SECURED EMAIL SYSTEM USING ENCRYPTION

Manasa Jandhyala
Manasajandhyala8@gmail
SRM UNIVERSITY

Aparna Suriaraj
Aparna2123@gmail
SRM UNIVERSITY

Sampriti Barman
sampriti.barman2012@gmail
SRM UNIVERSITY

Dhathri Gallipelli
Dhathrig@gmail
SRM UNIVERSITY

ABSTRACT

The main reason for using email is probably the convenience and speed with which it can be transmitted, ir-respective of geographical distances. Similar to a post-card, an email has open access to the systems on its path. If anyone wants to intercept, copy or alter information, they can easily do so. Confidential information, such as bank statements, trade secrets, and even national secret information, is being exchanged through emails. There- fore, the contents of emails are more important and valuable than ever, and their security has raised many concerns. The main reason for not using encryption in email communications is that current email encryption solutions require expensive operations and hard key management. Therefore, research on simple, highly secure and efficient email systems are in great need. Current email systems that use symmetric and asymmetric cryptographic schemes super from key management problems. Identity Based Cryptography systems, which have been proposed to address such key management issues, also suffer from the key escrow problem, which violates the non-repudiation feature that should be offered by security systems. Most of the existing mailing systems provide limited authentication .In symmetric cryptography, the main disadvantage is that the same key is used. The main idea is to use asymmetric key encryption which is way more secured than symmetric encryption. The data is encrypted using AES algorithm (Advanced encryption standard).

Keywords: - *asymmetric, encryption, AES, secured, key*

1.Introduction

The main reason for using email is probably the convenience and speed with which it can be transmitted, ir-respective of geographical distances. Similar to a post-card, an email has open access to the systems on its path. If anyone wants to intercept, copy or alter information, they can easily do so. Confidential information, such as bank statements, trade secrets, and even national secret information, is being exchanged through emails. There-fore, the contents of emails are more important and valuable than ever, and their security has raised many concerns. The main reason for not using encryption in email communications is that current email encryption solutions require expensive operations and hard key management. Therefore, research on simple, highly secure and efficient email systems are in great need.Current email systems that use symmetric and asymmetric cryptographic schemes super from key management problems. Identity Based Cryptography systems, which have been proposed to address such key management issues, also suffer from the key escrow problem, which violates the non-repudiation feature that should be ordered by security systems.

1.1 Overview of platform

The NetBeans Platform is a generic framework for Swing applications. It provides the "plumbing" that, before, every developer had to write themselves—saving state, connecting actions to menu items, toolbar items and keyboard shortcuts; window management, and so on. The NetBeans Platform provides all of these out of the box. You don't need to manually code these or other basic features, yourself, anymore. See what some

NetBeans-based applications look like. The platform does not add a lot of overhead to your application — but it can save a huge amount of time and work.The NetBeans Platform provides a reliable and flexible application architecture. Your application does not have to look anything like an IDE. It can save you years of development time. The NetBeans Platform gives you a time-tested architecture for free. An architecture that encourages sustainable development practices. Because the NetBeans Platform architecture is modular, it's easy to create applications that are robust and extensible. NetBeans allows applications to be developed from a set of modular software components called modules. NetBeans runs on Microsoft Windows, macOS, Linux and Solaris. In addition to Java development, it has extensions for other languages like PHP, C, C++ and HTML5.[3], Javadoc and Javascript. Applications based on NetBeans, including the NetBeans IDE, can be extended by third party developers.[4] The platform offers reusable services common to desktop applications, allowing developers to focus on the logic specific to their application. Among the features of the platform are:

- User interface management (e.g. menus and toolbars)
- User settings management
- Storage management (saving and loading any kind of data)
- Window management
- Wizard framework (supports step-by-step dialogs)
- NetBeans Visual Library
- Integrated development tools

1.2 User interface

The user interface (UI), in the industrial design field of human computer interaction, is the space where interactions between humans and machines occur. The goal of this interaction is to allow effective operation and control of the machine from the human end, whilst the machine simultaneously feeds back information that aids the operators' decision-making process. A good user interface is required for any ap-plication to be successful. The user interface (UI), in the industrial design field of human computer interaction, is the space where interactions between humans and machines occur. The goal of this interaction is to allow effective operation and con-trol of the machine from the human end, whilst the machine simultaneously feeds back information that aids the operators' decision-making process.

User interface is the front-end application view to which user interacts in order to use the software. User can manipulate and control the software as well as hardware by means of user interface. User interface is part of software and is designed such a way that it is expected to provide the user insight of the software. UI provides fundamental platform for human-computer interaction. UI can be graphical, text-based, audio-video based, depending upon the underlying hardware and software combination. UI can be hardware or software or a combination of both.

1.3 Hardware interface

An architecture used to interconnect two devices together is called hardware interface. It includes the design of the plug and socket, the type, number and purpose of the wires and the electrical signals that are passed across them. Android devices have multiple different types of hardware that are built in and accessible to developers. Sensors, such as a camera, accelerometer, magnetometer, pressure sensor, temperature sensor, and proximity sensor, are available on most devices. Telephony, Bluetooth, and other wireless connections are also accessible to the developer in some form.

1.3.1 Hardware components

Following are the hardware requirements for developing Email Security System:

1.Processor i3 2.93 GHz

2.RAM 2GB

3.HDD Space 4GB

1.4 Software interface

A software interface may refer to a wide range of different types of interface at different ”levels”: an operating system may interface with pieces of hardware. Applications or programs running on the operating system may need to interact via streams, and in object oriented programs, objects within an application may need to interact via methods. User interface is a part of software interface.

1.4.1 Software requirements

Following are the software requirements for Email Security System:

1.Java Development Kit

2.SQL Database

3.SQLite

4.Netbeans

2. Conclusion

These days with the growing technology it is required to keep up with the latest technologies, especially in the filed of security. AES is an email tool that using asymmetric key algorithm which provides the confidentiality of the data during transmission. The system is developed by using the combination of RSA algorithm and AES algorithm for making it more secure. The system should be giving more security mechanism in protecting the attachment documents or files for the email services such as Gmail, Yahoo! Mail, and so on. In a conclusion, the AES may help users in protecting their confidential files from unauthorized third party while sending the files to the authorized recipients. This accomplishes two functions: authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

3. References

1. Rivest RL (1990) Cryptology. Handbook of Theoretical Computer Science.
2. https://www.eff.org/secure-messaging-scorecard
3. Paar C, Pelzl J, Preneel B (2010) Understanding Cryptography: A Textbook for Students and Practitioners. Springer.
4. Liddell HG, Scott R, Jones H, McKenzie R (1984) A Greek-English Lexicon. Oxford University Press.
5. Diffie W, Hellma M (1976) New Directions in Cryptography. IEEE Transactions on Information Theory 22.
6. Schneier B (2014) Cryptanalysis of MD5 and SHA: Time for a New Standard. Computerworld.
7. Diffie W, Hellman M (1976) Multi-user cryptographic techniques. AFIPS Proceedings 45: 109-112.
8. Kahn D (1979) Cryptology Goes Public. Foreign Affairs.