ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 11, Issue, 01, pp.488-490, January, 2019

DOI: https://doi.org/10.24941/ijcr.34010.01.2019

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

REVIEWARTICLE

A NOVEL METHOD TO COMMUNICATE IN ANONYMOUS SOCIAL NETWORKS

***Nripesh Trivedi**

Department of Mathematical Sciences, Indian Institute of Technology, Banaras Hindu University, India

ARTICLE INFO

Article History:
Received 20th October, 2018
Received in revised form
10th November, 2018
Accepted 19th December, 2018
Published online 31st January, 2019

Key Words:
Anonymous Social Network, Messaging, Privacy, Server, Users.

ABSTRACT

The trend of anonymous messaging, social networking, and general communication applications (e.g. Whisper, Secret, etc.) has been gaining traction recently. This stems from a growing need among internet users for speaking and communicating freely, without associating their content with their identities. However, in all the existing applications, anonymity is guaranteed by the server managing the network, where the users' messages have to go directly through the server before they are anonymously shared with the selected audience. In the light of the recent revelations on mass surveillance, the general trust in servers to guarantee users' privacy has been diminishing. Hence, we develop a technique for making such types of communications anonymous to both the server and the intended audience. Such a technique guarantees that the server would not know that a certain message came from a specific person. We term the technique, Scheme of Trusted Users. The scheme is implemented using Java SE.

***Citation: Nripesh Trivedi,* 2019.** "A novel method to communicate in anonymous social networks", *International Journal of Current Research*, 11, (01), 488-490.

INTRODUCTION

Trust is an important concern and issue in social networks. The most important relation in a social network is mutual trust between the organization working behind a social network and its users. In order to discard this notion of trust and allow users to express themselves, anonymous social networks give users the liberty to post and communicate without disclosing their identities. Even though this gives anonymity to users, their identities may be disclosed on the server supported by the organization. To protect a user's identity, we propose a scheme of trusted users in which identity of a user can be protected on both client and server side. In (Patel, 2013), an access control mechanism is described in which users are an active part of authentication and then access to resources. The mechanism described in this paper deals with the privacy of users by using groups, roles and permissions. In (Trivedi, 2018), users communicate anonymously to listeners (Calzarossa, 2016) who offer emotional support. This paper may be first of its kind to propose a mechanism to provide privacy to users on client and well as on server side.

Scheme of Trusted Users

The scheme that we implement is for trusted users where a group of users trust each other.

****Corresponding author: Nripesh Trivedi,***
Department of Mathematical Sciences, Indian Institute of Technology, Banaras Hindu University, India.

The term anonymous social network refers to social networks where users have the privilege to post anonymously, for example- whisper. The scheme is implemented on both server and client side. The scheme is as follows—

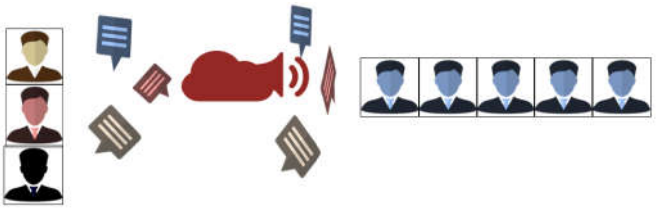

Figure 1. Anonymous social network

- Clients (the group of users who trust each other) decide on a particular group key.
- The server generates a pair of public and private keys.
- The public key is available to the clients while the private key is maintained at the server side.
- The clients encrypt their messages using the public key first and then using group key secondly. The server receives these encrypted messages (encryption of public key and group key). Instead of broadcasting the messages, server waits till it receives a message from every client, say N messages.
- The server broadcasts these N encrypted messages (encryption of public key and group key) to all the

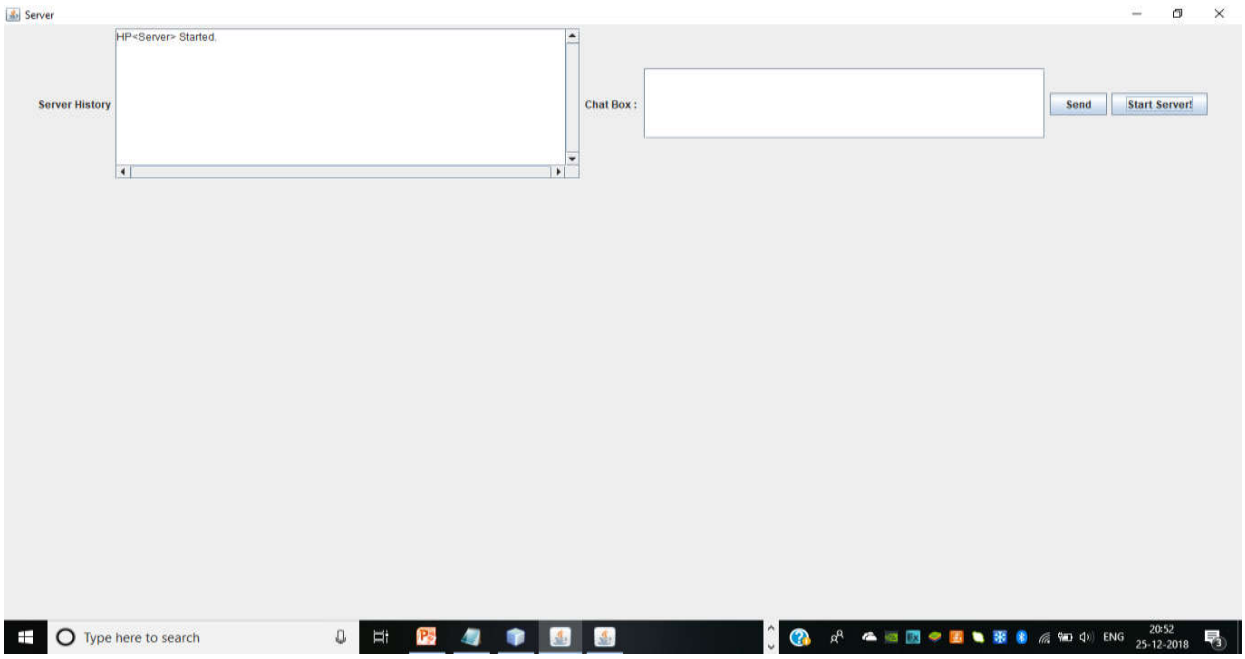

Fig. 2. Server

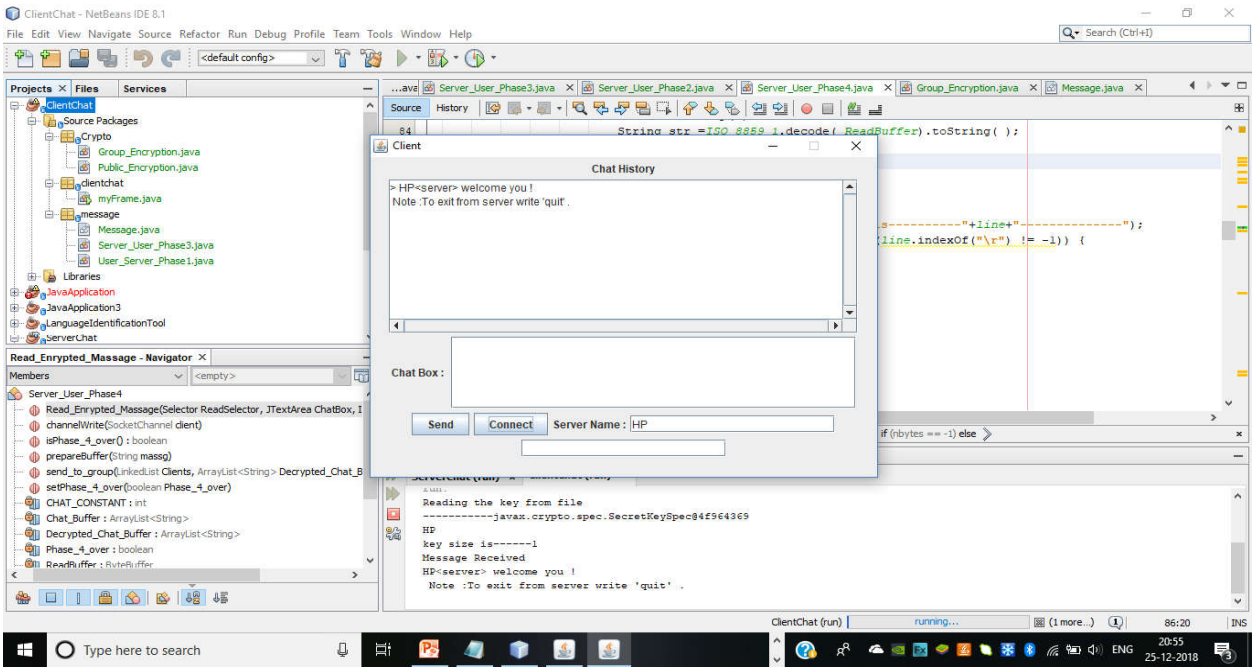

Fig. 3. Client

clients such that each client receives the N encrypted messages (encryption of public key and group key). Each client decrypts the N encrypted messages using the group key and then randomly shuffles these messages. The N messages still remain encrypted using public key.

- Each client sends the set of N encrypted messages (encryption of public key) to the server. The server waits till it receives one set of N encrypted messages (encryption of public key) (Server takes into account the first message set received). After receiving the first set of N encrypted messages, the server decrypts these messages using the private key, giving a set of N unencrypted messages (no encryption).
- As a last step, Server broadcasts the set of N unencrypted messages to all the clients such that each client receives N unencrypted messages.

This scheme provides privacy to identity of users on both client as well as on server side.

Implementation

The above scheme is implemented as a broadcast server-client application in java. The server application could be started in a standalone manner. Similarly, say N number of clients could be started in a standalone manner. These N clients could connect to the server once they know the name of the server running. For this purpose, NIO library in java is used. The server and the client are shown in Figure 2 and 3 above. RSA Encryption is used for public and private key encryption and for group key encryption, PBEWithMD5AndDES is used. The generation of public and private key takes place on server side. The message from the client is encrypted using a padded cipher using the group key first and then encrypted using the public key.

For encoding purpose, ISO-8859-1 is used since this encoding facilitates transformation from bytes to string and vice versa without any loss of data. After building the two applications (server and client) and the encryption schemes, the rest of the approach is carried out according to the scheme of trusted users as in the previous section.

RESULTS AND CONCLUSION

As evident from the proposed scheme and implementation, the scheme provides privacy to user's identity on server as well as on client side. The assumption is that users trust each other. When every user is anonymous, trust becomes implicit. Since identity of every user is unknown, there is no notion of trust explicitly. Trust becomes implicit since a user do not need to be concerned with identity of any other user, therefor one user cannot be distinguished from any other user. Therefore, generating the notion of trusted users.

REFERENCES

Calzarossa, M. C., Massari, L., Doran, D., Yelne, S., Trivedi, N., & Moriarty, G. (2016, June). Measuring the users and conversations of a vibrant online emotional support system. In *Computers and Communication (ISCC), 2016 IEEE Symposium on* (pp. 1193-1199). IEEE.

Patel, S. C., Umrao, L. S., Singh, R. S., Gupta, M., & Trived, N. 2013. Access Control Using Mobile Verification System For Cloud. *International Journal of Information and Computation Technology* (IJICT) ISSN, 0974-2239.

Trivedi, N., Asamoah, D. A. and Doran, D. 2018. Keep the conversations going: engagement-based customer segmentation on online social service platforms. *Information Systems Frontiers*, *20*(2), 239-257.

****