INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Providing Security by HMAC Algorithm in P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains

A. Chandrakala
M.Tech. Student, Department of CSE,
Sri Venkateswara College of Engineering and Technology, Etcherla, Srikakulam, India
S. Bhaskara Rao
Associate Professor, Department of CSE,
Sri Venkateswara College of Engineering and Technology, Etcherla, Srikakulam, India

Abstract:
The main concern of this paper is to keep the Peer-to-Peer network system more secure and at the same time to keep the speed of Peer-to-Peer network system at the maximum functionality. In this paper we introduce a new encryption protocol for the security of Peer-to-Peer network system called HMAC algorithm, which is low in cost and probably best in function. Peer-to-Peer network systems are decentralized network systems which pose them vulnerable for attackers/hackers. The vulnerability may be in the form of Peers who cheat, who propagate malicious code or sometimes the peers who simply leech on the network. This can be counteracted by our encryption protocol. Moreover we establish a trusted self certification system which minimizes the access of our network to these attackers. The other main problem being decreasing network functionality by dynamically changing number of users that are logging in & logging out. We answer this by sorting them into small groups and limiting the dynamicity in the subgroup. This provides secure transfer of information without any malicious data with efficient functionality of the Peer-to-Peer network system.

Keywords: *Peer-to-Peer network system, HMAC algorithm, Identity certificate, Cryptography (encryption).*

1. Introduction

Data sharing network systems can be centralized, partially decentralized and completely decentralized systems. Centralized network systems are efficient but the efficiency can be decreased by increased number of users in a particular time. To avoid this people started partially decentralized network systems which are more efficient than centralized network systems but it has its own demerits like member unavailability and incompatibility at a particular time make this system a little slower. Then came the completely decentralized system known as Peer-to-Peer network system. Peer-to-Peer network systems are self configuring networks with minimal or no central control[1].

Peer-to-Peer network system is not limited by number of clients, server break down or any other interference. So, the Peer-to-Peer network system becomes more popular and more used. Due to this the attackers are targeting Peer-to-Peer network system at the vulnerable sites. The most vulnerable site being security, they are easily getting access and attacking the Peer-to-Peer network system. Due to vulnerability in security there may be dissemination of malicious or spurious content, malicious code, viruses, worms, Trojans than the traditional Client-server networks(Which are centralized network systems)[1]. There is another problem called leaching. Leeching is unnecessary usage of system where peers work only for selfish interests[2]. So, it should be discouraged. The client-server system has scalability problem as the performance of the server will decrease as the number of communicating clients, which are requesting services from the server increase[2]. Peer-to-Peer network systems are almost unlimited in their scalability. There is no need for a centralized server as the users' computers are themselves used as resources and power. So, Peer-to-Peer network system becomes more popular. To protect this system there should be an efficient secure system which functions securely with minimal efforts and most reliability. We believe that one system is HMAC as one of the best secure systems.

2. Review of Literature

There are two types of Peer-to-Peer network systems, Structured, unstructured. The proposed system can be applied to both structured, unstructured P2P networks. In structured networks, the location of the data is a function of data itself or its metadata. As a result, the

search how much space is constrained by the metadata. The overlay networks like Chord, content addressable network and PASTRY are structured networks and as a result the search in these networks is much more efficient than in purely unstructured P2P networks because there are no super nodes. In structured networks, all the nodes can know the fundamental structure of the network and hence can cut short their search to the relevant nodes\. The architecture of unstructured P2P networks is not that good. In unstructured networks, there is no relationship between the data or metadata and its location.

Publius# is a monolithic system. It consists of a set of servers which are independently managed. It is prevents censorship and lets the publisher to publish anonymously by using cryptographic secret sharing techniques and divides the secret among a set of servers. [# Publius was named after the pen name used by a group of writers for writing Though the *authors* of The federalist papers in 1787-1788, had an impact on the US constitution.]Groove, A commercial application, builds self-administering, context-sensitive and synchronized share spaces for exchanging files of small size only. SDSI is a Simple Distributed Security Infrastructure simplifies the X.509 client certificate design and provides the means for self-certification, local name spaces, secure formation of groups and simple access control mechanisms. Dynamic Trust Management encapsulates trust management in dynamic distributed environments. The members of this system change their roles frequently.

Role-Based Access Control was introduced in 1992 by Ferraiolo and Kuhn. Role Based Access Control associates permissions are authorized for roles and roles are authorized for users. Blinding was introduced by Chaum in 1983. Cryptographic blinding enables an authority to *digital* signature of a document without seeing the content of the document.

COCA uses a set of distributed CA servers and provides *Fault-tolerance* and redundancy against denial of service attacks. Improving security By Quantum Cryptography in Peer to Peer Reputation Management in Distributed Identities and Decentralized Recommendation Chains but the efficiency of the system has been in question.

Implementation of P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains.

2.1. Lacunae in the Literature

Above all systems used complex and cumbersome algorithms which may give unidentifiable problems. The HMAC algorithm is simple, foolproof and efficient. There is not much metadata available about this newer system. So, we want to present this system and introduce this to the present generation.

3. Reputation Models

Resnick defined the reputation system as "a system that assembles, administers and aggregates feedback about consumer's ancient behavior." Pseudo spoofing is the use of the multiple pseudonyms in a System by the same real-life entity. Peer Trust system is generally applicable to the reputation information to a certain node on the network for storage, by applying hash functions. Abdul-Rahman and Hailes have proposed another trust model with corresponding criterion.

4. System Architecture

The *client-server* architecture permits the *clients* to make *requests* that are *network* enables remote data *access* through *client-server* for the required documents or files. The Server has to provide the access for the client; otherwise the client cannot access the data. Further if the demand is more and the server capacity to respond to clients is less, then the system will become slow. In Peer-to-peer (P2P) network system each individual peer acts as a server and as a client both. As it is a type of decentralized and distributed network, the architecture is designed in a way such that individual nodes in the network can provide access and can request data from other nodes.

The peers provide data a bit faster than the centralized servers because there is less traffic and the data providing peer is much less distant. The work load is shared among the peers and data is propagated through them with much more pace.

4.1. Existing System

The Peer-to-Peer network system is ideal network system if all the peers in the network are legitimate and foolproof. But it will become less efficient if the peers in the system are not functioning well or propagating malicious code. There is another problem called leeching where work for their selfish needs peers. Leeching in the P2P network has to be discouraged to protect the system capability. It has been shown that a system where peers work only for selfish interests while breaking the rules failure to death. Securing these networks is extremely difficult due to the decentralized and ad hoc nature of these networks.

The traditional mechanisms for generating trust and protecting client-server networks cannot be used for pure P2P networks. Because the trusted central authority used in the traditional client-server networks is absent in P2P networks. So, providing a central authority to identify and authorize peers will make the system less vulnerable to security related threats. The difficulty in securing legitimate peers will become much easy and much reliable. The main problem with centralized security system is, if it is not reliable the whole network will become unsecured. If there is no central authority then there is no cover to the network system which makes it vulnerable for malicious peers.

4.2. Proposed System

In cryptographic algorithms, a keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code involving a cryptographic hashing function in combination with a secret cryptographic key. As with any Message Authentication Code, it may be used to simultaneously verify both the data integrity and message authentication. Any cryptographic

hash function, such as Message Digest-5 or Secure Hash Algorithm-1, may be used in the calculation of a Hash Message Authentication Code. The resulting Message Authentication Code algorithm is named as Hash Message Authentication Code - Message Digest5 or Hash Message Authentication Code–Secure Hash Algorithm-1 accordingly. The cryptographic strength of the Hash Message Authentication Code depends upon the cryptographic strength of the hash function, the size of its hash output, and on the size and quality of the key. An iterative hash function breaks up a message into pieces of a fixed size and iterates over them with a compression function. For example, Message Digest5 and Secure Hash Algorithm-1 operate on 512-bit blocks. The size of the output of Hash Message Authentication Code is the same as that of the hash function (128 or 160 bits in the case of Message Digest5 or Secure Hash Algorithm-1, respectively), although it can be truncated if desired.

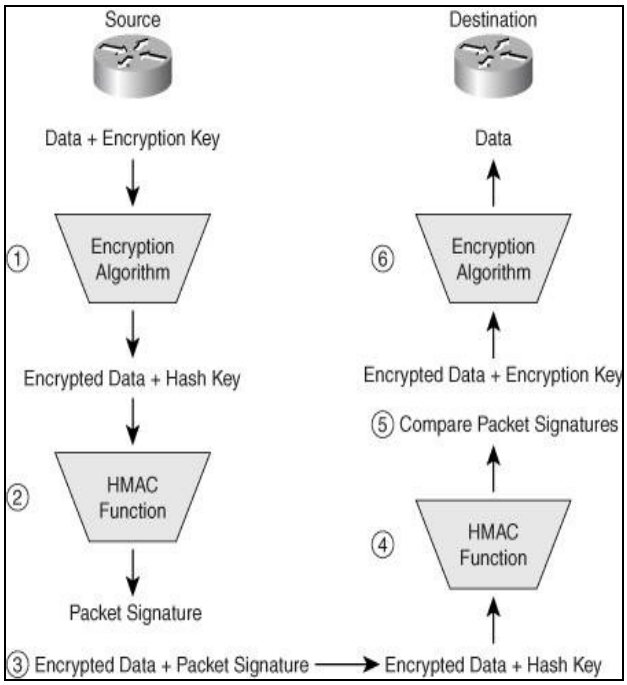

Figure 1

5. Implementation

The implementation starts with either by logging in (if the user is already a member of that group) or by signing in (if the user is a new member). The user who is going to log in should provide the correct password in order to enter into the group to receive message. The new user should sign up by providing its genuine identity which is already given by trusted certification authority. This is the major security providing zone by which anonymous users can not even enter the group. So, the illegitimate users are prevented to enter the network. There is no question of propagation of malicious code, viruses, Trojans etc as we are preventing the entry of malicious peers at the entry only.

The entered user can access the group data from the time of entry to till the time of exit only as we are also providing forward as well as backward secrecy. As the groups are divided into small subgroups there won't be much change in the number of users which makes the system much faster than traditional system. The members have authorized persons for every group which is the prime important thing in distributing the work and sharing the responsibilities among the group members. The main motto of our paper is based upon this distribution. The group controller (authorized person) will monitor the identity and legitimacy of the other group members.

The encryption and decryption occurs only through the keyed-hash message authentication code (HMAC) which is the heart of our paper. The Hash Message Authentication Code provides the simplest and the best protection for the network system with much efficacy and functionality. The data is transferred to those who are active at the time of data sharing and who are having the correct Hash Message Authentication Code matched authentication. Once the user has come out of the group the whole subgroup system will be reset and new Hash Message Authentication Code authentication code will become activated to protect the system from the logged out or thrown peer. This makes the system more protective than other proposed security systems where data is transferred and decrypted even after the user has come/thrown out of the group.

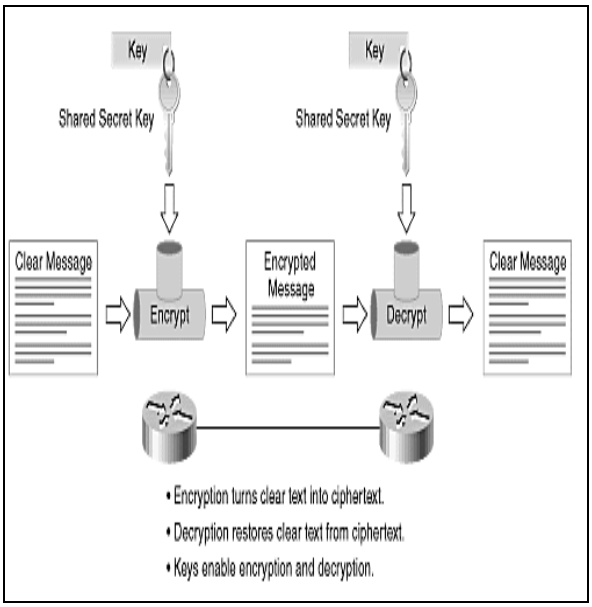

Figure 2

6. Conclusion

This paper presents Security of Peer-to-peer network system by a keyed-hash message authentication code (HMAC), Self certification mediated reputation system by which malicious peers are prevented from entering the network. This system provides a cryptogenic protocol that enhances the foolproofness of the Peers. The HMAC prevents unauthorized user entry at the first place only by disabling them at the time of log in only. This makes the system less contagious by preventing even minute levels of malicious code duplication and propagation. So, this makes the system more legitimate. Each and every peer joined in the network is trustable and no malicious code, virus, worms are propagated; in fact they are not able to enter into the system.

This paper also presents secure routing which can be joined with existing techniques to build applications that are strong even in the presence of malicious participants. The scalability of the system is maintained and it can be more improved by various combinations of the procedure. Due to all the above mentioned merits the HMAC algorithm is one of the most suitable Security systems. We hope that this encryption system will be useful in many more applications in the future.

7. References

i. Prashant Dewan and partha dasgupta, "P2P Reputation management Using Distributed Identities and Decentralized Recommendation Chains".
ii. M.Srikanth and K.B.Madhuri, " Secure and Effective P2P reputation system using Trust Management and Self certified Cryptographic Exchanges".
iii. I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M.F. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," Proc. ACM SIGCOMM, pp. 149-160, Aug. 2002.
iv. S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A Scalable Content-Addressable Network," SIGCOMM Computer Comm.. Rev., vol. 31, no. 4, pp. 161-172, 2001.
v. A. Rowstron and P. Druschel, "Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems," Proc. IFIP/ACM Int'l Conf. Distributed Systems Platforms (Middleware), pp. 329-350, Nov. 2001.
vi. G. Networks, "Groove Networks," http://www.groove.net/products/workspace/securitypdf.gtml, 2009.
vii. R.L. Rivest and B. Lampson, "SDSI: A Simple Distributed Security Infrastructure," Proc. Crypto '96, pp. 104-109, Aug. 1996.
viii. D. Ferraiolo and R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., May 1992.
ix. D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Advances in Cryptology (Crypto '82), 1983.
x. L. Zhou, F. Schneider, and R. Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.
xi. V V Murali Babu Polukonda et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4738 – 4742.
xii. P Satheesh et al, International Journal of Computer Science & Communication Networks,Vol 2(3), 338-342.
xiii. P. Resnick, R. Zeckhauser, and E. Friedman, "Reputation Systems," Comm. ACM, vol. 43, pp. 45-48, Dec. 2000.
xiv. L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.
xv. A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. Hawaii Int'l Conf. System Sciences, Jan. 2000.