JCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-10 E-ISSN: 2347-2693

Visual Cryptography Based Authentication For Parallel Network File Systems

R. Keerthivasan[1*], K.S. Srivastavan Iyer[2], Vyshnav A.K[3], M. Vishal[4]

[1*] Department of Computer Science And Engineering, SRM University, Chennai, India
[2] Department of Computer Science And Engineering, SRM University, Chennai, India
[3] Department of Computer Science And Engineering, SRM University, Chennai, India
[4] Department of Computer Science And Engineering, SRM University, Chennai, India

**Corresponding Author: keerthivasan10e@gmail.com, Ph.: +91 74010 74338*

Available online at: www.ijcseonline.org

Received: 21/Sep/2017, Revised: 30/Sep/2017, Accepted: 12/Oct/2017, Published: 30/Oct/2017

Abstract**—** The problem of securing multiple communications in large-scale network files systems supporting parallel access to multiple storage devices. That is, we consider a model of communication where there are a high number of clients accessing multiple remote and distributed storage devices in parallel. Particularly, focusing on exchange key materials and establishing secure parallel sessions between the clients and the storage devices in the parallel Network File System (pNFS) the current Internet standard is in an scalable and efficient manner. The development of pNFS is driven by Netapp, Panasas, Sun, EMC, IBM, and UMich/CITI, and thus it shares many common features and is compatible with many existing commercial/proprietary network file systems. Networking is considered as the practice of linking multiple computing devices together for sharing of resources. Without the implementation of network, businesses, government agencies, and schools would be unable to operate as efficiently as they do. An organization is able to connect dozens of computers to a single printer is a seemingly simple, yet extremely useful capability. Perhaps even more valuable is the ability to access the same data files from various devices throughout a building. This is incredibly useful for companies that may have files that require access by various employees daily. By the use of network, a same file is made available to several employees on separate computers simultaneously, which improves the efficiency of the organization. Our objective is to implement visual cryptography for strong authentication for parallel network file systems.

Keywords**—** Authentication, Networks, Visual Cryptography, Cryptography, Network File System

I. Existing System

The Kerberos version 5 and the Low Infrastructure Public Key (LIPKEY) GSS-API mechanisms uses Public key infrastructure (PKI) to perform cross-domain user authentication independently and hybrid symmetric key and asymmetric key method[1], allow a capability to span any number of storage devices, while maintaining a reasonable efficiency-security ratio .

A. Disadvantages of Existing System

1. Restricts a capability to authorizing I/O on only a single device, rather than larger groups of blocks or objects which may reside on multiple storage devices.
2. Do not come with rigorous security analysis.
3. Compromise of the metadata server or any storage device allows the adversary to impersonate the server to any other entities in the file system.
4. Past session keys can be exposed if a storage device's long-term key Shared with the metadata server is compromised[2]
5. Key escrow.

II. Proposed System

1. PNFS-AKE-I: Diffie-Hellman key agreement techniques[1,2] to both provide forward secrecy and prevent key escrow.
2. PNFS-AKE-II: A protocol that achieves full forward secrecy and escrow-freeness.
3. Visual cryptography based authentication system[5].

A. Scope and Objective

The objective of this project is to implement visual cryptography for strong authentication .DiffieHelman key exchange technique and hash function to provide forward secrecy and escrow freeness for parallel network file system[3]. A variety of authenticated key exchange protocols and visual cryptography[2] are designed to address the issues such as weak authentication, higher workload on metadata sever, key escrow. Metadata server executing our protocols has much lower workload than that of the Kerberos-based approach.

B.Advantages of Proposed System

1. Provide forward secrecy.
2. Escrow-free.
3. Lower workload than that of the Kerberos-based approach.
4. The metadata server executing our protocols has much lower workload than that of the Kerberos-based approach.
5. One is partially forward secure (with respect to multiple sessions within a time period), while the other is fully forward secure (with respect to a session).
6. Not only provides forward secrecy, but is also escrow-free.

III. SYSTEM DESIGN

The issue of the secure many to many communications in the large scale network file systems which support parallel fetch to multiple storing devices. We consider the communication model where there are a large number of the clients accessing multiple remote and distributed storage devices[4] in parallel. Particularly, we try to focus on how to exchange the key materials and establishment of the parallel secure sessions between clients and storage devices in the parallel Network File System (pNFS), the current Internet standards is efficient and in scalable manner. The development of pNFS is driven by Sun, EMC, IBM, and UMich/CITI, and thus it shares many similar features and is compatible with many existing commercial network file systems. Our main goal in this work is to design visual cryptography[5] and secure authenticated key exchange protocols[3] and that meet specific needs of pNFS. Particularly, we attempt to meet the following desirable properties, which have not been satisfactorily achieved or are not achievable by current Kerberos-based solution.

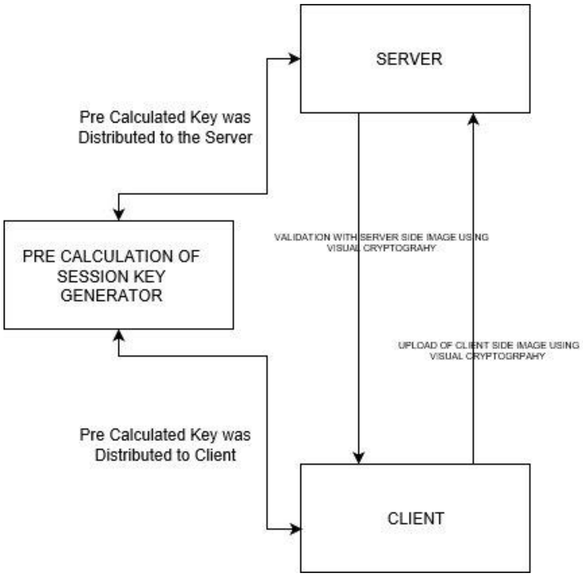
SERVER
Pre Calculated Key was Distributed to the Server
PRE CALCULATION OF SESSION KEY GENERATOR
VALIDATION WITH SERVER SIDE IMAGE USING VISUAL CRYPTOGRAHY
UPLOAD OF CLIENT SIDE IMAGE USING VISUAL CRYPTOGRPAHY
Pre Calculated Key was Distributed to Client
CLIENT

Figure 1. System Architecture

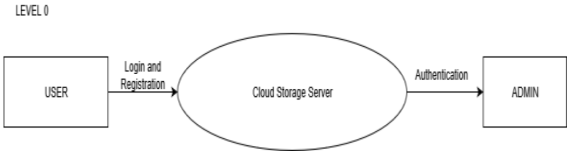

Figure 2. Level 0 Data Flow Diagram

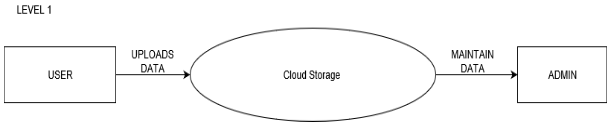

Figure 3. Level 1 Data Flow Diagram

IV. SYSTEM IMPLEMENTATION

Our primary goal is to design an efficient and secure authenticated key exchange protocols that will meet specific requirements of pNFS. The main results of this paper is to implement visual cryptography based authentication along with two new provably secure authenticated key exchange protocols. We describe our design goals and provide some intuition for a variety of pNFS authenticated key exchange (pNFS-AKE) protocols[1] that we consider in this work.

The protocol should guarantee the security of past session keys when the long-term secret key of a client or a storage device is compromised. And also the protocol does not provide any forward secrecy. To address key escrow while achieving forward secrecy simultaneously, we incorporate a Diffie- Hellman key agreement technique into Kerberos-like pNFS-AKE-I[3]. However, note that we achieve only partial forward secrecy (with respect to v), by trading efficiency over security. So, we use one more protocol hash key function to provide full forward secrecy and escrow freeness.

Our main goal is to implement visual cryptography based authentication to provide strong authentication[5,6] which is lacking in the current kerberos based system. It is an image based authentication technique.

V. CONCLUSION

Proposed visual cryptography based authentication along with two authenticated key exchange protocols for parallel network file system (pNFS). Protocols offer three appealing advantages over the existing Kerberos-based pNFS protocol. First, these protocols provide forward secrecy: one is partially forward securing (with respect to multiple sessions within a time period), while the other is fully forward secure (with respect to a session). Second, we have designed a protocol which not only provides forward secrecy, but is also escrow-free.

A. Future Enhancement

Authentication using Password authenticated key exchange using distributed server (PAKEUDE) is done where a cryptographic key - exchange of messages. According to Security analysis our protocol is secure against active and passive attacks in case any of the two servers is compromised.

VI. TESTING

Table 1. Test Cases

TEST CASE	DESCRIPTION	BASIC CONDITION	TEST DATA	EXPECTED RESULTS	TEST RESULTS
Account registration	A user will register an account by giving name mail id and other details.	Enter a proper detail for example: A phone number should not have alphabets.	wity test@gmail.com	Registration will be successful and redirected to next page.	PASS
Login	A registered user will log into the account.	Registered user name and password should be valid.	test@12345	User name and password matches.	PASS
Upload image	The user will upload an image.	The image should be in .img .	Flower.img	Image is uploaded.	PASS
Upload File	The file should be uploaded .	The File should be in .txt format.	Details.txt	File will be uploaded.	PASS

REFERENCES

[1] Hoon Wei Lim and Guomin Yang, " *Authenticated Key Exchange Protocols for Parallel Network File Systems*", IEEE transactions on parallel and distributed systems, vol 27, No. 1, January 2016.

[2] Stuti Nathaniel, Syed Imran Ali, Sujeet Singh, "*A Review of Authenticated Key Exchange Protocol Using Random Key Selection with Minimum Space Complexity*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.6, pp.191-196, 2016.

[3] C. Adams, "The simple public-key GSS-API mechanism (SPKM)," Internet Eng. Task Force (IETF), RFC 2025, Oct. 2014.

[4] Vinod. L. B and Nithyanada. C. R, "*Visual Cryptographic Authentication for Online Payment System*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.8, pp.109-114, 2015.

[5] M. K. Aguilera, M. Ji, M. Lillibridge, J. MacCormick, E. Oertli,D. G. Andersen, M. Burrows, T. Mann, and C. A. Thekkath,"*Block-level security for network-attached disks,*" in 2nd International Conference in File Storage Technology, pp. 159–174, Mar. 2003.

[6] D. Boneh, C. Gentry, and B. Waters, "*Collusion resistant broadcast encryption with short ciphertexts and private keys*," in 25th Annual International Conference of Advanced Cryptology, pp. 258–275, Aug. 2005.

Authors Profile

Mr R. Keerthivasan is currently pursuing his Bachelor of Technology in Computer Science and Engineering at SRM University, Chennai, India. He is a Experienced Technical Student with a demonstrated history of working in the computer and network security industry. Skilled in Photography, Operations, Management and Analytics. He is a trained security analyst and a professional graphics designer . His research works emphasis on Information Security, Access Control and Cyber Forensics.

Mr K.S.Srivastavan Iyer is currently pursuing his Bachelor of Technology in Computer Science and Engineering at SRM University, Chennai, India. His main research work emphasis on Visual Cryptography and Software Manufacturing .He has exceptional Skills in Management, Adminstration Social media analytics and marketing. Presently working as an administrator and data analyst in a esteemed society.

Mr Vyshnav A.K. is currently pursuing his Bachelor of Technology in Computer Science and Engineering at SRM University, Chennai, India. He has professional experience in Application Testing and security. Trained and certified for Cloud Data Management. His research interest includes Security Management. His skills include business management and marketing, who is currently working as web administrator and finance manager in a esteemed society.

Mr M. Vishal is currently pursuing his Bachelor of Technology in Computer Science and Engineering at SRM University, Chennai, India. He has experience in the field of web development and administration, who is passionate towards the Cloud Computing domain. His skills include marketing and management, who is currently working in technical team of an esteemed Society.