Secure Transformation of Data Using Smiley Encoder Algorithm

S. Usharani, D. Saravanan, D. Jayakumar

Department of CSE, IFET College of Engineering, Villupuram, Tamil Nadu, India

ABSTRACT

The proposed system helps to provide a secured transformation of data through each end server and receiver with the help of smiley encoder algorithm. The purpose is to provide a more secured message to the legitimate recipients using smiley Encoder, a special encoding technique. The idea is to create more secure transfer of message from one person to another person using Simple Message Service (SMS). After the user logs into the account, the message will be encrypted to emoticons. For further secure, MD5 algorithm is used. MD5 algorithm is used to pass hash value for encrypted message, before sending message. The encrypted message is sent to the specified email id. The recipient needs a secret key to view the original message. Finally, the encrypted message is decrypted to original message, which is viewed by the recipient. These two encryptions provide more security to content of user and delivery safely to required user without any interruption.

Keywords: Emoticon Encoding, Secure Messaging System (SMS), MD5 Algorithm, Secret key.

I. INTRODUCTION

From the encoder messaging system helps to encode the data along the distributed network who can serve a secured transformation of message together. Web services are self-contained, modular, distributed, dynamic applications that can be described, published, located, or invoked over the network to create products, processes, and supply chains. These applications can be local, distributed, or web-based. Web services are built on top of open standards such as TCP/IP, HTTP, Java, HTML, and XML. A web service is a collection of open protocols and standards used for exchanging data between applications or systems. Software applications written in various programming languages and running on various platforms can use web services to exchange data over computer networks like the Internet in a manner similar to inter-process communication on a single computer. This interoperability (e.g., between Java and Python, or Windows and Linux applications) is due to the use of open standards. The basic web services platform is XML + HTTP. All the standard web services work using the following components

- ✓ SOAP (Simple Object Access Protocol)
- ✓ UDDI (Universal Description, Discovery and Integration)
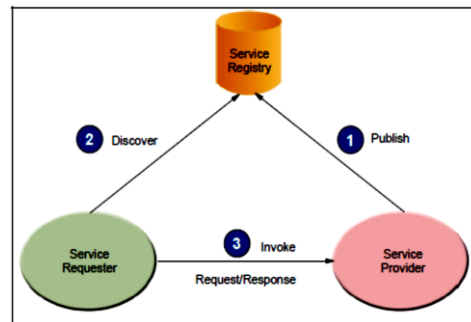- ✓ WSDL (Web Services Description Language)
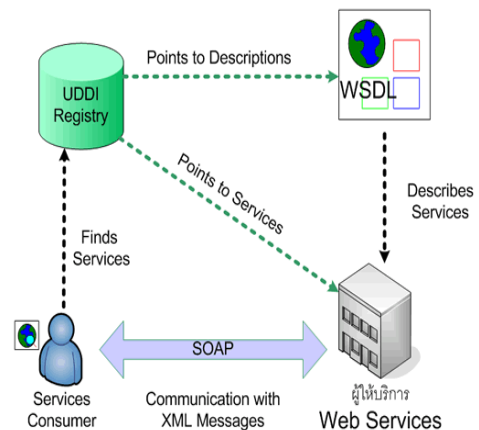

Figure 1: Web Services Basic Flow

Figure 2: Webservices Architecture

II. EXISTING SYSTEM AND PROPOSED SYSTEM

a) Existing System:

Email on the internet is now commonly sent by the Simple Mail Transfer Protocol (SMTP). This does not encrypt the text of emails and so intercepted mail can be read easily unless the user adds their own encryption. Email may be protected by methods such as a strong password, encryption of the contents or a digital signature. Email is based around the use of electronic mailboxes. When an email is sent, the message is routed from server to server, all the way to the recipient's email server. More precisely, the message is sent to the mail server tasked with transporting emails (called the **MTA**, for *Mail Transport Agent*) to the recipient's MTA. On the Internet, MTAs communicate with one another using the protocol SMTP, and so are logically called **SMTP servers** (or sometimes *outgoing mail servers*). The recipient's MTA then delivers the email to the incoming mail server (called the **MDA**, for *Mail Delivery Agent*), which stores the email as it waits for the user to accept it. Retrieving mail is done using a software program called an **MUA** (*Mail User Agent*). When the MUA is a program installed on the user's system, it is called an email client. When it is a web interface used for interacting with the incoming mail server, it is called webmail. The identity of the sender or addressee of an email is not authenticated and this provides opportunities for abuse such as spoofing. Email has to go through potentially un trusted intermediate computers before reaching its destination, and there is no way to tell if it was accessed by an unauthorized entity. This is different from a letter sealed in an envelope, where by close inspection of the envelope, it might be possible to tell if someone opened it. In that sense, an email is much like a postcard whose contents are visible to everyone who handles it. Implementing security measures is a necessity such as installing a sniffer as well as an intrusion detection system (IDS) to make sure that nobody is accessing your network without permission and to detect any network intrusion attempts.

b) Proposed System:

The idea is to create more secure transfer of message from one person to another person using **SECURE MESSAGING SYSTEM**. It provide a more secured message to the legitimate recipients using **EMOTICON ENCODING**, a special encoding technique. After the user logs into the account, the message will be encrypted to emoticons. For further secure, **MD5** algorithm is used. MD5 algorithm is used to pass hash value for encrypted message, before sending message. The encrypted message is sent to the specified email id. The recipient needs a secret key to view the original message. Finally, the encrypted message is decrypted to original message which is viewed by the recipient. These two encryptions provide more security to content of user and delivery safely to required user without any interruption. Nowadays Email on the internet is now commonly sent by the Simple Mail Transfer Protocol (SMTP). This does not encrypt the text of emails and so intercepted mail can be read easily unless the user adds their own encryption. Email may be protected by methods such as a strong password, encryption of the contents or a digital signature. The identity of the sender or addressee of an email is not authenticated and this provides opportunities for abuse such as spoofing. To protect this kind of activity using special encoding techniques for protecting data before sending mail to other user. This application can stop that kind of activity and protect data from intruders.

III. WORKING PROCESS

A web service enables communication among various applications by using open standards such as HTML, XML, WSDL, and SOAP. A web service takes the help of:

✓   XML to tag the data
✓   SOAP to transfer a message
✓   WSDL to describe the availability of service.

You can build a Java-based web service on Solaris that is accessible from your Visual Basic program that runs on Windows. You can also use C# to build new web services on Windows that can be invoked from your web application that is based on Java Server Pages (JSP) and runs on Linux.
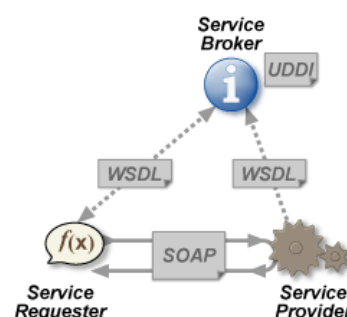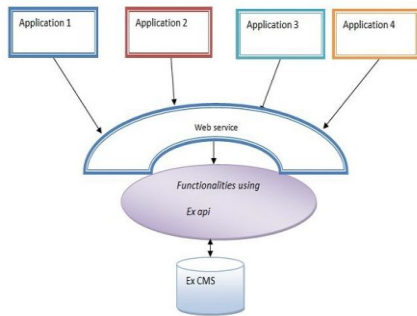

Figure 3: Working of Web Services

Figure 4: Web Service Exposing Functionalities as Service

❖ **Modules**
- Authentication
- Smiley encryption
- Dispatch the mail
- Decipher the message

➢ **Authentication**

Users are the ones who are going to access the information stored in the Server database. We implement the User Interface frame to send the user's request. The user logs into the content page by entering the username and password. The content page allows the user to enter the specific recipient's mail id and the message to be sent to the recipient. The message will be submitted in the content page after the user has entered the text.

➢ **Dispatch The Mail**

After the process of encryption gets over, the encrypted message will be sent as mail to the specified email id. The mail will be sent in a secured format .The mail should contain only link so that the hackers cannot hack the contents of the mail, so it provide data security.

➢ **Decipher The Message**

The contents will be decrypted or double decryption is performed to display the original message content to the recipient. Thus the decryption makes only the authorized recipients to view the message.
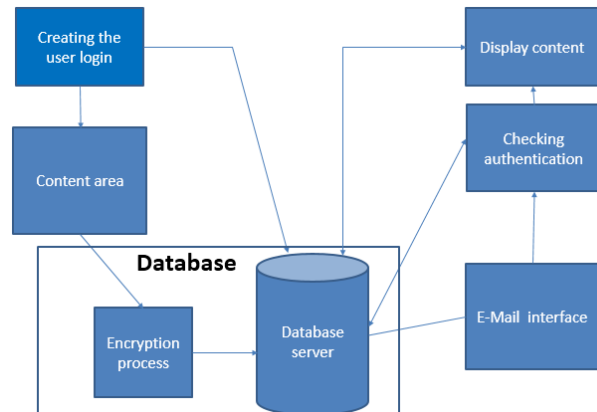
IV. SYSTEM ARCHITECTURE

Figure 5: System Architecture

V. CONCLUSION

Since web services are the vast developing technology, security is the major factor in the web services environment. To overcome this drawback many existing approaches has been introduced but they have not fulfilled the security issue. At this situation storing and sending message or data in web services environment is the major issue, because the data will be hacked (corrupted) or modified by the unauthorized person in the network. So we need a new mechanism to be implemented in the web services environment for storing and sending the message in web services. By implementing this project we can allow the authorized users to enter into the network and respond to the queries submitted by the registered user in the web services network using special encrypting techniques mechanism so that we get more result protecting data from intruders.

VI. FUTURE ENHANCEMENT

In future we allow all type of character including special characters, smiley based encryption scheme to view the records so that we can increase the security level. Additional security can be added to verify the individual's identity.

VII. REFERENCES

[1]. Use of Human Cognition in HIP Design via Emoticons to Defend BOT Attacks Nayeem,M.T, Dept.of Computer. Sci. & Inf.Technol. (CIT), Islamic Univ.of Technol.(IUT), Gazipur,

Bangladesh ,Mukta,M.S.H. ; Ahmed,S.;Rahman,M.M. 2012

[2]. Polarity Identification of Sentiment Words Based on Emoticons ShuiguiHuang, WenwenHan,X irongQue, Wendong Wang 2013

[3]. A Generational Approach to using Emoticons as Non Verbal Communications Krohn F.B 2003

[4]. EMOTION+ ICON =EMOTICON =SMILEYC live Dadida, kinsuk Kalyan Sarker, Paul Dhilwayoand Prof. Dr DhruboJyotiSen2011

[5]. Visual Cues in Computer -Mediated Communication : Supplementing Text with Emoticons Rezabek,Landra L.; Cochenour,John J 2008