INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 4 (2016) PAGES 1142 - 1149
RECEIVED : 12/08/2016. PUBLISHED : 19/08/2016
August 19, 2016

AN AUTHENTICATION AND INTEGRATED TRUST SYSTEM FOR PEER TO PEER NETWORK

[1]Deepika.N, [2]Mrs.G.Sasikala,
[1]M.Phil Scholar, Dept of Computer Science, Adhiparasakthi College of Science, Vellore,
[2]Asst.Prof, Dept of Computer Science, Adhiparasakthi College of Science, Vellore.

Abstract

The most important challenge in Peer-to-Peer (P2P) network is to assure positive interaction and satisfactory transactions. To promote positive interactions and reduce the risk involved in dealing with unknown peers; peers need to establish peer authenticity and reason about trustworthiness of the peers. The main aim of this research is therefore, to develop an Integrated Authentication and Trust Assessment System (IATAS) for P2P applications. Authentication would establish that the peer is legitimate, that is, "who it claims to be". Trust assessment would enable peers to distinguish genuine peers from malicious peers and decide on the level of trustworthiness of the peers. In closed P2P systems resource sharing and collaboration happens within a closed community such as Business Organizations, Academic Institutions or Government Departments. Web of Trust and Zero Knowledge Protocol based authentication uses public key cryptography for peer identity verification. It can be used to authenticate peers in both open and closed P2P Systems. Web of Trust is constructed to verify the binding of the public key with the peer identity. Zero Knowledge protocol is designed to verify peer possession of the corresponding private key without revealing any secret information about the private key of the peer. Trust assessment mechanisms for open and closed P2P Systems; have been designed for evaluating trustworthiness on basis of local trust, global trust or a combination of the two methods. Local trust is computed based on the peer's own experience with other peers. IATAS has been designed to provide flexibility in customizing the authentication and trust assessment process. Authentication policy rules and trust related parameters can be tailored to provide the degree of security and anonymity required by the P2P applications.

Keywords – P2P, Authentication, Trust, Private Key, Public Key, Security, Anonymous, Cryptography.

1. INTRODUCTION

Peer-to-Peer (P2P) networks break the dominant network paradigm of standard Client-Server model of information distribution and information exchange by allowing heterogeneous multipurpose machines to interact and share resources and functionality. P2P systems link different computer systems as 'peers' and allow them to interact on top of existing network configurations without the need for central coordination by servers or stable hosts. Collaboration and sharing are the major characteristics of P2P computing. Peers make a portion of their resources directly available for sharing and use by other peers in the network. Peers can collaborate to execute tasks or workload that can be partitioned among the peers who are equally privileged and equipotent participants in the application. P2P systems have many advantages of resource sharing, functionality sharing, ad-hoc collaboration, improved reliability and scalability. However, the open and anonymous nature of P2P systems can raise serious security concerns for a peer. Peers can join and leave the network dynamically and many of the peers in the network may not have interacted with each other earlier. There is no control or accountability on the content or resources that a peer can share on the network. Hence, malicious peers can exploit the property of anonymity to inject malware into the network, to carry out attacks on the genuine peers so that P2P systems can be made unreliable. The primary goal of P2P systems is to aggregate resources and makes it available for sharing cooperatively among the

peers. P2P networks require security mechanisms that can protect the system against malicious attacks and in addition have measures in place to distinguish malicious peers from genuine peers. The main aim of this research work is to develop an Integrated Authentication and Trust Assessment System (IATAS) that is able to authenticate peers and also establish the level of peer trustworthiness. The proposed system aims to provide the degree of security and anonymity as per application requirements. Specifically, the main objectives of the research work are as follows: Devise a decentralized solution that provides for peer authentication while maintaining peer anonymity at the level desired by the users and applications.

2. RELATED WORKS

P2P architecture, indexing, techniques used for searching the required content and P2P applications have been discussed in this chapter. P2P network vulnerabilities and security attacks have been presented. This chapter also discusses in detail trust management and how it can be effectively used for providing security for the shared resources. Haiying Shen et al [1] proposed a Proximity-Aware and Interest-clustered P2P file sharing System (PAIS) based on a structured P2P, which forms physically-close nodes into a cluster and further groups physically-close and common-interest nodes into a sub-cluster based on a hierarchical topology. PAIS uses an intelligent file replication algorithm to further enhance file query efficiency. It creates replicas of files that are frequently requested by a group of physically close nodes in their location. Moreover, PAIS enhances the intra-sub-cluster file searching through several approaches. This Most of these methods are on unstructured P2P systems that have no strict policy for topology construction.Guoxin Liu et al [2] present an Efficient and trustworthy file querying is important to the overall performance of peer-to-peer (P2P) file sharing systems. Emerging methods are beginning to address this challenge by exploiting online social networks (OSNs). However, current OSN-based methods simply cluster common-interest nodes for high efficiency or limit the interaction between social friends for high trustworthiness, which provides limited enhancement or contradicts the open and free service goal of P2P systems. Little research has been undertaken to fully and cooperatively leverage OSNs with integrated consideration of proximity and interest. This approach propose different strategies to guide nodes to forward a file query to friends that are more trustworthy and more likely to resolve the queries or forward the query to file holders. This also proposes follower- and cluster-based file replication algorithms to enhance file search efficiency.Yong, X et al [3] discussed and research about P2P network structure and communication. This P2P network is mainly using the distributed hash table (Distributed Hash Table, abbreviated as DHT) technology to organize the network nodes. DHT is a huge hash table that is jointly safeguarded by the wide range of numerous nodes. Hash table is divided into discrete blocks; each node is assigned to a hash block of their own, and became the manager of this hash block. By cryptographic hash function, an object name or keyword is mapped to 128- bit or 160-bit hash value. Distributed hash table originated in the SDDS (Scalable Distribute Data Structures) study, Gribble have achieved a highly scalable, fault-tolerant SDDS cluster. DHT class structure can adapt the dynamic join / leave of node, has a good scalability, robustness, the uniformity and self-organizing capacity of node ID distribution. This approach cannot be directly applied to general DHTs in spite of their higher file location efficiency.

3. PROPOSED APPROACH

The proposed research work is therefore focused on the key security challenges of Peer Authentication and Trust Assessment for P2P systems. Peers must first be authenticated to establish that the peer is legitimate or authentic or in other words is “who it claims to be”. However,

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 4 (2016) PAGES 1142 - 1149
RECEIVED : 12/08/2016. PUBLISHED : 19/08/2016
August 19, 2016

Authentication does not guarantee that the peer is genuine or trustworthy. Trust and Trust Assessment mechanisms aid in evaluating the reliability and genuineness of a peer. Trust assessment would enable peers to distinguish genuine peers from malicious peers and decide on the level of trustworthiness of the peers. The requirement for decentralization of the process and data involved in peer authentication and trust assessment has been another major design consideration. P2P systems can be categorized as open and closed systems depending on the approach used by peers to connect to the network.

The proposed Authentication and Integrated Trust System addresses the two key security issues of authentication and trust assessment of peers for P2P networks. AITS has been designed to directly interface with the peers and provide an integrated solution to P2P applications for peer authentication and trust assessment. Peers who share the resources can use AITS to authenticate the service requesters and verify their trustworthiness. Likewise, service requesters can also verify the legitimacy of the service providers. The architecture of AITS is given in Figure 1.

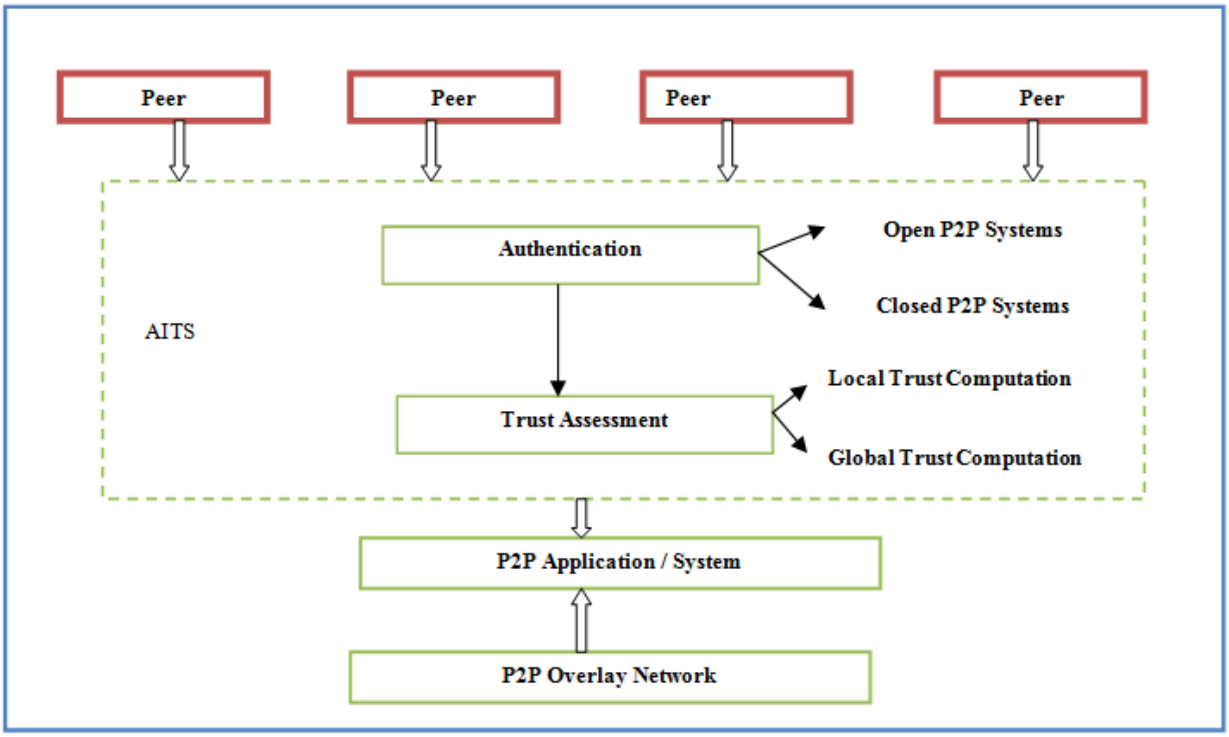

Figure.1. Architecture of Authentication and Integrated Trust System (AITS).

The proposed solution comprises of two layers: Authentication and Trust Assessment. The system integrates these two layers in such a way that the authentication of a peer is verified prior to its trust assessment. Authentication process verifies the peer identity while trust assessment helps to evaluate the reliability and genuineness of the peer. The proposed trust assessment addresses the issue of trust evaluation of both the peers; service provider and service requester. The proposed trust assessment takes into consideration the need for providing flexibility in determining the degree of trust for a peer based on the security requirements of the applications. AITS acts as an intermediate layer between the peers and P2P applications.

3.1. System Design

The Authentication and Integrated Trust System has been designed as a two layer architecture. The authentication layer incorporates authentication solutions for open and closed P2P systems; Role

based authentication and Web of Trust (WoT) and Zero Knowledge based Protocol (ZKP) based authentication. The Trust Assessment layer incorporates Profile based trust assessment for local trust assessment and Reputation based trust system with outlier detection for global trust score computation.

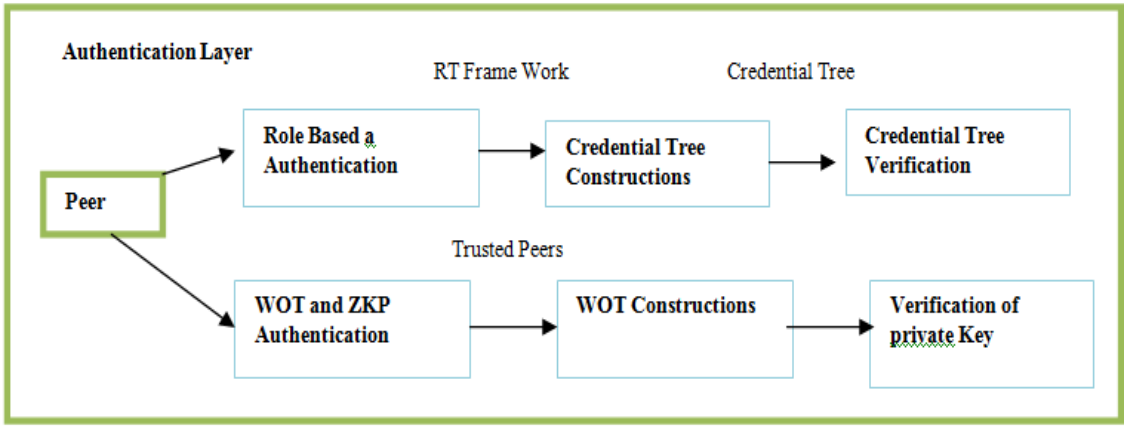

Figure.2. Design of Authentication Layer of AITS.

Role based authentication mechanism is used to authenticate a peer based on the credentials given by the peer. The credential representation follows the semantics of Role based Trust (RT) framework which is used to build the credential tree. The constructed credential tree would aid in the process of authentication of peers in closed P2P systems where peers have assigned roles and responsibilities. The WoT and ZKP authentication technique uses public key to verify a peer identity. The Web of Trust is constructed using trusted peers for verifying the binding of the public key with the peer identity. The possession of the corresponding private key is verified using Zero knowledge based protocol. This authentication technique can be used for verifying peer identity in both open and closed P2P systems.

3.2.TRUST ASSESSMENT

The trustworthiness of a peer has to be assessed to distinguish genuine peers from malicious ones. Trust assessment mechanisms have been proposed for computing the local trust and global trust. Local trust assessment is based on the peer's own experience and global trust is computed on the basis of recommendations obtained from other peers in the network. Profile based trust assessment mechanism is proposed for local trust assessment. Peer profile is maintained based on the history of prior transactions. Genetic Algorithm (GA) is used to optimize the peer profile that is used for anomaly detection. Reputation based trust assessment scheme collects the opinion about the peer from other peers in the form of reputation scores. Rough set theory has been applied to the collected scores to detect and eliminate outlier or wrong scores. Only the correct scores are then used for computing trustworthiness of peers. The proposed trust assessment schemes are generic and can be used by service provider to determine the trustworthiness of the service requester.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 4 (2016) PAGES 1142 - 1149
RECEIVED : 12/08/2016. PUBLISHED : 19/08/2016
August 19, 2016

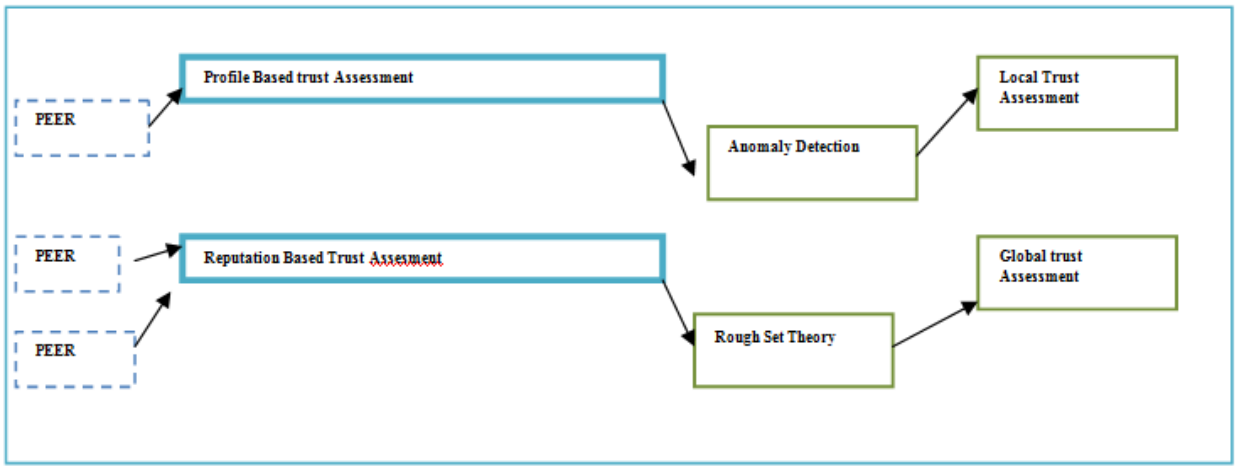

Figure.3. Design of Trust Assessment Layer of AITS.

3.3 BENEFITS OF THE PROPOSED SYSTEM

The research work, AITS, addresses the two key security challenges of Peer Authentication and Trust Assessment for P2P systems. The system provides facility to authenticate peers, that is, establish that the peer is "who it claims to be". Trust assessment enables peers to distinguish genuine peers from malicious peers and decide on the level of trustworthiness of the peers. There is always a tradeoff between anonymity and authentication in P2P systems. Peer anonymity is an essential characteristic of P2P systems, but malicious peers can use anonymity as a cloak to shelter and masquerade themselves to spread malicious content or malware. Hence, authentication is necessary to verify the identity of the peer. AITS authentication solutions have been designed to provide a suitable balance between authentication and anonymity. The solutions provide security against key security attacks related to peer identity and authentication. Role based authentication can be used to authenticate peers who form a closed P2P system with defined roles and responsibilities. Authentication is performed based on the role played in an organization and can be used in Business, Commercial Organization, Academic Institution or Government Departments where the employees are peers who form a closed group or community. Credentials signed by proper authority are issued to the peers and are verified to establish the authenticity of the peers. Peer profile based trust assessment method is used to assess the local trust based on the direct interactions with the peer.

The peer profile is maintained based on the history of transactions with a particular peer. Anomaly detection method is used to differentiate between normal and anomalous behavior. Genetic algorithm, a well-known powerful mathematical tool has been used to optimize peer profile to detect anomalous behavior. Detection of anomalous behavior helps to determine the trustworthiness of a peer. Reputation based trust assessment mechanism is another trust assessment scheme that has been used for global trust score computation. This mechanism relies on the recommendations about a peer collected from all other peers in the form of trust scores. Rough set theory has been used for analyzing the trust scores and finding hidden patterns in the data to eliminate wrong or outlier scores. The correct trust scores are then used for trust evaluation that has given the right decision with regard to trustworthiness of the peers.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 4 (2016) PAGES 1142 - 1149
RECEIVED : 12/08/2016. PUBLISHED : 19/08/2016
August 19, 2016

4. EXPERIMENTAL RESULTS

Role based authentication solution has been implemented and tested for a sample application in the software project development domain. The roles and responsibilities typically present in any organization for software development were defined and tested with a sample group of 25 peers. The software development department would generally constitute a closed group and the P2P network can be considered as a closed system. The authentication scheme was coded and implemented using .NET. The WoT and ZKP authentication was tested using a sample file sharing application. The authentication mechanism was implemented with 5 connected peers and the application was coded using .NET. Request for file download was implemented using flooding technique. The performance of the WoT and ZKP authentication was analyzed. The execution time for authentication was computed for the combined approach of WoT and ZKP. The graph showing the comparison of execution time with the number of trusted peers is given in Figure 4.

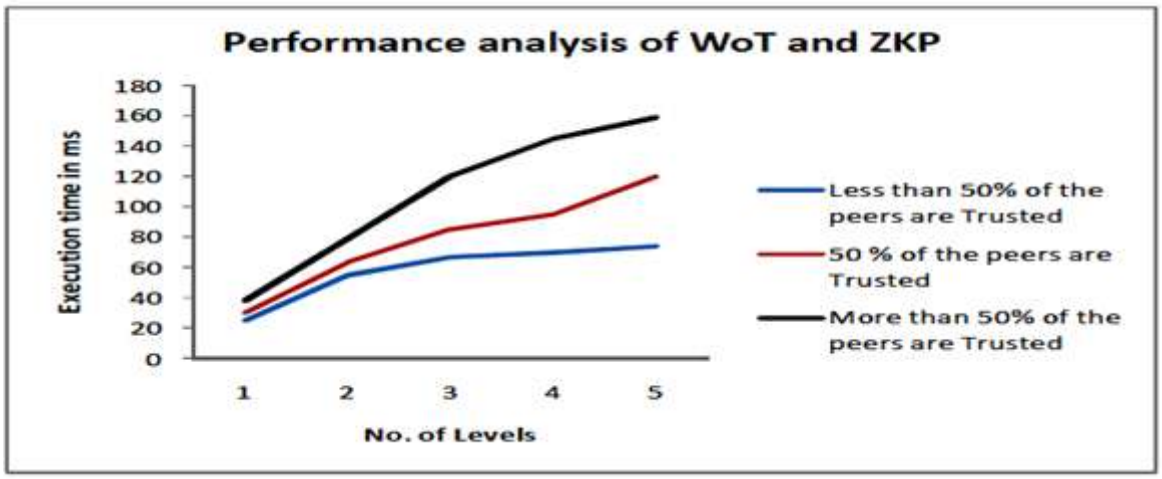

Figure.4.Performance Analysis of WoT and ZKP Authentication.

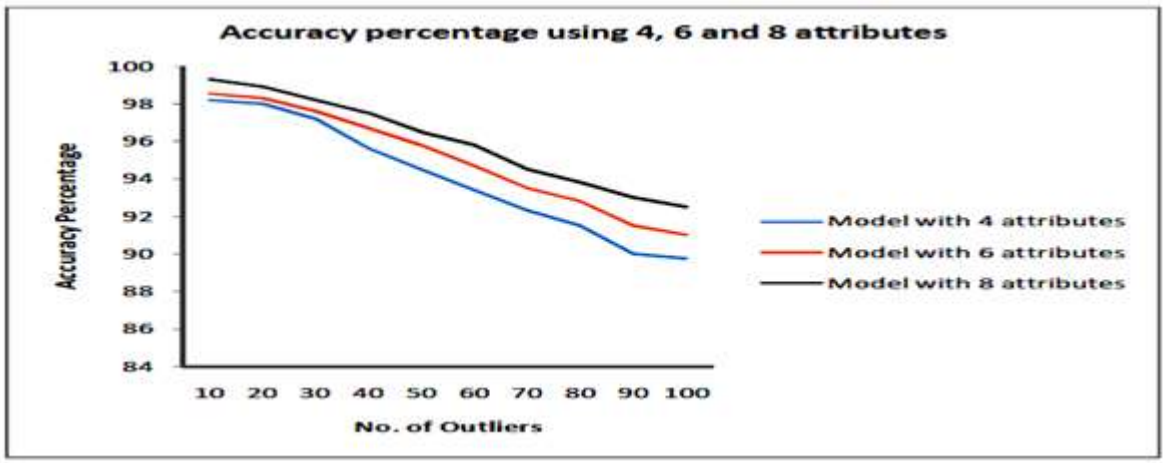

Fig.5. Accuracy Percentage of the system for 4, 6 and 8 attributes.

The number of reputation records increases with the number of peers and hence the rule generation time shows a corresponding increase. The time also shows an increase as the

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 4 (2016) PAGES 1142 - 1149
RECEIVED : 12/08/2016. PUBLISHED : 19/08/2016
August 19, 2016

number of attributes used in the evaluation method for the rule generation increases and the best results were obtained for 4 attributes.
The total time taken for trust assessment was computed for varying number of peers and the plotted graph is shown in Figure 6.

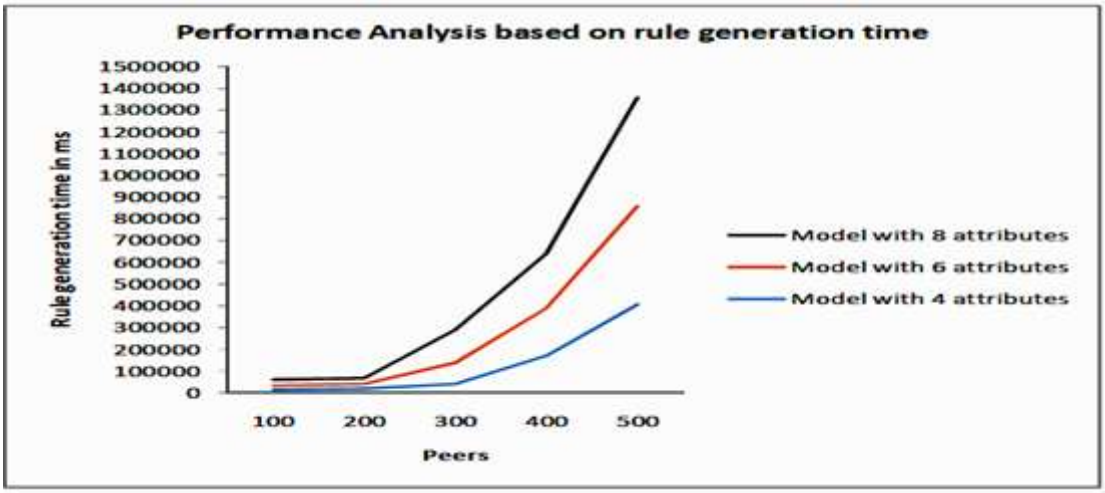

Fig.6. RST Rule Generation Time for Varying Number of Peers.

The proposed solution is a decentralized solution that assumes that peers would collaborate and provide the necessary data. For example, for global trust assessment, peers must cooperate and provide their recommendation as trust scores. While this is a reasonable assumption, WoT and ZKP based authentication and RST based Reputation Trust Assessment systems mandate that peers should cooperate to make sure that authentication and trust assessment are successful.

5. CONCLUSION AND FUTURE WORK

AITS provide a suitable balance between authentication and anonymity. Anonymity is a desirable characteristic of P2P systems which enhances resource sharing. However, anonymity also helps the malicious peers to disguise themselves, so authentication of peers is essential to ensure security. AIT has been devised as a decentralized solution that provides for peer authentication while maintaining peer anonymity at the security level desired by the applications. Role based authentication of AITS authenticates a peer based on its role played in an organization. Roles establish functionalities and authorities. Authentication policies define roles authorized to issue and sign credentials. The security techniques and methodologies of AITS are decentralized in nature to satisfy the distributed and dynamic nature of P2P networks. In role based authentication, credentials of peers are not stored at any central location. AITS , therefore, presents a decentralized, distributed and scalable security solution for P2P resource sharing and collaborative applications. The research work can be extended in future to address other security requirements such as confidentiality, access control, authorization and non-repudiation.

REFERENCES

[1]. Haiying Shen, Senior Member, IEEE, Guoxin Liu, Student Member, IEEE and Lee Ward ”A Proximity- Aware Interest- Clustered P2P File Sharing System” IEEE transactions on parallel and distributed systems, vol. 26, no. 6, June 2015.

[2]. “An Efficient and Trustworthy P2p and Social Network Integrated File Sharing System” www.lemenizinfotech.com 2015.

[3].Yong, X., Deng Chi and Gao Min, "The Topology of P2P Network", Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 8, pp. 1213-1217, August 2012.

[4]. Sebastian, M. and Oliver P. Waldhorst, "Autonomous Detection of Connectivity", Proceedings of IEEE International Conference on Peerto- Peer computing (P2P 11), pp. 44-53, 2011.

[5]. Guibing, G., Zhang, J. and Vassileva J. "Improving PGP Web of Trust through the Expansion of Trusted Neighborhood", IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), Vol.1, pp.489,494, 2011.

[6]. Hiroya, N. and Kazuyuki, S., "Flexible Routing Tables: Designing Routing Algorithms for Overlays Based on a Total Order on a Routing Table Set", Proceedings of IEEE International Conference on Peer-to- Peer computing (P2P 11), pp. 72-81, 2011.

[7]. Christian, G., Max, L. and Christoph M., "Towards a Comparative Performance Evaluation of Overlays for Networked Virtual Environments", Proceedings of IEEE International Conference on Peer-to-Peer Computing (P2P 11), pp. 34-43, 2011.

[8]. Damiano, C., Moritz S. and Pietro, M., "Adaptive Load Balancing in KAD", Proceedings of IEEE International Conference on Peer-to-Peer Computing (P2P 11), pp. 92-101, 2011