International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 656-659
Published Online June 2020 in IJEAST (http://www.ijeast.com)

SECURE GROUP COMMUNICATION: AT HIGH ALERT

Arusi Kumari
BCA Student
Computer Science Department,
Kalinga University, Atal Nagar,
Chattisgarh India

Rahul Kumar Chawda
Assistant Professor
Computer Science Department,
Kalinga University, Atal Nagar,
Chattisgarh, India

Abstract - Now a days every network Application which is emerging based on a model of group communication that totally means authenticity, providing confidentiality and integrity of messages delivered between member of group. WSN, which is a wireless sensor network which consist of sensor nodes in a large number and in harsh unattended environment, it often deployed. In the world full of cyberattacks, this sensors-based application needs to be secured. WSN is basically used in many application like security monitoring and object tracking. This paper introduces What Why How secure group communication is. It tell us why and how should a group communication can be secured with the impactful example of Zoom. In This paper we present the importance of Admission and Access control with its definition.

I. INTRODUCTION

Group Communication System (GCSs) are known for middleware and secure communication occur when two entities don't want any interference of third party and for that they need to have a Secure Communication.

In Sensor Network, Security is a crucial issue. There is need to established a trusted communication by the capability in the network. A group Communication through P2P network is insecure for data exchange. For communication, there is no centralized coordinator and this happens only because in P2P network of computer work as either client or as server. Also because of the central server exclusion.

P2P divides all the work among all the peer or the member involved in network as it is a distributed network.

II. BACKGROUND OF P2P NETWORK.

As the only basic and important problem with P2P is the resources and discovery of peers. Server may changes so it is not fixed for the peers for that they rely on some other method to connect fellow peer.

Centralized directory is the most basic approach, where in central server resources are indexed and peer find other peer.

What is peer infrastructure?

The Peer infrastructure is combination of various APIs that are strong and fully flexible. Some important component are as follow :-

- Peer Graphing API –In this infrastructure, it provides graphic technology in reliable form with efficiency among peer's member. It is helpful for

A. creating and managing group,

B. Data are send in form of record to every node

C. For interacting purpose with other peer

- Peer Grouping API—Its name defines its work as it enhance grouping and combining the peer. PNRP (Peer Name Resolution Protocol) & grouping API and Similarly two more components are added that is multiple application allowed by multiplexing layer running on one peer just for connecting a group.

- Peer Identity Manager API – Here you can create a secure peer names, by using the Peer Identity Manager API so that PNRP ensures that the person will only owns the name when the name is published by that person only. It is also named as identity which helps to identify the particular peer in the peer group. This

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 656-659
Published Online June 2020 in IJEAST (http://www.ijeast.com)

is only used to create, enumerate and manage peer identities.

- PNRP Namespace Provider API – Peer Name Resolution Protocol Namespace Provider API is a server less name resolution technology which has been provided by Peer infrastructure. Peer group end point can be manage, register, unregister and resolve another end point in a cloud of PNRP by using the Winsock 2 PNRP namespace provider API.

III. BENEFITS OF PEER NETWORKING

P2P Networking Application is a complete solution provided by Peer-To-Peer infrastructure.P2P graphing, grouping, identity Manager and PNRP Namespace provider API can be used to create new, exciting and robust Peer-to-Peer applications. There is a Solid Networking infrastructure which is used for developing applications is also provided by Peer-To-Peer infrastructure.

It has following feature like Secure, Serverless, Self-tuning, Scalable, Self-repairing, Sharing.

There are various kind of application can be developed using Peer-To-Peer infrastructure like-Collaboration, Content Distribution, Real tine networking and communication, Internet technologies and protocol and last but not the least Distributed Processing Coordination.

Let's start with the brief description of the three words written above :-

Secure:- protect or fixed something so that it cannot be lost .

Group :-a number of people gathered together.

Communication:-exchanging of ideas ,information by speaking ,writing.

So let's add these word together "SECURE GROUP COMMUNICATION".

It is not any rocket science which cannot be easy to understand but infact it the most emerging and helpful technology to our whole world. Now exactly what it means is that the Secure group communication is the telephonic interaction of the group of people from different place for exchanging ideas information regarding any project but in a secure way so that there data of the project should not leak.

Can you relate this to the pendamic situation which we all are facing specially the economic field of the world, as due to sudden lockdown, everything has clicked its pause button. But nothing can stop us to work, develop, create, design. Yes, this is our technology which had made working, interacting in an official meeting just through some clicks, exchanging ideas over internet, in a group much easier in this lockdown. This is non other than video call meeting app.

Now let's get to the point. What exactly this technology is meant for. What? How? Why? This Secure Group Communication which is also called as Peer to Peer Communication, which is emerging as a faster growing technology.

Peer is a workstation and Peer to Peer is a network of workstation where every peer is having equal responsibility. P2P relies on each and every workstation or peer to take active part in the network communication's management There is a growing demand of group-oriented application over internet like:-Teleconferencing ,Chat room, Multi-user Games, Replicated server.

Now why peer to peer? Eventually the goal of peer to peer is to provide with better resources of bandwidth, storage and moreover computing power. This is not a case of client-server mechanism where adding more clients means slower data transfer to all the client. There is no problem of internet traffic jam. It permits a decentralized communication where they avoid single point failure .With the help of this decentralized nature it can withstand to Denial-of-service (DoS) attack whereas in client-server architecture there can be trouble of server down due to load .As its name define that there must be a group and group can be of many in numbers which are connecting to a same server and to handle all these ,we need a high performance machine at the server end and which is much more costlier than P2P architecture.

In P2P scenario every peer is communicated to each other for exchanging messages as well and it required the messages should be minimum. Adding all these features we also require the group communication should be secure and all the traffic should be encrypted using some key technology for group security and privacy.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 656-659
Published Online June 2020 in IJEAST (http://www.ijeast.com)

Now the point is How P2P secure the group traffic, Answer is simple, It is just by using Admission and Access Control Policies to provide Secure Group Communication.

IV. ADMISSION AND ACCESS CONTROL.

In P2P scenario there are some standard which permits, who can join the group meeting and after joining there are again some resources which are provided to the user for better and understandable meeting and the use of these resources depends upon all the user or peer. Here's may be some confusion regarding these two terms let's make it clear first, In admission control where it's name defines its work that it totally control the admission of the peer to group whereas in access control it implies secure access to group conversation in messages, which gives it an important role.

Admission control:- In Peer group everyone is free to join but what if anyone from the group ,anyhow access the group key easily then the security management will become useless so for avoiding such leakage issue .peer2 peer have some key rule to determine whether the user is allowed to enter the group or not .Membership control or we can say admission control should allow the authorized user to enter the group .Membership control is very important and for that the authorized allowance should be taken seriously .All the information in the group is electronically encrypted

Access Control:-In a group ,there is a need to mention which resources is accessible to which peer .And the access control policy will set the key rule to access any specific resources .Generally the group can be Static and Dynamic .In Static the information about all the members are given in advance so here management of accessing resources is pretty easy and which is done by Access Control Lists which is nothing but a list which determine which resources should be access by the user on a particular system. whereas in dynamic group anyone can join at any time between the meeting and can leave the group whenever the respective user wants, in which its really very difficult to set some kind of access key. Access Control is basically divided into 2 categories: The first one is Role Based Access Control (RBAC) and secondly Attribute Based Access Control (ABAC).

V. CONCLUSION

The Secure Group Communication provide secure end to end or point to point communication. The peer 2 peer messages are encrypted by the key words shared by the two ends. It makes the messages unique by adding the identities of the sender and the receiver ,a sequence number and a timestamp like – (Receipient_Id , Sender_Id , Timestamp , Message_Body).

By formatting the messages in this sequence, it ensures there will be no reuse of messages in different time, place or context. As today privacy of people's is at risk and this is our fundamental right. Currently we are enjoying a very safe communication for transferring messages through video call to many people at the same time. The only problem in this system is how to tacle with the malicious attacks to protect the system. And ZOOM app is facing the same problem, yes there is no doubt to question the availability of the resources and the easy understandable features in this app but what we all want is the best security level among the group and which lacks behind this app and this only disadvantage washed out all the advantages and features of zoom.

Let's take a very familiar example in front of you.

The ongoing pandemic have resulted in lockdown across the globe, this led to employees working from home. Also the students had to be kept up to the mark with their academics. This brought in demand the use of video-conferencing platform, ZOOM; Hence the security reasons too. Politicians and other high profile figures use this app for conferencing as the work from home. Later it was claimed to be a "PRIVACY DISASTER". Where in zoom-bombing i.e. video hijacking took form. Being an easily accessible platform, holding a no end-to-end encryption, it made easier for hacker to invade.

Being a major concern of security, zoom was clearly not a suitable platform to be trusted with data. On contrary to the outcomes, zoom changed some of its policies in response; increasing the security. It has claimed to be working on this privacy flaw.

From the point cited above the security issues and data leakage problem are clearly noticeable and are needed to be worked upon. the vulnerabilities are a crucial topic of concern, neglecting which, could lead to measure damage. People basically from big firm and MNC'S are very particular about their confidential information. In this scenario, intrusion of a malware is a threat. Zoom on the other hand, has assured to revisit its security parameters creating a vast impact on user's privacy.

VI. REFERENCES

1. Ajit Burad, Computer Science and Engineering Indian Institute of Technology, November 13, 2006

https://www.cse.iitb.ac.in/~madhumita/access/gcs/aps-2/btp.pdf

2. Li Gong, Fri May 17 15:07:56 PDT 1996 https://www.usenix.org/legacy/publications/library/proceedings/sec96/full_papers/gong/node10.html

3.Secure Group ,Year Founded:2009

https://securegroup.com/about-secure-group/

4. Makoto Takizawa and Hiroya Mita, Computer and Systems Engineering Tokyo Denki University.

file:///C:/Users/arush/Downloads/Secure_group_communication_protocol_for_distribute.pdf

5. Journal of Network and Computer Applications February 2016

https://dl.acm.org/doi/10.1016/j.jnca.2015.10.011

6. Abuzneid AS, Sobh T, Faezipour M. An enhanced communication protocol for location privacy in wsn. Int J Distrib Sens Netw

https://scholar.google.com/scholar?hl=en&q=Abuzneid+AS%2C+Sobh+T%2C+Faezipour+M.+An+enhanced+communication+protocol+for+location+privacy+in+wsn.+Int+J+Distrib+Sens+Netw+2015%2C+Article+62+%28January+2015%29%2C+1.+10.1155%2F2015%2F697098.+10.1155%2F2015%2F697098+

7.IEEE/ACM Transcations on Networking 1 Feb 2000

https://ieeexplore.ieee.org/document/836475

8.Honeywell,Technology solutions Laboratory

https://www.researchgate.net/publication/4233302_Secure_Group_Communication_in_Wireless_Sensor_Networks

9. P. Vijayakumar, Dean i/c, University College of Engineering Tindivanam, Melpakkam, Tamilnadu

https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.1578#:~:text=Data%20exchange%20performed%20in%20group,to%20secure%20the%20communi%2D%20cation.&text=Peers%20are%20equally%20privileged%20participants,is%20called%20as%20a%20node.

10. James Li.in a survey

https://www.cse.wustl.edu/~jain/cse571-07/ftp/p2p/

11.Microsoft Docs

https://docs.microsoft.com/en-us/windows/win32/p2psdk/what-is-the-peer-infrastructure-

12. What is peer infrastructure.,Google Docs.

https://docs.microsoft.com/en-us/windows/win32/p2psdk/what-is-the-peer-infrastructure-

13. Benefits of Peer Networking ,Google Docs.

https://docs.microsoft.com/en-us/windows/win32/p2psdk/benefits-of-peer-networking

14. Secure Communication,Wikipedia

https://en.wikipedia.org/wiki/Secure_communication