

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

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

International Journal of Current Research Vol. 11, Issue, 01, pp.488-490, January, 2019 DOI: https://doi.org/10.24941/ijcr.34010.01.2019

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	ABSTRACT
Article History: Received 20 th October, 2018 Received in revised form 10 th November, 2018 Accepted 19 th December, 2018 Published online 31 st January, 2019	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
Key Words:	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
Anonymous Social Network, Messaging, Privacy, Server, Users.	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.
Copyright © 2019, Nripesh Trivedi. This	s is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use,

Copyright © **2019**, Nripesh Trivedi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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

server Server		– 🗗 🗙
HP <server> Started.</server>	*	
		Count Count Count
Server History	Chat Box :	Send Start Servert
1000		
4		
		5 0m du ruc 20:52
U Type here to search		25-12-2018 3
	Fig. 2 Server	
	112. 2. DUI VUI	
	Fig. 2. 501 vci	
GlientChat - NetBeans IDE 8.1	rig. 2. 50 ver	- 0 ×
 ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tex 	m Tools Window Help	- 🗇 🗙 Q• Search (Ctrl+I)
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tet	m Tools Window Help	— ☐ × Q - Search (Ctrl+I)
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter	Tools Window Help $\widehat{\mathbb{W}} \rightarrow \widehat{\mathbb{W}} \rightarrow \widehat{\mathbb{W}} \rightarrow \widehat{\mathbb{W}}$	X
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tet Projecta × Files Services	m Tools Window Help	-
ClientChat - NetBeans IDE 8.1 File Edit: View Navigate Source Refactor Run Debug Profile Ter	Tools Window Help Tools Window Help → · · · · · · · · · · · · · · · · · · ·	- ○ × Q• Search (Ctrl+1) 2 Message,java × 4 → • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tex Comparison of the source set of the source s	m Tools Window Help Tools Windo	- ♂ × Q Search (Ctrl+1)
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Projects × Files Services Projects × Files Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Concentration Services Se	rig. 2. Servel m Tools Window Help	- ○ × Q• Search (Cbi+i)
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tet Projecta × Files Services Control Services	Tig, 2. Server m Tools Window Help	- □ × Q Search (Ctri+t) Message_java × ↓ → ♥ □ B
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tet File Edit View Navigate Source Refactor Run Debug Profile Tet Forgetex × Files Services	Tig, 2. Server m Tools Window Help	- ○ × Q Search (Ctri+t) Message,java × ↓ ↓ ↓ C B A A A A A A A A A A A A A
ClientChat - NetBeans IDE 8.1 File Edit: View Navigate Source Refactor Run Debug Profile Ter Composite X Files Services Composite Refaces Composite Reface	Tools Window Help Tools Window	- ○ × Q • Search (Cbi+t)
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Projects × Files Services Projects × Files Cource Packages Cource Packages Cou	Tig. 2. Server m Tools Window Help Tools Window Help Tools Window Help Tools Server_User Phase3.java X @ Server_User Phase4.java X @ Group_Encryption.java X @ Server_User Phase3.java X @ Server_User Phase4.java X @ Group_Encryption.java X @ Server_User Phase3.java X @ Server_User Phase4.java X @ Group_Encryption.java X @ Server_User Phase3.java X @ Server_User Phase4.java X @ Group_Encryption.java X @ Server_User Phase3.java X @ Server_User Phase4.java X @ Group_Encryption.java X @ Server_User Phase4.java X @ Server_User Phase4.java X @ Group_Encryption.java X @ Server_User Phase4.java X @ Server_User Phase4.java X @ Group_Encryption.java X @ Server_User Phase4.java X @ Group_Encryption.java X @	- ○ × Q • Search (Cbi+i) Message.java × • • • • • • • 8 8 1 1 1 1 1 1 1 1 1 1 1 1 1
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Project × Files Services Control Services	Tig. 2. Server m Tools Window Help	- □ × Q • Search (Ctri+1) Message.java × • • • • □ B B B C L)) {
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tet Project × Files Services Control Control Contro	Tig. 2. Server m Tools Window Help Tools Window Help 	- ○ × Q Search (Ctri+t) Message.java × ↓ ↓ ↓ ↓ Hessage.java × ↓ ↓ ↓ ↓ Hessage.java × ↓ ↓ ↓ ↓
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Tet Control	Tig. 2. Serveri m Tools Window Help	- ○ × Q • Search (Cbi+i) Message.java × • • • • • • • Hessage.java × • • • • • • Hessage.java × • • • • • • • Hessage.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBenns IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Composition of the services Projects × Files Services Projects × Files Projects × Files Projec	Tig. 2. Server m Tools Window Help	- ○ × Q • Search (Cbi+i) Message.java × • • • • • • • 8 1 1 1) {
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Project × Files Services Froject × Files Services Control Se	Tig. 2. Server m Tools Window Help Tools Window Help Tools Window Help Tools Window Help Tools Window Help Tools Provide Phase3.java X @ Server_User_Phase4.java X @ Group_Encrypton.java X @ Server_User_Phase3.java X @ Server_User_Phase4.java X @ Server_	- ○ × Q • Search (Cbi+l) Message.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Control Control	Tig. 2. Servel	- □ × Q Search (Ctri+1) Message_java × () → C B B 1 1 1 1 1 1 1 1 1 1 1 1 1
ClientChat - NetBens IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Sector Run Debug Profile Ter Sector Run Debug Profile Ter Sector Run Debug Profile Ter Sector Run Debug Profile Projects × File Projects × File P	Tig. 2. Serveri m Tools Window Help Tools Window Help Tools Server_User_Phase3.java X @ Server_User_Phase4.java X @ Group_Encrypton.java X @ Server_User_Phase3.java X @ Server_User_Phase4.java X @ Group_Encrypton.java X @ Server_User_Phase4.java X @ Server_User_Phase4.java X @ Group_Encrypton.java X @ Server_User_Phase4.java X @ Server_User_Phase4.java X @ Group_Encrypton.java X @ Server_User_Phase4.java X @ Server_User_Phase4.java X @ Group_Encrypton.java X @	- ○ × Q • Search (Cbi+i)
ClientChat - NetBenns IDE 8.1 File Edit View, Navigate Source Refactor Run Debug Profile Ter Projects × Files Services Projects × Files Cocup_Encryption.java Projects × Files Projects ×	Tig. 2. Server m Tools Window Help Tools Window Help Tools Window Help Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Phase3.java X @ Group Encryption.java X @ Tools Server User Phase3.java X @ Server User Ph	- ○ × Q • Search (Chi+1) Message.java × • • • • • • • B Hessage.java × • • • • • • B Hessage.java × • • • • • • • B Hessage.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Control Control	Tig. 2. Server m Tools Window Help Tools Window Help	- ○ × Q • Search (Cbi+l) Message.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Control Control	Tig. 2. Server m Tools Window Help Tools Window Help Tools Window Help Tools Window Help Tools Server User Phase3.java X @ Server User Phase4.java X @ Group_Encrypton.java X @ Server User Phase3.java X @ Server User Phase4.java X @ Group_Encrypton.java X @ Server User Phase3.java X @ Server User Phase4.java X @ Group_Encrypton.java X @ Server Hetery @ - + - Q @ @ I @ I @ I @ I @ I @ I @ I @ I @ I	- □ × Q Search (Ctri+1) Message java × () → C H H H H H H H H H H H H H
ClientChat - NetBens IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Projects × Files Services Projects × Files Services Project × Files Services	m Tools Window Help Tools Window Help → + Server_User_Phase3.java × Server_User_Phase3.java × Server_User_Phase4.java ×	- 0 × Q • Search (Cbi+1) Message.java × 4 > • 0 Hessage.java × 4 > • 0 Hes
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Projects × Files Prove Content of the services Prove Content	Tig. 2. Server m Tools Window Help	- ○ × Q • Search (Chi+1) Message.java × • • • • • • • B Hessage.java × • • • • • • B Hessage.java × • • • • • • • B Hessage.java × • • • • • • • B Hessage.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Project × Files Services Project × Files Group_Encryption.java Project × Files Group_Encrypted_Group Project × Files Group_Encrypted_Group Project × Files Group_Encrypted_Chal Project × Files Group_Encrypted_Chal Project × Files A_ser(poolean Rese, 4_over()	Tig. 2. Server m Tools Window Help	- ○ × Q • Search (Cbi+1) Message.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Trojecta × Files Services Control Chail (Control Control Contro	Tig. 2. Server m Tools Window Help	× Q • Search (Cbi+i) Message.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBens IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Projects × Files Project s Files Project s Files Project s Files Project phase Project s Files P	m Tools Window Help Tig. 2. SCIVCI m Tools Window Help	- ○ × Q • Search (Chi+1) Message.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Trojects × Files Composition Co	Tig. 2. Server m Tools Window Help	- ○ × Q • Search (Chi+1) Message.java × • • • • • • • 8 1) (• • • • • • • • • • • • • • • • • • •
ClientChat - NetBeans IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Troject × Files Froject × Froject × Frojec	Tig. 2. Server m Tools Window Help Tools Window Help Tools Window Help Tools Server User Phase3.java X @ Server User Phase3.java X @ Server_User_Phase4.java X @ Server_User_User_User_User_Phase4.java X @ Server_User_User_U	- ○ × Q • Search (Cbi+l) Message.java × • • • • • • • • • • • • • • • • • •
ClientChat - NetBens IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Projects × Frie Services Projects × Frie Project Services Pr	Tig. 2. Server m Tools Window Help Toward Server User Phase3 Java X Server User Phase3 Java X Server User Phase4 Java X Server User Tool Sets J Ldecode/ ReadPuffer) + toString(); HP-server welcome you I Note: To exit from server write 'quit'	- C × Q • Search (Cbi+i) Message.java X • • • • • • Hessage.java X • • • • • • • Hessage.java X • • • • • • • Hessage.java X • • • • • • • • Hessage.java X • • • • • • • • • • • • • • • • • •
ClientChat - NetBens IDE 8.1 File Edit View Navigate Source Refactor Run Debug Profile Ter Trojects × Files Projects × Files Project = Services Project = Services Project = Services Project = Services Project = Services	m Tools Window Help Image: Server User Phase3.java X @ Server Name : HP Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP If (cbytes == -1) else X Image: Server Name : HP Image: Server Name : HP Image: Server Name : HP Image: Server Name : HP I	- ○ × Qr Search (Cbi+i) · · Image: Search (Cbi+i) · · ·
ClientChat - NetBens IDE 8.1 File Edit View, Navigate Source Refector Run Debug Profile Ter Project × Files Services Project × Files Prove Services Project × Files Prove Services Project × Files Prove Services Prove Se	<pre>m Tools Window Help m Tools Window Help w + + + + + + + + + + + + + + + + + +</pre>	× Qr< Search (Cbi+i)

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.
