International Journal of Science Engineering and Advance Technology

Distributed File System Supporting Parallel Access To Multiple Storage Devices

[1*]G Jyothi Naga Devi, [2]A. SRIVALLI
[1](P.G.STUDENT) M.Tech in CSE, [2] Assistant Professor in CSE
Dept. computer science and engineering
Kakinada Institute of Engineering and Technology, for Women,, Korangi,AP, INDIA

ABSTRACT:
Our audit of the current Kerberos-based protocol demonstrates that it has various impediments: (i) a metadata server encouraging key trade between the customers and the storage devices has substantial workload that limits the scalability of the protocol; (ii) the protocol does not give forward mystery; (iii) the metadata server produces itself all the session keys that are utilized between the customers and storage devices, and this inalienably prompts key escrow. In this paper, we propose an assortment of confirmed key trade protocols that are intended to address the above issues. We demonstrate that our protocols are fit for lessening up to roughly 54% of the workload of the metadata server and simultaneously supporting forward mystery and escrow-freeness. This requires just a little division of expanded calculation overhead at the customer.

KEYWORDS: network file systems, forward secrecy, key escrow.

1 INTRODUCTION:
We explore the issue of secure many to-numerous correspondences in substantial scale organize record frameworks that bolster parallel access to different storage devices. That is, we consider a correspondence model where there are countless (possibly hundreds or thousands) getting to numerous remote and conveyed storage devices (which likewise may scale up to hundreds or thousands) in parallel. Especially, we concentrate on the most proficient method to trade key materials and set up parallel secure sessions between the customers and the storage devices in the parallel Network File System (pNFS) the present Internet standard—in a productive and versatile way. The advancement of pNFS is driven by Panasas, Netapp, Sun, EMC, IBM, and UMich/CITI, and in this way it shares numerous basic components and is good with many existing business/restrictive system document frameworks.

2LITERATURE SURVEY:
[1] We propose new verification protocols for question based storage systems in which a succession of settled size articles include a document and glimmer group are likely. We subjectively assessed the security and dangers of every protocol, and, utilizing hints of a logical application, thought about the overhead of every protocol. We found that, shockingly, a protocol utilizing open key cryptography caused minimal additional cost while giving more noteworthy security than a protocol utilizing just symmetric key cryptography.

[2] We created Maat, a security protocol intended to give solid, adaptable security to these frameworks. Maat presents three new methods. Augmented capacities restrict the quantity of abilities required by enabling a capacity to approve I/O for any number of customer document sets. Programmed Revocation utilizes short capacity lifetimes to enable ability close to go about as worldwide disavowal, while supporting non-denied capacity recharging. Secure Delegation enables customers to safely follow up in the interest of a gathering to open documents and circulate get to, encouraging secure joint calculations. Probes the Maat model in the Ceph petascale document framework demonstrate an overhead as meager as 6-7%.

3PROBLEM DEFINITION:
A portion of the soonest work in securing huge scale conveyed document frameworks, for instance, have officially utilized Kerberos for performing verification and authorizing access control. Kerberos, being founded on for the most part symmetric key strategies in its initial organization, was by and large accepted to be more reasonable for rather shut, very much associated circulated conditions.

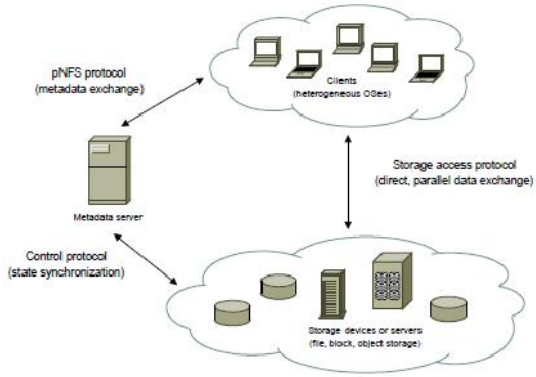
Then again, information frameworks and record frameworks, for example, OceanStore, LegionFS and FARSITE, make utilization of public key cryptographic procedures and public key infrastructure (PKI) to perform cross-area client validation.

4PROPOSED APPROACH:
Our essential objective in this work is to plan proficient and secure confirmed key trade protocols that meet particular prerequisites of pNFS. The fundamental consequences of this paper are three new provably secure validated key trade protocols. Our protocols, logically intended to accomplish each of

the above properties, exhibit the exchange offs amongst effectiveness and security.

We demonstrate that our protocols can diminish the workload of the metadata server by roughly half contrasted with the current Kerberos-based protocol, while accomplishing the coveted security properties and keeping the computational overhead at the customers and the capacity gadgets at a sensibly low level. We characterize a fitting security display and demonstrate that our protocols are secure in the model.

5SYSTEM ARCHITECTURE:



6PROPOSED METHODOLOGY:

6.1 Parallel sessions

Parallel secure sessions between the customers and the storage devices in the parallel Network File System (pNFS) The present Internet standard—in a productive and adaptable way.

This is like the circumstance that once the enemy bargains the long haul mystery key, it can take in all the subsequence sessions. In the event that a genuine customer and a legit stockpiling gadget finish coordinating sessions, they process a similar session key.

Second, two our protocols give forward mystery: one is somewhat forward secure as for numerous sessions inside a time period.

6.2 Authenticated key exchange:

Our essential objective in this work is to outline productive and secure validated key trade protocols that meet particular necessities of pNFS. The fundamental consequences of this paper are three new provably secure confirmed key trade protocols. We depict our outline objectives and give some instinct of an assortment of pNFS authenticated key exchange (pNFS-AKE) protocols that we consider in this work

6.3 Forward secrecy:

The protocol ought to ensure the security of past session keys when the long haul mystery key of a customer or a storage device is traded off.

Be that as it may, the protocol does not give any forward mystery. To address key escrow while accomplishing forward mystery at the same time, we join a Diffie-Hellman enter understanding procedure into Kerberos-like pNFS-AKE-I.

In any case, take note of that we accomplish just fractional forward mystery (regarding v), by exchanging productivity over security.**7ALGORITHM:**

Notations:

M metadata server
C client
Kx secret key
Kxy secret key sharing
SK session key
pNFS-AKE protocol:

INPUT:M,C,KX,KXY,SK

STEP1: When *C* submits an access request to *M*, the request contains all the identities of storage devices.

STEP2: For each *Si*, *M* issues a layout *C* then forwards the respective layouts, authentication tokens and encrypted messages of the form to all *n* storage devices.

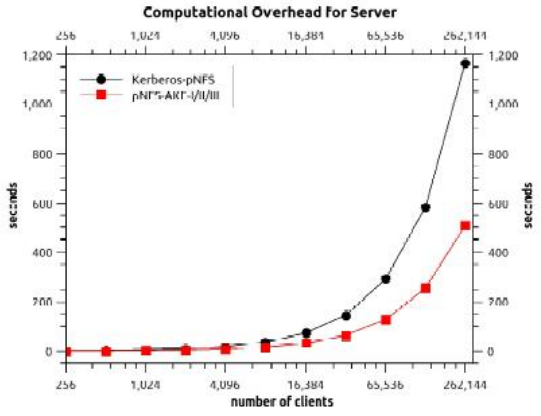
STEP3: Upon receiving an I/O request for a file object from *C* check if the layout is valid.

STEP4: decrypt the authentication token and recover key.

STEP5: compute keys for verification.

STEP6: decrypt the encrypted message, check if *IDC* matches the identity of *C* and if *t* is within the current validity period.

8RESULTS:



Comparison in terms of computation times for M and C at a specific time t.

9EXTENSION WORK:

To reduce the communication and computation overhead use ECC-128 bit algorithm for efficient communication.

10CONCLUSION:

We proposed three confirmed key trade protocols for parallel network file system (pNFS). Our protocols

offer three engaging focal points over the current Kerberos-based pNFS protocol. To begin with, the metadata server executing our protocols has much lower workload than that of the Kerberos-based approach. Second, two our protocols give forward mystery: one is somewhat forward secure (as for different sessions inside an era), while the other is completely forward secure (as for a session). Third, we have planned a protocol which gives forward mystery, as well as sans escrow.

11REFERENCES:

[1] M. Abd-El-Malek, W.V. Courtright II, C. Cranor, G.R. Ganger, J. Hendricks,A.J. Klosterman, M.P. Mesnier, M. Prasad, B. Salmon, R.R. Sambasivan,S. Sinnamohideen, J.D. Strunk, E. Thereska, M. Wachs, andJ.J. Wylie. Ursa Minor: Versatile cluster-based storage. In Proceedingsof the 4th USENIX Conference on File and Storage Technologies (FAST),pages 59–72. USENIX Association, Dec 2005.

[2] C. Adams. The simple public-key GSS-API mechanism (SPKM). TheInternet Engineering Task Force (IETF), RFC 2025, Oct 1996.

[3] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken,J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer.FARSITE: Federated, available, and reliable storage for an incompletelytrusted environment. In Proceedings of the 5th Symposium on OperatingSystem Design and Implementation (OSDI). USENIX Association, Dec2002.

[4] M.K. Aguilera, M. Ji, M. Lillibridge, J. MacCormick, E. Oertli,D.G. Andersen, M. Burrows, T. Mann, and C.A. Thekkath. Blocklevelsecurity for network-attached disks. In Proceedings of the 2nd International Conference on File and Storage Technologies (FAST).USENIX Association, Mar 2003.

[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski,G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A viewof cloud computing. Communications of the ACM, 53(4):50–58. ACMPress, Apr 2010.

[6] Amazon simple storage service (Amazon S3). http://aws.amazon.com/s3/.

[7] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchangesecure against dictionary attacks. In Advances in Cryptology– Proceedings of EUROCRYPT, pages 139–155. Springer LNCS 1807,May 2000.

[8] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcastencryption with short ciphertexts and private keys. In Advances inCryptology – Proceedings of CRYPTO, pages 258–275. Springer LNCS3621, Aug 2005.

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

[10] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols andtheir use for building secure channels. In Advances in Cryptology –Proceedings of EUROCRYPT, pages 453–474. Springer LNCS 2045,May 2001.

[11] CloudStore. http://gcloud.civilservice.gov.uk/cloudstore/.

[12] Crypto++ 5.6.0 Benchmarks. http://www.cryptopp.com/benchmarks.html.

[13] J. Dean and S. Ghemawat. MapReduce: Simplified data processingon large clusters. In Proceedings of the 6th Symposium on OperatingSystem Design and Implementation (OSDI), pages 137–150. USENIXAssociation, Dec 2004.

[14] M. Eisler. LIPKEY - A Low Infrastructure Public Key mechanism usingSPKM. The Internet Engineering Task Force (IETF), RFC 2847, Jun2000.

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