DATABASE ENCRYTPION/DECRYPTION USING AES AND DES

ABDULKADIR ABUKAR HAJI SUFI

UNIVERSITI TEKNOLOGI MALAYSIA

DATABASE ENCRYTPION/DECRYPTION USING AES AND DES

ABDULKADIR ABUKAR HAJI SUFI

A project report submitted in partial fulfillment of the
Requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE, 2014

To my beloved Family and Friends

To my respected supervisor

ACKNOWLEDGEMENT

First and foremost, I wish to express my sincere appreciation to my thesis supervisor **Dr. Ismail Fauzi Isnin**. For his precious guidance, encouragement, constructive criticisms, advice, knowledge, and motivation. Without his continual support and interest, this thesis would not have been the same as presented here.

Besides that, I would also like to express my thank you to all my fellow postgraduate course mates for their support. My sincere appreciation also extends to all my colleagues, friends and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. A very special appreciation goes to all my family members and my beloved parents for their continual supports (funding and moral support), love and care.

ABSTRACT

The application of database on storing data of computer applications is nowadays very common. Whether the system is a simple or a complex one, the security of the data should be remain important if the systems do deal with private and confidential data. Security countermeasures need to be taken in both whether before and after the intrusion of the database system. This project focusing on post-intrusion domain, which the attacker have been successfully access the database file and the data became exposed to the attacker. Counter measuring this attack, it is common that the system admin encrypts some columns, that containing private and confidential data, of the database. Related to that domain, this project goal is to investigate the computational time performance of two cryptography algorithms known as AES and DES, on encrypting and decrypting the critical columns of the databases. In this project, AES and DES algorithms are implemented in a prototype database-equipped application. The prototype is developed using Microsoft VB.NET 2010 and Microsoft SQL Server. The DES uses 64-bit long plaintext and 56-bit encryption key (8 bits of parity) and produce output of 64-bit block. The AES in the other part uses three different key length such as 128, 198 and 256 bits. From the comparison of results, it is found that the computational time of AES(128-bit) is faster than the other schemes, followed by the DES(58-bit), AES(198-bit) and AES(265-bit), subsequently.

ABSTRAK

Penggunaan pangkalan data dalam menyimpan data aplikasi komputer adalah sangat umum pada masa kini. Sama ada sistem adalah sistem yang mudah atau system yang kompleks, keselamatan data, kekal penting jika sistem berurusan dengan data peribadi dan sulit. Langkah-langkah keselamatan perlu diambil dalam kedua-dua kes, sama ada sebelum dan selepas pencerobohan sesuatu sistem pangkalan data. Projek ini memberi tumpuan kepada kes selepas pencerobohan, penyerang yang telah berjaya mencapai fail pangkalan data akan menyebabkan data menjadi terdedah kepada penyerang. Adalah perkara biasa pentadbir sistem menyulitkan beberapa lajur jadual data, yang mengandungi data sulit dan persendirian. Berkaitan dengan domain tersebut, matlamat projek ini adalah untuk menyiasat prestasi masa pengiraan dua algoritma kriptografi yang dikenali sebagai AES dan DES, dalam menyulitkan dan menyahsulitkan lajur kritikal dalam pangkalan data. Dalam projek ini, AES dan DES algoritma dilaksanakan dalam sebuah prototaip system yang menggunakan pangkalan data. Prototaip ini dibangunkan menggunakan Microsoft VB.NET 2010 dan Microsoft SQL Server. DES menggunakan teks data bersaiz 64-bit dan kunci penyulitan 56-bit (8 bit pariti) dan menghasilkan output 64-bit blok. AES di pula menggunakan tiga saiz kunci yang berbeza panjangnya iaitu 128, 198 dan 256 bit. Dari perbandingan keputusan yang diperolehi, didapati bahawa masa pengiraan AES (128-bit) adalah lebih singkat daripada skim yang lain. Secara turutannya, AES(128-bit) diikuti dengan DES (58-bit), AES (198-bit) dan AES (265-bit).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

CHAPTER 1

INTRODUCTION

1.1 Introduction

Computers and technology have become a normal part of human life. Computers have become basic tools of operation in almost every business sector. With the information load arose the need for information or data processing and storage which has given rise to powerful database systems for managing business and other corporate information. The need for the protection of such sensitive data has also increased the need for security measures including encryption of sensitive data. This is one of the most current measures which involves conversion of plain text to cipher text which can then be taken through the decrypting process to restore the plain text when necessary (Xing-hui, W. and M. Xiu-jun, 2010).

The plan text is only obtainable from the encrypted cipher text with the use of corresponding database encryption key obtained from selected encryption algorithms with encryption / decryption engine, and key management (Xing-hui, W. and M. Xiu-jun, 2010) and assigned to designated users. Hence, illegal possession or access to the data without the key makes access to the plain text impossible, thereby enhancing the database security.

The techniques and procedures involved in the establishment and maintenance of keying relationship between authorized parties in an organization is referred to as key management. According to (Vanastone ,S.A.,Van oorschort ,P.C. & Menezes ,A 1996), this include initialization of users within a domain, generation, installation and distribution of keying material, control, update as well as other processes including storage, back-up and archival.

Symmetric key cryptography makes use of the same key for the twin processes of encryption and decryption while for asymmetric key cryptography; different keys are employed for these two purposes. With symmetric key cryptography, all users use the same key and thus all have equal access to the data. This reduces the level of security as any act of compromise on the part of any of the key users compromises the entire data (Van Tilborg and Jojodia 2011).

In public/asymmetric key cryptography, pairs of keys are involved in the performance of different/inverse operations for example, digital signature creation and digital signature verification. These key pairs are designated private and public key. As implied in the designation, the private key resides in the custody of a designated user and is not accessible to the generality of users apart from situations where a back-up is kept with another trusted party. The public key on the other hand is available to all users without exception. Thought these keys are mathematically related, the information obtainable through such means is insufficient for total verification by an attacker. This characteristics lends strength to the concept of asymmetric cryptography which though was introduced since the mid-1970s did not get enough technological support for functioning until the mid-1990s (Van Tilborg and Jojodia 2011)

Key management is a critical aspect of a cryptography security system because each user must be in possession of secret or public key as required. The system must make provision of the secure generation and distribution of these keys as well as the capability for verification and management of the secret/private keys and the ability to verify and manage the keys of other users in a public keys system.

These may be in the form of digital certificate. Figure 1.1 provides an overview of the key management activities according to (Jaworrki, J., Perrone, p & chaganti, v. s (2000).

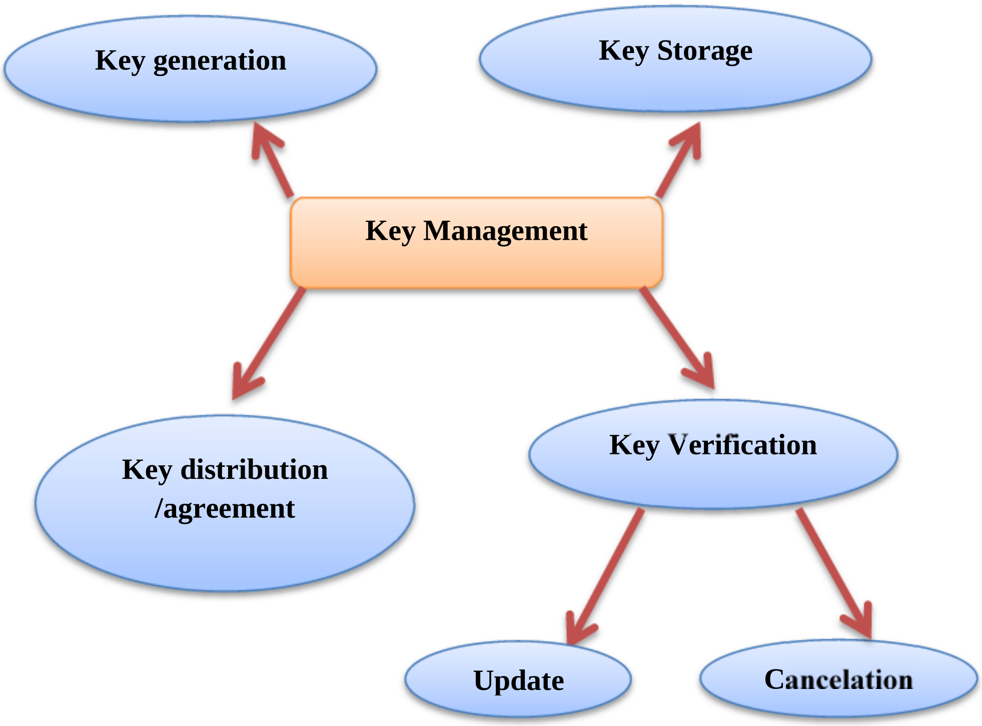

Figure: 1.1 Key Management (Jaworrki, J., Perrone, p & chaganti, v. s (2000)

1.2 Problem Background

Threats are sources of potential harm that are capable of damaging a system. They are a major concern in database information systems. Threats could be physical or logical in nature. Logical threats are software-supported unauthorized access to information database. They are intentional malicious attacks from illegal users that could result into the disclosure of sensitive information, loss of integrity as well as loss of access to authorized users. Such access could result in the dangerous alteration or disclosure of information in the system (Zailani, 2004)

Database technique in the key generation and database encryption during implementation processor of database, some of difficult private key technology of encrypt /decrypt (Xing-hui, W. and M. Xiu-jun (2010).

The encryption system in the IBE (identity based encryption) system is a centralized private key management system. The PKG or Private Key Generator is the users' private keys. The key management is similar to the PKI system in CA. the main challenges of such a system in practical application is that with increasing load and resultant expansion to the system, updating of private key becomes more complicated. In addition, based on the system master key, the system faces the risk of a single point failure as all private keys can be calculated (Zheng, L. and H. Yi "(2012). This can constitute a source of dangerous compromise.

1.3 Problem Statement

Security is still a great challenge in database management. The database encryption/ decryption still face many problems. The user encryption/ decryption especially when private data from source to destination within the network for the sake of storing or retrieving them from main system involved is a difficult or complex technology and still requirement a lot of attention

1.4 Objective

The main objective of this research is to investigate the performance of AES and DES area and Database security. Specifically, the project attempts to achieve the following objective:

1. To Study AES algorithm and DES Algorithm encrypt/ decrypt technique.
2. To Implement Database encryption/decryption using DES and AES.

3. To compare the performance of AES Algorithm and DES Algorithms and measure time.

1.5 Scope of the study :

This research project focused on the following development:

1. Provide the confidentiality of data against attackers in the organization
2. Focused on database Encryption or Decryption a column level in (SQL server)
3. User Interface for data manipulation should work on client/server manner.

1.6 Significance of the study :

1. Ensure confidentiality by protecting the data from unauthorized exposure.
2. To sustain access control mechanism through encryption scheme
3. Provide user-friendly environment.

1.7 Thesis organization

Chapter one provides an introduction to the whole study. It presents a brief introduction to place the study in the context of current research in the field. The background of the study was presented with a statement of the problem. Chapter presents a review of related research. Chapter 3 covers the methodology applied in the study; chapter 4 Presentation of system design and analysis while chapter 5 focuses on the implementation of the recommended and enhanced system.

Chapter 6 covers the conclusions from the study and the recommendations of the researcher.

References

XING-HUI, W. AND M. XIU-JUN 2010. Research of the Database Encryption Technique Based on Hybrid Cryptography. Computational Intelligence and Design (ISCID), 2010 International Symposium on, IEEE.

ZAILANI M.S.2004. Design and Implementation of a new multilevel scheme for database management system .Thesis PhD University Technology Malaysia.

VAN TILEBORG,H.C.A.V.&JAJODIA ,S.2011 k-Anonymity. Encyclopedia of cryptography and security.

VANASTONE ,S.A.,VANOORSCHORT ,P.C. &MENEZES ,A 1996 Handbook of applied cryptography .XP -002250459.

JAWORRKI, J., PERRONE, P &CHAGANTI, V. S 2000 java security handbook,mechillan press ltd.

ZHENG, L. AND H. YI " 2012 A Management Scheme of User Private Keys in an IBE System."

ZHANG, X., C. XU, ET AL. 2013.Efficient Chosen Ciphertext Secure Threshold Public-Key Encryption with Forward Security.Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on, IEEE.

KSHIRSAGAR, R. AND M. VYAWAHARE 2012.FPGA Implementation of High Speed VLSI Architectures for AES Algorithm.Emerging Trends in Engineering and Technology (ICETET), 2012 Fifth International Conference on, IEEE.

DING, Y. A ND K. KLEIN 2010. Model-driven application-level encryption for the privacy of e-Health data.Availability, Reliability, and Security, 2010.ARES'10 International Conference on, IEEE.

SHMUELI, E., R. VAISENBERG, ET AL. 2010. "Database encryption: an overview of contemporary challenges and design considerations." ACM SIGMOD Record **38**(3): 29-34.

PASHA DESHMUKH, A. AND R. QURESHI 2013."Transparent Data Encryption Solution for Security of Database Contents."

DENG-HONG, Z. 2010.Encryption design for the database under the VFP environment based on Chaos algorithm.Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, IEEE.

VERMA, H. K. AND R. K. SINGH 2013.Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6. Advance Computing Conference (IACC), 2013 IEEE 3rd International, IEEE.

BURNETT,S&PAIN,S. 2001.The RSA security official Guide to cryptography ,McGraw-Hill,inc

VANSTILBORG,H.C.A&JAJODIA ,S. 2011 Encyclopedia cryptography and security, Springer Burnett,S. & Paine ,S.2004 RSA Security’s official Guide Cryptography , McGraw-Hill,Ince

BARKER ,E, BARKER ,W.,BURR,W.,POLK,W.& SMID,M.2011 Recommendation for key management part1:General (revision3).NIST special Publication 800,57.

SHARMA, S., P. SHARMA, ET AL. 2011. RSA algorithm using modified subset sum cryptosystem. Computer and Communication Technology (ICCCT), 2011 2nd International Conference on, IEEE.

BOUGANIM, L. AND Y. GUO 2009."Database encryption." Encyclopedia of Cryptography and Security: 1-9.

BATINI, C., CERI, S. & NAVATHE, S. B. 1992. *Conceptual database design: an*

Entity-relationship approach, Benjamin/Cummings Redwood City, CA.

SPOFFORD, G., HARINATH, S., WEBB, C. & CIVARDI, F. 2005. *MDX Solutions: With Microsoft SQL Server Analysis Services 2005 and Hyperion Essbase*, John Wiley & Sons, Inc.

EDDEMA, H. 2001. *Microsoft Access version 2002 inside out*, Microsoft Press.GREENWALD, R., STACKOWIAK, R. & STERN, J. 2013. *Oracle Essentials: Oracle Database 12c*, " O'Reilly Media, Inc.".

LEE, B. (2010). Unified Public Key Infrastructure Supporting Both Certificate-Based and ID-Based Cryptography. Availability, Reliability, and Security, 2010. ARES'10 International Conference on, IEEE.

MATTSSON, U. T. 2005. A practical implementation of transparent encryption and separation of duties in enterprise databases: protection against external and internal attacks on databases. E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on, IEEE.

THAKUR, J. AND N. KUMAR 2011. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International Journal of Emerging Technology and Advanced Engineering **1**(2): 6-12.

PATTARANANTAKUL, M., A. JANTHONG, ET AL. 2012. Secure and efficient key management technique in quantum cryptography network. Ubiquitous and Future NETWORKS (ICUFN), 2012 Fourth International Conference on, IEEE.

CLARKE, A. AND R. STEELE 2012. Secure and reliable distributed health records: Achieving query assurance across repositories of encrypted health data. System SCIENCE (HICSS), 2012 45th Hawaii International Conference on, IEEE.

WEERASINGHE, T. 2013. An Effective RC4 Stream Cipher. 8th IEEE International Conference on Industrial and Information Systems (ICIIS).

CHENG, H. AND Q. DING 2012. Overview of the block cipher. Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012 Second International Conference on, IEEE.

CHENG, H. AND Q. DING 2012. Overview of the block cipher. Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012 Second International Conference on, IEEE.

MOGHADDAM, F. F., M. T. ALRASHDAN, ET AL. 2013. "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments."Journal of Advances in Computer Network **1**(3).

MALLAIAH, K., S. RAMACHANDRAM, ET AL. 2013. Performance analysis of Format Preserving Encryption (FIPS PUBS 74-8) over block ciphers for numeric data. Computer and Communication Technology (ICCCT), 2013 4th International Conference on, IEEE.

KAHATE, A. 2013. Cryptography and network security, Tata McGraw-Hill Education.

ROY, S., S. NAG, ET AL. 2013. "International Journal of Advanced Research in Computer Science and Software Engineering."International Journal **3**(6).

PADMAVATHI, B. AND S. R. KUMARI 2013."A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique."International Journal of Science and Research **2**(4).