Crypto Service

Julie P A
Guest Lecturer
Computer Science Dept
S H College,
Chalakudy

Minu Thomas
Guest Lecturer
Computer Science Dept
S H College,
Chalakudy

***Abstract*--This document provides a complete description of all the functions and specifications of the Crypto Service, a kind of Web service. The general purpose of Crypto Service is to encode and decode the text as well as files. A Web developer can create the Crypto Service and deploy it in the Web server. Several applications in different platform can access this service over the Internet. Crypto Service uses different algorithms for encryption and decryption such as symmetric and hash functions. The programmatic interfaces made available are referred to as Web services. Web services are reusable programs it is defined by the W3C as a software system designed to support interoperable machine to machine interaction over a network. By using Web service applications can publish its functions or messages to the rest of the world. Web services uses XML to encode and decode our data and SOAP to transport it. One of the techniques for ensuring privacy of files and communications is Cryptography. Cryptography is the art or science encompassing the principles and methods of transforming an original intelligible message (Plain text) into one that is unintelligible (Cipher text) and then re-transforming that message back to its original form using algorithms called cipher. Crypto Service is a Web service which uses Cryptography. Web developers or External sites can use this service without writing the code for the service within each application.**

I. INTRODUCTION

The aim of the project is to implement a web service named crypto service on the network. In this project crypto service is applied into an application named YourMail.Com.

Using the server software the user can is able to:

- Encrypt the password stored in the database
- Encrypt the message stored in the database
- Verify the password at login
- User can have a secured storage of password and message stored in the database is not easily readable

The general purpose of Crypto Service is to encode and decode the text as well as files. A Web developer can create the Crypto Service and deploy it in the Web server. Several applications in different platform can access this service over the Internet. Crypto Service uses different algorithms for encryption and decryption such as symmetric and hash functions. The programmatic interfaces made available are referred to as Web services.

Web services are reusable programs it is defined by the W3C as a software system designed to support interoperable machine to machine interaction over a network. By using Web services applications can publish its functions or messages to the rest of the world. Web services use XML to code and decode our data and SOAP to transport it.

One of the techniques for ensuring privacy of files and communications is Cryptography. Cryptography is the art or science encompassing the principles and methods of transforming an original intelligible message (Plain text) into one that is unintelligible (Cipher text) and then re-transforming that message back to its original form using algorithms called cipher. Crypto Service is a Web service which uses Cryptography.

Crypto Service is a web service, it is developed by the Web developer and deploy it in the Web server. Several applications from different platform can access the service via Internet. The general purpose of Crypto Service is encrypt the plaintext into cipher text and decrypt the cipher text back to plaintext using different algorithms such as symmetric and hash functions.

A. Symmetric cryptography

This technique uses a single key for both encrypt and decrypt data. They are also referred to as block ciphers. Important symmetric key encryption algorithms used in Crypto Service are,

1)DES uses a 56 bit key and maps a 64 bit input block of plaintext onto a 64 bit output block of cipher text. DES decryption is essentially done by running this process backwards.

2)TDES also referred to as 3DES, a mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).

3) RC2 is a64 bit block cipher with a variable size key.

4)Rijndael is a block cipher with variable size key which uses 128-bit, 192-bit or 256-bit keys.

B. Hash Functions

Hash Functions also called message digests and on way encryption algorithm.

Hash Functions use no key. Instead, a fixed length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. This includes:

1)MD5 [Message digest] processes a variable-length message into a fixed-length output of 128 bits.

2)SHA-1 produces a 160 bit hash value

3)SHA-256 produces a 256 bit hash value

4)SHA-384 produces a 384 bit hash value

5) SHA-512 produces a 512 bit hash value

II. SYSTEM STUDY AND ANALYSIS

A. *Existing System*

The Existing System is somewhat like a stand-alone application that has a number of limitations.

Want to write the encryption and decryption functionality in DLL and plug in DLL into our application to use that functionality, which is time consuming. This cannot be accessed by other application or developer. It is planned to implement the Crypto Service as a new solution for the existing system.

B. Proposed System

The drawbacks of the existing system has encouraged the need of a new system .It will be very useful for the Web developers .

The Proposed System will overcome all the limitations.

1.It is designed to be run on Windows-based systems.

2.This software can be used in multi user environments where many users will login and perform operations at the same time.

3.Can be used by any applications

4. Single web service for different algorithms

5.Accessible via Internet

6. In future, this can be enhanced with more features

C. Advantages of Proposed System

1.This software can be used in multi user environments where many users will login and perform operations at the same time.

2.Can be used by any applications
3. Single web service for different algorithms
4.Accessible via Internet

Feature of this tool is:

Any webdeveloper can access the server software

D. Feasibility Study

The aim of the feasibility study is to check whether it is possible to develop a system at a reasonable cost which will completely meet the user requirements. At the end of the feasibility study a decesion is taken whether to proceed or not. The proposed system was subjected to 3 types of feasibility tests.

1)Technical Feasibility

Technical feasibility centers around the existing computer system and to what extend it can support the proposed addition.

The Hardware resources required are and Software resources required are ,SQL Server. since these requirements are available with the proposed system, it is technically feasible.

2) Economical Feasibility

Economical analysis involves questions such as whether the company can afford to build the system and whether its benefits should substantially exceed it costs. The amount of fund that the company can pour into the development of the the system is limited and the expenditure must be justified. The developed system work will within the budget of the company and most of the technologies used are easily available today.

3)Operational Feasibility

The new system is very user friendly. This system provides a security for the user. This is very easy to operate and very much understandable.

III . SYSTEM SPECIFICATION

A. Hardware Specification

Processor: Intel® Pentium IV Processor 3.20GHz, 512K / 800MHz FSB
Operating System: Microsoft® Windows XP Professional/ Microsoft® Windows 2000
Memory: 128MB (min) RAM
Keyboard: Entry Level Quiet key Keyboard, PS/2
Mouse: PS/2, 2 button with scroll
Monitor: 15 inch Monitor

B. Software Specification

Software Specification for the Workstations
AS.NET with C# -- Code behind
Visual Studio 2005
NET framework 2.0
IIS 6.0
Internet Explorer 6 or Mozilla Fire Fox
MS SQL SERVER 2005 Database Management System – Back end
Tested on : IIS Web Server on Windows2000/XP Platform

IV. SYSTEM DESIGN

System design is a solution, a how to approach to the creation of a new system. Based on the system analysis report the new proposed system is divided into two modules. These modules itself describes the different functionalities of the system.

A. Design Methodology

The process of system design involves designing the form layouts ,input design and output design. In the design phase of this project both input and output are designed. The project will provide button click options to the user.

B. Input Design

Input design is the process of converting the user originated inputs to a computer based format. The collection of input data is considered to be most important, since the inputs have to be planned in such a way to get the relevant information, extreme care to taken to obtain the pertinent information .The goal of input data is to make data entry as easy, logical and free from errors as possible.
The design of the input for this project focuses on:

- Controlling the amount of input required
- Controlling the errors
- Avoiding extra steps
- Keeping the process simple

Overall inputs to this project include the following:
The main inputs of this project are Web service Test Page .The web service contains different web methods for encryption and decryption using different algorithms.
The different algorithms are:

1. Symmetric algorithms
2. Hash functions

The input required for testing the web method of the web service is the plain text entered the text box of the test page and press the 'invoke' button. Then it invokes the corresponding web method. It is used in an application named Your Mail.Com. The inputs to this application is username and password of the user as a plain text
Inputs for client Application

- Username and password of the user or details of new user entered into the login form.
- Username and password compare with the elements in the database and entered into the second webform.
- New users details registered or stored in the database.
- Specifying one of the following modes

a. Inbox
b. Compose
c. Change password
d. My profile
e. Logout

C. Output Design

Computer output is the most important and direct source of information to the user. Efficient, intelligible output design should improve systems relationships with the user and help in decision making. Without quality output the entire system may appeal to be useless. Designing computer output should be done in an organized manner.
The output design of proposed system focuses on:
Assure purposeful output
Make meaningful output
Assure timeliness
Choose effective output method

The main Outputs of this project are:
The web service gives the output in an XML file. After encryption the plain text will be converted to cipher text using the algorithm and the cipher text will be displayed in the XML file. Also after decryption the plain text will be displayed in the XML file.
Output for client application is:

A form with following modes:

a. Inbox
b. Compose
c. Change password
d. My profile
e. Logout

- List of Inbox of a particular user
- If we select Inbox it shows Subject, Sender
- if we click Subject it will shows message
- If we select Compose we can able to Compose mail
- If we select Change password we can change password
- If we select My profile we can see users profile
- If we select Logout we can Loggoff or click login again button

a. Form Design

Form is physical carrier of data. A form should be self instructing. Actually Crypto Service needs no forms. But for making an application we must prepare some forms. The forms are described below:

1. Login Form :
   This form consists login and new user sign up. In new user sign up we registered the new user. In login user name and password are entered.
2. Inbox: This form consists of inbox of the user.
3. Read: This form shows the message and details.
4. Compose: This form used for composing messages.
5. My profile: This form seeing user's profile.
6. Change password: This form used for changing password.
7. Logout: This form is used for logout or login again.

V. SYSTEM DEVELOPMENT

A. Module

A module is an independent unit of execution that forms part of one or more larger applications. Each module will have its own specific task to perform. Module systems incorporate collections of abstraction in which each functional abstraction, each data abstraction and each control abstraction handles a local aspect of the problem being solved.

Main Modules included in this project are:
1. Encryption
2. Decryption

Module1: Encryption

Encryption is basically an indication of users' distrust of the security of the system, the owner or operator of the system, or law enforcement authorities." Encryption transforms original information, called plaintext or clear

text, into transformed information, called cipher text, code text or simply cipher, which usually has the appearance of random, unintelligible data. The transformed information, in its encrypted form, is called the cryptogram. Encryption algorithm determines how simple or how complex the process of transformation will be

(*1)Symmetric-key encryption algorithms used are,*
(a)DES[Data Encryption Standard]an algorithm that takes a fixed-length string of bits and transforms it through a series of complicated operations into another bit string of the same length, it uses a block size of 64 bits and key length 56 bits.

(*b)Triple DES*[TDES] also referred to as 3DES, is a block cipher formed from the DES cipher by using it three times.

(c)RC2 **(**Ron's Code version 2) is a block cipher algorithm with variable size key.
Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits.

(2)Hash function includes the following algorithms
(a)MD5[Message digest] processes a variable-length message into a fixed-length output of 128 bits.
(b)SHA-1 produces a 160 bit hash value
(c)SHA-256 produces a 256 bit hash value
(d)SHA-384 produces a 384 bit hash value
(e) SHA-512 produces a 512 bit hash value
Decryption: Any procedure used in cryptography to convert cipher text (encrypted data) into plaintext is called decryption ,it is the reverse process of encryption. Decryption requires a secret key or password. Same algorithms above are used for decryption also .

B. Algorithm
1) Crypto Service
Step1 : Start
Step2 : Create a Web service named CryptoService.asmx
Step3 : Each web method for encryption and decryption and comparison using symmetric algorithms and hash function is added into the web service
Step4 : If we run the web service each web method is added and listed in the test page
a. DES decrypt
b. DES encrypt
c. MD5 computeHash
d. RC2 decrypt2
e. RC2 encrypt1
f. Rijndael decrypt
g. Rijndael encrypt
h. SHA1 Compute Hash
i. SHA256 Compute Hash
j. SHA384 Compute Hash
k. SHA512 Compute Hash
l. TripleDES decrypt
m.TripleDES encrypt
Step5 : If we select the option (a) we can use DES decrypt
Step6 : If we select the option (b) we can use DES encrypt
Step7 : If we select the option (c) we can use MD5 compute Hash
Step8 : If we select the option (d) we can use RC2 decrypt2
Step9 : If we select the option (e) we can use RC2 encrypt1
Step10 : If we select the option (f) we can use Rijndael decrypt
Step11 : If we select the option (g) we can use Rijndael encrypt
Step12 : If we select the option (h) we can use SHA1 Compute Hash
Step13 : If we select the option (i) we can use SHA256 Compute Hash
Step14 : If we select the option (j) we can use SHA384 Compute Hash
Step15 : If we select the option (k) we can use SHA512 Compute Hash
Step16 : If we select the option (l) we can use TripleDES decrypt
Step17 : If we select the option (m) we can use TripleDES encrypt
Step18 : Now the web service can be added on a web reference into any client application
Step19 : Stop

2) Application
Step1 : Start
Step2 : Enter the username or password or new user registration
Step3 : if username or password is entered it passes to next form. Then we can go to different steps
Step4 : If we run the web service each web method is added and listed in the test page
a. Inbox
a.1 Message
b. Compose
c. Change password
d. My profile
e. Logout
Step5 : If we select the option (a) we can see the inbox. From the inbox if we select "SUBJECT" we can see message
Step6 : If we select the option (b) we can compose mails
Step7 : If we select the option (c) we can change password
Step8 : If we select the option (d) we can see my profile
Step9 : If we select the option (e) we can move logoff option or login again
Step10 : If w select the new user sign up registration we can move to registration form and we can store the user's details into database
Step11 : Stop

VI. TESTING AND IMPLEMENTATION

A. System Testing

Testing is the major quality measure employed during software development. After the coding phase, computer programs are available that can be executed for testing purpose. Testing not only has to uncover error introduced during coding but also locate errors committed during the previous phase. Thus the aim of testing is to uncover requirements, design or coding error in the program.

System testing is an expensive but critical process that can take as much as fifty percent of the budget for program development. Consequential, different levels testing are employed in fact as a successful is one that find an error the system performance. Criteria deals with turnaround time backup, file protection and human factor. A test for the user acceptance should be carried out. The package development was taken through different level of testing and required modifications were made

Type of testing

The different types of testing are:

1. Unit Testing
2. Integration Testing
3. Validation Testing
4. Output Testing
5. User acceptance Testing

1) Unit Testing

Here they test module individually and integrate the overall system. Unit testing focuses verification efforts even in the smallest unit of the software design in each module. This is also known as “Module Testing" .

The modules of the system are tested separately. This testing carried out in the programming style itself. In this testing each module is focused to work satisfactorily as regard to expected output from the module.. There are some validation checks for the fields.

2) Integration Testing

Data can be lost across an interface; one module can have an adverse effect on the other sub functions, when combined may not produce the desired functions. Integrated testing is the systematic testing to uncover the errors within the interface. This testing is done with simple data and the developed System has run successfully with this simple data. The need for integrated system is to find the overall system performance. At the culmination of the black box testing, software is completely assembled as a package.

3) *Validation Testing*

At the culmination of the black box testing, software is completely assembled as a package. Interfacing errors have been uncovered and correct and final series of test. i.e. , validation test van is defined with a simple definition that validation succeeds when the software function in a manner that can be reasonably accepted [by the customer.

4)Output Testing

After performing validation testing the next step is output testing of the proposed system. Since the system cannot be useful if it does not produce the required output. Asking the user about the format in which the system is required tests the output displayed or generated by the system under considerations. Here the output format is considered in two ways . One is on screen format and other is on printed format. The output format on the screen is found to be corrected as the format was designed in the system phase according to the user needs. As for the hard copy the output comes according to the specification requested by the user. Here the output testing does not result in any correction in the system.

5)User Acceptance Testing

User acceptance testing of the is the key factor for the success of any system. The system under consideration is tested for the user acceptance by constantly keeping in touch with prospective system at the time of development and making change whenever required. This is done with regard to the input screen design and output screen design.

B. Implementation

Implementation is the stage where the theoretical design is turned into a working system and giving confidence on the new system for the users that will work efficiently and effectively. It involves careful planning, investigation on the current and its constraints on implementation, design of methods to change over, an evaluation of change over methods. Apart from planning major task of preparing the implementation are education and training of users. The more complex system being implemented, the more involved will be the system analysis and the design effort required for implementation. An implementation coordinating committee based on the policies of individual organization has been appointed. The implementation process starts with preparing a plan for the implementation of the system. According to this plan, the activities are carried out, discussion made regarding the equipment and resources and the additional equipments needed to implement the new system.

Implementation is the final and important phase. The most critical stage in achieving a successful new system and in giving the users confidence that the new system will work effectively. The implementation can be done only after testing is done and if it found to working according to the specifications. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain types of transactions while using the new system.

And the beginning of the development phase a preliminary implementation plan is created to schedule and manage the different activities that must be integrated into plan. The implementation plan is updated throughout the development phase, culminating in changeover plan for the operation phase. The major elements of implementation plan are test plan, training plan, equipment installation plan and a conversation plan.

There Are Three Types of Implementation:

1. Implementation of a computer system to replace the manual system.
2. Implementation of a new computer system to replace an existing system.
3. Implementation of a modified application to replace an existing one, using the same computer.

VII. CONCLUSION

The Web Service CryptoService is successful in meeting its requirement specification. It is considered to be furistic and secure. This is very helpful because

1. Can be used by any applications
2. Single web service for different algorithm
3. Accessible via Internet

The world of computers is not static, it always subject to change. The technology that is popular today will become outdate the very next day. So the project is not concluded yet it will improve the further enhancements.

VIII. REFERENCES

[1] www.msn.com
[2] Computer Networks-Andrew S Tanenbaum (Fifth Edition)
[3] Data Communications and Networking-Behruz Forouzan (Fourth Edition)