seperti rajah (A). Pengguna akan mendaftarkan nama, kata laluan dan emel pada antara muka 'Daftar Masuk'.

Rajah (A) : Daftar Masuk

Setelah pengguna berjaya ‘Daftar Masuk’ ke dalam sistem antara muka yang seterusnya iaitu rajah (B) yang ditunjukkan iaitu antara muka ‘Log Masuk’ ke dalam sistem bagi pengguna yang telah berdaftar.

Rajah (B) : Log Masuk

Setelah itu, hasil kajian dari segi keselamatan dapat dilihat dalam fungsi penyulitan yang dilakukan semasa menekan butang ‘muat naik’. Rajah (C) menunjukkan antara muka untuk menyimpan maklumat pesakit. Dalam antara muka ini pengguna dikehendaki memasukkan ‘nombor pesakit’ , ‘nama’ , ‘tarikh masuk’ dan ‘tarikh discaj’ untuk dimuat naik. Seterusnya, pengguna juga perlu memasukkan kunci rahsia untuk digunakan ke dalam penyulitan AES. Setelah proses penyulitan berlaku, pengguna juga boleh menyahsulit maklumat yang telah disulit untuk melihat maklumat asal. Kemudian maklumat pesakit yang telah disulitkan akan disimpan ke dalam pangkalan data PHP MyAdmin seperti yang ditunjukkan pada rajah (D).

Rajah (C) : Penyulitan/Penyahsulitan berlaku terhadap maklumat pesakit

Rajah (D) : Pangkalan data maklumat pesakit yang sulit telah disimpan

6 KESIMPULAN

Sistem keselamatan data pesakit menggunakan teknik AES ini dijangka dapat membantu meningkatkan keselamatan terhadap suatu pengurusan maklumat pesakit. Teknik AES juga mampu melakukan penyulitan secara cepat dan berkesan berbanding teknik lain. Keselamatan suatu maklumat peribadi ini memain peranan penting bagi tujuan melindungi maklumat pesakit tersebut daripada dicerobohi atau hilang.

Penggunaan perisian PHP, PhpMy Admin dan JavaScript dalam projek ini dapat memudah kerja pelaksanaan mengimpelementasi algorithma AES ke atas sistem keselamatan ini. Proses penyulitan dilakukan dalam sistem kemudian disimpan ke dalam pangkalan data.

7 RUJUKAN

Symantec. (2013). Internet security threat report 2013, 18.

Cankaya, E. C., & Kywe, T. (2015). *A Secure Healthcare System: From Design to Implementation*. *Procedia Computer Science*, *62*, 203–212.

Secure database management system for confidential records using separately encrypted identifier and access request. (1999).

Michael Cobb. (n.d.). What is Advanced Encryption Standard (AES)? - Definition from WhatIs.com. http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

Kansallinen Terveysarkisto (Kanta). (n.d.). Introduction to the Patient Data Repository, Healthcare services. http://www.kanta.fi/en/web/ammattilaisille/earkiston-esittely

Rahmat Tulloh, Aditia, Permanasari, Yurika, Harahap, Erwin. (n.d.). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File DocumentEncryption.

Rista Maya, Widiatri. (2013). Analisis Kinerja Algorithma Rabin Dan Rivest Shamir Adleman (RSA) Pada Kriptografi.

TheSkop. (2010). "Data Orang Sakit Pun Dalam Bahaya."http://theskop.com/2010/10/data-orang-sakit-pun-dalam-bahaya/

Zheng, Yao. (2011). Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption

Tsai, Kun-Lin, Leu, Fang-Yie, Wu, Tien-Han, Chiou, Shin-Shiuan, Liu, Yu-Wei. (2014). A Secure ECC-based Electronic Medical Record System.

Pratama Samosir, Rio Auditya. (2015). Pengamanan Data Teks Dengan Kombinasi Algorithma Data Encryption Standard (DES) Dan First Of File (FOF)

Mahajan, P., & Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for security. *Global Journal of Computer Science and Technology*, *13*(15).