ENHANCED STORAGE MECHANISM FOR SECURED PARALLEL NETWORK FILE SYSTEM

LATESH KUMAR K J

A Thesis Submitted to Asia e University in
Fulfilment of the Requirements for the
Degree of Doctor of Philosophy

June 2018

ABSTRACT

The main aim of this dissertation is to study how parallel network file system and storage appliances are integrated to storage computing. The prime focus is on file locking techniques, state maintenance of file locks and layouts, data compression and data protection across network attached storage and parallel network file system. The problem statement relies how the enhancement of storage mechanism for secured parallel network file system will benefit the storage computing environment. In order to comply with these objectives, a study is conducted and data is collated by visiting storage customer data sites, references of storage summit articles, journal references and by participating in storage conferences and workshops across globe.

Based on the analysis of data, the legacy usage of network lock manager and network status monitor in file locking mechanism, unhandled locks and layouts, legacy security model used with pNFS client and servers, a single pattern of file-based data compression and non-dynamic external data protection techniques on storage computing system has resulted high impact on network attached storage computing.

The challenges faced translates how the new techniques, lease and delegation algorithm for file locking, snapshot enabled locks and layouts for data state, integration of highly secured Kerberos security on storage for pNFS locks and layouts, data block size algorithm enabled deduplication on file, block and object patterns and the redundant array of independent disk data protection can create impact on storage computing system. The proposed techniques resulted synchronous LEASE file locking, capturing of state of locks and layouts, Kerberos secured the pNFS locks and layouts on storage, new algorithm enabled the scalable data compression using data block size compression algorithm and better dynamic data protection using RAID.

APPROVAL PAGE

I certify that I have supervised / read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in quality and scope as a thesis for the fulfilment of the requirements for the degree of Doctor of Philosophy.

Prof Dr R Lawrance
Director, Department Master of Computer Application
Ayya Nadar Janaki Ammal College
Supervisor

Examination Committee:

Dr Sundresan A/L Perumal
Senior Lecturer, Faculty of Science and Technology
Universiti Sains Islam Malaysia
Examiner

Prof Dr Saadiah Yahya
Faculty Computer and Information Technology
University of Jeddah
Examiner

Dr Massudi Mahmuddin
Senior Lecturer, School of Computing
Universiti Utara Malaysia
Examiner

Prof Dr Siow Heng Loke
Dean, School of Graduate Studies
Asia e University
Chairman, Examination Committee

This thesis was submitted to Asia e University and is accepted as fulfilment of the requirements for the degree of Doctor of Philosophy.

Prof Dr Titik Khawa Abdul Rahman
Dean, School of Science & Technology
Asia e University

Prof Dr Siow Heng Loke
Dean, School of Graduate Studies
Asia e University

DECLARATION

I hereby declare that the thesis submitted in fulfilment of the Ph.D. degree is my own work and that all contributions from any other persons or sources are properly and duly cited. I further declare that the material has not been submitted either in whole or in part, for a degree at this or any other university. In making this declaration, I understand and acknowledge any breaches in this declaration constitute academic misconduct, which may result in my expulsion of from the programme and/or exclusion from the award of the degree.

Name: Latesh Kumar K J

Signature of the Candidate: **Date:**

ACKNOWLEDGEMENT

First, I would like to convey Pranamas to Supreme Power, ALMIGHTY the GOD. My warmest regards and thanks to the Asia e University, Malaysia for giving me an opportunity to carry out this research work.

I express my deepest gratitude and indebtedness to my supervisor, Dr. R. Lawrance, Director, Department of Computer Applications, Ayya Nadar Janaki Ammal College (Autonomous), Sivakasi, INDIA for his excellent level of guidance, caring, patience and his donation of extreme strength of domain knowledge.

I would like to express my sincere gratitude to Dr. M.N Channabasappa, Director, SIDDAGANGA INSTITUTE OF TECHONOLGY, Tumkur, INDIA for his outstanding moral support and valuable suggestions.

I would like to express my thanks to Prof. Dr. Saadiah Yahya and Prof. Dr. Sundaresan Perumal for their outstanding support and valuable suggestions for writing thesis.

Finally, I thank my parents and family, who were always supporting and encouraging me with their best wishes. Particularly, I would like to thank my wife Leena who cheered me up all the time and stood by me through the good times and bad and most importantly to my lovely daughter Diya who stood next me saying "papa".

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ACL	ACCESS CONTROL LIST
CIFS	COMMON IN FILE SYSTEM
FC	FIBRE CHANNEL
GNU	GROUP NOT UNIX
IP	INTERNET PROTOCOL
KDC	KERBEROS DOMAIN COTNROLLER
MIT	MASSACHUSSETS INSTITUTE OF TECHNOLOGY
MDS	META DATA SERVER
NAS	NETWORK ATTACHED STORAGE
NFS	NETWORK FILE SYSTEM
PNFS	PARALLEL NETWORK FILE SYSTEM
NLM	NETWORK LOCK MANAGER
NSM	NETWORK STATUS MONITOR
POSIX	PORTABLE OPERATING SYSTEM INTERFACE
PID	PROCESS ID
RPC	REMOTE PROCEDURE CALL
SEAM	SIDEWINDER EXPANDED ACQUISION MODE
SCSI	SMALL COMPUTER SYSTEM INTERFACE
TCP	TRANSMISSION CONTROL PROTOCOL
UNIX	UNIXPLEXED COMPUTING SYSTEM

CHAPTER 1.0 INTRODUCTION

1.1 Introduction

Storage management and data security are key sources that rooted the study on enhanced mechanism of storage and file sharing protocol parallel network file system. The storage data processing involves intelligent techniques like snap-shot, snap-volume, snap-mirror and many other methods that ensures and enables a better storage processing mechanism. Gone are the days then storage appliances are used to store data, but now storage appliances are not just racks of disks to hold data but they are specialized in many features like automated sanitizing data, integration of data, data transformation, pattern evaluation and data presentation. Network file system is a native storage communication protocol created for transferring data via remote procedure calls and inter-message processor of transmission control protocol and user datagram protocol (Balasubramanian & Pendse, 2004) across any kind of computing system.

At first International Business Machines (IBM) contributed a file system named distributed file system (IBM Corporation, 2000) that removed the pain of storing data inside the entire computer's internal disk drive connected across local area network. Enabling the single point of disk volume/aggregate in which the data shall be stored, shared, fetched and accessed with various access modes as supported by the native advanced interactive executive operating system of UNIX style. Parallel Network File System (pNFS) is the next generation (Bernardo & Hoang, 2010) protocol of NFS (Hamilton & Olsen, 2013) communication system; pNFS incepted to eradicate long time bugs, issues and performance concerns of the legacy NFS (Katcher, 1997) and its versions.

The implementation of pNFS establishes a metadata-processing server; distinct from data movers are incorporated into the physical storage modules. This allows direct transfer of files to all the accessing pNFS clients, a direct access to application server enabled for multiple clients to access data simultaneously by supporting multiple concurrent or parallel file system operations. With parallel data access, it can maintain and scale performance as capacity expands since adding data movers or data servers also increases data access points. The distributed architecture that allows the file system and storage (Haeberlen & Druschel, 2005) processing functions scaled independently from the data handling function, giving the system additional flexibility, the key fact that pNFS has been developed, as an open standard will enable the client to be packaged with major operating systems.

1.2 Background of the study

With diminishing data security, duplicated data storage, time consuming data communication and un-optimized data recovery across the storage appliances from the native data storage protocol are the key causes for the research study. Critical customer data stored on primary data site requires a prime attention of data safety, quick access, and optimized disk layout storage must be available on high demand for vivid applications and services. The native storage controller follows dedicated protocol approach in processing the storage data from clients and fails to support the changing technology, which requires patching heavily to synchronize the storage appliances for seamless versions of clients, applications and services.

This research study reports the findings of a systematic study to establish factors that have led the basics of parallel network file system, intelligences of storage and how to enhance security layers on pNFS protocol for communicating across storage appliances. The core challenges of data sanitization, file locks, data protection methods and absence of data-deduplication across the storage protocols are the open hurdles in managing the critical data.

I contend that the lack of continuous technology support on sensitive technology information transactions is resulting on customer's data and prosperity of the trusted business. Since, these are not open to external world on routine basis the awareness and importance is in less focus to outside world though things discussed at storage summits and community levels. However, the effect of these will be heavily on the infrastructure since the data sanitization (Net 2000, 2013) data organizing, quick data delivery, instant data access, data protection and eliminating the redundant data blocks on the storage grids will become the payload on the vendor and operations management task group.

On top of this supporting the side band services, applications and third-party clients for the business is another overhead risk for the data computing system environment since heterogeneous hardware, software, customized protocol, services ports and compromised service levels needs to be supported in the business. To engage all these circumstances to go further in computing grid and business across the data centres are challenging task because of timely changing data and service levels.

An uncontrolled growth of (Islam & Suryadevara, 2016) Internet of Things (IoT), web applications, web services and gadget app services that are producing the enormous amount of data on the global data sites. These are the set examples of hybrid incoming data that are very difficult to understand and analyze on service points of file, block and objects. Hence, storage protocol input and output baud rate are high and the traffic on communicating pipeline is heavy. Analyzing and interpreting to these vivid services for the duplicate data, un-sanitized data is the key challenge as there is no control on client/user file and level of access. In addition, the multiple services accepted on file and layouts by parallel network file system, which exposes a higher risk and challenge.

The research has incorporated interviews with lead architects of data sites to understand core limitations, issues, routine challenges of user, protocol communication, data housing and at the end backup system for a better approach before building novelty methods for technology. The study also involved to root level of understanding the legacy protocols, migrations, data movement methods, protocol communication, security systems, network management and finally the hierarchy of data operations.

A detailed study conducted on various small, medium and large-scale business applications that are connected to vivid modes of storage in data sites. The application that serves online, offline, cache service for (Chen & Tu, 2016) Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) (Feng, 2015) Content Management System (CMS) (Jerkovic & Dadic, 2016), Marketing Automation Platform (MAP), Product Information Management (PIM) (Tan & Bonollo, 2002) are part of this study for data, communication and security.

1.3 Statement of the problem

There is ample research available on the benefits of network file system and parallel network file system by internet engineering task group, engineering protocol research community and big contenders of Storage Company like Network Appliance (NA). This study begins to address issues that are surrounding the inefficiency involved in secured storage communication, storage data protection and optimized data storage (Sparenberg & Foessel, 2013) by data deduplication on data sites, web business and disaster sites. This includes how different storage communities and protocol groups can build and close the gap between the vivid storage shortfalls over communicating protocols.

The community released the first draft version of pNFS called NFS version 4.1 for storage and peer supporting clients of UNIX and Windows across globe in 2010. This was identified as minor release on the protocol since basic enumerations on network file system was exposed linking the directory delegation, session management across clients and pNFS protocol. Adding to the contribution of pNFS community group, major information storage manufacturer and technology contenders of storage domain like NetApp, IBM, and DELL-EMC shared their support in extending the features, technology, services across their in-house storage operating system that enables the pNFS communication to various clients.

The storage industry focused on expanding the storage intelligence by adding various features and enabling the support to cross plat form business needs, however key areas of patching is missed during big releases are as their target was to release higher features network attached storage and parallel network file system protocol to acquire scalable business products. The major product upgradation/ release from NFS to pNFS resulted few concerns inside the protocol and storage appliance.

To begin with first, the upgraded file locking architecture resulted the unsynchronized file locking mechanism across NFS and pNFS clients as NFS supports legacy network lock manager and network status monitor, however pNFS support these sideband services to a limited edition. This issue was logged in storage bug-files but no patching is established to address this issue as pNFS aims to eliminate NSM and NLM.

The network attached storage customers further expressed their concerns of losing the state and history of pNFS clients with storage during failover and panics. To address this issue pNFS community released a patch that captured data of clients based on volume of transaction but this was not useful as NAS business file sharing activity involves tiny to bulk size of file sharing via pNFS protocol and this resulted pain in the storage industry.

The storage vendors and customers always concerned about data safety, which was major threat to cloud based services as security mechanism integrated are only storage appliances but not on client's application servers and third-party environments.

The new storage models and services offered various features that imbibed large and heterogeneous data forms on cloud and non-cloud sites but the key worry of storage vendors is that only few types of file pattern data is compressed by which big chunk of data is still residing on disk aggregates that resulted more racking of disks at customer data sites. Soon or later storage appliances managed this by replacing the old legacy disks with flash disks that could store huge data inside.

These flash disk data sites are protected with disaster site technology but small scale network attached storage business unable to invest on such large technology hence the data protection with legacy disks are concern for storage customer and vendors.

1.4 Objectives of the study

The primary objective of this research is to enhance the mechanism on storage and parallel network file systems by identifying their current limitations across storage processing and file sharing protocols in connection to file locking techniques, file-data sharing modes, data protection across the client-server communication modes and data compression methods that aims in saving storage space by storing optimized data. The below points list the complete objectives of study,

- Unsynchronized pNFS file locking techniques
- No state based pNFS file lock management (Failover and Recovery)
- Unsecured and Lack of integrated data protection for pNFS locks and layouts
- Lack of optimized data storage technique (Limited to File based data compression)
- Lack of storage integrated data security (Lack of Application and Storage RAID)

The pNFS protocol study captures the data on file locking, mount operations, sharing issues and un-stateful data handling across clients, servers and storage appliances. The study on security involves the current data security practices and challenges across storage computing system. The study on data compression aims to analyze the current limitations of supporting only file type data operations, and at last the data protection study investigates why data protection techniques are being non-integral part of storage appliances and their key challenges against growing storage computing techniques.

The investigation and novelty implementations on above listed are depending on below listed storage and file sharing protocol segments, the Table [1.1] lists the study area and basic description of the challenges identified with file locking, unhanding of data history, pNFS data layouts, space saving technique and data protection intelligence.

The first three objectives are connected to pNFS protocol and hence they are mapped to protocol section in the below listing. The first objective of the study is on pNFS file locking and layout that involved issues on mounting, file locking and asynchronous lock management by protocol. The lack of flexible file locking mechanism architecture found to be key concern and this can be handled by enhancing the lock and layout architecture to flock-based activity that supports end to end communicating sockets.

Study Area	**Domain**	**Description**
pNFS PROTOCOL	Lock NFS & pNFS	Enabling Synchronous Lock mechanism using flock ()
		Building smooth communication across NFS and pNFS
	Mount & Share Issues	Creating Snapshot to avoid mount and share issues
	Un-stateful data handling	Creating Hand shaking techniques for File Locks and Layout sockets
SECURITY	Storage, Protocol & Security	Securing pNFS Locks, layouts data and communication with clients on storage appliance using Kerberos
Data Compression	Storage data optimization	Saving Storage Space using Data Deduplication technique
Data Protection	Storage aggregate data protection during panics	Protecting Storage Data using RAID techniques

Table 1.1 Objectives of Study

Addition to this a snapshot technology called time-based data copying system is induced to store the complete data and transaction history of client and servers at all time to reserve the state of transaction by supporting the failovers. The second and third objective of the study is on data and communication security of pNFS that proves better than NFS.

This is done by using the basic RPCSEC_GSS security which found to be insufficient across developing distributed and parallel computing techniques, hence Kerberos based security will be integrated to enhance the security.

A new dimension of security intelligence is devised for pNFS that ensures level of file sharing using lease-based file locking and secured snapshot-based layout transferring across server and client.

The fourth objective is on reducing the storage bars and controllers while meeting the demand for storage by storing more and more in less intelligent space occupying schemes. This study aimed in space savings technique for storage data which found to be supporting only file pattern data and identified to be non-integral part of the storage appliances, hence an integration of space saving techniques on file, object and block-based data are the key concern of this study.

The last objective of the study is to analyze the data protection schemes involved in protecting the data during panics and fault injections across storage computing system, which resulted un-stateful transaction and no recovery during failovers and hence a new protection mechanism that enabled end to end data protection across pNFS, clients and servers using redundant array of independent disk services.

1.5 Research questions

Why study on storage is the primitive question? Because major sections of information technology world rely on data and analytics. Technology depends on three key stages like input, processing and output. Storages are responsible for the last stage of data operations and opted to store and share data across users that raise challenges and concerns. Why it requires a seamless communication between network attached storage appliances and file sharing communication protocols across various platforms is listed in the below Table [1.2], these questionnaires demand core and detailed information analysis on storage computing system.

Q. No	Description of Question	Description of Requirement
1	Why asynchronous pNFS file locking techniques on storage appliances?	Why not Synchronous file locking techniques
The file sharing protocol is designed with basic NLM and NSM side band protocols, these kernel modules are limited on storage appliances. The core modules of file locking algorithm do not support open end transactions and information sharing across communicating sockets.		
2	Why Data state and history of pNFS file locks and layout are not managed (Failover and Recovery)?	State and History must be Integral part of File Lock and Layouts
The file locks and layouts of pNFS protocol are designed to store current active information of client as timeout is restricted to 15 seconds and the NSM architecture design is not capable of storing parallel computing client's data. As pNFS allows parallel computing it must capture data timely for all clients.		
3	Unsecured and Lack of Integrated data security for pNFS locks and layouts	Secured Architecture
Most interesting question part of the study is that no internal architecture for data protection and revision system for data. Meaning anytime when a file lock or layout transaction fails then data is lost with history, which is hit concern. Process and communications must be safe, they cannot be plain on the communication channel, and hence a highest-level security and a secured smart file locking procedure is must to increase the performance and user file locking processes effectively from architecture.		
4	Lack of optimized data storage technique (Limited to Fie based data compression)	Scalable Storage Architecture supports (File, Object and Block)
Logical storage management is a key technique to save space and enable optimized data browsing technique for storage appliances.		
5	Lack of storage integrated data protection	Application and Storage data protection during panics
Data protection intelligence must be part of storage computing and they cannot be external as computing environment involves various objects. The server, client and external interfaces must not lose their data.		

Table 1.2 Research questions