DATA SECURITY SYSTEM FOR CHAT APPLICATIONS USING CRYPTOGRAPHY, STEGANOGRAPHY AND IMAGE PROCESSING

SC Mataraarachchi[1] and N Wedasinghe
Faculty of Computing General Sir John Kotelawla Defence University, Rathmalana1, Sri Lanka.
[1]*shashikalac38@gmail.com*

Abstract- The privacy plays a major role in the personal life. Due to the vast development in communication technology, people have the privilege to perform various operations seamlessly in their day to day life. But at the same time, privacy of some of those things such as confidentiality of communication is lacking due to the actions of some other parties. A message sent by the sender(s) should only be revealed by the intended recipient(s). Due to privacy issues, from the past, people have used various secret methods to preserve confidentiality of their information. Out of those, one of the developing science was steganography. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. To read an encrypted file, one must have access to a secret key or password that enable them to decrypt it. At present this is widely used in various areas to secure valuable information. But in most existing systems, their security has not been trusted. Under this research, proposed a secure, flexible steganography mechanism to encrypt highly confidential messages that avoid them from being accessed by an unauthorized party.

Keywords- Data Security, Steganography, Encryption, Communication Technology, Confidentiality

I. INTRODUCTION

Instant messaging is a real-time communication medium that has grown increasingly popular for both social and professional use. In the Military sector, messaging can be used advantageously in scenarios where phone use is not possible or appropriate, for an example when communicating with geographical distributed teams, or for technical discussions in which the sending of URLs or operating system commands can be instantaneous. However, the military forces would be more concerned about security issues than a casual user who uses the software to keep in touch with friends because very critical & confidential information is passed among military officers.

One major disadvantage of most instant chat applications is that they are prone to security attacks. For instance, Yahoo messenger is vulnerable to security attacks when instant messages are sent between a source and a destination machine. The reason is the fact that, messages which are sent over the network is in a plaintext format with no encryption and decryption protection, thereby enabling intruders with no privileges to gain authentication sequence to alter the message content and make modifications to the message stream, learn the traffic pattern and cause denial of service.

The idea behind this research is to implement a simple messaging application that users can use to communicate sensitive information, which is highly secured with advanced stenographic mechanisms and encrypted on the front end to disallow outsiders from extracting secret information and at the same time succeeds in being unsuspicious and easy to use.

This system can be divided into 3 main parts. They are the front end, intermediate services and the back end. The front end consists of the interface and functionalities

related to the actions performed by the user. The intermediate services are the services provided by the server. Finally the back end consists of the services provided to the other user. The intermediate services allows to manage the database activities and encryption and decryption. The system will be using cloud server. At the other end there will be another interface for the recipient to receive the message.

The system has to cover different aspects such as register and log users, generate a virtual keyboard of user own language, cryptographic encryption, generate bit map images, send and receive secure message, send images and location tracking. Objective of the system is to develop a reliable, secure and a highly accessible messaging application which uses advanced data encryption standards and image processing mechanisms in such a way that it would benefit military and government personnel on secret surveillance or military intelligence missions.

II. LITERARURE REVIEW

A. MSN Messenger

Windows Live Messenger is a deprecated instant messaging client developed by Microsoft for Windows, Java ME, and S60 on Symbian operating system. It connected to the Microsoft Messenger service. Windows Live Messenger uses the Microsoft Notification Protocol (MSNP) over TCP (and optionally over HTTP to deal with proxies) to connect to Microsoft Messenger service. The American online service developed a buffer overflow bug, which causes it to execute a bit of machine code sent by the server. When this code runs, it determines if the client is MSN ID and sends a message back to verify the client.

The disadvantage of this application is the software has only allowed connections to its own service, requiring a Windows Live ID.

B. Yahoo Messenger

Yahoo Messenger is an advertisement-supported instant messaging client and associated protocol provided by Yahoo. It allowed Yahoo Users to create public chat rooms, send private messages, and use emoticons. On October 13, 2005, Yahoo and Microsoft announced plans to introduce interoperability between their two messengers, creating the second-largest real-time communications service worldwide. This allows Yahoo and Windows Live Messenger users to chat to each other without the need to create an account on the other service, provided both contacts use the latest versions of the clients. Yahoo messenger is designed to be compactable with windows, Mac OSX and Linux/Unix environment with their Operating system versions respectively.

Though it has some advance features, it was not possible to talk using the voice service among both messengers. According to thorough statistics, yahoo messenger has the weakest security features out of the two major IM providers (MSN and AOL), as it does not encrypt usernames and passwords, thereby running risk of data interception when the user logs onto the system.

C. Facebook Messenger

This is sometimes abbreviated as "Messenger". This app is an instant messaging service and software application. Over the years, Facebook has released new apps on a variety of different operating systems, launched a dedicated website interface, and separated the messaging functionality from the main Facebook app, requiring users to use the web interface or download one of the standalone apps. Users can send messages and exchange photos, videos, stickers, audio, and files, as well as react to other users' messages and interact with bots. The service also supports voice and video calling. The standalone apps support using multiple accounts, conversations with optional end-to-end encryption.

It uses data as its fuel and will not work when offline, like MMS and Text Messaging system. It can be taken as a big disadvantage of this application.

D. WhatsApp

WhatsApp is a freeware, end-to-end encrypted cross-platform instant messaging and Voice over IP (VoIP) service. The application allows the sending of text messages and voice calls, as well as video calls, images and other media, documents, and user location. The application runs from a mobile device though it is also accessible from desktop computers. The service uses standard cellular mobile.

The disadvantages of this application is, while changing to a new device using the same number, the existing chat stored in the old device cannot be retrieved into the new device incase of not having a chat backup.

E. Viber

Viber is an instant messenger app and communication tool for mobile devices. It is one of the many apps out there and is quite far behind the major players in the market such as WhatsApp and IMO. In order to remain in the game, it gambles on its free high-quality video and voice calls. It is a good app for video calls, with decent quality given all necessary conditions for good VoIP calling are there and scores quite high on Google Play and Apple App Store.

Though it is a good app for chatting, some unwanted messages like images and videos may take all the space in the device and also storing the chat backup mat be messy and takes time.

III. PROPOSED SYSTEM SOLUTION

There are various methods for data hiding like the Spatial Domain, Frequency Domain and Compressed Data Domain. Among them, this system has used the spatial domain. In this method, the image pixels in the spatial domain are arranged in order to incorporate the data to be embedded. This technique is simple to implement. It offers a high hiding capacity. The quality of the image in which the data embedding is done can be easily controlled.

This system uses AES encryption algorithm as the solution. A cipher in AES has a variable block length and key length. AES comprises of three block ciphers AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits respectively.

According to the Symmetric Cipher Model of the system, the encryption algorithm performs various substitutions and transformations on the plaintext. The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depends on the key. Cipher Text is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible. Decryption Algorithm is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

IV. METHODOGOLOGY

The system will be using an encryption algorithm to transform the user message (plain text) into encrypted text (cypher text) and it will be using a special formula for encryption purposes. Then mapping these cipher text characters with pixels with different RGB values so that it would form a random image. This image is the element that will be sent to the recipient. Even if an intruder retrieves the conversations, it will only be able to see a meaningless set of images. So in this way the system could effectively disguise the message preserving the confidentiality. When the message reaches the destination it will be retransformed into the encryption text and the cipher text will be decrypted using a decryption algorithm to provide the recipient with the original message.

After the application is setup on the android platform the user can access the login page for authentication. Then the relevant user name and password should be entered in order to login if the user already has an account. If not user can create a new account and afterwards login. After authentication is successful the user will be taken to the home page where the user will be able to see the other users who are currently online. Then the user can click another person's account who he/she wishes to chat with.

This enables a secure connection between the two users. Then the user will be taken to the messaging page, and there will be an option provided to the user as to alter the key mapping by assigning preferred keys by replacing default characters on keyboard keys. And when the user has finished assigning the keys he can click the generate button. Then the key map will be sent to the other user. Afterwards user can type the text and encrypt it and send it to the other user. In the user end the encrypted text will be decrypted and shown to that user after resolving the relevant mapping.

V. TECHNOLOGY

This system is mainly based on Java and Android. By using java, it will reduce extra cost that need to be bared for purchasing some components and tools. Because java is open source and all components are free to use. For development of this system java with NetBeans platform will be more suitable. Java is fully object oriented by design and more flexible in handling. Java is used in programming with NetBeans platform which provides an easier and flexible environment for the programming purposes and GUI developments. Java is platform independent, so it will be able to reuse the system components in effective manner at a later time. If the platform is going be changed then, no redevelopment will be required for the system. So, it will be more beneficial for the users if they are intending to change the system requirements in the future.

VI. SYSTEM DESIGN

This system can be divided into 3 main parts. They are the front end, intermediate services and the back end. The front end consists of the interface and functionalities related to the actions performed by the user. The intermediate services are the services provided by the server. Finally the back end consists of the services provided to the other user. The intermediate services allows to manage the database activities and encryption and decryption. The system will be using cloud server. At the other end there will be another interface for the recipient to receive the message.

The system has to cover different aspects such as register and log users, generate a virtual keyboard of user own language, cryptographic encryption, generate bit map images, send and receive secure message, send images and location tracking. Objective of the system is to develop a reliable, secure and a highly accessible messaging application which uses advanced data encryption standards and image processing mechanisms in such a way that it would benefit military and government personnel on secret surveillance or military intelligence missions.

This is intended to develop as an instant chat application known as Secured Java Chat Messenger (SJCM). SJCM is an instant chat application that provides an intuitive and reliable way of exchanging instant messages over a network using two or more computers. However SJCM (Secured Java chat messenger) provides an assurance of network security where plaintext are transformed into cipher text (Unintelligible message), thereby making it difficult for a cryptanalysis or an intruder attempts to alter message content, to make modifications to module (independent) and to the client chat application module (dependent). The server chat application module provides a graphical user interface with settings and options which enables an effective and secured exchange of instant messages between two or more communicating entities. Similarly, the client chat application module also contains a graphical user interface and provides a reliable and secured communication.

Secured java chat messenger would be built upon the ideology of the client server architecture model. However, these two modules (server and client chat module) can communicates with each other on a network upon a connection establishment which would be dependent on the host computer's port numbers and IP addresses. Each model would contain an encryption and decryption scheme using the encrypt the plaintext into a cipher text with a private symmetric key before making the transmission on the network and decrypt the cipher text into a plaintext with the same private symmetric key at the receiving end of the communication.

A symmetric private key is a unique pass code that is used to secure an encrypted plaintext at the transmission end of the communication and used to decrypt the cipher text into a plaintext at the receiving end of the communication. The key will be generated by the user according to his/her preference when they are assigning keys to the keyboard. Each key assigned to be relevant for the keyboard click will be converted into Unicode values and they will be the RGB values relevant for a single pixel. After developing all this pixels on a plane, can send it to the other user. Then that user can compare parts of the message with the received key map in order to determine the original message.

VII. SYSTEM FEATURES

Receiver can view the plain text of the message with a click of the button provided with chat message. They can click the button again to display the text in secret language.

Figure 1. Process flow of the system

Specialized encryption and decryption techniques are included in the application and the users have to login with the password they provided for registration, every time they use the application.

Auto destruction of viewed messages after a user defined time period. A chat can be started only with a person who has accepted the chat request. Session time-out will occur when kept idle for some time and re-login will be required to pursue.

The users can delete messages from application, from server and from receiver's chat history. Messages can be sent with a time limit so that it self-destructs after time-out.

Reducing database access time by using SQLite for some frequent data needs. Navigation on system would be user-friendly and accessible. System has simple and interactive user-interface. Reduced data usage on the application.

System should be available at all times and the central database should be updated each time user data interaction happens on the system.

VIII. SYSTEM ARCHITECTHRE

The architectural design of the system is elaborated in this section. The key components are illustrated further more. Overall system will be split in to three layers named presentation layer, application layer and data link layer. Based on this structure, the components will be divided in to separate modules to manage the operations of all components.

The presentation layer shows the interactions with users by controlling interfaces to display requested information and accept the inputs provided by the end user. Information gathered by presentation layer will be provided to the application layer in order to manipulate according to the given instructions.

Application layer can be named as the heart of the overall system and whole encryption logics and processes of the system will be executed at this layer in order to gain the proposed objectives of the system. This layer will interact between application layer where the interfaces are operated and data layer where the information is stored. Data gathered by user inputs or by other processes will be executed according to the predefined operational instructions at this layer. Data layer controls the data storage operations of the overall system where the database management applications are running. Also system uses log files to keep messages.

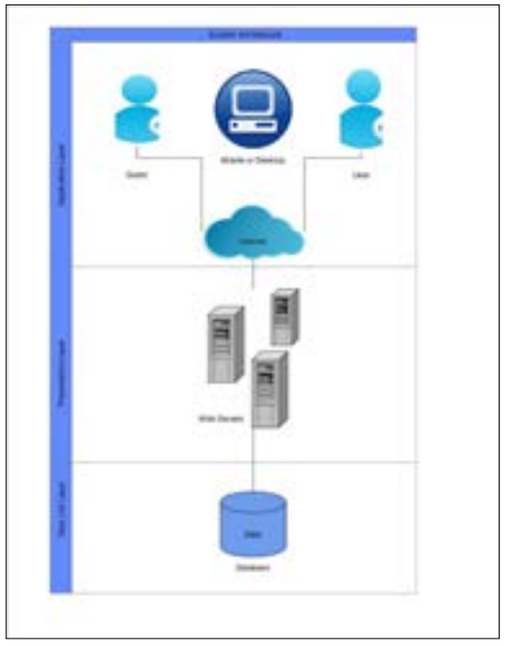

Figure 2. Three layer architecture of the system

IX. CONCLUSION

The proposed system is a low-cost, secure, flexible steganography mechanism for all users to encrypt highly confidential messages that avoid them from being accessed by an unauthorized party. This system has revolutionized the instant messaging service, minimizing the drawbacks of the existing systems and improving the performances of the technological features. With the help of the above technological features, allows the system to recognize multiple panoramas in unordered image sets, and stitch them fully automatically without user input. It has put forth a new system which combines text cryptography and image steganography which could be proven a highly secured method for data transactions in the near future.

ACKNOWLEDGEMENT

I would like to thank my supervisor Ms. N Wedasinghe for her constant support & guidance. Her active cooperation & involvement have helped me through the various stages of project development.

REFERENCES

Madden, M. (2003) America's online pursuits: the changing picture of who's online and what they do. Washington D.C.: Pew Internet & American Life Project.

Adams, C. "Simple and Effective Key Scheduling for Symmetric Ciphers." Proceedings, Workshop in Selected Areas of Cryptography, SAC' 94. 1994.

Bellare, M.; Kilian, J.; and Rogaway, P. "The Security of the Cipher Block Chaining Message Authentication Code." Journal of Computer and System Sciences, December 2000.

Beth, T.; Frisch, M.; and Simmons, G. eds. Public-Key Cryptography: State of the Art and Future Directions. New York: Springer-Verlag, 1991

Biham, E., and Shamir, A. Differential Cryptanalysis of the Data Encryption Standard. New York: Springer-Verlag, 1993 Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001

ElGamal, T. "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." IEEE Transactions on Information Theory, July 1985

Jueneman, R.; Matyas, S.; and Meyer, C. "Message Authentication." IEEE Communications Magazine, September 1988.

Kohnfelder, L. towards a Practical Public-Key Cryptosystem. Bachelor's Thesis, M.I.T., May 1978 Rapp, D. (2002) I've got to get a message to you. Technology Review, 105, 8, 88.

Broughton, K. (2002) Usage and user analysis of a real-time digital reference service. The Reference Librarian, 79/80, 183-200.

"Automatic Panoramic Image Stitching using Invariant Features", Matthew Brown and David G. Lowe of Computer Science,University of British Columbia,Vancouver, Canada.

Jones, Chris (August 17, 2010). "Windows Live Essentials 2011 beta refresh". Microsoft. Retrieved August 17, 2010

NavitaAgarwal, Himanshu Sharma "An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography", IJCSMC, vol. 2 issue 5, pp. 376385, May 2013.

Mohammadi S., Abbasimehr H., "A high level security mechanism for internet polls", ICSPS, vol. 3, pp. 101-105, IEEE, 2010.

Gary C.Kessler, "An Overview of Cryptography: Cryptographic", HLAN, ver. 1, 1999 2014.

MilindMathur, AyushKesarwani, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES", NCNHIT vol. 1 143-148, 2013.

Ashwin S., "Novel and secure encoding and hiding techniques using image steganography: A survey", ICETEEEM, vol. 1, pp. 171-177, IEEE, 2012

Chanu Y. J, "A short survey on image steganography and steganalysis techniques", NCETAS, vol. 1, pp. 52-55, IEEE, 2012.

Chung, H. M., & Silver, M. S. (1992). Rule-based Expert Systems and Linear Models: An Empirical Comparison of Learning-by-Examples Methods. Decision Sciences.

Cios, K., Pedrycz, W., &Swiniarski, R. (1998). Data Mining Methods for Knowledge Discovery. Norwell, MA: Kluwer Academic Publishers.