IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727Volume 7, Issue 4 (Nov. - Dec. 2012), PP 01-07
www.iosrjournals.org

Performance Evaluation of Cryptographic Algorithms: AES and DES for Implementation of Secured Customer Relationship Management (CRM) System

E. Kalai Kavitha
Assistant Professor, Department of Information Technology, Rathinam Arts and Science College, Eachanari, Pollachi Main Road, Coimbatore-641021, Tamil Nadu, India.

Abstract: *Implementation of Secured Customer Relationship Management (CRM) system is the core competitiveness of Small and Medium Enterprises (SME) to build an effective means. Main usage of CRM is to maintain the industry records and customer request. Those records are maintained very confidentially for other industries to increasing their growth. Existing system of CRM's are used to maintain records but they didn't concentrate on security criteria's. The Proposed idea of CRM is to implement security features on it (i.e.) encrypt the confidential data's of the industry using best encryption algorithm. For that best cryptographic algorithm is discovered and then use it over the CRM application. Cryptographic Techniques are evaluated on some points. These points are avalanche effect due to one bit variation in plaintext keeping the key constant, avalanche effect due to one bit variation in key keeping the plaintext constant, memory required for implementation and simulation time required for encryption. The secured CRM system builds a great help in the relationship between employees and companies and provide secured access of system and allow secured transactions.*

Keywords- *Advanced Encryption Standard (AES), Avalanche Effect, Data encryption standard (DES), CRM, SME*

I. Introduction

Customer relationship management (CRM) is a widely implemented model for managing a company's interactions with customers, clients, and sales prospects. It involves using technology to organize, automate, and synchronize business processes—principally sales activities, but also those for marketing, customer service, and technical support. The overall goals are to find, attract, and win new clients; nurture and retain those the company already has; entice former clients back into the fold; and reduce the costs of marketing and client service.

Transmission of sensitive digital data over the communication channel have emphasized the need for fast and secure digital communication networks to achieve the requirements for integrity, secrecy and non reproduction of transmitted information. Cryptography provides a method for securing and authenticating the transmission of information across insecure communication channels. It enables us to store sensitive information or transmit it over insecure communication networks so that unauthorized persons cannot read it. Cryptography is an indispensable tool for protecting sensitive information in computer systems. Cryptography makes the message unintelligible to out side the world by various transformations. Data Cryptography is method of scrambling the content of digital data like text, image, audio and video to make it unreadable or unintelligible for others during transmission.

The main goal of cryptography is to keep the data secure from unauthorized access. Data containing information that can be read and understood is called plaintext or clear text. The method of scrambling the plaintext in such a way that hides its substance is called encryption. Encrypting plaintext makes the information in unreadable information called cipher text. The process of converting cipher text to its original information is called decryption. A system that performs encryption and decryption is called cryptosystem. The complexity of encryption process depends on algorithm used for encryption, software used and the key used in algorithm to encrypt or decrypt the data. Security of any encryption system depends on the security principle proposed by Kirchhoff. According to the Kirchhoff, the security of the encryption system should depend on the secrecy of the encryption /decryption key rather than encryption algorithm.

II. Cryptography

Depending upon the number of keys used, cryptographic algorithms can be classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). In Symmetric keys encryption or secret key encryption identical key is used by sender and receiver. Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) are the example of Symmetric key encryption algorithms. In Asymmetric keys encryption two different keys (public and private keys)are used for encryption and decryption. Public key is used for encryption and private key is used for decryption Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptosystem (ECC) are the example of asymmetric key algorithms.A symmetric cryptosystem has five ingredients:

a. Plain text

This is the original data or message to be transmitted that fed into the algorithm as input.

b. Encryption Algorithm

The algorithm performs various transformations and substitutions on the plaintext.

c. Secret key

This is another input to the algorithm and the value of secret key is independent of the plaintext. Depending on the specific key the algorithm will produce a different output.

This is the scrambled or encrypted message produced as output. This output depends on the plaintext and the secret key.

e. Decryption Algorithm

This is essentially the encryption algorithm operate in reverse. It takes the ciphertext and the secret key as input and produces the original plaintext as output.

III. Des Algorithm

It was created in 1972 by IBM using the data encryption algorithm and was adopted by the US government as standard encryption method for DES begins the encryption process by using a 64-bit key. The NSA restricted the use of DES to a 56- bit key length, so DES discards 8-bits of the key and then uses the remaining key to encrypt data in 64-bit blocks. DES can operate in CBC, ECB, CFB and OFB modes, giving it flexibility. In 1998 the supercomputer DES cracker, assisted by 100,000 distributed PCs on the Internet, cracked DES in 22 h. The US government has not used DES since 1998. [6] Figure 2 shows the encryption process using DES.

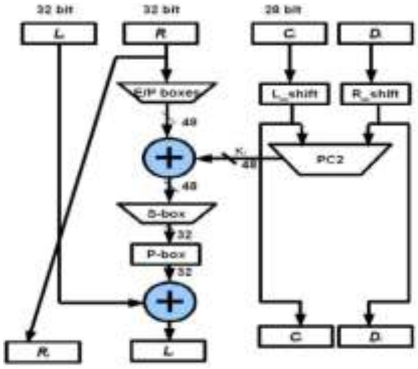


Figure 2 DES (Data Encryption Standard) process

IV. Aes Algorithm

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen.AES algorithm is can support any combination of data (128) and key length of 128, 192, and 256 bits. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For full encryption, Nr rounds (Nr = 10, 12, 14 for key length 128,192 and 256 respectively) of iteration are used. [7, 8]. Each round of AES is governed by the following transformations.

a.Bytesub transformation

It is a non linear byte Substitution, with the help of a substation table (s-box), which is generated by multiplicative inverse and affine transformation.

b. Shiftrows transformation

It is simple byte transpositions, the bytes in the last three rows of the state, depending upon the row location, are cyclically shifted; the offset of the left shift varies from zero to three bytes.

c. Mixcolumns transformation

This round is equivalent to a matrix multiplication of each

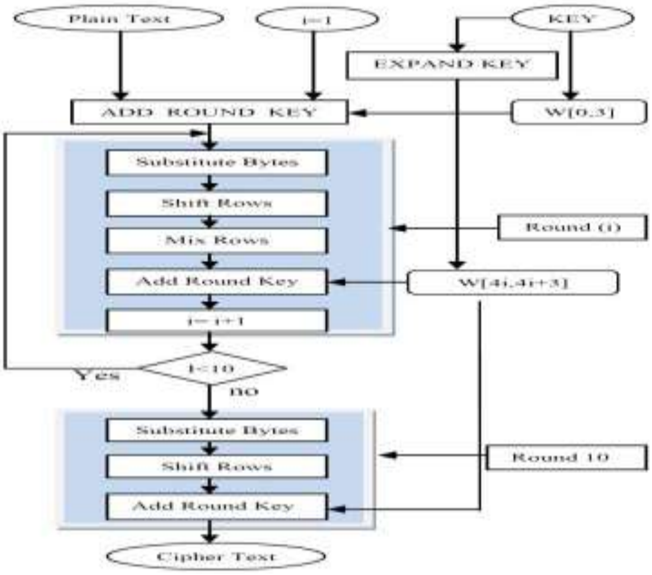


Figure 3 AES (Advanced Encryption Standard) process

Columns of the states.A fix matrix is multiplied to each column vector. In his operation the bytes are taken as polynomials rather than numbers.

d. Addroundkey transformation

It is a simple XOR between the present state and the round key. This transformation is its own inverse. The encryption process consists of several steps. Initially an addroundkey operation is performed then a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). This round operation is performed iteratively (Nr times) depending on the length of the key. The decryption operation has exactly the same sequence of transformations as the one in the encryption operation. The transformations Inv-Bytesub, the Inv-Shiftrows, the Inv-Mixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption.

V. Evaluation Parameters

Each of the encryption technique has their own strong and weak points. In order to apply an appropriate technique in a particular application we are required to know these strong and weak
points. Therefore the analysis of these techniques based on several features is necessary. In this paper analysis is done with following points under which the cryptosystems can be compared are described below:

A. Avalanche effect

A craving property of any encryption algorithm is that a small change in either the key or the plaintext should produce a significant change in the cipher text. However, a change in one bit of the key or one bit of the plaintext should produce a significant change in many bits of the cipher texts.

B. Memory required for implementation

Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm. It is desirable that the memory required should be as small as possible.

C.Simulation time

The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired. [6].

VI. Experimental Results And Analysis

Analysis for Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms is shown in Table I. Figure 4 shows comparison between DES and AES based on Avalanche effect. By analyzing the figure 4, it can be noticed that in AES algorithm avalanche effect significantly high i.e. it is 83 due to one bit variation in plaintext keeping the key constant and 81 due to one bit variation in key keeping the plain--text constant.

Whereas for DES it is 43. due to one bit variation in plaintext keeping the key constant and 41 due to one bit variation in key keeping the plaintext constant. Table II shows input plaintext, key used for encryption and ciphertext for maximum avalanche effect. Table III shows the same for AES.

TABLE I: COMPARISON BASED ON AVALANCHE EFFECT

Technique	1 bit variation in plaintext keeping the key constant	1 bit variation in key keeping the plaintext constant
DES	43	41
AES	83	81

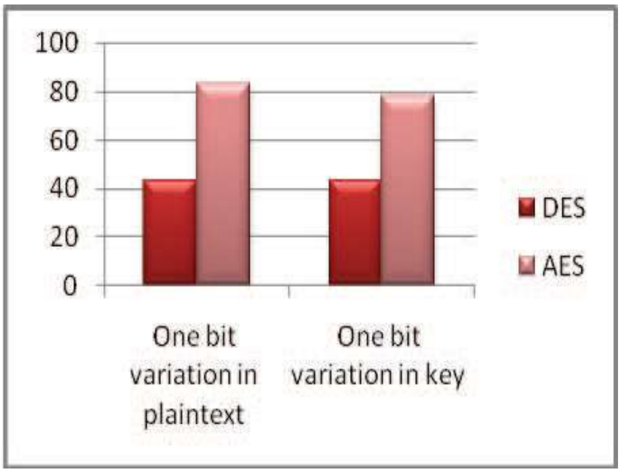


Figure 4 .Comparison of Memory usage by DES and AES

Technique	Memory Required for implementation (KB)	Simulation Time(Second)
DES	43.3	0.32
AES	10.2	0.0304

TABLE IV COMPARISON BASED ON MEMORY REQUIRE

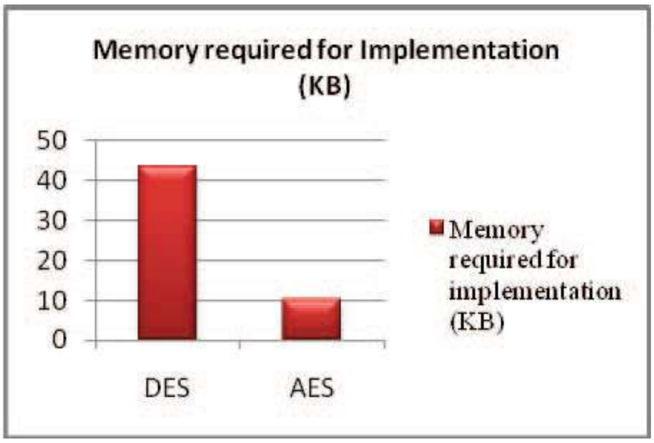


Figure 5 .Comparison of Memory usage by DES and AES

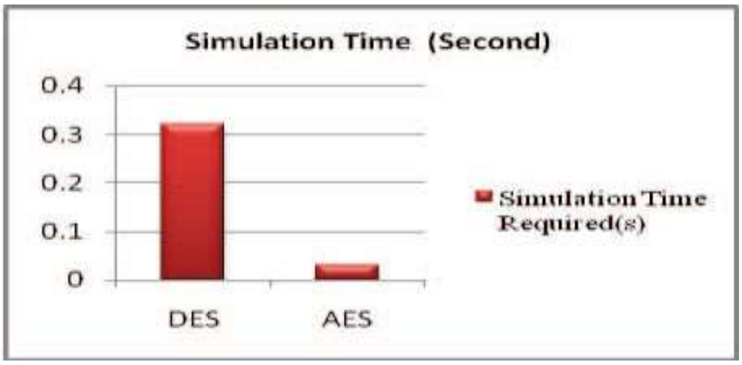


Figure 6 .Comparison of Memory usage by DES and AES

Table IV shows comparison between DES and AES based on memory required in hard disk for implementation and simulation time. By analyzing the figure 5 it is clear that memory required for implementation of AES is 10.2 KB and for DES 43.3 KB memory is required. So AES is a better option in case where less memory is required. Figure 6 shows simulation time required byboth algorithms for encryption of given data. By analyzing figure 6 it can be noticed that Simulation time is less for AES and greater for DES.

VII. Definition of Customer Relationship Management System

CRM (customer relationship management) is an information industry term for methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships in an organized way. For example, an enterprise might build a database about its customers that described relationships in sufficient detail so that management, salespeople, people whom provide service, and perhaps the customer directly could access information, match customer needs with product plans and offerings, remind customers of service requirements, know what other products a customer had purchased, and so forth. According to one industry view, CRM consists of:

- Assisting the organization to improve telesales, account, and sales management by optimizing information shared by multiple employees, and streamlining existing processes (for example, taking orders using mobile devices)
- Allowing the formation of individualized relationships with customers, with the aim of improving customer satisfaction and maximizing profits; identifying the most profitable customers and providing them the highest level of service.
- Providing employees with the information and processes necessary to know their customers understand and identify customer needs and effectively build relationships between the company, its customer base, and distribution partners.

i. Design principles of SME customer relationship management system

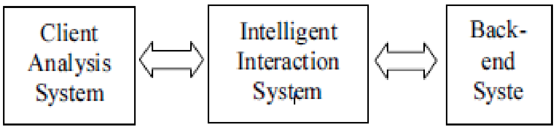
1) Meeting the internal demand CRM system to satisfy the business enterprise department first demand should be satisfied though especially some main department, like marketing, sales and customer service department. More specifically, marketing department conduct market activities management, follow-up and feedback are supported by CRM system, activities and obtaining the customer the evaluation form, distribution, discussing the information such as customer behavior to the customer, state classification; Supporting the sales department, and putting forward the sales task assigned to a task, evaluation and measure sales, and making the customer service department to be the system to provide for the customer service of accurate information, to ensure that the service center can treat customers consistent are also supported by CRM system.

2) Connecting the enterprise and market CRM must collect the enterprise market, sales and service, a collaborative up marketing, sales and service of the communication channel between, solve the enterprise in the process of the real-time information and meet channel optimization. Only in this way the analysis data real-time can be transferred to the sales and service department, so as to better understand customer behavior, keep old customers; In addition, the sales and service department of information gathered in the transfer market department to order to sales, service and complaint information analysis, and to work out in time more effective competition strategy.

ii.CONSTRUCTION THE CRM SYSTEM OF SME

A. Basic framework of CRM system of SME

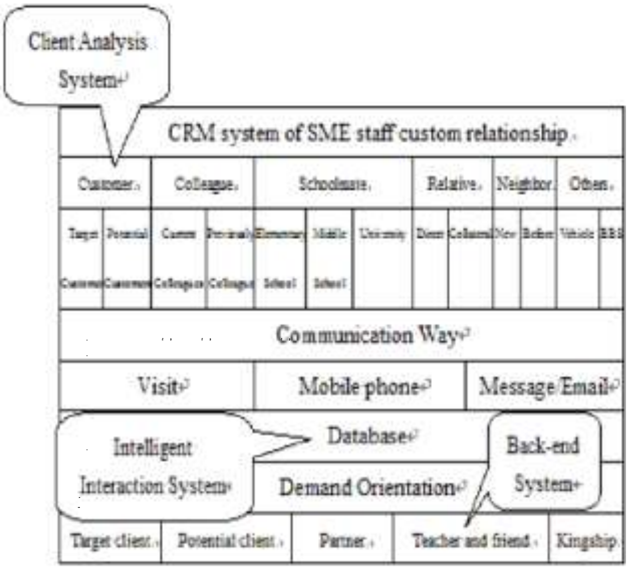
From above, the CRM system of SME module structure is shown in figure 1



The figure can see a more complete CRM system should be front-end system (customer interaction system), intelligence analysis system, and back-end system (enterprise information system) three system integration and integration. CRM is a kind of business strategy, its core is the customer as the center, realize the door value maximization guest and promote the enterprise competitiveness.

B. CRM system of SME staff custom relationship Based on the above module structure, small and medium-sized enterprise staff CRM system structure is shown in table 1

TABLE I. CRM SYSTEM OF SME STAFF CUSTOM RELATIONSHIP


Client Analysis System
Intelligent Interaction System
Back-end System

CRM system of SME staff custom relationship												
Customer		Colleague		Schoolmate			Relative		Neighbor		Others	
Target Customer	Potential Customer	Current Colleagues	Previously Colleague	Elementary School	Middle School	University	Direct	Collateral	New	Before	Vehicle	BBS
Communication Way												
Visit				Mobile phone					Message/Email			
Database												
Demand Orientation												
Target client		Potential client			Partner		Teacher and friend			Kingship		

iii.. CRM system for SME

Through to the CRM system of SME structure we know the needs of the enterprises is what, through the staff individual CRM system we mastered the staff what customers, so that to employees as the foundation, the service enterprises for the purpose, we construct the enterprise CRM model, as shown in figure.

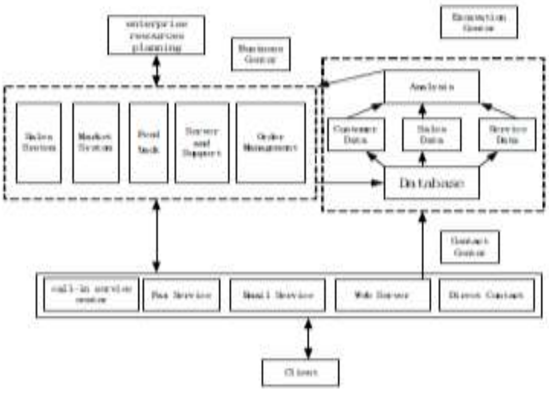


Figure 2. The model of CRM system for SME

The model includes three parts: the contact center, excavation center and business center. Contact center touch the customer, excavate center the customer information to input data excavation center, analyzes the data, to dig out the enterprise the useful information, and then excavation center take the information to send to business center, carries on the corresponding processing. The business centers can feedback information to the customer. This forms a useful information circulation. Of course there are many specific treatment methods and technical details.

Customer information contained in the great value of customers, through analysis and mining information found the customer to trade the law of value, found that customers form law and so on can be deeply understand the demand of customer, and the enterprise correct decision, the promotion enterprise business level has important significance.

The main purpose of CRM system is to make the enterprise in the process of communication with customers, continuous improvement and customer information, and will be accumulated over the past or not collection of direct customer information to accumulate gradually, medium and small-sized enterprise business personnel, sales directors and decision makers can be convenient for the customer information query and analysis to find the target customers, explore potential customers, create sales opportunity.

For example: sales order is the customer or agent to buy the product certificate, which details the customer or agent buy kinds of product, the amount and quantity. According to the contents of the enterprise is order to complete the sale receipts, distribution and other business operation of the shipment. Order management of this function is mainly realize products quotation, generating order, order review, executive orders, order tracking, payment collection on the purpose, and automatic tracking order execution, when sales receipts close to the time limit, the system can automatically remind gathering; Owe, the system can appear on the electronic collection.

VIII. Conclusion

CRM systems are designed and developed to solve all needs in an organization in much secured manner by applying cryptographic algorithms. In that the best cryptographic algorithm was analyzed by comparison of avalanche effect of those algorithms. By this approach organization details are maintained securely.

References

[1] NeetuSettia."Cryptanalysis of modern Cryptography Algorithms".International Journal of Computer Science and Technology. December 2010.

[2] Diaasalama, Abdul kader, Mohiy Hadhoud, "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of e-technology, Vol 2, No.1, January 2011.

[3] Kumar, "Customer Relationship Management", Wiley International Encyclopedia of Marketing , 2010: 24–30.

[4] Yang Jialu, "Customer Relationship Management of Smail-Medium Enterprises," Fudan University Press, 2004:113–120 (In Chinere).

[5] Russell S.Winer, "A framework for Customer Relationship Management " California Management Review, 2001, Vol 43(4).

[6] PC Verhoef, "Understanding the effect of customer relationship management efforts on customer retention and customer share development," Journal of marketing, 2003 Vol 74(2).