DATABASE ENCRYPTION FOR A WEB-BASED CLAIMS SYSTEM

by

SYED ZULKARNAIN SYED IDRUS
(0630210081)

A thesis submitted in fulfillment of the requirements for the degree of
Master of Science (Computer Enginering)

School of Computer and Communication Engineering
UNIVERSITI MALAYSIA PERLIS (UniMAP)

2007

DEDICATION

To my loving wife Sharifah Shereen,
who is seven months pregnant with our second child
and daughter Sharifah Shaqeerah Az-Zahara, 4,
for their support and understanding.

To my loving parents
Syed Idrus and Sharifa Zaharah,
for their guidance and assistance.

May Allah S.W.T. bless you all, Amin.
Thank you!

PREFACE AND ACKNOWLEDGEMENTS

This thesis is about the development of a computer system for institutions of higher learning particularly Public Institutions of Higher Learning (PIHL) so that staff can make online claims for official outstation duties. In fact, this system will be able to take over the whole administration of staff's travel claims within Malaysia, including Sabah and Sarawak.

The development of this system is based on the Treasury Circulars issued by the Ministry of Finance, Malaysia or other circulars related to it. The system must be promptly updated once there are amendments with regards to the Treasury Circulars. This system can also be applied to other government's departments. Apart from that, a security aspect of the system will be analysed for its effectiveness and performance, thus provide the necessary prevention from intruders that might want to steal data within the system.

This study is just a small portion of the entire university's administration. Nevertheless, it is my fervent hope that this study will lead to the development of other systems within the purview of university's administration so that computer systems will replace routine administrative duties. Let this study be the motivating factor for university's administrators to adopt hi-tech computer systems, which will ultimately achieve 'paperless' and 'wireless' administration. Although the development of this system is just a small contribution to knowledge but nonetheless, it can be an important step, which will bring about bigger contributions beneficial to the university's community at large.

I would like to take this opportunity to thank Allah S.W.T. the Almighty, who had given me the strength and inspiration to carry on in this study and above all during my lifetime. I beg of Him to continue His perpetually blessings. To develop a computer system is both stressful and a nerve-racking process. It requires utmost patience, conscientiousness and perseverance. I had an arduous time trying to get everything done within the shortest possible time. Fortunately, people around me in Universiti Malaysia Perlis (UniMAP) are so nice, cooperative and encouraging.

As such, I regard this as a great honour and privilege to be given the opportunity to do research in the field of Computer Engineering leading towards producing of a system for UniMAP staff to make claims online. Furthermore, the School of Computer and Communication Engineering had kindly financed my papers for an international journal in the area of security for publication and conference proceedings. This may not have happened had there be no guidance and collaboration from all UniMAP staff both academic as well as those in the administration.

Special mention should go to my Dean, Associate Professor Dr. R. Badlishah Ahmad, Associate Professor Dr. Syed Alwee Aljunid Syed Junid who is my leading supervisor, Madam Salina Mohd Asi and Mr. Suhizaz Sudin who acted as my co-supervisors. I am most indebted to all these individuals who gave me the support from the beginning to the end of my study. They had also given me the motivation and assistant in one-way or another whether directly or indirectly.

My gratitude should also go to other individuals especially my colleagues and friends in UniMAP, whom I am not able to mention here by names that have inspired me throughout the duration of this study. It was a pleasure and gratification working with them in UniMAP.

Last but not least, I would also like to express my cordial thanks to the Ministry of Science, Technology and Innovation (MOSTI), Malaysia who had supported this research for the duration of my study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF LISTINGS

LIST OF ABBREVIATIONS

3DES	Triple DES (Data Encryption Standard)
AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASP	Active Server Pages
Avg	Average
CAST-128	Carlisle Adams and Stafford Tavares (40 – 128 bits)
CAST-256	Carlisle Adams and Stafford Tavares (128, 192 or 256 bits)
DBLC	Database Life Cycle
Char	Character
CPOE	Computerised Provider Order Entry
CRC	Center for Research and Consultancy
CSS	Cascading Style Sheet
DBLC	Database Life Cycle
DBMS	Database Management System
Dec	Decimal
DES	Data Encryption Standard
DFD	Data Flow Diagram
DHTML	Dynamic Hypertext Mark-up Language
DLL	Dynamic-Link Library
DOM	Document Object Model
ED	Encryption and Decryption
ER	Entity-Relationship
ERD	Entity-Relationship Diagram
etc.	*et cetera* (and so on)
FPGA	Field-Programmable Gate Array
GUI	Graphical User Interface
HoRC	Head of Responsibility Centre
HTML	Hypertext Mark-up Language
Hx	Hexadecimal
i.e.	*id est* (that is)
Ice	Information Concealment Engine
Ice 2	Information Concealment Engine 2
IE	Internet Explorer
IEAK	Internet Explorer Administration Kit
IDEA	International Data Encryption Algorithm
IIS	Internet Information Services
IPES	Improved Proposed Encryption Standard
IT	Information Technology
Kbit/s	Kilobit per second
LAN	Local Area Network
MATLAB	Matrix Laboratory

MB	Megabyte
Mbit/s	Megabit per second
MHz	Megahertz
MIS	Management Information System
ms	Millisecond
MySQL	Multithreaded, Multi-user Structured Query Language
NA	Not Applicable
NCC	Net-Centric Computing
No.	Number
OS	Operating System
p.	Page
P3P	Platform for Privacy Preferences
PC	Personal Computer
PCR	Parent-Child Relationship
PES	Proposed Encryption Standard
PHP	Hypertext Pre-processor
PIHL	Public Institutions of Higher Learning
pp.	Pages
PPKKP	*Pusat Pengajian Kejuruteraan Komputer dan Perhubungan* (School of Computer and Communication Engineering)
PTA	Parent-Teacher Association
RAD	Rapid Application Development
RC	Responsibility Centre
RC2	Ron's Code or Rivest Cipher 2
RC4	Ron's Code or Rivest Cipher 4
RC5	Ron's Code or Rivest Cipher 5
RC6	Ron's Code or Rivest Cipher 6
RSA	Rivest, Shamir and Adleman
RsT	Response Time
SDLC	Systems Development Life Cycle
SMIL	Synchronised Multimedia Integration Language
TEA	Tiny Encryption Algorithm
Thin Ice	Thin Information Concealment Engine
Triple-DES / TDEA	Triple Data Encryption Standard / Triple Data Encryption Algorithm
UniMAP	Universiti Malaysia Perlis
URL	Uniform Resource Locator
USA	United States of America
UUM	Universiti Utara Malaysia
vs.	Versus
WWW	World Wide Web
XOR	eXclusive OR
XTEA	eXtended Tiny Encryption Algorithm

ABSTRAK (BAHASA MELAYU)

Penyulitan Pangkalan Data Untuk Sistem Tuntutan Berasaskan Web.

Kajian ini bertujuan untuk membentuk satu sistem komputer bagi seluruh staf Universiti Malaysia Perlis (UniMAP) supaya dapat membuat tuntutan melalui media elektronik. Pembentukan sistem ini adalah berdasarkan kepada Pekeliling Perbendaharaan Malaysia dan dokumen-dokumen yang berkaitan dengannya. Butir-butir yang penting telah dibentuk ke dalam sistem tersebut seperti gaji, gred, kelayakan dan sebagainya. Turut dibentuk ke dalam sistem ini ialah pengiraan secara automatik. Sistem ini juga boleh diletakkan ciri keselamatan untuk menghalang penggodam atau orang-orang yang tidak sah yang boleh dipilih daripada hasil-hasil analisis keselamatan. Ada tiga kategori pengguna yang terlibat di dalam pembentukan sistem ini. Mereka adalah Pemohon, Pusat Tanggungjawab dan Jabatan Bendahari. Pusat Tanggungjawab meliputi jabatan-jabatan pentadbiran dan juga pusat-pusat pengajian di mana bajet peruntukan diperolehi. Pembentukan sistem ini bermula dengan merekabentuk Gambarajah-gambarajah Aliran Proses yang menunjukkan langkah-langkah atau prosedur-prosedur yang perlu diikuti mengikut urutan yang betul. Ketiga-tiga pihak harus mengikuti aliran urutan masing-masing. Aliran proses adalah suatu aliran yang menentukan pengerakan borang dari mula ianya di hantar sehingga ke peringkat pembayaran. Proses ini diikuti dengan merekabentuk Gambarajah Aliran Data dan kemudiannya Pangkalan Data. Yang mula mencirikan bagaimana data akan mengalir dalam sistem, manakala yang kedua ialah tempat penyimpanan data seperti pengenalan log masuk, katalaluan, butir-butir peribadi staf, kelayakan dan sebagainya. Pembentukan Pangkalan Data wujud dalam empat bentuk iaitu Gambarajah Hubungan Entiti, Gambarajah Berhierarki, Gambarajah Pangkalan Data Hubungan dan Kamus Data. Daripada dua puluh algoritma penyulitan yang terdapat dalam fail Dynamic-Link Library (DLL), cuma lima daripadanya telah dipilih untuk diteliti dan dibuat analisis serta membuat perbandingan dari segi keupayaan dan kesesuaian dengan sistem yang dibentuk. Oleh kerana sistem ini adalah berasaskan kepada laman Web, semua bentuk tuntutan perjalanan boleh dilakukan di mana saja. Cara sebegini, bukan sahaja dapat mengelakkan kesilapan manusia, bahkan juga lebih efisien, cepat dan tepat. Oleh itu, sistem ini menjimatkan masa, tenaga dan juga kos pentadbiran. Active Server Pages (ASP) telah dipilih bagi membuat pengiraan dan juga menjana laporan-laporan. Setelah sistem tersebut siap dibentuk, satu ujian telah pun dibuat dengan menggunakan borang-borang yang dilakukan secara manual sebagai simulasi. Tujuannya ialah supaya pengkaji dapat membuat perbandingan serta mengesan kekurangan dan kelemahan simulasi manual di dalam sistem yang telah dibentuk. Ujian juga dilakukan ke atas algoritma penyulitan dan pelayar-pelayar Web yang telah dipilih dengan meningkatkan kedua-dua saiz panjang teks dan saiz panjang kunci dan memperhatikan prestasinya. Setelah dicatatkan masa responnya, satu analisis telah dibuat untuk menentukan prestasi algoritma dan pelayar-pelayar yang paling sesuai untuk sistem yang telah dibentuk dan dianggapkan terbaik iaitu rendah masa responnya dan terus berkeadaan begitu selanjutnya. Keputusan ujian-ujian tersebut nyata bahawa sistem yang dibentuk ini telah dapat mengesan kesemua kesilapan-kesilapan manusia dalam tuntutan sistem manual, di mana penuntut telah membuat beberapa kesalahan. Daripada analisis, algoritma penyulitan dengan pelayar-pelayar Web pula telah menunjukkan bahawa algorithma Twofish adalah paling sesuai untuk sistem yang dibentuk dengan bahasa pengaturcaraan Web ASP ke atas Internet Explorer. Di sini, menekankan bahawa kesemua objektif-objektif yang telah diletakkan pada peringkat awal penyelidikan telah pun dicapai.

ABSTRACT (ENGLISH)

Database Encryption For A Web-based Claims System.

The main purpose of this study is to develop a computer system for UniMAP staff to make claims via electronic media. The system development is based on the Treasury Circulars by the Ministry of Finance, Malaysia as well as other circulars related to it. Other important particulars had been built into the system such as salary, grade, entitlement and others. Another additional feature included is the automatic calculations. This system can also be equipped with a security tool to prevent hackers or unauthorised persons, which can be selected from the results of the security analysis. There are three categories of user involved in the development of the system. They are the Claimant, Responsibility Centre and Bursary Department. The Responsibility Centre consists of all administrative departments as well as centres of study from where the budget allocation is acquired. The development of the system begins by designing of the Process Flow Diagrams showing the steps or procedures that need to be followed in sequence respectively. All the three categories of users must follow their flow of the diagrams. Process flow is a flow that determines the movements of the forms from the moment they are submitted up to the stage where payments will be made. This process is to be followed by the designing the Data Flow Diagram and then the Database. The former specifies how the data will flow in the system, whereas the latter is for data storage where all data are kept such as login identifications, passwords, staff personal particulars, entitlements etc. The development of the Database comes in four forms namely Entity-Relationship Diagram, Hierarchical Diagram, Relational Database Diagram and Data Dictionary. Out of twenty encryption algorithms that are available in the Dynamic-Link Library (DLL), only five have been selected to go through and perform analysis for comparison in terms of its performance and compatibility with the developed system. Since this system is Web-based, staff can make claims anywhere, anytime and at any locations. This method can overcome not only human errors but also more efficient, fast and accurate. Therefore, this system can also save time, effort, and administrative costs. In this study, Active Server Pages (ASP) has been chosen to make the calculation and also to generate reports. After the system has been developed, a test was conducted using forms that have been simulated manually. The purpose is to enable the researcher to make comparison with the ones made using the developed system in order to detect errors or flaws from the manual simulation in the system. Testing was also done on the encryption algorithms and Web browsers selected by increasing both the text length size and key length size and observed its performances. Having noted its response times, an analysis was made in order to determine which encryption algorithms' and Web browsers' performances were most suited for the developed system and considered the best, which is lower and able to sustain its response times. The results of this study have shown that this system is able to detect all human errors in the traditional manual claim system, in which claimants have made some mistakes. On the other hand, the analysis of encryption algorithms with Web browsers, the results have shown that Twofish algorithm is best suited to the system that has been developed using ASP Web programming language on Internet Explorer. Hence, it is emphatic that all objectives that had been set at the beginning of this research have been met.

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The advent of computer technologies have revolutionised our life in many ways. It is no longer the monopoly of the elite class, but also has reached the masses. For the haves, they may posses their own personal computers, but for the have-nots there are various ways that they can feel the touch of the computer systems such as Internet and e-mails at designated places. For some, this is the time to make lucrative business of hiring them according to hours.

The impact from this explosion of new scientific knowledge in the form of computer technologies have altered the way we learn; the way we think; the way we communicate; and many other behavioural traits that are completely different from the earlier generations. Thus, computer literacy is fast growing among our young citizens.

Even children as early as Primary schools have been exposed to computer systems, whereby the education authorities and Parent-Teacher Associations

(PTAs) have provided them with computer laboratories under the schools' computer clubs. Computer literacy now has reached an unprecedented height and has gone far beyond the boundaries of urban areas into the rural areas. In short, it will become our way of life and for those who are still computer illiterate, will feel themselves out of place in this changing world. Such is the influence and significance of computer systems for the present generation and the next *ad infinitum*.

At the work place, computer systems are overwhelmingly essential that they cannot do without. No organisations can afford to lag behind with the development and progress of computer technologies. They have no choice but to keep up with it sooner or later. In fact, very soon it can be predicted that administrative bureaucracies will become things of the past and ultimately be replaced by computer systems.

This study is meant to develop a Web-based Claims system for Universiti Malaysia Perlis (UniMAP) staff who have to perform duties outstation or attending courses directed by UniMAP authorities. Currently, all claims have to be made manually by filling up the claim forms by the claimants. This is a very tedious process and time consuming. It is not unusual for the claimants that they have to refer to the Treasury Circulars Malaysia to check on their entitlements that they are unsure of each time they have to make claims.

The development of this system will be followed by selection of a security measures most suited to the Web programming language that will be used and also selection of a Web browser that best perform the chosen security measures within the system.

1.2 STATEMENTS OF THE PROBLEM

The novelty of the problem is derives from the current practise at UniMAP is processing all claims manually. Manual claims are vulnerable to human errors, but with the implementation of this system, all the problems to over come human errors can be eradicated. As UniMAP expands, the problems will be aggravated. The problems here are: -

a) The **administrative side** having to go through line by line on the claim forms.

b) They have to **check** in order to make sure that the **claimants have entered** the correct particulars such as their grades, entitlements, rates, calculations etc.

c) The **administrators** may have to **re-calculate the amounts** to make sure that the claimants have entered it correctly on their claim forms. Should there be **any discrepancies**, the claim forms may have to be sent back to the claimants for correction(s) before re-submitting for **another checking**.

Developing a computer system is only part of the solution to the problems, but keeping it safe from unscrupulous person is another. With so many people having ulterior motives and self-interest using high technologies waiting to steal information for whatever reasons known only to the culprits. Even Lessner (2005) had raised an issue on security, which is said to be an unsolved problem. This seems to be the case in the aspect of computer security.

There are various security measures that can be imposed in order to secure the information stored. As more and more technologies evolve, an irresponsible person would try to find a way to excavate any loopholes within the system in order to penetrate into the heart of its weaknesses. This is due to the fact that human-made designs can also be broken by another human. Thus, over time security measures must be constantly reviewed and strengthen in order to combat hackers or culprits hot on the heels of system developers who are also using high technologies.

In the aspect of a security for a computerised system that is going to be developed in this study, the problems here are: -

a) To search a **suitable** and an **almost impregnable** security measures to be attached to the system.

b) To determine the right approach as well as methodology in finding the **best** and **most suitable** security measures with the **Web-based Claims System** that will be developed.

1.3 OBJECTIVES OF THE STUDY

The main objective is to develop a computerised system for UniMAP staff to make claims online. This system would enable to cut down the time to submit and process the staff's claims. By doing it online, the claimants can execute it from anywhere and at anytime. The advantages of online claims are many and among them are to do away with administrative bureaucracies, avoiding human errors and unnecessary delays. The development of any computer system must be accompanied by security measures in order to safeguard the information stored. The following are the main objectives of this study: -

a) To design and develop a **Web-based** claiming system for UniMAP that can be used from anywhere and produces **automatic entitlements**, **correct** and **accurate** results, hence over come human errors.

b) The design and development of the system will focus on the **mileage claim**, **meal and/or day allowance** and **lodging and/or hotel allowance**.

c) To select a **security measures** for the system developed with an appropriate mean of use.

d) To analyse five selected encryption algorithms in term of their performance and compatibility.

e) To co-analyse four Web browsers to determine which algorithm perform best in terms of its speed with which Web browser.

1.4 SCOPE OF THE STUDY

There are many types of advances, allowances and claims that the staff are entitled to while on official duty or attending courses in the country or outside the country such as self-advance application, meal allowance, hotel or lodging allowances, travel claim, mileage claim etc.

However, the focus of this study is limited to three most common domestic transactions i.e. Self-Advance Applications, Travel and Mileage Claims. Even then, these transactions are limited to Peninsular Malaysia, East Malaysia (Sabah and Sarawak), South of Thailand and Kalimantan, Indonesia. Any other countries are considered overseas transactions.

The ambit of this research and system development is only meant for UniMAP staff whose particulars are built-in into the system. The Web-based features are built solely for the convenience of all claimants.

Although this study is done in UniMAP, using UniMAP's staff as samples, the scope and coverage of the system is actually very much wider than what it looks on the surface. This system can also be applied to other universities particularly in Public Institutions of Higher Learning (PIHL). The reason is obvious because all PIHL are subjected to the same financial procedures based on Treasury Circulars issued by the Ministry of Finance, Malaysia. Hence, financial administration in all PIHL by right should be akin in financial planning as well as implementation.

Realising the fact that security of the system is no less important than the development of the system itself, the emphasis should also be given to security measures. Thus, this study will adopt a bifocal approach: the development of the system and its engineering element of security. Both elements are inseparable because computer system *per se* without any kind of protection is of no significance at all to the system.

The scope of security measures for this system will be limited to the application of encryption. There are many encryption algorithms available at the present moment to choose from. Different algorithms will have different number of

bits key in size and forte comparatively. For the purpose of this study, the researcher has decided to apply five of the twenty-encryption algorithms, which is found to be compatible with the Web programming language that is to be used and also can be coded inside the programming language with ease.

CHAPTER 2

LITERATURE REVIEW

2.1 REVIEW OF PREVIOUS RESEARCH

There are numerous research done on security measures and systems development, however, after a thorough search of the literature, the researcher has yet to come across any development on Web-based Claims system. Nevertheless, there are various types of security that had been applied to other systems in a variety of ways. Therefore, the focus here will be on topics related and relevant to the field of research of this study.

In his thesis, Lessner (2005) stresses on security, which is a concern in the designing of a wide range of embedded systems but remains an unsolved problem. For this reason, it would create greater challenges in the future compared to security for the present mainstream computers. Hence, the promise of universal connectivity for embedded systems creates increased possibilities for malicious users to gain unauthorised access to sensitive information.

Lessner (2005) also investigates three cryptography algorithms namely RC4, AES and Rivest, Shamir and Adleman (RSA), and their relevance to the networked embedded systems. His focus was to find feasible security solutions for the networked embedded systems' applications by using the three cryptography algorithms, which have been ported to three hardware platforms namely Rabbit RCM3000; Xilinx Virtex 4 Field-Programmable Gate Array (FPGA) with MicroBlaze softcore; and a Linux desktop machine. Hence, these are to simulate some real world scenarios.

The applications that Lessner had developed are bi-directional transmission with encryption and decryption for various payload lengths; unidirectional transmission with very short payload; and encrypted data streaming. As a result, he managed to gather several timings and calculated the achieved throughput.

The Rabbit hardware platform was performed using the RC4 crypto algorithm with a throughput of about 155 kilobit per second (kbit/s) compared to the AES crypto algorithm with only 32 kbit/s. Thus, the RC4 has been proven to do better than the AES by a factor of 5.

The MicroBlaze hardware platform on the other hand, outperformed the Rabbit system by a factor of 5 – 10. Its throughput impressively attained up to 1.5 Megabit per second (Mbit/s) with RC4 and up to 130 kbit/s with AES. The researcher also performed on the RSA algorithm with 0.8 kbit/s of its throughput.