www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11437-11443

Encrypted Data Transmission for secured SMS over Web via E-Mail Platform

MugheleEse Sophia

School of Science and Technology, Department of Computer Science.Delta State School of Marine Technology, Burutu Delta State Nigeria.

Email: prettysophy77 **@yahoo.com,** prettysophy99@gmail **.com**

ABSTRACT
The rapid development of computers andthe way in which technology has been used to supportpersonal needs of users as well as businesses worldwide have been changed by the emergence of the internet. As the Internet becomes a more pervasive part of daily life,people fail to realize that the internet would establish itself as a powerful facilitator of the needs of the common man in such a short period of time. However, an individual's private information can be disseminated withouthis/her knowledge.Many different types of email security threats exist. The security of an email can be compromised by identity theft, spoofing, imposters and modification of existing messages. Hackers may use all or any of these aforementioned methods to have access into a user's computer.However, the computer architecture that is being used exchange of email are not very reliable and hence, does not provide for much privacy for the users.This undeniable fact is what has prompted the researcher to work on the Secured and Encrypted Data Transmission over the Web in order to protect information exchanged over the internet from being compromised.
Keyword: Data Transmission, Encryption, E-mail, SMS, E-mail.

1.1 INTRODUCTION

Acomputer based global information system isknown as an internet. It comprises many computer networks being interconnected (The Oxford Learning Dictionary, 2009). Thousands of computers may be linked in each networkenabling them to share information. So many aspects of human life have been transformed by the emergence of the internet. It has contributed immensely in the making of the world a global village. Internet usage has grown tremendously sinceits introduction. This is due toits flexibility. One of the most important benefits of the internet to mankind is the access to vast information.

Communication through the internet can be achieved through various forms of communication technologies used such as email, discussion groups, theemail is regarded as the most appealing and most used of all thecommunication technologies on web. In spite of the tremendous benefits of these communication tools, there however exist serious issues associated with their use. The email information and email transfer protocol was traced by Klensin (2008).The architecture of the computer that is used for email exchanges are not very reliable and does not provide for much privacy for the users.This undeniable fact is what has prompted this research work on the Secured and Encrypted Data Transmission over the Web in order to protect information exchanged over the internet from being compromised.

1.2 RESEARCH MOTIVATION

The transfer of information over the internet through various communication technologies and the manner in which communication is implemented on the Internet makes it susceptible to monitoring. In the case of email communication, the email system comprisesservers that store and process email

messages on behalf of users who connect to the email system via web interface or e-mail client. Whena message is sent or received, it resides on the machine of the email providers who can have access to its contents so as to monitor and ensure that its contents abide with the email provider's terms of service, hence the privacy of the messages are compromised. The inability to cancel message that has been sent, in most of the communication technologies used, it is very well near impossible to cancel a message that had been send in error. Once sent, it can never be canceled and will always reach the recipient. More also, wrong recipient is a very common mistake made by internet users to send messages to the wrong person's account. Due to the inability to prevent an already sent message from reaching its destination, possibly vital information could be exposed to wrongful persons and impersonation is possible. For unsuspecting users to have the passwords of their internet communication mediums account compromised, allowing the unauthorized users to impersonate them. The unauthorized users can also use their account to send messages to their contacts, impersonation the real owner of such account. Unscrupulous individuals can gain access to the accounts of users and gain access to their confidential information.

1.3 RELATED LITERATURE

It is a paradox that in spite of the development in technology being witnessed in this present time, an individual's privacy and security of data is frequently compromised to a very large extent. Often, personal information of individuals is stolen or financial data of companies are moved away by elements which could put to the wrong use such information. This has privacy of data become an issue of great importance for users of internet all over the world. Data privacy becomes extremely essential especially when one works in a public domain like the Internet(Pittsburgh Business Times Journal, 2001).

This paper review the security issues associated with sending electronic mails over the internet and various ways at how these issues can be addressed.

1.3.1 ELECTRONIC MAIL

Electronic mail (e-mail or email) is defined as a way digital messages are being exchanged between two agents i.e. from a source to one or more receiver. Modern email operates across various computer networks as well as the internet. Some early email systemssuch as instant messaging,required that the sender and the receiver both be online at the same time. This day, e-mail systems are based on a store- and-forward model. Messages are being accept, forward, deliver and store by e-mail servers. Neither the users nor their computers need to be online simultaneously; they need connect only for a short time, typically to an email server, for as long as it takes messages to be sent or received. (Craig, 2008).Three components which include the message header, the message body and the message envelope make up an e-mail message. The header contains control information, including, an originator's email address and one or more recipient addresses. Usually attributive information is also included, such as a subject header field and a message submission date/time stamp(Craig, 2008).

E-mail predates the beginning of the Internet, and was in fact a pivotal tool in its creation, but the modern history, global Internet email services reaches back to the early ARPANET. TheStandards for encoding e-mail messages were proposed as early as 1973 (RFC 561).In the early 1980s, theconversion from ARPANET to the Internet resulted to the essential part of the current services. An e-mail sent in the early 1970s looks quite similar to a basic text message sent on the Internet today.

1.3.2 CHALLENGES OF E-MAIL

Electronic mail communication usually encounters a lot of challenges such aslimitation of the size of attachment. E-mail messages may have one or more attachments. Attachments serve the purpose of binary or text files of unspecified size delivery. In standard, there is no technicalessential limitation in the SMTP protocol on the size or number of attachments. In practice, however,various restrictions on the allowable size of files or the size of a whole messageare being implemented by email service providers (Dierk& Dawson, 2008).Frequently, a small attachment can increase in size when sent due to technical reason.

1.3.3 E-MAIL SECURITY THREATS

Spamis defined as transmission of unrequested bulk (or commercial) e-mail, often to large or multiple number ofreceivers, or multiple postings

of the identical message sent to newsgroups or list servers. Spam is junk mail in electronic form. Studies have shown that approximately half of all spam mail is associated to money(such as advertisingdebt- reduction plans, gambling opportunities and get-rich-quick schemes).A third is porn-based, and this figure is set to increase. About 10 percent is health-related, and the rest covers a wide range of topics. A list of tips to aid an individual to respond appropriately to spam was highlighted by I-SAFE Inc. They are:

- **Ensure your e-mail address is protected.**

1. Make a separate e-mail address is created and used for public use (i.e. for registration, Web forums posting, or purchasing online etc.).
2. Givingpersonal email address to any other individuals apart from friends, family, or business associatesshould be avoided.
3. Read the website's privacy policy to make sure that your email address will not be used or sold to a third party before registration.
4. Do not display your email address onlineopenly, for instance, in chat rooms, on web forums, or inprofiles.
5. Copying and then pasting the text into a new emailwhen forwarding mail to others before sending. This is because "Forward" also forwards the email address (es) of the prior recipients of the email when clicked. Educate friends and family to use this method to prevent having your email address forwarded to a person(s) unaware(Shirley et al., 2008).

- **Use technology to block spam.**

1. E-mail clients, for instance Microsoft Outlook Express, possess spam- blocking features and message principle that can prevent email that are unrequested for. The "Help" tab can be checked to know how to activate these features in the email client.
2. Your Internet service provider (ISP) can be contacted to know the spam- blocking utilities being offered and how it can be activated.

- **Spam should never be responded to.**

"Unsubscribe" links in spam emails should be ignored. If the email received do not require a subscription, it is unlikelythe spam emails can be stopped by unsubscribing. Instead,response to the email essentially validates that your email address is active and being read.Your e-mail address would often subsequently be sold by professional spammersto others (AISW, 2004).

- **Spam emails should be reported.**

The United States has the CAN-SPAM ACT (Controlling the Assault of Non- Solicited Pornography and Marketing Act). In order for any spam emails to be reported, a copy should be forwarded to spam@uce.gov (SAFE Inc, 2006). Phishing Identity thieves often "phish" for information by sending pop-up messages or e-mail spam which appear legitimate (i.e. bank or online payment services that you may deal with). These phishes entice their victims to false Web sites that appear legitimate. Moreover, these are intended to deceive an individual into revealing information needed to steal his/her identity to perform fraudulent acts. Viruses or other malicious programs usuallyattach to emails and are secretly downloaded onto your computer to collect your personal and financial information(SAFE Inc, 2006).

Thoughidentifying phishing emails is not an easy feat, here are some tips for help:

i. Look out for wrong spelling and grammar. A careless scammer often makes spelling and grammar mistakes that a legitimate company's proofreaders would have observed.
ii. Greetings that are genericshould be observed. This is becausemost companies address an individual by his/her name or Web site "username" when corresponding with him/her.Greetings, such as "Dear Valued Customer," should raise a red flag. Companies do not send emails for urgent requests for personal information.
iii. Watch out for account suspension or cancellation warnings. Scammers frequently use these means to deceive their victims in order to disclose financial or personal information.

1.3.4 Email Encryption Solution

Entrust Intelligence Messaging Server:Entrust email encryption solutions work with a broad range of email applicationswhich includesLotus Notes/Domino and Microsoft Outlook/Exchange.It can be used by mobile users (such as RIM BlackBerry handheld devices) and through secure web mail. Entrust email encryption software uses PGP, S/MIME and Entrust encryption formats(Entrust, 2012). The users of Entrust email encryption benefit fromthe following; Automatic encryption, digital signatures, Transparent and easy-to-use email securityIntegration with content analysis tools for email compliance, Government strength' security validated against NIST standards.

Itis an appliance-based email encryption gateway that makes secure communication easy with customers and partners. Offering standards-based OpenPGP, S/MIME and Web-based encryption options for secure message delivery from Lotus Domino environments and Microsoft® Exchange, the risks, cost and time of conducting a wide range of tasks electronically can be reduced by Messaging Server, including the financial data distribution, contract negotiations, HR information, personalized customer communications and many more.

TheSymantec PGP Desktop Email Encryption Software**:** The Symantec PGP Desktop Email encryptionsoftware is one of the most detailed and intricate programs on the market. The email encryption software takes a comprehensive approach to security and meets the needs of even the most ardent and protective financial institutions and business owners. This is not a casual after thought approach to security. With true end- to-end security options utilizing several encryption programs and proxies, the system is foolproof (Symantec Corporation, 2012).

PGP Desktop Email automaticallyencrypts email as it is being received and sent on laptops desktops, without the end-user email experience being affected. It operates as a proxy, supports the two global email encryption standards, OpenPGP and S/MIME and discovers keys and certificates automatically as required. Features include:

- True end-to-end email encryption using standards-based OpenPGP and S/MIME message formatsis enabled.
- It functionsas a proxy to enhance performance while removing the need for application- and version- specific plug-ins and also works with standard email clients such as Lotus Notes, Thunderbird, Outlook, and many more.
- Provision of secured email solutions whichautomatically encrypts and decrypts sensitive email with the user experience unaffected.

Voltage Secure Mail: Voltage Secure Mail incorporates several components. Centralized management, policy-based encryption and reporting are being provided by the Secure Mail Gateway server. Seamless encryption is being provided since theclients integrate directly into Microsoft Outlook,while the Zero Download Messenger allows the recipient to access secure email without the need to download decrypters as well as other tools(Shore, 2012). Secure Mail also hassupport for wireless devices such as BlackBerryand anti- phishing capability.Secure Mailoffers a lot of flexibility. This product seems to have been designed with a Microsoft environment in mind.As they are.msi files, the clients can be deployed by individual users or by means of domain group policy.When that is coupled with direct Outlook integration and the fairly simple policy configuration, this product can really shine in seamless integration.The Voltage Secure Mail Desktop email encryption solution makes use of a simple, secure, Identity Based Encryption (IBE) Algorithm.

Proof point Protection Server: The Proof point Protection Server 2.0 product handles spam well by default. With its content filtering, reporting, and optional antivirus module (provided by Network Associates), companies can enforce confidentiality, compliance, and security policies. The Proof point Server acts as a relay between your mail server and the outside world. You reroute mail to the Proof point server with a DNS MX record (instead of pointing to your internal mail server), and the Proof point Server inspects all messages for spam, content violations, and viruses (if you buy that option). The Proof point Server uses rules configured by the administrator to quarantine or pass along e-mail. At the heart of the product is Proof point's MLX engine, which evaluates e- mail messages for spam and other problem content. The Proof point Server contains more than 50,000 rules that serve to separate spam from good e- mail, and the company updates the

rules weekly to address the latest spam trends. Customers can add custom rules to ensure that important e-mails are not quarantined. In this new version, individuals can create their personal safe lists and block lists using a clever e-mail interface to override any corporate spam rules. For companies concerned about confidentiality and regulatory compliance, the Proof point Server contains extensive reports and content filtering. Administrators can display, schedule, publish, and e-mail numerous reports concerning spam, viruses, or e- mail content. They can also catch specific phrases, such as patient names, using simple text checks or even regular expressions.

1.4 Methodology

System Algorithm

Algorithms represent the sequence of the actions or events to be performed by a program. The algorithm used for the development of the system is treated below.

Solution Algorithm

1. User logs into the system with username and password

2. User selects option to add contact, send message or decrypt message from the menu

3. If option chosen is add contact, goto 6

4. If option chosen is decrypt message, goto 7

5. If option chosen is send message, goto 10

6. User adds contact information and stores in database

7. User input encrypted message received into system

8. User supplies encryption key

9. Message is decrypted

10. User enters message into system

11. Message is encrypted

12. The encryption key is generated

13. SMS message is sent to the recipients' mobile phone

14. Message is sent to destination email address

1.5 USER CASE DIAGRAM

The user case diagram shows the users of the system, the components of the system and the interaction that exists between them. Below is the diagram.

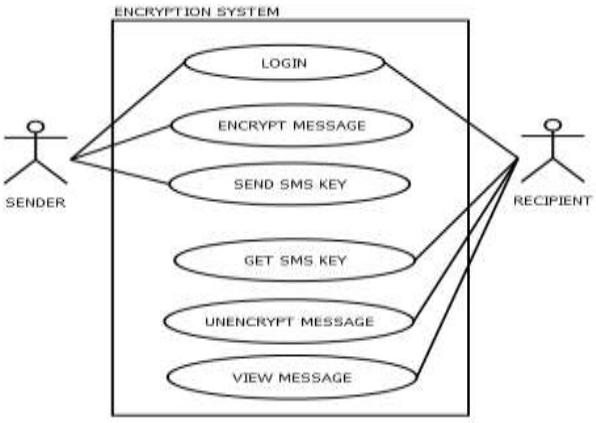


Fig1. User case diagram

1.6 DATABASE FILES

The database system that will be used to store the information for this system will be Microsoft Access. Below are the descriptions and structure of the database files to be used by the system:

User info file: This database file will contain the information about the users allowed to use the solution.

Table 1: User_info table structure

S/N0	FIELD NAME	DESCRIPTION	FIELD SIZE	DATA TYPE
1.	User_id	Unique identification number for the user	30	Int
2	User-name	Username for the user to login to the system	50	Varchar
3.	Password	Password for the user to login to the system	50	Varchar

Recp_info file: This database file will contain the information about the recipients of the messages.

Table 2: Recp_info table structure

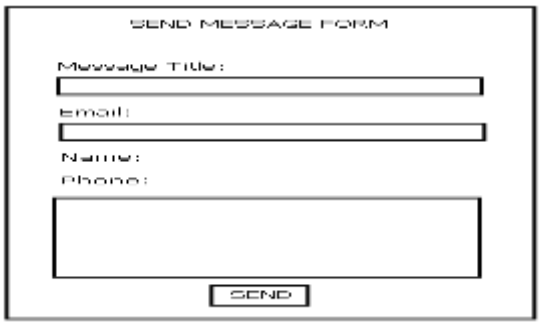
S/N0	FIELD NAME	DESCRIPTION	FIELD SIZE	DATA TYPE

1.	Recp_id	Unique identification number for the recipient	30	Int
2	Name	Name of the recipient	50	Varchar
3.	Email	Email address of recipient	50	Varchar
4.	Phone	Phone Number of recipient	11	Varchar

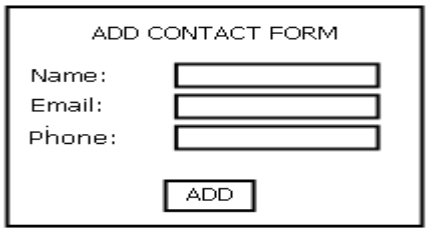
USER INTERFACE DESIGN: The user interface is designed with the Visual Basic programming language and will be able to run on and Microsoft Windows Operating System Platform.

Below are the design interfaces for the various modules of the system.

Send Message Form: This form lets the user encrypt and send messages to the electronic mail inboxes of the intended recipients.

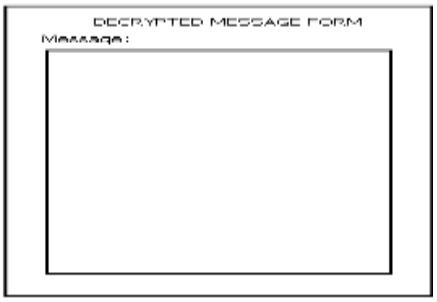


INPUT INTERFACE DESIGN

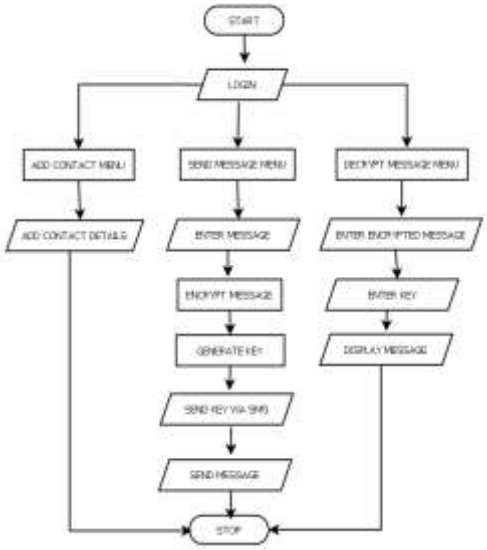


OUTPUT INTERFACE DESIGN

Decrypted Message Form: This interface will display the decrypted message for the user to read.



Decrypt Message Form: This interface lets the user to add the encrypted message along. Below is the diagram showing the flowchart with the key for the system to decrypt.



SYSTEM FLOWCHART of the proposed system

Add Contact Form: This interface lets the user to add the contact details of the recipients to the database.

1.7 SUMMARY

The internet provides us with a multitude of communication tools of which the one of the most widely used is the electronic mailing system (email). The e-mail has rapidly replaced the use of the traditional postal mailing services as it is less costly to use and much more efficient as the mails are delivered much faster and without the risk of it missing on the way. Despite its achievement, there exist security loop holes in the system, and like several other communication channels that are operated over the internet, the messages sent are susceptible to interception by unintended readers thereby making the information being exchanged to be insecure. This has led to the development of a Secure and Encrypted Data Transmission Solution that makes use of encryption algorithms

to encode the messages to be send through the electronic mailing system and produce an encryption key which will be sent to the intended recipient via some other secure means of communication who will use the key to decrypt and gain access to the contents of the message.

1.8 RECOMMENDATIONS

The following are recommended based the findings from this research;

1. The solution should be improved upon by including a means of reading encrypted mails sent to receiver's inbox without the need for the receiver to visit the email providers' website to log in and open the mail.

2. Findings from this solution should be used in developing means of securing information exchange in other communication tools used over the internet

3. The solution is suitable for use by any organizations using private mailing systems, such as bank, as the information exchanged between staff within the organization is bound to contain sensitive data that should be secured.

1.9 CONCLUSION

The successful implementation of this solution will provide a secure means of sending messages over the internet through the electronic mailing system. It is the hope of the researcher that the results from this paper will be used in the nearest future to aid in the development of means of securing information exchange in other communication tools used over the internet.

REFERENCES

A Matter of (Wired News) Style. Wired magazine "Email History, How Email was Invented, Living Internet". Pittsburg Business Times Journal, Vol 7, pp 223-236, 2001.

Bill Steward Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. "Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail." In CHI 2006 (Proceedings of ACM SigChi) "PGP Encryption Proves Powerful". PCWorld. 2003-05-26. Retrieved 2014-02- 08.

Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and SeungjaeYoo (2004), Secure Key Issuing in ID-based Cryptography ACS Conferences in Research and Practice in Information Technology - Proceedings of the Second Australian Information Security Workshop-AISW

Craig Hunt (2008). TCP/IP Network Administration. O'Reilly Media. p. 70. ISBN 978-0596002978.

John Klensin (October 2008). "Trace Information". Simple Mail Transfer Protocol. IETF. sec. 4.4. RFC 5321. Oxford Learning Dictionary (Draft.Ed.) March 2009 and Retrieve In 26th October &

T. Dierks, E. Rescorla (August 2008). "The Transport Layer Security (TLS) Protocol, Version 1.2". Herman, Tony L. (23 October 2014).