Anonymous and Cost-Efficient Organizational Data Sharing Application

Sameer Madhukar Jamsutkar[1] Geeta Ravindra Mhashilkar[2] Ms. Shweta Sharma[3] Mr.Pranav Nerurkar[4]
[1,2]B.E-CMPN (Pursuing) [3,4]Project Guide
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Atharva College of Engineering, Mumbai University,Mumbai, India

Abstract— This application is design for data sharing within small organization. The operating cost of current system is high, hence emphasis is given on reducing the cost of operation. This application is mainly design for an organization which can't afford costly solution. In the system users are divided in groups. Database maintains the information of all clients. Clients need to undergo the process of authentication before getting access to the server. Sender uploads data in encrypted form to server. Encryption is done to deal with problem of man in middle attack. Server provides that data to receiver's group anonymously. Then router provides that data to actual receiver. The data can retrieve using private key of receiver.

Key words: Anonymous, Cost-Efficient, data sharing, public key, authentication protocol, private key.

I. Introduction

Now a day's network security becomes a crucial problem. When we hear network security we might only think hackers. The main goal of network security is providing authentication, integrity, consistency etc. To maintain security of network data various methods, technology and algorithms are used. It prevents data to being hack by hackers. Maintaining the authenticity of the data that means only authorized or legitimate user can access the data which is shared by using network.

To check sender's authenticity and sender's data verification in network various techniques are used such as digital certification and VPN. But cost of such technology is very expensive. The project provides a cost efficient way to securely shared authentic data between clients.

It is a networking and information security based project used to overcome the cost of checking certification when data are shared on network based. The main concept of this application to provide cost efficient way for certification and data security. For small organization or start up organization the other techniques that are used nowadays are very expensive. Such organization can't afford such kinds of solution to checking certification. The project is suitable for small and start up organization. The structure and design of this application is user friendly. Anyone can easily operate this application. The project design and architecture are to support scalability for enhancements and ease of changes as well as friendly usage from users of the system.

II. Literature review

A. *Cost-Effective Authentic and Anonymous Data Sharing with Forward Security*

In modern world the use of cloud computing is increasing because of easy data sharing. In cloud computing maintaining efficiency, privacy and integrity are big issues. To overcome such problems ring signature is used. Ring signature provides anonymous and authentic data sharing. Identity based ring signature eliminates the need of certificate verification hence provides cost efficient solution [1].

B. *Efficient and Generalized Group Signatures*

The group signature allows any member of a group to sign message on behalf of group. Each group have group manager who is responsible for identify the originator of that signature in the group. The group signature provides anonymity by hiding the information of real signer [2].

C. *Kerberos: An Authentication Protocol*

It is an authentication protocol which is use for verification process of the user. Kerberos is secret key encryption technology. Client prove their identity by communication to the authentication server. This process completes without forwarding or sending any data in between client and server [3].

III. Approach

In this system the users are arranged in groups. The groups are generated using ring structure Fig. 1. The head person of the organization is responsible for assigning a particular group to particular user. Each group is assigned public key which can use for encryption and decryption of information at group level. Each user has own set of public key and private key.

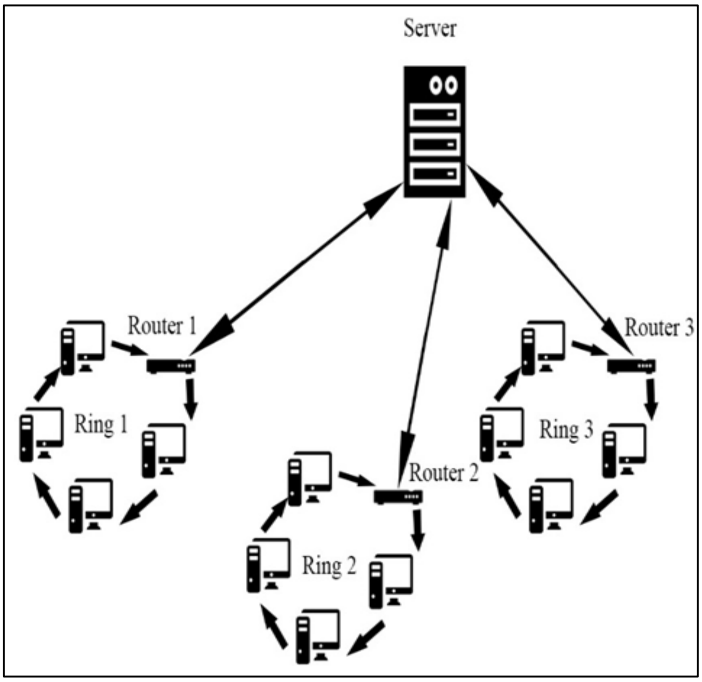
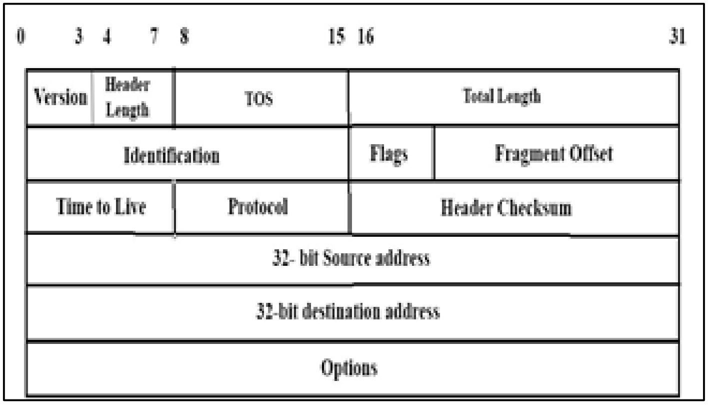


Fig. 1: Users connected in ring architecture forming groups which are connected to server.

The data is sent in form of data packets. The general structure of IPv4 is follows Fig. 2.



0 3	4 7	8 15	16 31	
Version	Header Length	TOS	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
32- bit Source address				
32-bit destination address				
Options				

Fig. 2: Structure of IPv4 header

In this project we are going to modify IPv4 header as per our requirements. Header checksum Fig. 2 is 16 bit block which is used to store hash value of destination address. This hash value is used to identify the correct receiver in the ring.32 bit source address Fig. 2 contain the address of sender.32 bit destination address Fig. 2 contains the address of receiver. In this project we are purposely going to make destination address blank such that when header with blank destination address arrive at server end it will broadcasted over to all connected rings. The options block contain permission bit which is use for determining privilege. The permission bits are Read(r), Write (w) and Execute(x) hence having following possible combinations TABLE I.

r	w	x	Privileges
0	0	0	no read, no write, no execute
0	0	1	no read, no write, execute
0	1	0	no read, write, no execute
0	1	1	no read, write, execute
1	0	0	read, no write, no execute
1	0	1	read, no write, execute
1	1	0	read, write, no execute
1	1	1	read, write, execute

Table 1: privileges On Data

A. PROCEDURE

Following are the steps for sharing data:

1) The users who want to share data over the network must authenticate themselves using Kerberos authentication protocol.
2) Kerberos verifies legal users and provide access to server.
3) Sender calculates the hash value of destination address and put it in header checksum block of IPv4 header. Sender leaves 32-bit destination block of IPv4 header blank to achieve anonymity.
4) Sender obtains the receiver's public key and receivers group key. Then sender encrypts the data using public key of receiver then encrypted data again encrypted using receiver's group key. When server receives packet with blank IP header then it broadcast that packet over the network. That packet arrives at each ring.
5) Receivers ring router decrypts the packet using public key of receivers ring to obtain destination address hash value and encrypted data.
6) Then in receiver's ring hash value of each user's MAC is compared with received hash value. The user having same hash value is actual receiver of that data. After that data packets are given to that receiver for decryption purpose.
7) When data arrives at receivers end it is in encrypted form which can be decrypt using private key of receiver.

This procedure ensures that data is given to correct ring and appropriate receiver in the ring.

IV. Scope

As a business grows, it might expand to multiple sections. To keep things running efficiently, the people working in different sections need a fast, secure and reliable way to share information across computer networks. The big companies or organizations can afford the cost of advance techniques like Digital certificates and VPN to securely transfer data between clients. This project attempts to provide solution to such problem and help small organizations to reduce data sharing cost.

V. Limitations

1) It has single layer architecture. If router fails system stops working.
2) It is vulnerable to flooding attack.

VI. Conclusion

Anonymity, integrity and confidentiality are important aspects of information security. Hence maintaining data security is big challenge. Technology like VPN and Digital certificate provides costly solution to problem. Start-up organization may not afford such costly solution. The project proposes solution to such problems in cost efficient manner by eliminating need of checking certificate.

The authentication is done using Kerberos which ensures that only legal users have access to system which provides integrity. Some systems may undergo man-in-middle attack which revel the data as well as identity of sender and receiver. In this project ring signature is used which hides identity of sender and receiver. Since destination address is kept blank, attacker won't have any clue regarded to destination of data hence data anonymity is maintained. Data is encrypted using receivers public key and only decrypted using private key of receiver hence other group member cannot able to decrypt message which preserves confidentiality, hence this project provide anonymity, integrity and confidentiality to data in cost efficient manner.

References

[1] Xenia Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," in IEEE transactions on computers, vol. 64, no. 4, April 2015.

[2] Jan Camelish, Department of Computer Science ETH Zurich, CH-8092 Zurich, Switzerland, "Efficient and Generalized Group Signatures," in W. Fumy (Ed.): Advances in Cryptology - EUROCRYPT '97, LNCS 1233, pp. 465-479, 1997. Springer-Verlag Berlin Heidelberg 1997

[3] Trapti Ozha, Department of Computer Science & Engineering Sushila Devi Bansal College of Engineering, Indore, "Kerberos: An Authentication Protocol," in Int.J.Computer Technology & Applications, Vol 4(2), 354-357.