International Journal For Technological Research In Engineering
Volume 2, Issue 7, March-2015 *ISSN (Online): 2347 - 4718*

IMPLEMENTING ADVANCED SECURITY MECHANISM FOR MESSAGING (DIGISAFE)

Manu Kapoor[1], Mr. Amit Asthana[2]
M. Tech, SUBHARTI INSTITUTE OF TECHNOLOGY AND ENGINEERING (SITE) Meerut

Abstract: The security of information available to an organization was primarily provided through physical and administrative means. For example, rugged file cabinets with a combination lock were used for storing sensitive documents and personnel screening procedures were employed during the hiring process. With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system and the need is even more acute for a network. Computer networks were primarily used by university researches for sending e-mail, and by corporate employees for sharing printers. Under these conditions, security was not given much attention. Today, since the world is going global, and trillions of data are transferred daily across networks, security is looming on the horizon as a potentially massive problem.

Keyword: cryptography, security, RSA,

I. INTRODUCTION

Internet safety, or online safety, is the knowledge of maximizing the user's personal safety and security risks to private information and property associated with using the internet, and the self-protection from computer crime in general. As the number of internet users continues to grow worldwide, internet safety is a growing concern for both children and adults. Common concerns regarding safety on the internet include: malicious users (spam, phishing, cyber bullying, cyber stalking etc.), websites and software (malware, computer viruses, etc.) and various types of obscene or offensive content. Several crimes can be committed on the Internet such as stalking, identity theft and more. Most social networking and chat sites have a page about safety. Numerous groups, governments and organizations have expressed concerns about the safety of children using the Internet. The aim of this project i.e. DIGISAFE is all about sending and receiving emails from anywhere, anytime. The extra feature involved in our mailing site is that it is secured in a way that there is use of CRYPTOGRAPHY for mails i.e mails send will be encrypted by the user and on receiving they will be decrypted by the user. The project is confined to the intranet in an organization. This application makes sure that security services such as secrecy, authentication, integrity and non-repudiation are provided to the communicating parties.

II. OBJECTIVE

The main objectives of using Relational Database Management System are as follows: -

A. CONTROL REDUNDANCY: The System should identify existence of common data and avoid duplicate recording relationships of pointers should be used to locate data which are used many times selective redundancy is sometimes allowed to improve performance or far better reliability.

B. DATA INTEGRITY: Consistency of data values and relationships must be preserved in order to achieve this the system must ensure validity of data by using good editing, synchronize updating and propagating changes to other related data element it also involves maintaining audit trails to enable recovery if errors are deleted.

C. DATA SECURITY: This is concerned with protecting access to data protection is needed at many levels for access, modification, deletion or display access restriction may be for individual data items or group of items.

D. DATABASE PERFORMANCE: The system should be able to provide timely information as required. The cost of storing and retrieving the data should be commensurate with the value of information provided.

E. MANAGEMENT CONTROL: As the dependence of an organization on a data base increases positive management controls should be exercised over addition, deletion, changes and disposition of data must be protected to start legal accounting and auditing requirements.

Main Objectives are

- The Secure Mail System is meant to keep the security of the mail send between the users in a LAN.
- A user can easily encrypt the mail by using RSA Algorithm or by using Unicode BIT32 system.
- A user can insert his topic in the LAN to see the views of the other users.
- You can easily search the member if you know his email id or his contact number.
- The main concern of this project is to improve the efficiency and effectiveness of the whole system.

III. LITERATURE SURVEY OF SYSTEM

A System makes sure that security services such as secrecy, authentication, integrity and non-repudiation are provided to the communicating parties. This application makes use of RSA algorithm.

A. Disadvantage in Existing System

- Delay in information search and retrieval
- Problem in updation of current information and maintaining proper backup of information
- Possible damage of paper carrying the information thereby chance of losing valuable information.
- Much time required in giving correct information
- Less reliability and maintainability of data
- Secrecy of information may not be maintained due to visible facts on paper.

B. Proposed System

The system provides

- Easy storage and retrieval of data
- Giving correct information with less effort and high accuracy
- Secrecy and less chance of change of loss of data
- Easy data updating facility
- Data integrity and inconsistency

IV. FEASIBILITY STUDY OF SYSTEM

Feasibility is the determination of whether or not a project is worth doing. The process followed in making this determination is called a feasibility study. This type of study determines if a project can and should be taken. The objective of the feasibility study is not to solve the problem but to acquire a sense of its scope . During the study, the problem definition is crystallized and aspects of the problem to be included in the system are determined

Feasibility of the system should include the following things:
1. Statement of the problem: A carefully worded statement of the problem that led to analysis.

2. Summary of finding and recommendations: A list of the major findings and recommendations of the study. It is ideal for the user who requires quick access to the results of the analysis of the system under study.Conclusion are stated , followed by a list of the recommendation and a justification for them .

3. Details of findings : An outline of the methods and procedures under-taken by the existing system, followed by coverage of the objectives and procedures of the candidate system. Included are also discussions of output reports, file structures, and costs and benefits of the candidate system.

4. Recommendations and conclusions: Specific recommendations regarding the candidate system, including personnel assignments, costs, project schedules, and target dates.

Three key considerations are involved in the feasibility analysis these are

A. Economic Feasibility:

Economic analysis is the most frequently used method for evaluating the effectiveness of a system. More commonly known as cost/ benefit analysis, the procedure is to determine the benefits and savings that are expected from a system and compare them with cost. Earlier in Compu Craft the work has been done manually which takes lot of time as well as man power which is more economical. Now the same work is computerized which is more effective and efficient, less time consuming, reduces man power which in turn proves to be less economical

B. Technical Feasibility:

Technical Feasibility centers on the existing computer system (hardware/ software) and also it can support the modification. In manual processing there are more chance of errors are there, creating lot of complications, less technical or logical. Through proposed system we can set this process in a very systematic pattern, which is more technical, full proof, authentic, safe and reliable.

C. Behavior Feasibility:

Our proposed system works to minimize the human errors, take less time, easy interaction with user, bug free. This project/software is further expanded by connecting various interrelated departments and by installing an extension part of this software

V. ALGORITH IMPLEMENTATION

RSA is an algorittm for public-key cryptography that is based on the presumed difficulty of factoring large integers , the factoring problem . RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it was classified until 1997. A user of RSA creates and then publishes the product of two large prim numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem.

Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random
2. Compute n = pq.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.

- e is released as the public key exponent.
- e having a short bit-length.

5. Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)).
   - This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm.
   - d is kept as the private key exponent.

Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \pmod{n}.$$

This can be done quickly.

Decryption

Alice can recover m from c by using her private key exponent d via computing

$$m = c^d \pmod{n}.$$

Given m, she can recover the original message M by reversing the padding scheme.

VI. SCOPE OF THE SYSTEM

The main advantage of this system is all about sending and receiving emails from anywhere, anytime. The extra feature involved in our mailing site is that it is secured in a way that there is use of CRYPTOGRAPHY for mails i.e mails send will be encrypted by the user and on receiving they will be decrypted by the user. In future, we can have the SMS facility for the employees and employee search engine that can provide the result on the basis of different criteria to search. We can also have one more module of implementing this project on web.

REFERENCES

[1] http://opensmpp.logica.com/introhtml/menu.htm
[2] www.devshock.com
[3] www.msdn.com
[4] http://www.asp.net/
[5] http://msdn.microsoft.com/netframework/windowsforms/
[6] www.sas.com
[7] www.bonrix.net

