Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Proposed Concept for Secured Data Sharing using cryptography over Peer to Peer Network

Rajesh Tiwari, Piyush Garg, Bhavana Gupta
[1,2,3] CSE Deptt CIST, Bhopal

Abstract : In this Paper, we have presents an idea to form secured P2P network and information security through cryptography technique. To secure P2P network we have used unique identification factor of peers is physical address, with the help of this factor we can established a P2P network uniquely and then we have designed key. Through key, we can encrypt information and send it to the other end. It significantly simplifies concept written as security purpose while improving the efficiency of cryptography algorithm as well as peer-to-peer network. Further more we are also proposed key concept which will be used in this work.

Keywords: Information security, Encryption, Decryption, P2P Network

In this, we have presented study of previous researches on P2P Network and detailed description of P2P Network, how it's working, advantage and disadvantage and more important thing, security of information over P2P Networking. We have also presented various security issues in P2P network, how it is useful for us. In this, we have presented important loop hole of security in P2P Network and how we can improve to those loop hole. What will be the approach of our research work and many more?
In section-I, we have presented introduction about P2P Network, in section-II, we have presented detailed description of P2P network, in section-III, we have presented proposed work and in section-IV, we have presented conclusion and references.

SECTION I - INTRODUCTION

P2P is general term for a Peer to Peer network or software and with this software we can share our files on Peers to other people around the world. Not only share our files we can download files which are available on other people's computers. Files can be music files, movies, documents files or any kinds of software. The biggest reason of popularity of peer to peer software and network is the possibility to get music, movies and other software free.

We can define a Peer as a device working as client and server at the same time. A more precise definition of a Peer-to-Peer system [1] was initially given by Oram et al. in [2] and further refined in [3]: a Peer-to-Peer system is a self-organizing system of equal, autonomous entities (peers) which aims for the shared usage of distributed resources in a networked environment avoiding central services. We can classify Peer-to-Peer Systems into two main categories: structured and unstructured [4]. Figure 1 (taken from [4]) shows this classification with some network examples. These systems were originally conceived around the year 2000, when the bandwidth became wide enough to enable other cooperation models than the traditional client-server one.

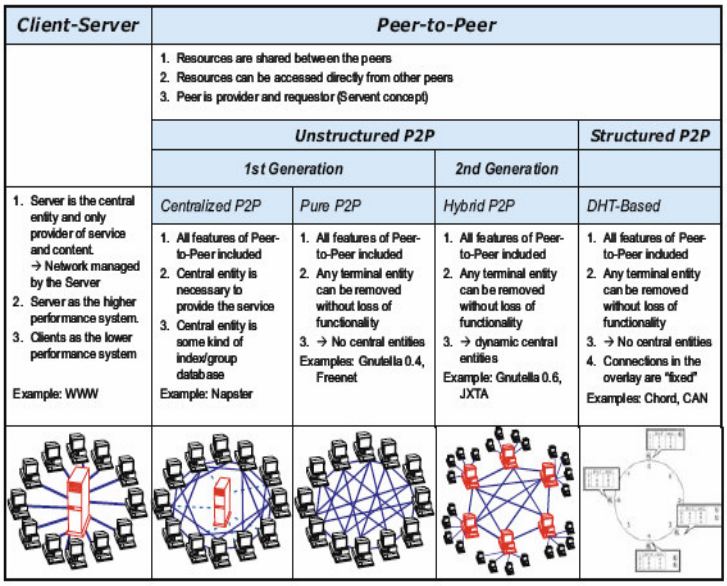

Figure 1: Overview and classification of Peer-to-Peer Systems [4]

Unstructured Peer-to-Peer Systems can be divided into two main generations. The first generation was implemented in two different ways, one very close to the client-server model with a central manager (superpeer), and one, at the opposite side, based on a fully decentralized system, where the location of a specific item is unknown and has to be discovered dynamically. Examples of centralized systems were Napster [5] and BitTorrent [6], while examples of the de-centralized ones were gnutella0.4 [7] and Freenet [8]. All these systems have revealed points of failure and are no more used in actual deployments.

Second generation unstructured Peer-to-Peer Systems have a significant scalability limit: the number of hops necessary to reach a resource. Research has progressed in a new direction to solve this problem: structured Peer-to-Peer Systems which are giving some kind of self awareness of the network. Hashing algorithms as well as simple hash tables have played a major role in helping the researches to solve this issue. The third generation of Peer-to-Peer Systems is actually built on top of Distributed Hash Tables (DHT) [11] that still represents an active and interesting research area. Nowadays we have several DHT implementations, such as Chord [12], Pastry [13], CAN (Content Addressable Network) [14], etc. and research is currently analyzing how to deal with huge amount of multimedia items in DHT-based Systems in a scalable and efficient way. Since DHT has opened a new world for experimentation, a very powerful approach is the one that is applying a metric space to DHT, i.e. by providing Metric Content Addressable Networks (MCAN) [15] as well as GHT* (Generalized Hyperplane Tree) [16], Metric-Chord (Mchord) [17], etc. We have to point out that the Network Infrastructure described in the following is mainly responsible for providing Contents in a distributed environment and for indexing and searching metadata in a suitable topology.

SECTION – II P2P NETWORK DESCRIPTION

What is Peer-to-Peer Network:- Peer-to-Peer is a communications model in which each peers has the same capabilities. We have already known that other models which it might be contrasted include the client/server model and the master/slave model. In figure 2 we have seeing peer-to-peer architecture that how a peer can communicate with other peer.

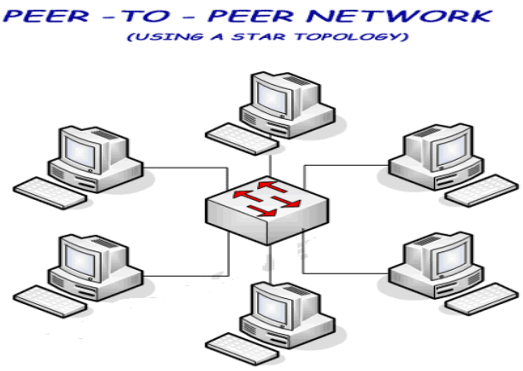

Figure 2: General Architecture of Peer to Peer Network

Presently peer-to-peer network are using with internet to exchange files with each other for this it is using mediating server. For example IBM's Advanced Peer-to-Peer Networking (APPN) of a product that supports the peer-to-peer communication model.

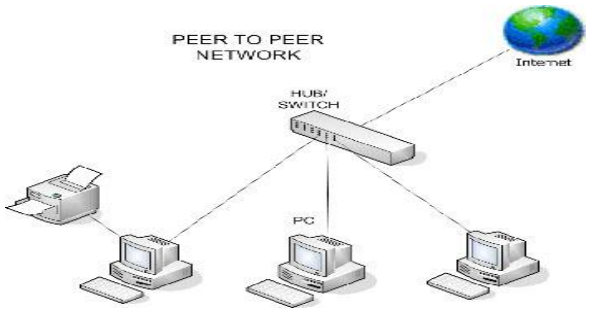

Figure 3: Peer to Peer Network Using Internet

On the Internet, peer-to-peer (referred to figure 3) is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives. Napster and Gnutella are examples of this kind of peer-to-peer software. We have already know that advantages of using P2P as a way for employees to share files without the expense involved in maintaining a centralized server and as a way for businesses to exchange information with each other directly. Peer-to-Peer (P2P) networking is a fairly popular concept. If we want to share files or data between two computer with unknown peer over public Internet, which is the causes of breaking basic principles of securing information on our computer. It is recommended that we have a firewall, either built into our router or using personal firewall software like Zone Alarm. However, in order to share files between peers and sometimes in order for us to access files on other peer within a P2P network, we must open a specific TCP port through the firewall for the P2P software to communicate. In effect, once we have opened the port we are no longer protected from malicious traffic coming through it. Another security concern is that when we have downloaded files from other peers on the P2P network we don't know for sure that the file is what it says it is. So, with all of that in mind, here are four key points to consider when using P2P networks to try use them as securely as possible:

Awareness Point against P2P Network:-

- Beware The Client Software
- Don't Share Everything
- Scan Everything

How Does Internet P2P Work: The user must first download and execute a peer-to-peer networking program. After launching the program, the user enters the IP address of another computer belonging to the network. (Typically, the Web page where the user got the download will list several IP addresses as places to begin). Once the computer finds another network member on-line, it will connect to that user's connection (who has got their IP address from another user's connection and so on).Users can choose how many member connections to seek at one time and determine which files they wish to share or password protect.

Challenges in P2P Networks:-

- Limited bandwidth
- Spyware and Malware
- Inappropriate Material
- Security Issue
- Privacy Issue

SECTION – III PROPOSED WORK

After study of peer-to-peer network, we find out that security over p2p network is a main concern, so basically this paper focused on the security of the p2p network. First we have established a p2p network and apply cryptography technique on that network. The particular type of cryptography concept we have used is the symmetric cryptography. The main concern of security when archived the remaining challenges of the p2p network like limited bandwidth, spyware and malware, inappropriate material, privacy issue etc will automatically achieved.

The concept behind using symmetric key cryptography is basically the ease of implementation and less complexity of the symmetric key algorithm. Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption. An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keys a public key to encrypt messages and a private key to decrypt them. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This in turn will reduce the space and time complexity of algorithm and improve the performance.

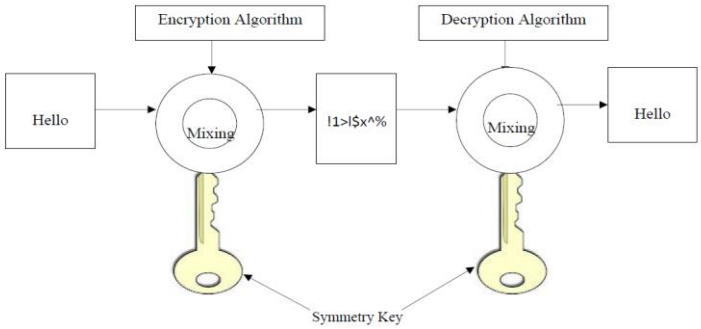

Figure 4:.Symmetric Key Cryptography

Reasons for use of Symmetric Approach for Encryption and Decryption:-

- The encryption process is simple.
- Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.
- Security is dependent on the length of the key.
- High rates of data throughput.
- Keys for symmetric-key ciphers are relatively short.
- Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms.
- Symmetric-key ciphers can be composed to produce stronger ciphers
- Symmetric-key encryption is perceived to have an extensive history.

Proposed Network: Here we are presenting proposed peer's network.

Handshaking Configuration between Peer's: Figure 5 is showing simple handshaking concept between peer's so communication can be easily.

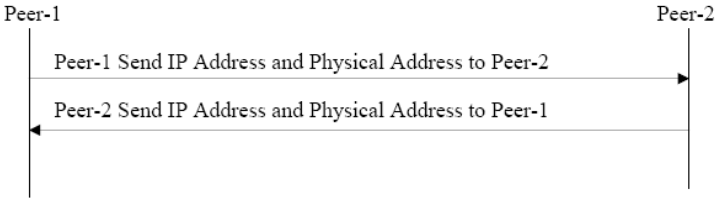

Figure 5: Handshaking between Peer's

Connection Configuration between Peer's: Figure 6 is showing proposed concept of connection configuration between peer's that mean how two peer's are connecting with each other using unique factor known as physical address.

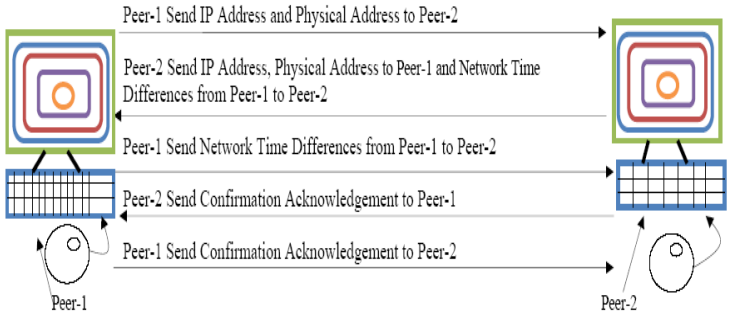

Figure 6: Architecture for Peers Synchronization

Steps during Connection Configuration between Peer's

1. Peer-1 send a request to peer-2 for connection establishment with this request Peer-1 send his physical address to Peer-2.
2. Peer-2 sends an acknowledgment for peer-1 against connection request. With this request Peer-2 send his physical address and one More Network Time Differences between Peer-1 to Peer-2.
3. Peer-1 sends confirmation acknowledgment to peer-2. With this acknowledgement Peer-1 send Network Time Differences from Peer-2 to Peer-1.
4. Peer-2 sends last confirmation acknowledgment to Peer-1 from his side.
5. Finally Peer-1 send final confirmation acknowledgement to Peer-2 from his side.

Evolution of Symmetric Key: To evaluate key by Peer-1 and Peer-2 following value have required
Peer-1 → IP Address IPA-1
Peer-1 → Physical Address PA-1
Peer-2 → IP Address IPA -2
Peer-2 → Physical Address PA-2
Peer-1 to Peer-2 → Network Time Differences NTD-1
NTD-1 = | System Clock Time-1 – System Clock Time-2 |
Peer-2 to Peer-1 → Network Time Differences NTD-2
NTD-2 = | System Clock Time-1 – System Clock Time-2|
Once we have collected these values using connection configuration figure 6. We have prepared key matrix (KM) in the following manner.

$$\mathbf{KM} = \begin{pmatrix} \text{IPA-1} & \text{IPA-2} & 1 \\ \text{PA-1} & \text{PA-2} & 1 \\ \text{NTD-1} & \text{NTD-2} & 1 \end{pmatrix}$$

With the help of this key matrix we have produced key of 128 bits.

Key Algorithm:

First we have solved key matrix using matrix calculation function

$$KM = X$$

Multiply this X into all key matrix (KM) content in the following way

$$\mathbf{KM\text{-}1} = \begin{pmatrix} X * \text{IPA-1} & X*\text{IPA-2} & X*1 \\ X*\text{PA-1} & X*\text{PA-2} & X*1 \\ X*\text{NTD-1} & X*\text{NTD-2} & X*1 \end{pmatrix}$$

Apply Transpose Matrix function on key matrix (KM-1) matrix.

$$\mathbf{KM}\text{-2} = \begin{pmatrix} X*\text{IPA-1} & X*\text{PA-1} & X*\text{NTD-1} \\ X*\text{IPA-2} & X*\text{PA-2} & X*\text{NTD-2} \\ X*1 & X*1 & X*1 \end{pmatrix}$$

Apply Circular Function on key matrix (KM-2) contents.

$$\textbf{KM-3} = \begin{pmatrix} X*NTD-2 & X*1 & X*1 \\ X*NTD-1 & X*PA-2 & X*1 \\ X*PA-1 & X*IPA-1 & X*IPA-2 \end{pmatrix}$$

Apply Row Mixing Function on key matrix (KM-3) in following way.

$$\textbf{KM-4} = \begin{pmatrix} X*PA-2 & X*NTD-1 & X*1 \\ X*1 & X*NTD-2 & X*1 \\ X*PA-1 & X*IPA-1 & X*IPA-2 \end{pmatrix}$$

Apply Column Mixing Function on key matrix (KM-3) in following way.

$$\textbf{KM-5} = \begin{pmatrix} X*PA-2 & X*IPA-2 & X*IPA-1 \\ X*1 & X*1 & X*NTD-2 \\ X*PA-1 & X*1 & X*NTD-1 \end{pmatrix}$$

Now finally concatenate all content of key matrix (KM-5) in the following way.

Proposed Key = {(X*PA-2) +(X*IPA-2) +(X*IPA-1) +(X*1)
+(X*1) + (X*NTD-2) +(X*PA-1) +(X*1)
+(X*NTD-1)}

And Calculate key matrix (KM-5) using matrix calculation function

$$\left\{ \textbf{KM-5} = Y \right. \qquad \text{for future use}$$

Block diagram of Proposed Encryption System: Figure 7 showing the concept of encryption. In this concept we will select data from storage pool to encrypt, then we will select proposed encryption algorithm with the key value. After execution of this process we will get cipher data.

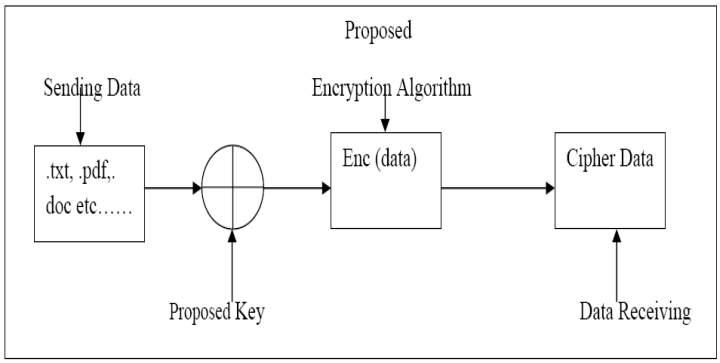

Figure 7: Proposed Encryption System

Block diagram of Proposed Decryption System: Figure 8 showing the concept of encryption. In this concept we will select cipher data from storage pool to decrypt, then we will select proposed decryption algorithm with the same key value. After execution of this process we will get original data.

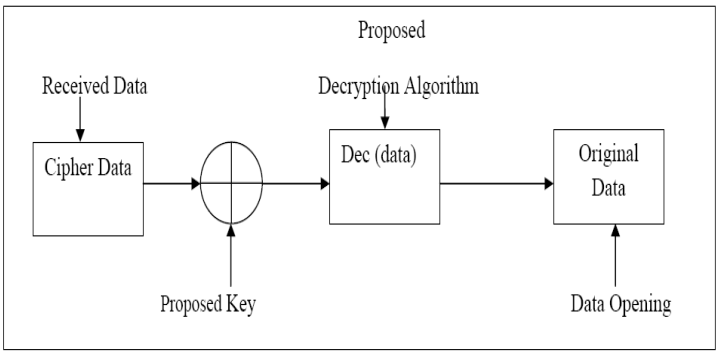

Figure 8: Proposed Decryption System

Benefits of p2p Network: - In P2P Network complexity and distribution efforts are traded for the following benefits:

- Easily availability of data.
- Access to large number of resources.
- Link availability is high.
- It expands the usefulness of the network by sharing music, video and other types of services.
- In business applications like:
  - Collaboration
  - Edge Services
  - Distributed computing and resources.
  - Intelligent agents
- Content delivery
- Exchange of physical goods, services or space:- Peer to Peer renting platforms enable people to find and reserve goods, services and space on the virtual platform but carry out the actual P2P transaction in the physical world.
- Science
  - In bioinformatics, drug candidate identification.
  - The science net P2P search engine.

- BOINIC
- Search: YaCy a free distributed search engine built on principles of P2P network.
- Communication networks
  - Skype
  - VOIP
- Military network: US department of defense has started research on P2P network as part of its modern network warfare strategy US military is using P2P networks.

Characteristics of Proposed System:-

1) **Robustness**: - System can cope with errors during execution to operate in abnormalities.
2) **Availability:** - The system is available for all the time because for same type of service a large number of resources are available.
3) **Reliability:** This system is reliable because communication between the peers is secured.
4) **Security:** The system is secured with the help of cryptography.
5) **Privacy:** System is secured due to which privacy is maintained.
6) **Efficient:** As we are applied symmetric key cryptography time complexity and space complexity is less hence the system is efficient.
7) **Low response time:** We applied less complex algorithm hence response time is low.
8) **Memory utilization:** Memory utilization is less due to less space complexity of the algorithm.

CONCLUSION

The purpose of our paper is to study work down on the security over p2p network and various strategies regarding them. In this paper we present the basic idea of securing p2p communication over public network that is internet. With various techniques present our technique easy and efficient method to secure the communication between peers over the p2p network. Our algorithm is based on symmetric key concept with a hybrid approach of asymmetric cryptography concept and hence is a new of providing security over p2p network.

REFERENCES

I. R. Steinmetz and K. Wehrle. What is this peer-to-peer about? In Peer-to-Peer Systems and Applications, volume 3485 of LNCS, pages 9–16. Springer-Verlag Berlin Heidelberg, 2005.
II. A. Oram. Peer-to-Peer: Harnessing the Power of Disruptive Technologies. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2001.
III. R. Steinmetz and K. Wehrle. Peer-to-peer-networking and computing. In Informatik-Spektrum, volume 27(1), page 5154. Springer-Verlag Berlin Heidelberg, 2004.
IV. J. Eberspacher and R. Schollmeier. First and second generation of peer-to-peer systems. In Peerto-Peer Systems and Applications, volume 3485 of LNCS, pages 35–56. Springer-Verlag Berlin Heidelberg, 2005.
V. Napster. http://free.napster.com/. Last visited on Dec 30th 2007.
VI. BitTorrent. http://www.bittorrent.com. Last visited on Jun 30th 2007.
VII. Gnutella. http://www.gnutella.com. Last visited on Dec 30th 2007.
VIII. Ian Clarke et al. Freenet: A distributed anonymous information storage and retrieval system,1999.
IX. Li Gong. Jxta: A network programming environment. IEEE Internet Computing, 5(3):88–95,2001.
X. Skype. http://www.skype.com. Last visited on Dec 30th 2007.
XI. Stefan Gotz Klaus Wehrle and Simon Riech. Distributed hash table. In Peer-to-Peer Systems and Applications, volume 3485/2005 of LNCS, pages 79–93. Springer-Verlag Berlin Heidelberg, 2005.
XII. Ion Stoica, Robert Morris, David R. Karger, Frans M. Kaashoek, and Hari Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In IIn Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM 2001), pages 149–160, San Diego, California, 2001. ACM Press.

XIII. Antony Rowstron and Peter Druschel. Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems. In IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), pages 329–350, November 2001.

XIV. Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, and Scott Schenker. A scalable content-addressable network. SIGCOMM Comput. Commun. Rev., 31(4):161–172, 2001.

XV. Fabrizio Falchi, Claudio Gennaro, and Pavel Zezula. A content-addressable network for similarity search in metric spaces. In DBISP2P '05: Proceedings of the the 2nd International Workshop on Databases, Information Systems and Peer-to-Peer Computing, Trondheim, Norway, volume 4125 of LNCS, pages 98–110. Springer, 2005.

XVI. Michal Batko, Claudio Gennaro, and Pavel Zezula. Similarity grid for searching in metric spaces. In Peer-to-Peer, Grid, and Service-Orientation in Digital Library Architectures - 6th ThematicWorkshop of the EU Network of Excellence - DELOS, Cagliari, Italy, June 24-25, 2004, Revised Selected Papers, volume 3664 of LNCS, pages 25–44. Springer, 2004.

XVII. David Novak and Pavel Zezula. M-chord: a scalable distributed similarity search structure. In InfoScale '06: Proceedings of the 1st international conference on Scalable information systems, page 19, ACM NY, 2006. ACM Press.

