International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

A Novel protocol between clients and storage devices

A. Anusha[1]Raghu Balaraj[2]

[1] *M. Tech Student,CSE, SVS Group of Institutions, Warangal, Telangana.*

[2] *Asso.Prof, CSE, SVS Group of Institutions, Warangal, Telangana.*

Abstract - ***Our purpose is to design resourceful as well as secure protocols of authenticated key exchange that meet up particular requirements of parallel Network File System. With the increasing usage of extremely network-attached storage systems, several works has focussed on scalable security. The proposed protocols can decrease workload of metadata server by means of about half compared to present Kerberos-based protocol, whereas achieving required security properties as well as keeping computational overhead at clients and storage devices at practically low level. Our work focuses on present Internet standards specifically parallel Network File System which makes usage of Kerberos to begin parallel session keys among clients and storage devices. We make a study of difficulty of key establishment for efficient many-to-many communications.***

Key Words**:** ***Authenticated key exchange, Storage devices, Parallel Network File System.***

1.INTRODUCTION

This is normally used in important cluster computing that spotlight on high performance as well as reliable access to huge datasets. Independent of cluster development as well as high performance computing, appearance of clouds and MapReduce programming model has resulted in file systems. More of the recent proposals, which implemented hybrid symmetric key as well as asymmetric key method, permit an ability to span several storage devices, while managing of practical efficiency-security ratio [1]. In parallel file system, file data is distributed all across numerous storage devices to permit concurrent access by several tasks of parallel application. This consecutively has increased wide-spread usage of distributed as well as parallel computation on huge datasets in numerous organizations. Our intention is to design efficient as well as secure protocols of authenticated key exchange that meet up particular requirements of parallel Network File System. We try to meet following pleasing properties, which moreover have not been suitably achieved or are not attainable by current Kerberos-based solution. Scalability–metadata server facilitates access requests from client to numerous storage devices have to bear as small workload as possible so that server will not become a performance blockage, but is able to support huge number of clients. Forward secrecy: protocol has to assurance security of previous session keys when long-standing secret key of client or else storage device is compromised. Escrow-free: metadata server has to not study any data concerning any session key used by client and storage device, offered there is no collusion between them [2]. Our protocols can decrease workload of metadata server by means of about half compared to present Kerberos-based protocol, whereas achieving required security properties as well as keeping computational overhead at clients and storage devices at practically low level. Our aim is to decrease workload of metadata server. The computational as

well as communication transparency for client as well as storage device has to stay on practically low. Our protocols, intended to attain each of above properties, reveal trade-offs among efficiency as well as security.

2. METHODOLOGY

We make a study of difficulty of key establishment for efficient many-to-many communications. The problem is inspired by increase of major distributed file systems that supports parallel access to numerous storage devices. In our work we suggest several authenticated key exchange protocols that are considered to deal with above issues. Our work focuses on present Internet standards specifically parallel Network File System which makes usage of Kerberos to begin parallel session keys among clients and storage devices. These protocols, reveal trade-offs among efficiency as well as security and can decrease workload of metadata server by means of about half compared to present Kerberos-based protocol, whereas achieving required security properties as well as keeping computational overhead at clients and storage devices at practically low level. In our work we examine problem of efficient many to-many communications in important network file systems that manages parallel access towards numerous storage devices. We make a consideration of a communication model in which there are huge numbers of clients that access numerous remote as well as distributed storage devices in parallel. Mainly, we spotlight on how to exchange key materials and set up parallel secure sessions among clients as well as storage devices within parallel Network File System. Parallel network file system allows direct, synchronized client access to many storage devices to get better performance as well as scalability. More particularly, Parallel network file system includes collection of three protocols such as Parallel network file system protocol that transfer file metadata, moreover known as layout, among metadata server as well as a client node; storage access procedure that specify how client accesses data from linked storage devices in relation to corresponding metadata; and control protocol that harmonize state among metadata server as well as storage devices. This system separates file system protocol processing into metadata processing as well as data processing. Metadata is information concerning file system object [3].

3. AN OVERVIEW OF PROPOSED SYSTEM

However, they are extended easily to the multi-user setting that is many-to-many communications among clients as well as storage devices. We suggest several authenticated key exchange protocols that are considered to deal with the existing issues and these reveal trade-offs among efficiency as well as security and can decrease workload of metadata server by means of about half compared to present Kerberos-based protocol, whereas achieving required security properties as well as keeping computational overhead at clients and storage devices at practically low level [4]. We try to design efficient as well as secure protocols of authenticated key exchange that meet up particular requirements of parallel Network File System. In our solution, we spotlight on efficiency as well as scalability regarding metadata server. Specifically, our ambition is to decrease workload of metadata server. The computational as well as communication transparency for client as well as storage device has to stay on practically low. We would like to meet each and every goal while making sure not less than approximately related security as that of Kerberos-based protocol. Our three variants of parallel Network File System authenticated key exchange procedures are summarized as follows: parallel Network File System authenticated key exchange- I is our first protocol which is regarded as a modified version of Kerberos that permits client to make its own session keys. Specifically key material used to obtain a session key is pre-computed by means of the client and forwarded to corresponding storage device as an authentication token. We explain our design goals and provide some perception of a variety of parallel Network File

System, authenticated key exchange protocols that are considered in ur work. In these protocols, we spotlight on parallel session key establishment among a client and various storage devices all the way through a metadata server. Like with Kerberos, symmetric key encryption protects the privacy of secret data used in the procedure. On the other hand, the procedure does not offer any forward secrecy [5]. Later the key escrow issue continue here as authentication tokens includes key materials for the sessions of computing keys are produced by server. Parallel Network File System authenticated key exchange procedures-II handles the key escrow problem while achieving forward secrecy at the same time. Particularly, client and storage device each choose a secret value and pre-computes Diffie-Hellman key component. A session key is subsequently produced from Diffie-Hellman components. On expiry of time period, the secret values as well as Diffie-Hellman key components are permanently removed, so that attacker will no longer contain access to key values necessary to work out past session keys. Parallel Network File System authenticated key exchange procedures-III aims to attain full forward secrecy, specifically introduction of an enduring key affects only present session key but not the entire of other earlier period session keys. We would moreover like to put off key escrow. In a nutshell, we improve Parallel Network File System authenticated key exchange procedures-II with a key update method on the basis of any resourceful one-way function, like a keyed hash function [6].

4. Experimental Results

These Experimental results are made with Microsoft dot net and sql server. This results are more accurate and effectively manner.

Fig 4: user search

As shown in figure 4 ,user can search and uploads required data .

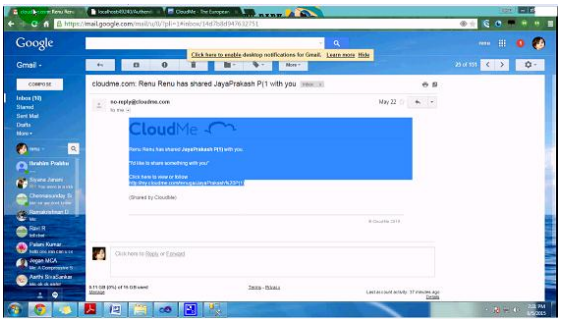

Fig 5:Key Exchange

As shown in figure 5, users shares key in network .this keys provides security date .based on that shared key user can download required data form network.

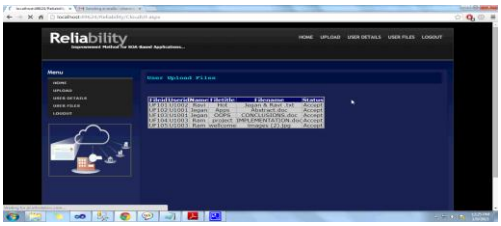

Fig 6: Information in cloud.

5. CONCLUSION

Parallel network file system permits direct, synchronized client access to many storage devices to get better performance as well as scalability. This system separates file system protocol processing into metadata processing as well as data processing. Our objective is to design efficient as well as secure protocols of authenticated key exchange that meet up particular requirements of parallel Network File System. Mainly, we spotlight on how to exchange key materials and set up parallel secure sessions among clients as well as storage devices within parallel Network File System. The protocols which are designed can decrease workload of metadata server by means of about half compared to present Kerberos-based protocol, whereas achieving required security properties as well as keeping computational overhead at clients and storage devices at practically low level.

REFERENCES

[1] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Advances in Cryptology

– Proceedings of EUROCRYPT, pages 139–155. Springer LNCS 1807, May 2000.

[2] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Advances in Cryptology – Proceedings of CRYPTO, pages 258–275. Springer LNCS 3621, Aug 2005.

[3] B. Callaghan, B. Pawlowski, and P. Staubach. NFS version 3 protocol specification. The Internet Engineering Task Force (IETF), RFC 1813, Jun 1995.

[4] M. Eisler. XDR: External data representation standard. The Internet Engineering Task Force (IETF), STD 67, RFC 4506, May 2006.

[5] M. Eisler. RPCSEC GSS version 2. The Internet Engineering Task Force (IETF), RFC 5403, Feb 2009.

[6] Hoon Wei Lim Guomin Yang "authentication exchange protocols in parallel network file system

[6] M. Eisler, A. Chiu, and L. Ling. RPCSEC GSS protocol specification. The Internet Engineering Task Force (IETF), RFC 2203, Sep 1997.