High Efficiency Encryption of Data Using Modified Advanced Cryptography Algorithm
(Data Sentinel)

Rohit Chandak[1],Keertikeya Gupta[2], Sanket Gandhi[3], Taher Husain[4]
[1234]Computer Science department, G. H. Raisoni Institute of Engineering and Technology, Pune, India

Abstract: Cryptography may be categorized according to the profile of its users. Military, government bodies and industrial giants savor the state of the art digital security for their top secret missions, while a common man suffers the vicious probing from agencies like the NSA. With the exponential growth in cyber crime in the recent years, a layman cannot afford to live under the misconception of having high security, when actually his critical data is under constant threat of being hacked. In such times that require the masses to pay high attention to information security, our system 'Data Sentinel' focuses on providing a high degree of safety to its users' critical data. The system can be accessed from any device that can access the Internet, hence cutting out any problems raised by platform dependencies. It allows the users to share their encrypted files with other registered as well as non-registered users by setting sharing permissions, thus restricting any unauthorized attempts at decryption. We have used a modified version of Advanced Cryptography Algorithm by generating the encryption key through image mapping. Logical operations like XOR and shifting are used in the encryption/decryption algorithms, and the practical implementations show the high efficiency of the entire process.

Keywords: Information Security, Encryption, Decryption, Cryptography, Image mapping.

Introduction

The principal of any encryption application is to present robust security to its user's important data and files. The process of generating the key for encryption plays a crucial role in deciding the strength of the security the application provides. Aside from offering stronger protection to the data, cryptography also serves to provide data integrity, authentication and authorization, and restoring the exact original data upon decryption. Every other day new key generation algorithms are coming out that belittle their predecessors. However, no algorithm is perfect. To be efficient, every one of them depends on a number of factors like the key space, time and space complexity, their type (symmetric/asymmetric) and many more.

Problem Definition

The basic meaning of the word sentinel is protection. Data sentinel is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data. Data security is part of the larger practice of Information security. Data sentinel is aimed towards the better protection of data from corruption and to keep it personalized. Hence the data is encrypted using advanced modified cryptography algorithm. This shielded encrypted data is then either stored or allowed to be shared. This shielded cannot be decrypted by anyone else other than the system. Hence the vitally important data can be protected from prying eyes. This project envisages the ease in handling of precious and important data between clients.

Motivation

The biggest problem with sharing crucial information in the digital era is that neither the information, nor the medium of transferring this information is secure. The most we can do is to secure the data that we want to share with others, and with high-end hacking tools, accomplishing this safety is a big hurdle. Even the good encryption tools out there in the market have their own shortcomings. Most of them need to be installed on your computers before you can actually use them. Such applications are usually accompanied by problems related to platform dependencies, memory consumption and installation overheads. Those applications that work over the Internet face issues like file size limits, slow processing speed and user authentication.

Objectives

The major objectives of systems are:

- To improve the current system of cryptography method.

- To provide powerful encryption.
- To allow guest feature.
- No installation.
- To allow users to access the system at any given time.

Existing System

At the present moment, there are a number of cryptography applications that provide with security of data, but in some way or the other they have their own setbacks that make them very much unreliable. Most of these systems work offline, meaning you have to install them. This gives rise to a variety of different hitches. Platform dependency is one of the most common amongst these problems. This is not just a problem for the users who work on several operating systems but also for the developers of the software itself. Next is the problem of installation overheads, i.e. the user must waste some of her precious time before she can actually get started with protecting her important data. Besides wasting your time, these application programs also consume a part of your computer's memory.

There are few cryptography applications that are web-based. Although this removes the problem of platform dependency, these applications provide with additional issues. The most widely noted one is the file size limitations that such systems impose upon their users. Combined together, the existing systems also fail to provide true security as the authentication and authorization mechanisms are poorly built. In numerous encryption applications, any person can decrypt a previously encrypted file. No verification of identity is needed. Thus despite having a great encryption algorithm, the system may entirely fail in providing real security

Proposed Work

The proposed system not only offers stronger encryption, but also covers other aspects of security such as authentication, authorization, non-repudiation, availability, scalability, ease of access and others. The following key features allow our system to accomplish the above:

- Size of key which is 512 Bytes which lays off an immense key space.
- Image mapping for key generation. This produces a very random key.
- Sharing permission that allows users to authorized other user to decrypt their shielded file.
- Guest features that allow non-registered users (Guest) to decrypt the shielded file that has been shared with them on system.
- No limitation on size of file you want to shield.

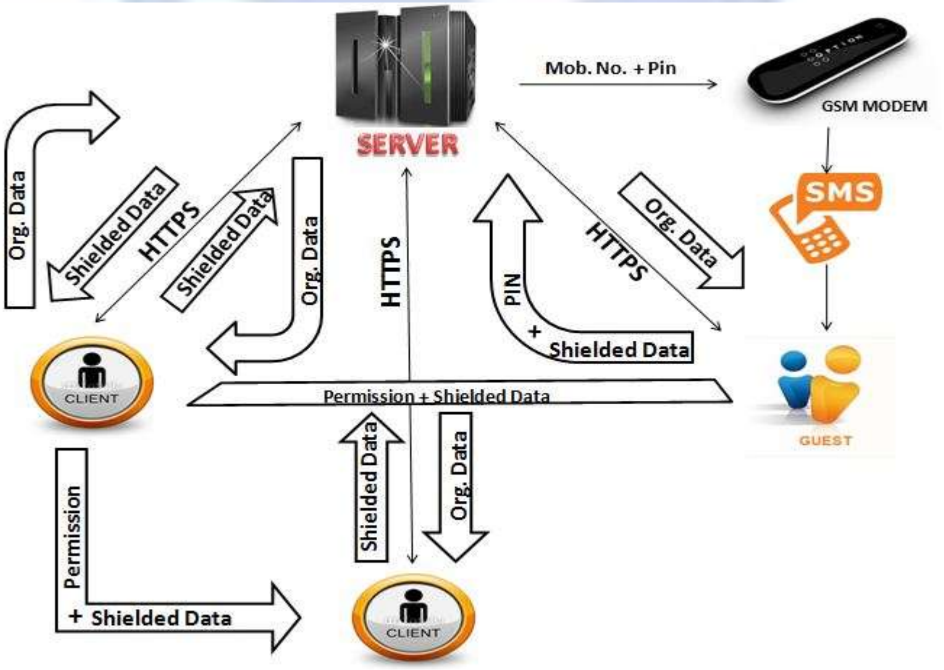

Fig 1: Overall System Workflow

Key Generation Algorithm

The key generation algorithm is used for genaration of encryptioon key is as follows:

- Select or create any private key of varying size from 128 bits to 512 bits i.e. 16 to 64 characters.
- Select owner's image and load it in memory.
- Map the ASCII value of characters in private key with 64 pixels of owner's image.
- Fetch 64 bytes from RGB Bands of 64 pixels.
- Divide 64 bytes into 4 blocks of 16 bytes each. Call them Key_Block1, Key_Block2, Key_Block3, Key_Block4.
- Apply XOR operation between Key_Block1 and Key_Block3. Results will store in new Key_Block13.
- Apply XOR operation between Key_Block2 and Key_Block13. Results will store in new Key_Block213.
- Apply XOR operation between Key_Block213 and Key_Block4. Results will store in new Key_Block4213.
- The new Key_Block4213 is the final key.

.

Encryption Algorithm

The encryption algorithm is used for encryptioon of file is as follows:

- Initially let Cipher_BlockX = Key_Block4213.
- Fetch 16 bytes from original file and put it in a block. Call it Data_Block.
- Apply XOR operation between Cipher_BlockX and Data_Block. Result will store in Cipher_Block1.
- Apply right circular shift with 3 values. Result will store in new Cipher_Block2.
- Apply XOR operation between Cipher_Block2 and Key_Block2. Result will store in new Cipher_Block3.
- Apply XOR operation between Cipher_Block3 and Key_Block4. Result will store in Cipher_Block4.
- Cipher_Block is written in encrypted file and is the input of the next round as a Cipher_BlockX.

Decryption Algorithm

The decryption algorithm is used for decryptioon of file is as follows:

- Initially let DeCipher_BlockX = Key_Block4213.
- Fetch 16 bytes from encrypted file and put it in a block. Call it EncData_Block.
- Apply XOR operation between EncData_Block and Key_Block4. Result will store in DeCipher_Block3.
- Apply XOR operation between DeCipher_Block3 and Key_Block2. Result will store in new DeCipher_Block2.
- Apply left circular shift with 3 values. Result will store in new DeCipher_Block1.
- Apply XOR operation between DeCipher_Block1 and DeCipher_BlockX. Result will store in Decrypted_ Block.
- Decrypted_ Block is written in decrypted fileT and EncData_Block is the input of the next round as a Cipher_ BlockX.

Table 1: Encryption/Decryption Time Comparison

Plain Text Size	DJSA algorithm	Data Encryption through AES Methodology	Advanced Cryptography Algorithm
1.66 mb	0:01:34	0:01:32	0:01:25
560 kb.txt	0:00:37	0:00:35	0:00:28
187 kb .txt	0:00:18	0:00:16	0:00:09
46 kb .txt	0:00:11	0:00:09	0:00:02
16 kb .txt	0:00:10	0:00:08	0:00:01

Software Requirement Specification

Operating Environment :

- The system is web based application. Hence it is platform independent and can be accessed through any device that can access internet.

Software quality attributes :

Following quality attributes helps the system to run efficiently

- Availability: The system is always available as it is a web based application.
- Performance: The system delivers efficient performance as expected by analysis of our studies.
- Manageability: The system is very easy to handle and the whole system is controlled by admin.

- Security: The system is secured as Https protocol is used.

Technical Specification

Advantages :

- Easily accessible.
- Always available.
- Safer sharing.
- Scalability.
- Powerful encryption.
- No limit on file size.
- Guest features.
- No installations.

Applications :

- Securing Sensitive information.
- Government Communication.
- Bank electronic fund transfer.

Conclusion/Results

By use of modern technologies data sentinel helps end users to protect their valuable information from being viewed/copied/misused by anti-social elements and to share it with near and dear ones.

References

[1]. IJARCSSE paper for Advanced cryptography algorithm for improving data security by Vishwa Gupta, Gajendra Singh, Ravindra Gupta, January 2012.
[2]. IJAIEM paper for Advacned crptoanalytic algorithm for data security by Mukund.S.Wankhede, Pravin.D.Soni, March 2103.
[3]. IJCST paper for Comparative analysis of encryption algorithm for data communication by Shashi Mehrotra Seth, Rajan Mishra, June 2011.
[4]. ICSA paper for Encryption techniques: a timeline approach by T Morkel, JHP Eloff.
[5]. Cryptoghraphy and Network Security Principles and Practices,5th Ed- William Stallings.