iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

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

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Guarantee and Service Provider Based GeTrust Model in Chord-Based P2p Networks

Sindhu N[1], Sriparna R[2], Venugeetha Y[3]
[1,2](BE(CSE)) 8th Sem, [3]Associate Professor, Dept of CSE, Global Academy of Technology, Bengaluru

Abstract: ***more and more users are attracted by p2p networks characterized by decentralization, autonomy and anonymity. However, users' unconstrained behavior makes it necessary to use a trust model when establishing trust relationships between peers. Most existing trust models are based on recommendations, which, however, suffer from the shortcomings of slow convergence and high complexity of trust computations, as well as huge overhead of network traffic. Inspired by the establishment of trust relationships in human society, a guarantee-based trust model, getrust, is proposed for chord-based p2p networks. A service peer needs to choose its guarantee peer(s) for the service it is going to provide, and they are both required to pledge reputation mortgages for the service. The request peer makes evaluations on all the candidates of service peer by referring their service reputations and their guarantee peers' reputations, and selects the one with highest evaluation to be its service provider. In order to enhance getrust's availability and prevent malicious behavior, we alo present incentive mechanism and anonymous reputation management strategy. Simulation results show that getrust is effective and efficient in terms of improving successful transaction rate, resisting complex attacks, reducing network overhead and lowering computational complexity.***

General terms: peer-to-peer, trust model, guarantee, reputation mortgage, incentive mechanism, computational complexity, secure hash algorithm(sha-i), advanced encryption standard algorithm.
Keywords: guarantee provider, service provider, trust

I. INTRODUCTION

A. Knowledge and Data Engineering

Data & Knowledge Engineering (DKE) stimulates the exchange of ideas and interaction between these two related fields of interest[1]. DKE reaches a world-wide audience of researchers, designers, managers and users. The major aim of the journal is to identify, investigate and analyze the underlying principles in the design and effective use of these systems. DKEachieves this aim by publishing original research results, technical advances and news items concerning data engineering, knowledge engineering, and the interface of these two fields. Data and knowledge engineering covers the following topics:

1) *Representation and Manipulation of Data & Knowledge:* Conceptual data models, Knowledge representation techniques, Data/knowledge manipulation languages, and techniques.
2) *Architectures of Database, Expert, or Knowledge-Based Systems:* New architectures for database / knowledge base / expert systems, design and implementation techniques, languages and user interfaces, distributed architectures.
3) *Construction of Data/Knowledge Bases:* Data / knowledge base design methodologies and tools, data/knowledge acquisition methods, integrity/security/maintenance issues
4) *Applications, Case Studies, and Management Issues:* Data administration issues, knowledge engineering practice, office and engineering applications
5) Tools for specifying and developing Data and Knowledge Bases using tools based on Linguistics or Human Machine Interface principles
6) Communication aspects involved in implementing, designing and using KBSs in Cyberspace. And conference reports, calendar of events, book reviews etc.

To reflect the current trends in knowledge and data engineering research and development practice, *TKDE* gives priorities to submissions on the emerging topics, including but not limited to big data and applications, new frontiers of knowledge and data engineering, such as social networks, social media, and crowd sourcing. Submissions purely focusing on the topics centered in some other sister IEEE Transactions, such as core machine learning theory, pattern recognition, image processing, computer vision, neural networks, and fuzzy systems, will not be considered. This transfer and transformation of problem-solving expertise from a

knowledge source to a program is the heart of the expert-system development process. Building a KBS means building a computer model with the aim of realizing problem-solving capabilities comparable to a domain expert. It is not intended to create a cognitive adequate model, i.e. to simulate the cognitive processes of an expert in general, but to create a model which offers similar results in problem-solving for problems in the area of concern[1].While the expert may consciously articulate some parts of his or her knowledge, he or she will not be aware of a significant part of this knowledge since it is hidden in his or her skills. This knowledge is not directly accessible, but has to be built up and structured during the knowledge-acquisition phase. Therefore, this knowledge acquisition process is no longer seen as a transfer of knowledge into an appropriate computer representation, but as a model construction process.

In principle, the modeling process is infinite, because it is an incessant activity with the aim of approximating the intended behavior. The modeling process is a cyclic process. New observations may lead to a refinement, modification or completion of the already built-up model. On the other side, the model may guide the further acquisition of knowledge. The modeling process is dependent on the subjective interpretations of the knowledge engineer. Therefore, this process is typically faulty and an evaluation of the model with respect to reality is indispensable for the creation of an adequate model. According to this feedback loop, the model must, therefore, be revisable in every stage of the modeling process. PSMs contain inference actions which need specific knowledge in order to perform their task. For instance, Heuristic Classification needs a hierarchically structured model of observables and solutions for the inference actions abstract and refine, respectively. So a PSM may be used as a guideline to acquire static domain knowledge.

A central technical aspect of knowledge management is the construction and maintenance of an Organizational Memory as a means for knowledge conservation, distribution and reuse. Typically, the knowledge within an Organizational Memory will be a combination of informal, semi-formal and formal knowledge. Furthermore, such onto logies may be used for supporting the users in finding relevant knowledge, for example by offering the appropriate concepts for posing queries. Nevertheless, one should be aware, that although a considerable effort is put into knowledge management, the construction and application of Organizational Memories is still in a very early stage.

II. RELATED WORK

Peer-to-peer file-sharing networks are currently receiving much attention as a means of sharing and distributing information. However, as recent experience shows, the anonymous, open nature of these networks offers an almost ideal environment for the spread of self-replicating inauthentic files. We describe an algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value, based on the peer's history of uploads. We present a distributed and secure method to compute global trust values, based on Power iteration. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network. In simulations, this reputation system, called Eigen Trust, has been shown to significantly decrease the number of inauthentic files on the network, even under a variety of conditions where malicious peers cooperate in an attempt to deliberately subvert the system[2]. Trust is required in file sharing peer-to-peer (P2P) systems to achieve better cooperation among peers and reduce malicious uploads. In reputation-based P2Psystems, reputation is used to build trust among peers based on their past transactions and feedbacks from other peers. In these systems, reputable peers will usually be selected to upload requested files, decreasing significantly malicious uploads in the system. This chapter surveys different reputation-based P2P systems. We will breakdown a typical reputation system into functional components. We will discuss each component and present proposed solutions from the literature. Different reputation-based systems will be described and analyzed. Each system presents a particular perspective in addressing peers' reputation[3]. Peer-to-Peer ecommerce communities are commonly perceived as an environment offering both opportunities and threats. One way to minimize threats in such an open community is to use community-based reputations, which can be computed, for example, through feedback about peers' transaction histories. Such reputation information can help estimating the trustworthiness and predicting the future behavior of peers. This paper presents a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. There are two main features of our model. First, we argue that the trust models based solely on feedback from other peers in the community is inaccurate and ineffective. We introduce three basic trust parameters in computing trustworthiness of peers. In addition to feedback a peer receives through its transactions with other peers, we incorporate the total number of transactions a peer performs, and the credibility of the feedback sources into the model for evaluating the trustworthiness of peers. Second, we introduce two adaptive factors, the transaction context factor and the community context factor, to allow the metric to adapt to different domains and

situations and to address common problems encountered in a variety of online communities. We present a concrete method to validate the proposed trust model and report the set of initial experiments, showing the feasibility and benefit of our approach[4]. Nowadays security and privacy issues take a major role in multi-agent system. Mostly multi-agent systems are open and dynamic in nature. This nature surely introduces a problem by providing secured communication. Message-Digest5 is presented to some security problems in multi agent systems based on distributed trust and the delegation of permissions and credibility. In particular, an agent will receive requests and assertions from other agents and must decide how to act on the requests and assess the credibility of the assertions, because sometimes malicious agents start to behave in unpredictable way. The multi-agent systems which is becoming critical for sustaining good service quality, is the even distribution of workload among service providing agents. For that a dynamic trust computation model called secured trust is introduced. This reduces to authentication the reliable identification of agents' true identity. In this project the Multi-Agent System (MAS) concepts is applied to facilitate the authentication and the authorization process in order to work with multi-clients more dynamically and efficiently. The key pair and Certification Authority are deployed to encrypt/decrypt electronic data or transaction, or sign/authenticate the sender and the recipient[5].

III. RELATED DEFINITIONS

For easy understanding, we first present several concepts used in the following sections.

A. Definition 1

Service peer and service reputation. Service peer is a peer that provides service in a transaction, while service reputation represents the credibility of the service provided by the service peer and it is in [0,1]. Each peer's initial service reputation is set to 0.5 when it just joined the network according to the finding in [16].

B. Definition 2

Guarantee peer and guarantee reputation. Guarantee peer stands for a peer that provides guarantee for a service. Guarantee reputation represents the credibility of the guarantee provided by the guarantee peer. Each service peer must have at least one guarantee peer if it wants to provide a service. In case a service is inauthentic, both the service peer and its guarantee peer(s) have responsibility for their behavior. Only when a peer is qualified
to be a guarantee peer could its guarantee reputation come into effect.

C. Definition 3

Archive peer. Archive peer is a peer that manages the service reputations, the guarantee reputations and the transaction records of the peers it is responsible for. In this paper, since we adopt a Chord-based reputation management mechanism, each peer has chance to be an archive peer.

D. Definition 4

Request peer. Request peer is a peer that requests service in a transaction. After the transaction, the request peer has to provide feedbacks on the service peer and guarantee peer(s) to their archive peers, respectively.

E. Definition 5

Direct trust. Direct trust represents a trust evaluation on a target peer made by a request peer based on its historical transaction records. According to the different roles the target peer has acted, direct trust is classified into service direct trust and guarantee direct trust, and they are both calculated and stored locally on the request peer.

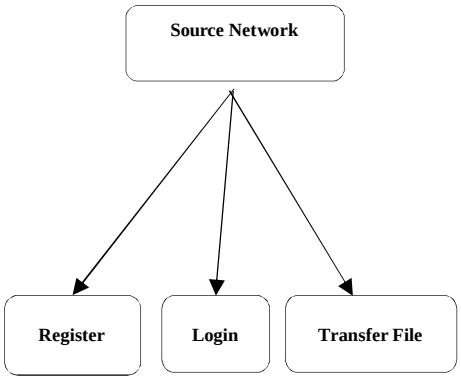
IV. MODULES USED

Source Network, Guarantee Provider, Service Provider, and Destination Network are the modules.

A. Source Network

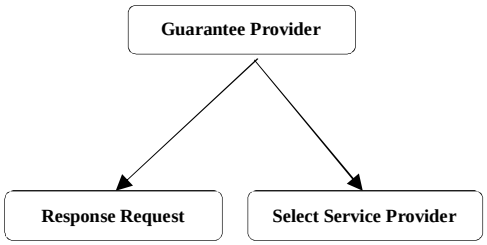
In this module, network user registers with the Network Guarantee Provider. User login and Select Guarantee Provider sends a request to Guarantee Provider for data transmission[13].

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



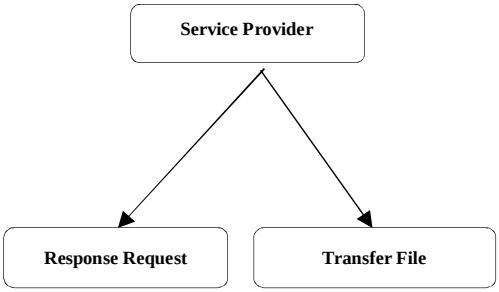
B. Guarantee Provider

In this module, Guarantee provider receive the request from network user. And search the valid service provider. Choose the service provider based on the feedback. After choosing service provider sent to network user[13].



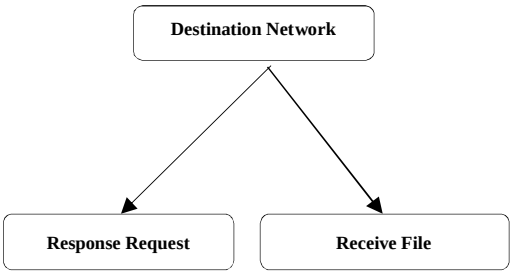
C. Service Provider

In this module, Service Provider will process the request from network user which was sent as a request to transfer the file to another network. It Responses the request and receive the file from the network user[13]. After receiving the file, it transfer to destination network user.



D. Destination Network

In this module, Source Network chooses the destination network. Service provider sends a request to destination network[13]. Destination network response the request and receive the file.



Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. IMPLEMENTATION

Implementation of software refers to the final installation of the package in its real environment, to the satisfaction of the intended users and the operation of the system. The people are not sure that the software is meant to make their job easier. The active user must be aware of the benefits of using the system .Their confidence in the software built up. Proper guidance is impaired to the user so that he is comfortable in using the application

Before going ahead and viewing the system, the user must know that for viewing the result, the server program should be running in the server. If the server object is not running on the server, the actual processes will not take place.

A. Secure Hash Algorithm (SHA-1)

In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long. SHA-1 forms part of several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPSec. Those applications can also use MD5; both MD5 and SHA-1 are descended from MD4. SHA-1 hashing is also used in distributed revision control systems like Git, Mercurial, and Monotone to identify revisions, and to detect data corruption or tampering. The algorithm has also been used on Nintendo's Wii gaming console for signature verification when booting, but a significant flaw in the first implementations of the firmware allowed for an attacker to bypass the system's security scheme[15].

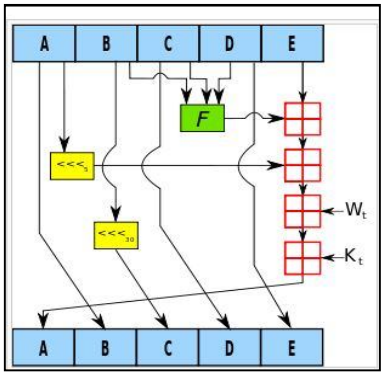


Fig:One iteration within the SHA-1

Figure above shows One iteration within the SHA-1 compression function:A, B, C, D and E are 32-bit words of the state;F is a nonlinear function that varies;<<<n denotes a left bit rotation by n places;n varies for each operation;Wt is the expanded message word of round t;Kt is the round constant of round t; ⊞ denotes addition modulo 232.

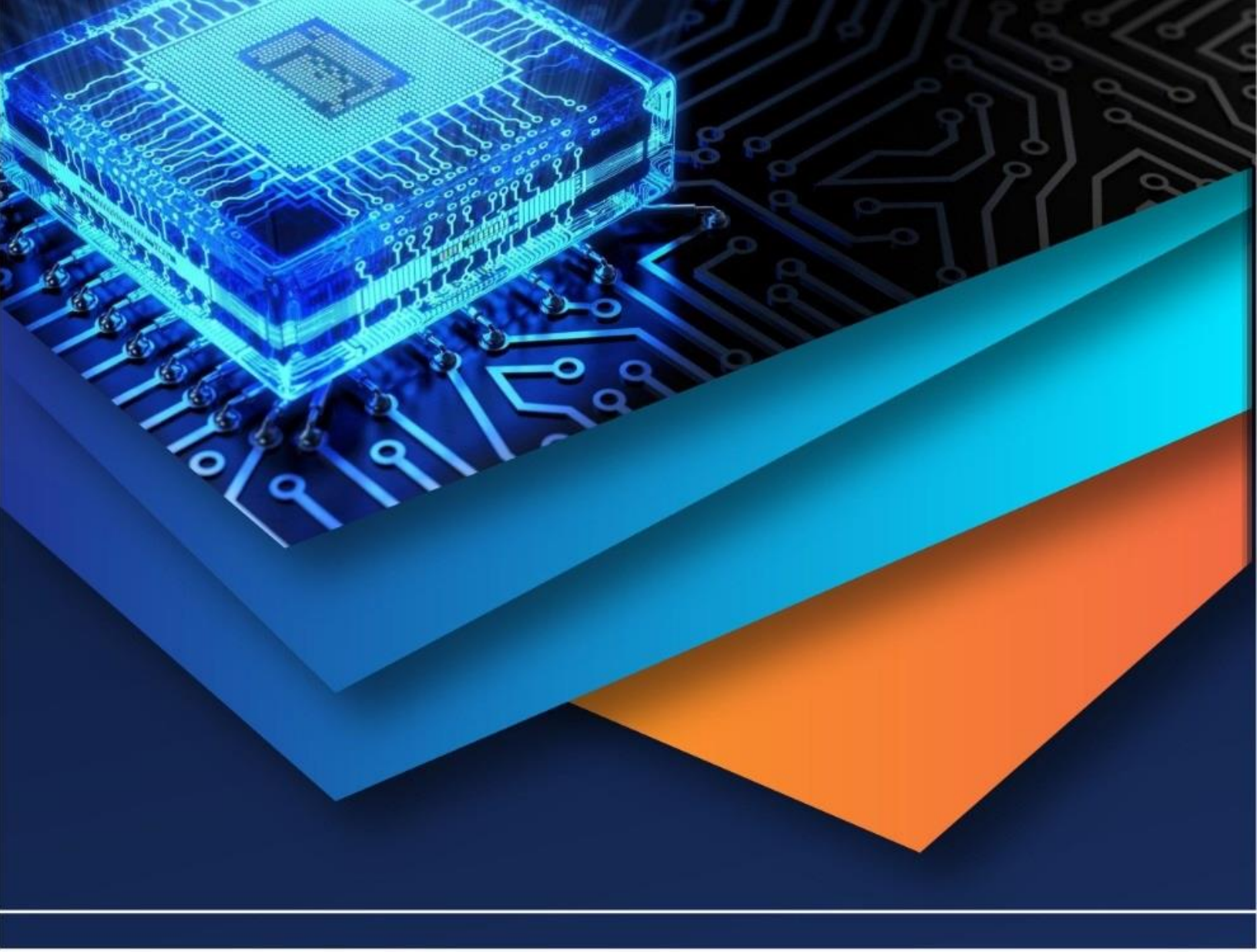
B. Advanced Encryption Standard

AES is based on a design principle known as a substitution-permutation network, a combination of both substitution and permutation, and is fast in both software and hardware[16]. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. Advanced Encryption Standard (AES) is the current standard for secret key encryption. AES was created by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, replacing the old Data Encryption Standard (DES). The Federal Information Processing Standard 197 used a standardized version of the algorithm called Rijndael for the Advanced Encryption Standard. The algorithm uses a combination of Exclusive-OR operations (XOR), octet substitution with an S-box, row and column rotations, and a Mix Column. It was successful because it was easy to implement and could run in a reasonable amount of time on a regular computer.

REFERENCES

[1] Xianfu Meng, Dongxu Liu, "GeTrust: A guarantee-based trust model in Chord-based P2P networks",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING.
[2] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks,”Proc. 12th ACM Int’l World Wide Web Conf. (WWW ’03), pp. 640-651, 2003.
[3] M. Loubna, Y. Iraqi, and R. Boutaba, "Reputation-based trust management in peer-to-peer systems: taxonomy and anatomy," Handbook of Peer-to-

PeerNetworking, Springer US, pp. 689-732, 2010.
[4] M. He, Z. Gong, L. Chen, H. Wang, F. Dai and Z. Liu, "Securing network coding against pollution attacks in P2P converged ubiquitous networks," Peer-to-Peer Networking and Applications, pp. 1-9, 2013
[5] L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trustfor Peer-to-Peer Electronic Communities," IEEE Trans. Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, July 2004.
[6] W. Dou, H. Wang, Y. Jia and P. Zou,"ARecommendation-Based Peer-to-Peer Trust Model," J. Software, vol. 15, no. 4, pp.571-583, 2004.
[7] http://www.webopedia.com/TERM/J/Java.html
[8] http://www.theserverside.com/definition/J2EE-Java-2-Platform-Enterprise-Edition
[9] JavaFX Rich Client Programming on the NetBeans Platform Published: November 2014, Addison-Wesley Professional
[10] http://www.webopedia.com/TERM/J/J2EE.html
[11] https://techterms.com/definition/wamp
[12] MySQL Reference Manual: Documentation from the Source Book by David Axmark and Michael Widenius
[13] Xianfu Meng, Dongxu Liu, "GeTrust: A guarantee-based trust model in Chord-based P2P networks",*IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*.
[14] X. Meng, Y. Ding and Y. Gong, "@Trust: A trust model based on feedback-arbitration in structured P2P network,"Computer Communications, vol. 35, no. 16, pp. 2044-2053, 2012.
[15] Domke, Felix aka "tmbinc" (2008-04-24). "Thank you, Datel". Retrieved 2014-10-05. "For verifying the hash (which is the only thing they verify in the signature), they have chosen to use a function (strncmp) which stops on the first nullbyte – witha positive result. Out of the 160 bits of the SHA1-hash, up to 152 bits are thrown away."
[16] Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno; et al. (May 2000). "The Twofish Team's Final Comments on AES Selection" (PDF).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY