iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Key Issuing Scheme For Communication In Peer To Peer Networks

Anantha D N[#1], Bhimashankar[*2], Girisha A V[#3], Mahalakshmi M C[*4], Asha G R[#5]

Dept of Computer Science & Engineering,BMSCE Bangalore

Abstract-Identity based cryptography (IBC) was introduced into peer-to-peer (P2P) networks. In this paper we propose a secure key issuing scheme for P2P networks using IBC. We are present an IBC infrastructure, which consists of setup phase, a peer registration solution using Shamir's (k, n) secret sharing scheme, and a secure key issuing scheme, which adopts key generate center (KGC) and key privacy authorities (KPAs) to issue private keys to peers or nodes securely, in order to enable the IBC systems to be more acceptable and applicable in real-world P2P network.This enables the IBC systems to be more acceptable and applicable in real-world P2Pnetworks.

Keywords: Peer to Peer, Secured key issuing, Identity based Cryptography, Message Authenticators, KGC, KPA, Public Key Infrastructure, Phishing Attacks.

I. INTRODUCTION

"Peer-to-peer computing is the sharing of computer resources and services by direct exchange between systems [1-3]. These resources and services include the exchange of data, data processing cycles, cache data , and disk storage for files however, P2P now also is used to describe some new uses of computers and networking. In particular, it is becoming more common for systems to play both the server and client roles simultaneously. P2P networking now is being used to present new services and functions. P2P is more than just the universal file sharing model popularized by Napster. According to the Peer-to-peer working group, business applications for P2P [4] computing fall into a handful of scenarios. P2Pnetworks are extremely vulnerable to large wide range of attacks, mainly due to the lack of a certification and authentication service responsible for peer's identity verification and for authentication purposes[6]. Traditional certificate-based public key infrastructure (PKI) can be used here to solve some of the problems by verifying the authenticity of nodes' identities and issuing public key certificate to each node[7-9]. Peer-to-peer (P2P) [10] networks becomes more popular because of sharing files without need of centralized servers. It doesnot maintaining any huge amount of routing state[11]. With help of a scalable and fault-tolerant it easily determine the specific nodes in network. It decrease the distribution cost of large media files for the original provider of the data significantly[12]. The identity of a peer (e.g., peer identifier or peer geometric coordinate) in P2P overlay networks [13] is used to generate public key, so its hide from the use of any certificates. The IBC-based systems are measurable, simple to organize, and each user can carry out any where any time encryption,build secure communication channels, and prove its recognize to other nodes and verify protected messages and produce a type of signature with non-repudiation property[14-16]. Certification service responsible for identity verification and for authentication purposes. We can solve some of the problems by verifying the authenticated nodes identities and by issuing public keys to the nodes for certification using traditional certificate-based public key infrastructure (PKI) [5].Security protocol is difficult to deployed as many nodes that store certificates to each node, it may become invalid quickly as node churn is highly frequent in P2P network. Securing Key issuing [17] trust level that is to be placed on third party is important .In regular transmission of data that the users supplies information must be blinded which is also called as blinding[18]. The third party provides a partial private key which is called as blinded. That key is passed on many other third party. Once the users gets the key the users can unblind the keys and retrieve the information[19]. Here the secured key is divided into several parts and any three of the key part can be used by the user to retrieve the information.

II. RELATED WORK

IBC was introduced in 1984 by Shamir. Though IBC overcomes the problems of the traditional PKI [5], it suffers from some inherent defects, which is the one of secure channel requirement, key issuing requires secure channel to avoid eavesdropping. IBC uses the user's identity as the public key. The private keys of the users are provided by a keygenerate center (KGC) after verifying

©IJRASET 2015: All Rights are Reserved

the user's credentials. In real-world P2P networks, it is important to have a key issuing scheme in order to keep in secret whether the private key corresponding to a certain identity has been requested. In this paper, a secure key issuing scheme for P2P networks, which addresses the shortcomings of and makes IBC more applicable in the real world, is presented. The Shamir's secret sharing scheme [6] has a good abstract foundation which provides an excellent framework for proofs and applications. One straightforward way to establish a shared secret between two devices [7] is that the two end users of the P2P link interactively set up a secret key via human negotiation. Secret sharing has been used to design group key distribution protocols. There are two different approaches using secret sharing: one assumes a trusted offline server active only at initialization, and the other assumes an online trusted server, called the key generation center, always active. Shamir's Secret Sharing is an algorithm [6] in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore we sometimes use the threshold scheme where any k of the parts are sufficient to reconstruct the original secret.

Advantages for our group key transfer protocol are: 1) key freshness; 2) key confidentiality; and 3) key authentication. Key freshness is to ensure that a group key has never been used before. Thus, a compromised group key cannot cause any further damage of group communication. Key confidentiality is to protect the group key such that it can only be recovered by authorized group members; but not by any un-authorized user. Key authentication is to provide assurance to authorized KGC [17] . The proposed an efficient group key transfer protocol based on secret sharing. Every user needs to register at a trusted KGC initially and preshare a secret with KGC. KGC broadcasts group key information to all group members at once. Security analysis for possible attacks is also included. In the proposed protocol, we only focus on protecting group key information broadcasted from KGC to all group members. Here briefly explained that how to provide user authentication and authenticate messages transmitted from group members to KGC. In this paper, a novel secure key issuing scheme for P2P networks is proposed along with the setup scheme of IBC infrastructure. A peer registration protocol which can register peers adopting Shamir's secret sharing scheme is introduced. Finally a secure key issuing protocol which can issue private keys securely without the requirement of secure channels is introduced. The protocol enables IBC more acceptable and applicable in real-world P2P networks.

KGC: There is a trusted core node which acts as KGC at the center of the system, which provides peer registration and key issuing service.

KPA: N nodes are selected as Key Privacy Authorities (KPAs) [1] in order to provide the key privacy service in the key issuing phase, which are not required to be as reliable as KGC. In addition, malicious attackers can potentially compromise some of these nodes to perform inside attacks.

Peer: A peer is an ordinary node in P2P networks, which is vulnerable to all kinds of attacks.

This is expensive and difficult to achieve in a large scale P2P network. In real-world P2P networks, it is important to have a key issuing scheme in order to keep in secret whether the private key corresponding to a certain identity has been requested. In this paper, a secure key issuing scheme for P2P networks, which addresses the shortcomings of and makes IBC more applicable in the real world is presented [18-21].In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication [22]. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical [23]. Such sites ask for personal information, including banking passwords or offer software downloads. Phishing is an online scam that attempts to defraud people of their personal information such as credit card or bank account information. We are going to detect, locate and remove the phishing e-mail [24]. Phishing [225] attempt acquire sensitive information by masquerading as a trustworthy entity in an electronic communication purporting to be from popular social websites, auction sites, banks, online payment processors. Phishing emails may contain links to websites that are infected with malware[26]. This is the problem of the people facing today. To overcome this problem we use the technique called Shamir's secret key sharing algorithm[9].

III. OVERVIEW

©IJRASET 2015: All Rights are Reserved

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

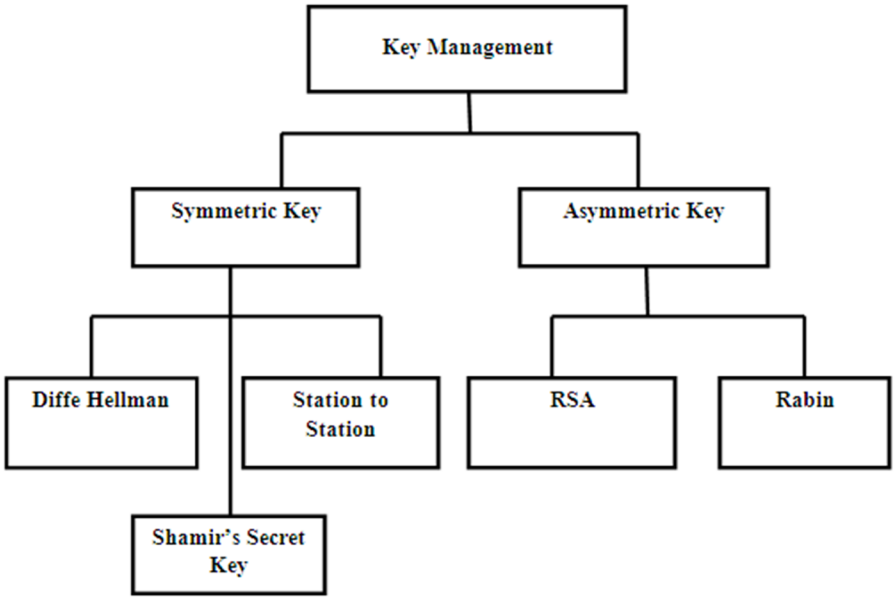


Fig.1 Key Management Protocol [26]

Definition: Key Management is the set of techniques and procedures supporting the establishment and maintains of keying relationship between authorized parties .Key management is broadly classified as shown in the figure 1.

Symmetric Key: Symmetric key uses single secret key between sender and receiver which are involved in the communication [26].

Symmetric Key Examples: Diffie Hellman and Station to station algorithm [26].

Comparisons:

Symmetric Key:

1) The secret key must be shared between 2 parties.
2) It is based on permutation and substitution.
3) Single key used for Encryption/ Decryption.
4) It is faster than Asymmetric Key
5) For Encipherment of large message symmetric key cryptography is still needed.

Asymmetric Key:

1. Each person creates and keeps his/ her own secret key.
2. Whenever application is personal secret we need this key in cryptography.
3. It is based on applying Mathematical function to Numbers.
4. It is uses two separate key that is public and private key.
5. Plaintext and cipher text treated as a integers in asymmetric key cryptography.

Deffie-Hellman: It is a specific method of securely exchanging cryptographic keys over a public channel and was the first specific example of public-key cryptography as originally conceptualized by Ralph Merkle. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communicationchannel. This key can then be used to encrypt subsequent communications using a symmetric

©IJRASET 2015: All Rights are Reserved

key cipher.Two parties create a symmetric key Without the need of KDC [26].

Station to Station: It is a method based on Deffie-Hellman.In public-key cryptography, the Station-to-Station (STS) protocol is a cryptographic key agreement scheme based on classic Diffie–Hellman that provides mutual key and entity authentication. In addition to protecting the established key from an attacker, the STS protocol uses no timestamps and provides perfect forward secrecy. It also entails two-way explicit key confirmation, making it an authenticated key agreement with key confirmation (AKC) protocol. It uses digital signature with public key certificate to establish a session key between to parties [26].Shamir's Secret Key: It is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any ***k*** of the parts are sufficient to reconstruct the original secret. The goal is to divide secret ***S*** (e.g., a safe combination) into ***n*** pieces of data $S_1 \ldots S_n$ in such a way that: a) Knowledge of any **k** or more $\mathbf{S_i}$ pieces makes ***S*** easily computable.b)Knowledge of any ***k-1*** or fewer $\boldsymbol{S_i}$ pieces leaves ***S*** completely undetermined (in the sense that all its possible values are equally likely).This scheme is called ***(k,n)*** threshold scheme. If ***k=n*** then all participants are required to reconstruct the secret.

Asymmetric Key: Asymmetric key uses two secret keys(public key and private key) between sender and receiver which are involved in the communication.

Asymmetric Key example: RSA and Rabin.

RSA: which uses modular exponentiation for encryption/decryption [26]. RSA is one of the first practicable and is widely used for secure data transmission. In such the is public and differs from the which is kept secret.

Rabin: The Rabin cryptosystem is an asymmetric technique, whose security is related to the difficulty. The Rabin cryptosystem was the first asymmetric cryptosystem where recovering the entire plaintext from the cipher text could be proven to be as hard as factoring.

IV. CONCLUSION

As the networks are evolving, they also give rise to a requirement of strong security There have been a large number of ways to efficiently handle the security requirement in networks. In this project we have developed a secure key issuing scheme for P2P networks using IBC, SKIP. SKIP provides a peer registration service using Shamir's(k,n) secret sharing scheme. We develop a secure key issuing protocol, which adopts KGC and KPAs to issue private keys to peers securely.To maintain the security of KPAs, authenticate KPAs, remove malicious ones and find out alternate ones to join in the system using the BFT protocol.

V. ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITYIMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

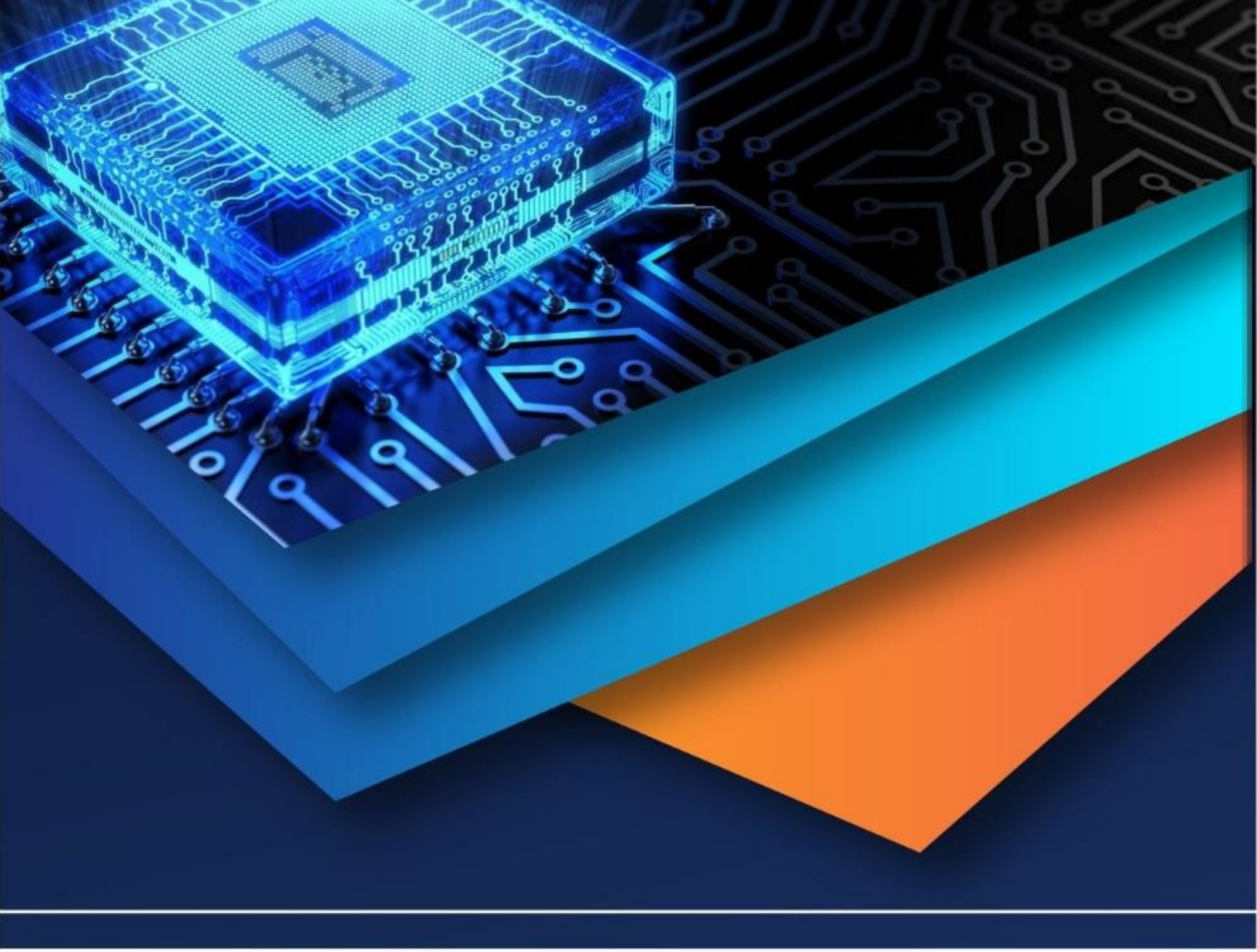
REFERENCES

[1]Mohammed Azharuddin, Annapurna P Patil,"Secure Key Scheme for Communication In P2P Networks", in International Journal of Wireless & Mobile Networks, Volume 4, No. 1, February 2012
[2] Shane Balfe, Amit D. Lakhani and Kenneth G. Paterson, "Trusted Computing: Providing Security for Peer-to-Peer Networks"PP. 117-124, 31 Aug.-2 Sept. 2005
[3] Dushyant B.Sisode ,Sanjay Thakur, "IBC Secured Key Partition for A Peer-To-Peer Network in Delivery of Message", International Journal of Latest Trends in Engineering and Technology, Volume 3, Issue 3, January 2014.
[4] Eng Keong Lua, Jon Crowcroft, and Marcelo Pias,"A Survey and Comparison of Peer-to-Peer Overlay Network Schemes", IEEE Communications Surveys & Tutorials Second Quarter 2005 Volume 7, NO. 2, 2005.
[5] Mario Cagalj, Srdjan Capkun, "Key Agreement in Peer-to-Peer Wireless Networks", Proceeding of the IEEE, Volume 94, Issue 2, February 2006.
[6] Dan Bogdanov, "Foundations and properties of Shamir's secret sharing scheme, Research Seminar in Cryptography", May 1st, 2007.
[7] Ankur Guptaand Lalit K, "Peer-to-Peer Networks and Computation: Current Trends and Future Perspectives",Computing and Informatics, Volume 30, 2011, 559–594.
[8] Wenlong Shen, Weisheng Hong, Xianghui Cao, Bo Yin, Devu Manikantan Shilay and Yu Cheng, "Secure Key Establishment for Device-to-Device

©IJRASET 2015: All Rights are Reserved

Communications", 9 Oct 2014.
[9] B.V. Baiju, "Secret Key Sharing Scheme Based On Key Generation Centre For Authenticated Exchange of Messages", in ISSN, Volume 2, Issue 1, November 2013, PP.15-21.
[10] N.Sandeep- Chaitanya, P Sruthi,A Nandini, T.V Suresh Kumar SP, "Authentication, Key Establishment & Cooperative Cache maintenance in Wireless P2P Environments", International Journal of Engineering Science and Innovative Technology, Volume 2, Issue 1, January 2013.
[11] Abbasi A, Zahedi .YanChen "Phishing tool attack" "PP. 12-17,2012
[12] Suneeta Peddireddy, Lokesh A
Prapulla C, Suneeta Peddireddy, Lokesh A "IBC Secured Key Partition for A Peer-To-Peer Network", American Journal of Engineering Research, Volume 02, Issue 09, pp. 154-162.
[13] Kolja Eger, "Efficient Simulation of Large-Scale P2P Networks", 15th EUROMICRO International Conference on Parallel, Distributed and Network-Based Processing (PDP'07), 2007, pp. 467-
474
[14] Nirmala Jagadale, Thaksen Parvat
"A Secure Key Issuing Protocol for Peer-to-Peer Network",International.
Journa. of Recent Trends in Engineering & Technology, Volume 11, June 2014.
[15] Wu Liu,Ping Ren,Donghong Sum, Ke Lie, Jianping Wu, "P2P social network with admission control model based on trust",
AASRI Conference on Parallel and Distribiuted Computing and Systems, pp. 281 – 286.
[16] Yuhua Liu a, Yuling Li a, Naixue Xiong, Jong Hyuk Park, Yang Sun Lee,
"The incentive secure mechanism based on quality of service inP2P network",
Computers and Mathematics with Applications 60 (2010), pp. 224-233.
[17] S.Arun, D.Anandan, T.Selvaprabhu, B.Sivakumar, P.Revathi, H.Shine,
"Detecting Phishing Attacks In
Purchasing Process Through Proactive Approach", Advanced Computing: An International Journal, Volume 3, Issue 3, May 2012.
[18] Mayur Bhati and Rashid Khan, "Prevention Approach of Phishing on Different Websites",International Journal of Engineering and Technology,
Volume 2, Issue 7, July, 2012.
[19] Rashmi Gupta,"Token Based Security for Prevention of Phishing Attack at Client Side", International Association of Scientific Innovation and Research,PP. 345 – 354,2008
[20] Peer-to-PeerSecurity Allan Friedman,
[21] Lin Wang Helsinki , "Attacks Against Peer-to-peer Networks and ounter measures", Seminar on Network Security, 2006-12-11/12.
[22] Md.Sadek Ferdous, Farida Chowdhury and Md. Moniruzzaman, "A Taxonomy of Attack Methods on Peer-to-Peer Network", Published in the Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security, 2007 (ICCIIS, 07), pp132-138.
[23] Avinash Chaudhari and Pradeep Gamit, "Analysis of various attacks on P2P networks",International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 1 January – February 2014
[24] Mansoor Ebrahim, Shujaat Khan, and Umer Bin Khalid,"Security Risk Analysis in Peer 2 Peer System;An Approach towards Surmounting Security Challenges", Asian Journal of Engineering Science and Technology, Volume 2, Issue 2, September 2012.
[25] Chander Diwakar, Sandeep Kumar, Amit Chaudhary, "Security Threats In Peer To Peer Networks", Journal of Global Research in Computer Science, Volume 2, Issue 4, April 2011, pp. 81-84.
[26] Behrouz A Forouzan, "Cryptography & Network Security", second edition.
.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)