Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.414 – 418

RESEARCH ARTICLE

SECURED DATA TRANSMISSION USING CRYPTOGRAPHY

S.Suresh M.Sc.,M.Phil.,
Muthayammal College of Arts & Science,
Rasipuram.
Sureshs722@gmail.com

L.Gomathi MCA.,M. Phil.,
Assistant Professor, Department of BCA,
Muthayammal College of Arts & Science
Rasipuram.
gomathici2007@gmail.com

Abstract--- Each company as many branches in different location. Each branches having different configuration of hardware and software. This configuration may have raising issues of regarding the data transfer from various branches to corporate office vice versa. To overcome this problem this application project is alternative solution. The data transfer through the network is insecure due to data is plain text format. Regarding the Data Restoration make incompatible of software as well as hardware. In security concern the security process handling data encryption and data decryption using cryptic service provider for RSA encryption and decryption using public and private key. The keys were stored in server as a XML format. This encryption is an asymmetric encryption. This data also accessed through device independent system like mobile, PDA etc... The File quality analysis to track the current status of the file on which users working on after getting the files , the file send to quality analysis person and get back to it with status before restoring the database. The quality of file is checked and sends back to the administrator. The unsatisfactory files are sends back to client for rectification.

1. INTRODUCTION

The paper entitled in secured data transmission in device independent system which deal regarding the issue of data security. The conventional method of data is plain text format. This method will raise the security issue of data when transfer from source to destination. Any registered employee who is trying to enter his work area is checked for his id and password. If he is authorized then he would be allowed to enter into his work area.

The administrator to get files from the client and register the file information, depending on the information, the encrypted file was decrypted and stored into server database. The restored data was fetch from database and processed by administrator. If the file to be unsatisfactory then the file is send back to the client for correction. The security process was handling data encryption and data decryption using cryptic service provider.

This paper consist of following modules

- Authentication Module
- Database Selection
- Key Generation Module
- Encryption
- Decryption

The authentication module deals with authentication. Any registered employee who is enters his work area after succeeding their authentication. Unauthorized persons were automatically redirected into authentication area. This module provides to create new user registration, change their password and recover password when they are forget it.

The server deals with the admin side. The administrator to gets files from the clients and registered to it. The files are in encrypted xml format. The files are decrypted and data will be restored into server database. The Administrator fetches data from database and converted into machine independent language then uploaded into server. The client module deals with the client side. The client fetches data from database and provides security to that data and converted into device independent language. This data was uploading to the server for administrator verification.

The security deals with handling data encryption and data decryption using cryptic service provider. The public and private keys will be created and stored in server as a XML format. The public key and private key was created and stored into Internet information server. The keys used when security was applied. The conversion module deals with the data convert xml format into plain text format vice versa. This conversion was taken place in server and client side.

The quality analysis module deals with the data verification of each file before restores. The files are sending to quality analysis persons for data verification. The analyzer was analyzed to it and sends back the file with status. This module helps us to track the data through various devices such as mobile phone, PDA, etc.

2. EXISTING SYSTEM

The Existing of data transfer was plain text format in insecure channel. It is possible to capture the data by intruders. The current system was incompatible due to software versioning. Bulk of data cannot transfer through the insecure channel.

2.1. DEMERITS OF THE EXISTING SYSTEM

- The data transfer is a plain text format.
- Due to plain text the data will be insecure
- Bulk data will not transfer from source to destination
- The database structure will be copied and restored
- The system occupy huge memory space
- The Network traffic will be increase
- Possible of missing data
- The version of software is incompatible

3. PROPOSED SYSTEM

The proposed system is a computer based system which overcomes the exiting system. This proposed system provided to fetch all the data from database and converted into encrypted XML format. This xml format do not dependent any operating system, Mail server, browser, server and any other hardware. So this data was software and device independent to the systems.

3.1 Benefits of Proposed System

- While fetching data the database structure will not copied.
- The RSA Encryption / Decryption standard was used for security.
- The Data will be converted into XML Format.
- The XML file will be checked for quality analysis person before restore database.
- Movement of data will be traced by both server side and client side persons.
- The data will be accessed through device independent system.

4. SYSTEM DESIGN

This paper has the process of Encryption and Decryption methods to send the data from one place to another place. To precede this process, we have to decide which data has to be sent. After the selection of database, we have to choose the algorithm to generate keys to encrypt and decrypt. The following sections define the algorithms which are used in this paper.

4.1. RSA

The RSA is an asymmetric algorithm. That is it has two keys, one is for encryption called public key. And the other one for decryption called private key. The key length for an RSA key is 1024bits.RSA key generation formula is:

Public Key : (n,e)
Private Key: (n,d)

4.2. RIJNDAEL/AES

Rijndael is a symmetric algorithm. The rijndael is also called AES (Advanced Encryption Standard). This has the key size of 128,192 or 256 bits. (32 bytes). The keys here are

Password,
Secret Key.

We are using salt to make it harder to guess our key using a dictionary attack**.**

4.3. RC2

RC2 (Rivest Cipher) was designed by Ron Rivest as a replacement for DES and boasts a 3 times speed increase over DES. The input and output block sizes are 64 bits each. The key size is variable, from one byte up to 128 bytes, although the current implementation uses eight bytes. The algorithm is designed to be easy to implement on 16-bit microprocessors.Here the keys are

Password,
IV (Initialization Vector)

4.4. DES

The Data Encryption Standard (DES) encrypts and decrypts data in 64-bit blocks, using a 64-bit key. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length.

4.5. TDES

Triple DES is three times slower than regular DES but can be billions of times more secure if used properly.

- Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits.
- The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple DES.
- The data is encrypted with the first key, encrypted with the second key, and finally encrypted again with the third key.

4.6 Electronic Code Block(ECB)

The ECB method is weak, as the same cipher text appears for the same blocks.

Hello -> ghd%43f=
Hello -> ghd%43f=

4.7 Adding Salt

This is typically clone with an IV(Initialization Vector) which must be the same on both sides. In WEB the IV is incremented for each data frame so that the cipher text changes.

5. DEVELOPMENT

5.1. File Design

While developing this paper we develops the executable files and the source code but also various type of documents such as user manual, software requirements specification document ,design document, test document.

5.2 Input Design

The input design is a part of the overall system design, which requires very careful attention. The collection of input data is the most expensive part of the system, in terms of both the equipment used and the number of people involved. The goal of the input data is to make data entry to be easy and make it free from the logical error. The objectives of the input design phase are to produce cost effective method input, to achieve the highest possible level of accuracy and input was acceptable and understandable. In this system the table authentication used to check the user authorization. Then we can choose tables to encrypt and decrypt. These tables are shown in Appendix I.

5.3. Output Design

The normal procedure is to design the outputs in details first and than to work back to the inputs. The input records have to be validated, edited, organized and accepted by the system before being processed to process to produce the outputs. Output design generally refers to the result generated by the system. For many end users on the basis of the output they evaluated the usefulness of the application. Efficient software must be able to produce efficient and effective reports. In this paper can layout the file register and file restore as a reports.

5.4 Code Design

Codes used in the system are essential to improve the process efficiency and to produce correct input and output. Following certain coding standards OS that if will be easy to debug, allocate less memory space and avoid memory lacks does the code.

5.5. Database Design

The purpose of Database Design is to identify the major modules in the software and describe its components and interfaces for each major module for the users to understand. The database has been designed based upon the entity relationship data model. The database has different tables which each table contain the various data needed for the package. Each table designed in the way that the other database can also take the data from this table. One database is located in server and another database is located in all the clients. So if any error occurred to the client that can be rectified by taking the data from the server.

In this paper tables are designed are authentication, employee, Emp_Details, Emp_Add. All the tables are normalized to avoid redundancy. All the tables are in the database are normalized to retrieve data in efficient manner. These tables are related using proper primary keys and foreign keys. The normalization carried out using following normal forms such as first normal form, second normal form, third normal form, Boyce code normal form. In this paper the database was normalized up to third normal form.

6. Table Structure

Fieldname	Data Type	Length	Constraints
Login	Varchar	50	Primary key
Password	Varchar	50	-

Table 6.1 Authentication

Fieldname	Data Type	Length	Constraints
EmpNo	Int	4	Primary key
EmpName	Varchar	50	-
EmpSal	Varchar	50	-

Table 6.2 Emp_Details

Fieldname	Data Type	Length	Constraints
EmpNo	Int	4	Foreign key
EmpName	Varchar	50	-
Address	Varchar	50	-
EmpPh	Varchar	50	-

Table 6.3.Emp_Add

7. CONCLUSION

This paper was successfully analyzed, designed and developed using Asp.net, C# and SQL server 2005 as a database. The Data was fetched from database and stored in data table. This data was in plain text format. This data was converted into bytes then converted into cyber bytes. These cyber bytes were converted into cyber text. These data was put into container and send to server through insecure channel. In other side the data was received and decrypted, analyzed and stored into database as single xml tag. The Security was applied using Encryption Standards [Asymmetric and Symmetric Encryption]. In Future may apply all symmetric and Asymmetric Encryption can be applied to the data as per user choice.

BIOBLIOGRAPHY

BOOKS

1. Bill Evjen, Scott Hanselman, Srinivas Sivakumar" **Professional ASP.Net2.0"** Wiley Publishing 2006 Edition.
2. David Sussman, Chris ullman **"Beginning ASP.Net with C#"** 2006 Edition
3. Christian Nagel, Morgan Skinner, Bill Evjen **"Professional C#"** Wiley publishing 2004 Edition.
4. Richards A. Mollin"**RSA and public-key cryptography"** CRC Press 2003 Edition.

AUTHORS

1. **S.suresh M.sc., M.Phil.,**
   M.phil(cs) - Muthayammal college of arts & science rasipuram.
   M.sc cs(Apr-2013) - KSR college of art science tiruchengode.
   B.Sc cs(Apr-2011) - Muthayammal college of arts & science rasipuram, Namakkal(DT), Tamil Nadu, India.

2. **L .Gomathi MCA., M.Phil., (Ph.D)**
   BCA(Apr-2002) - Amman Arts & Science College, Chitode
   MCA (Apr-2005)- Bharathidasan University, Trichy
   Mphil (jan 2007) - Periyar university , Salem
   I have been working in our college from 2005 december. My Experience 8 Yrs 10 Months

