Enhancing Security in Database Grid Infrastructure for Storage Clusters

N. W. CHANAKA LASANTHA[1], RUVAN ABEYSEKARA[1], M. W. P. MADURANGA[2]
[1]Faculty of Graduate Studies,
IIC University of Technology,
Phnom Penh 121206,
CAMBODIA

[2]Department of Computer Engineering,
General Sir John Kotelawala Defence University,
SRI LANKA

Abstract: - This research project primarily focused on improving security by addressing vulnerabilities and creating a cost-scalable storage cluster solution, for applications. The Oracle Grid Infrastructure for Storage Clusters (OGISC) represents cutting-edge advancements in this field. The research extensively explores the philosophy of OGISC. Explains its core methodology. Recognizing the weaknesses of existing security mechanisms, we propose a solution to enhance security measures. A key aspect of our investigation involves integrating Glusterfs, a system known for its ability to scale linearly. We delve into the architecture of the solution demystifying the storage scale-out processes to its operation. Our study goes beyond integration by developing an approach and metadata model specifically tailored for Glusterfs ensuring optimal performance and robustness. One noteworthy aspect of our research is the application of Glusterfs compression with OpenVPN. This exploration highlights the benefits derived from this integration emphasizing how OpenVPN enhances Glusterfs capabilities. Rigorous analysis stages serve as the foundation for our findings resulting in a forward-thinking solution. Finally, we conclude this research with an examination of avenues for future exploration in this dynamic field.

Key-Words: - Security Enhancement, Cost-Scalable Storage Cluster, Oracle Grid Infrastructure for Storage Clusters (OGISC), Glusterfs Integration, Storage Scale-Out Processes, OpenVPN and Glusterfs Compression.

Received: July 12, 2022. Revised: August 27, 2023. Accepted: October 8, 2023. Published: November 30, 2023.

1 Introduction

This project has been extended and generated important benefits for the various stakeholders by enhancing the security availability of the cluster system in secured Oracle grid infrastructure storage cluster (OGISC) delivery as well as evaluation. OGISC was heavily focused on security weaknesses and cryptographic backdoors over the distributed storage structure with high availability at a lower cost than expensive alternatives. The OGISC strongly addressed the specific major problems by facilitating adaptive software and hardware resources, that make it very efficient and, also provide usage capacity on demand over the securing mechanism, [1]. In addition, it is very low-cost effective compared to the traditional system, which effectively balances the load, sessions, and security weakness over the OGISC concept. The proposed architectural solution operates over different geographically clustered databases including the secure sheared concept, [2].

2 The Philosophy of OGISC

2.1 Hypothesis

1. The SSL/TLS ETE encryption at which storage cluster can perform secured tunnel security and accessibility among server nodes against compromising situations over the shearing storage area by using encryption algorithms such as RSA, AES were incorporated while the HMAC function

makes use of a hashing algorithm were built in OpenVPN.

2. The Initial key exchange (IKE) mechanism of the SSL/TLS process can be tightly coupled with the HMAC handshake method over the DH and STC key exchange algorithms. Also, a static key among both peer nodes before the certain tunnel was started of OpenVPN architecture to mitigate risk by adhering to The X.509 global standard according to the formation of the public key certificate with periodic key origin renegotiation process.

3. The digital signature and certificate make the concept of fingerprinting security mechanism which can digitally sign by genuine message sender by the trusted originator of the content. Also, the one-way hash function can check the integrity of the message. The multifactor authentications of OpenVPN have strongly mitigated the account hijack situation. It can have a powerful firewall with a manageable routing framework.

4. The intelligent self-driven metadata algorithm of the GlusterFS has mainly focused on the brick server to relocate files which can provide flexibility to add and delete VMs by continuing operations instead of traditional systems. It provides large scale-out architecture and minimum overhead on the cluster including the ability of data performance.

5. OpenVPN can engage highly compressed data packets to improve performance without adding extra overhead to OpenVPN protocol that is inherited from cryptographic functionality using AES-256-GCM. It contains a pushed routing feature among TCP or UDP traffic with fail-safe functionality.

6. The mechanism of the SPARC-M8 processor has hardware-assisted encryption data which can tightly couple with Linux kernel while Oracle ZFS storage appliances encrypt only at the file system level. Also, it does not provide compressions, replication, reduplication direct NFS support while direct NFS client optimizes NFS operations.

2.2 Methodology

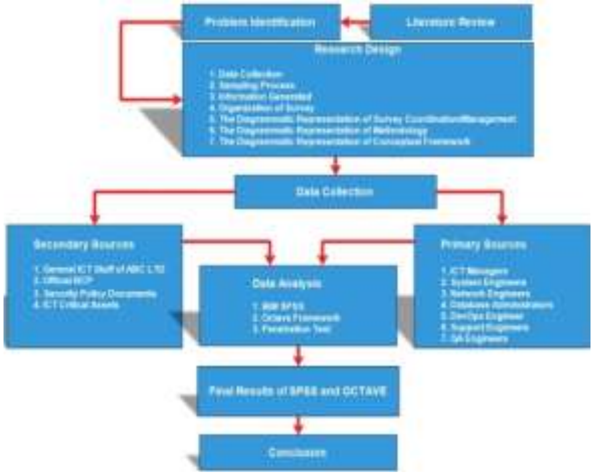


Fig. 1: Overview of Methodology.

Figure 1 shows that it is necessary to follow a certain methodology or scientific approach to conduct research. During the literature review, a research gap was found in the case of the security impact of secured OGISC in ABC LTD. and it was identified as the research problem to be addressed in this study.

2.3 Concept of Proposed Architectural Solution

Secured OGISC service facilitation has been achieved in more remote locations as well as in urban backend areas to access the Oracle database at any time without zero downtime under heavy encryption algorithms support with ultimate data compression mechanism to provide maximum performance between peers' nodes.

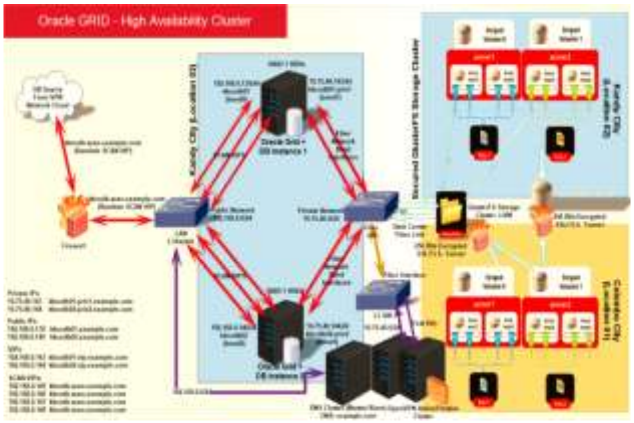

Oracle GRID - High Availability Cluster
Kandy City (Location 02)
Secured GlusterFS Storage Cluster
Kandy City (Location 02)
Colombo City (Location 01)
Oracle Grid - DB Instance 1
Firewall

Fig. 2: The Proposed Network Architecture.

Figure 2 shows that encrypted connectivity tightly binds with the GlusterFS nodes before the mounting process to provide secure connectivity for the strong reaction against cybercrime mitigation situations successfully instead of open connectivity among the storage cluster.

2.4 Existing Security Weaknesses of Mechanism

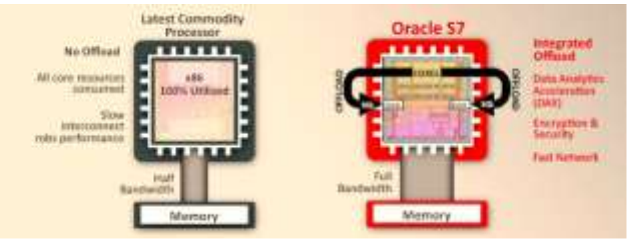
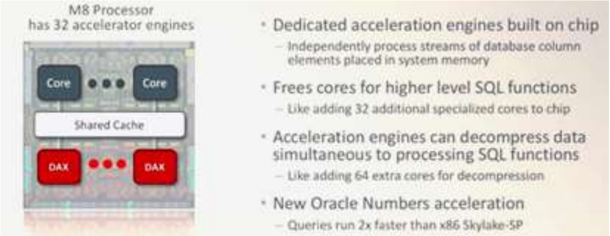


Fig. 3: Common CPU vs Oracle S7 CPU.

Figure 3 shows that the Operation of Oracle SPARC Processor has an advanced encryption capability for threat mitigation while the database instances faced a huge prime number de-factorization attack force by cryptanalyst. The SPARC servers used their dedicated contribution of hardware-assisted encryption security devices, [3].

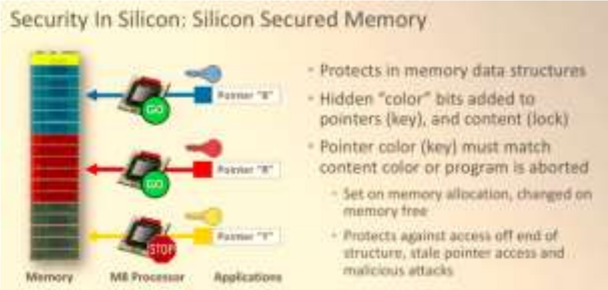
Oracle has developed a powerful and identical high-performance processor that was the target of security against known threats by hackers, in addition, Oracle created the powerful CPU called SPARC M7. It was made up of traditional 32 CPU cores to extend 512 CPU cores successfully.



- Dedicated acceleration engines built on chip
  - Independently process streams of database column elements placed in system memory
- Frees cores for higher level SQL functions
  - Like adding 32 additional specialized cores to chip
- Acceleration engines can decompress data simultaneous to processing SQL functions
  - Like adding 64 extra cores for decompression
- New Oracle Numbers acceleration
  - Queries run 2x faster than x86 Skylake-SP

Fig. 4: SQL in Silicon.

According to Figure 4, The 4.1GHz 32 cores and 256 threads CPU is touted to focus on the highly demanding workload flow with the specific enhanced high-performance architecture, the SPARC M7 processor has incorporated advanced software techniques and not only focused on increasing the performance of the CPU with major improvements to mitigate against programming errors were caused to happened serious security breaches, [4].


Security In Silicon: Silicon Secured Memory

- Protects in memory data structures
- Hidden "color" bits added to pointers (key), and content (lock)
- Pointer color (key) must match content color or program is aborted
  - Set on memory allocation, changed on memory free
  - Protects against access off end of structure, stale pointer access and malicious attacks

Fig. 5: Silicon Secured Memory.

Based on Figure 5, The Silicon Secured Memory structure of the SPARC M8 processor has its powerful encryption engine associated with it, and stronger encryptions and hashing algorithms are included such as RSA, 3DES, SHA 256, SHA 512, DH, MD5, and ECC. Therefore, to protect physical files from security threats and CPU core's scalability in the dynamic way of predictable optimization to overcome the slowness of the encryption process under heavy load, [5].

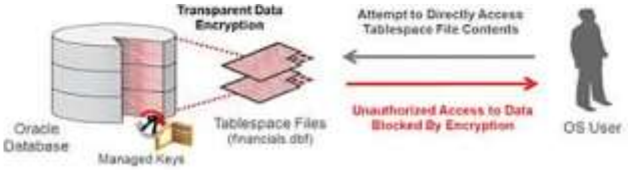

Transparent Data Encryption
Attempt to Directly Access Tablespace File Contents
Oracle Database
Managed Keys
Tablespace Files (financials.dbf)
Unauthorized Access to Data Blocked By Encryption
OS User

Fig. 6: Transparent Data Encryption.

Based on Figure 6, the execution of certain machine code was very straightforward, and it became very complex. At the same time, poorly programmed code examples have been caused by pointers attempting to get access to an allocated loaded memory location. This behavior was a maliciously exploited situation called the buffer overflow (over-read attack). The attacker took advantage of the security weakness of the code section in such a buffer overflow attack. Also, this badly allowed the attacker to modify (write) to an adjacent physical memory location in the flow of buffer overflow attack.

The above condition of the attack obtained data segments of the memory due to the case of a random overread attack. The side effect of the possibility of altering the ability of a program and executing attackable malicious code returned as informative details and access to exploited by an attacker, else it breaches system security, [6].

The CVE-2018-3639 vulnerability was the side channel disclosure attack to expose confidential information. All of them were identified in the same category of attacks. but it was different from the formation of remote code execution was exploited. In addition, these are the attacks that never allow for an unauthorized party to obtain access to a machine. However, it would have allowed a certain external party to access confidential unauthorized data, [7].

The Solaris-10 SPARC allowed a third-party unauthenticated cyber-attacker with the ICMP-enabled platform to compromise the SPARC system. After the successful attempts of attacks of this identified vulnerability was enabled backdoor access as the unauthorized ability to crash the system with DOS attacks over the SPARC systems successfully. Furthermore, the above exploitable vulnerability allowed deliberative outside privileges attackers to log in to the operation infrastructure with remote shell execution privileges, [8].

2.5 Linear Scaling and Introducing GlusterFS

The GlsuterFS Striped volume successfully except for strips that can distribute over a very large number of bricks, additionally, the numbers of bricks must be of the multiplication of the numbers of bricks, were led to increased volume size. The method of linear scaling was the much cuticle phase within the traditional cluster storage field.

Also, when an organization needs to increase performance by twice, that there is clustered storage system must deliver twice the performance and throughput within the same average response of time gap per external clustered file system. Equally, if they wanted to increase either capacity without decreasing performance or having a non-linear return in capacity. Unfortunately, most storage clustering systems do not perform linear scaling. Simply, when an organization needs to double the disk size of the available storage pool, then it must be required to provide enough peak CPU processing power, [9].

The latency takes place as the result of responses across the storage cluster network connected over the distributed cluster server nodes in those traditional types of storage system architectures and recently always impacted the overall performance. The overhead was the major risk while each node in an unacceptable situation led to risk.

Also, this was one of the main reasons for linear scalability caused by the reduced performance of traditional storage distributed architectures. Most of the traditional storage systems demonstrated logarithmic scalability when capacity grows very slowly as it gets larger. This was due to the rapidly increased average overhead required to maintain data flexibility, [10].

2.6 The Ultimate GlusterFS Architecture

When a traditional storage system adds more and more files and more server nodes with more disk arrays, then the centralized metadata server becomes the performance chokepoint, [11].

The GlsuterFS had the mechanism to find a file algorithmically. Therefore, all GlsuterFS storage server nodes within the cluster have a specially developed intelligent algorithm to locate any piece of physical data without depending on the metadata in a separate server instead of a traditional system. The Hashing Algorithm was used when scaling out a storage system, data, and workload. when the storage nodes have been physically located in many different locations as independent storage and cluster nodes to resolve difficulties while retrieving files and locations, [12].

2.7 Storage Scale-Out Process of the GlusterFS

The GlusterFS was designed to successfully provide extended scalable architecture on both capacity and performance with minimized overhead problems. This illustrated that the storage cluster system must be able to scale down or scale up among multiple dimensions. Also, by aggregating the CPU, HDD arrays, and I/O buses of very large numbers of a low-cost system without expending lots of money on expensive resources. In general, an enterprise organization must be able to implement a very scalable and performant cluster storage pool.

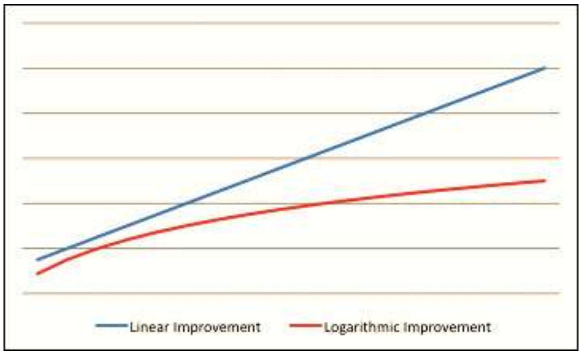


Fig. 7: Logarithmic Vs Linear Improvement.

Figure 7 shows that Logarithmic vs. linear Improvement over the GlusterFS has a unique and advanced architecture designed to deliver huge benefits for expanding scalability. Also, it can be defined as, more units for more capacity, more CPUs as well as more I/O capability which was archived over the storage cluster based on GlusterFS while avoiding the system overhead and, the critical risk associated when it has very large numbers of server nodes in the synchronization process.

Practically, both performance and the capacity of the storage cluster must need scaling out in the manner linearly in the GlusterFS architecture. The Illustration of GlusterFS cluster storage scalability, Figure 8, below shows how the enhancements of both performance and capacity have been archived over the baseline system. As an example, if they expected to obtain both four times capacity and performance, they must be distributed among 8 servers, [13].

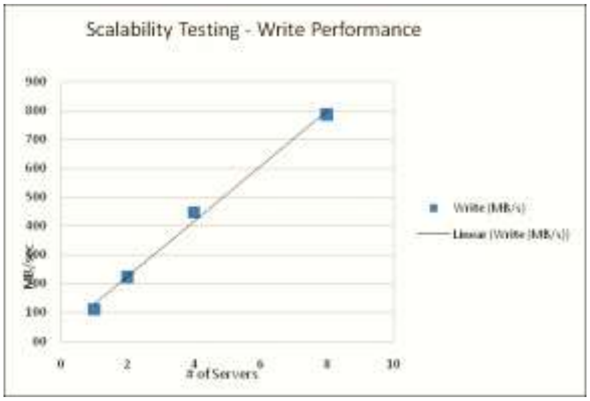


Fig. 8: Linear Scaling of GlsuterFS.

Figure 8 shows the illustration of theoretical numbers only for the example purpose of demonstrating and actual storage performance has been tested to prove the credibility of the linear scaling. The resultant of the storage cluster linearity has been demonstrated in Figure 9 below that shows the data write process of throughput scaling linearly started from 100MB/s to 800MS/s among the eight servers using the 1 Gigabit Interface environment.

Fig. 9: Cryptographic Operations with OpenSSL.

Therefore, the GlsuterFS storage cluster has been successfully deployed in the massive scale-out concept in practice. As a result, it can successfully deploy in the petabyte size clustering solution, [14].

2.8 The Algorithmic Approach and Metadata Model of GlusterFS

The metadata separate location was the main single point of failure, performance overhead as well and reliability concerns of most distributed cluster-based storages. There was no separate metadata server for the information data because the location can determine independently when the other nodes are up or down.

Therefore, GlusterFS called the above algorithmic file location mechanism called Elastic Hashing Algorithm, and it benefited had unique advantages of the GlusterFS architecture, [15].

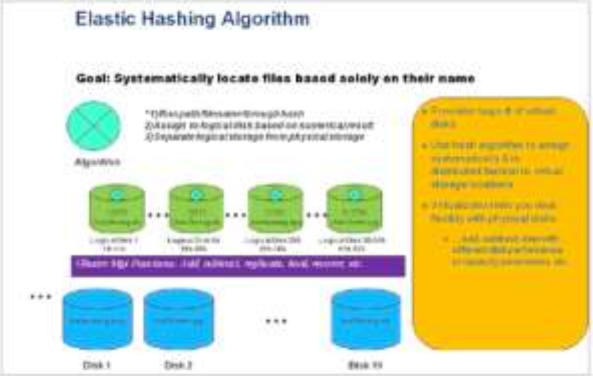

Elastic Hashing Algorithm
Goal: Systematically locate files based solely on their name
Algorithm
Disk 1
Disk 2
Disk N

Fig. 10: Node adds and deletes effect mitigation.

Figure 10 shows that the GlusterFS elastic hashing algorithm is based on a special mechanism called the Davies-Meyer hashing algorithm. The GlsuterFS way of algorithmic approach was unique in any clustered directory tree and ran through the GlusterFS elastic hashing algorithm. In the real infrastructure environment, if the array of disks fails, the capacity of the cluster is used up, and files need to be redistributed over the cluster to get back into the smooth working state without interrupting saved data, [16].

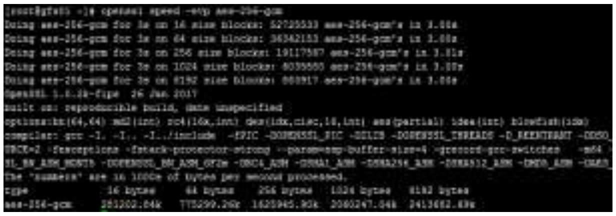
2.9 GlusterFS Compression over OpenVPN

The dedicated compression translator mechanism was embedded into the GlsuterFS architecture to archive high data compression and decompression processes while transferring between clients and bricks over Cluster nodes. The bricks of the server nodes compress the data before transferring it to the client side. The overall throughput measurement has been calculated using the open-source tool called iperf after turning off all pre-configured authentication and encryption operational processes as the cipher none state, and then only triggering the iperf connectivity test.

As a result, the way of compression comparison was illustrated actuality over the existing GlsuterFS storage cluster. The process of decompression and compression operations was done by using the developed ZLIB library bundle. In addition, the enhanced speed of the compressed data, [17].

3 A. The SSL/TLS Connectivity over the GlusterFS

Figure 11 shows, that there was a set of OpenSSL speed test commands to show that the decryption and encryption absolute performance over different networks depends on identical hardware units upon the encryption key already used. By default, the OpenVPN packets were configured at 1500 bytes. Also, The BlowFish cipher has been divided by CPU clock speed and its performance is hardly bound purely by CPU clock rate. But Older types of CPUs operating at a higher clock plus speed, cause them to outperform compared with newer CPUs.



```
[root@gfs01 ~]# openssl speed -evp aes-256-gcm
Doing aes-256-gcm for 3s on 16 size blocks: 52725533 aes-256-gcm's in 3.00s
Doing aes-256-gcm for 3s on 64 size blocks: 36342153 aes-256-gcm's in 3.00s
Doing aes-256-gcm for 3s on 256 size blocks: 19117587 aes-256-gcm's in 3.01s
Doing aes-256-gcm for 3s on 1024 size blocks: 6035580 aes-256-gcm's in 3.00s
Doing aes-256-gcm for 3s on 8192 size blocks: 883917 aes-256-gcm's in 3.00s
OpenSSL 1.0.2k-fips  26 Jan 2017
built on: reproducible build, date unspecified
options:bn(64,64) md2(int) rc4(16x,int) des(idx,cisc,16,int) aes(partial) idea(int) blowfish(idx)
compiler: gcc -I. -I.. -I../include  -fPIC -DOPENSSL_PIC -DZLIB -DOPENSSL_THREADS -D_REENTRANT -DDSO_
URCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches   -m64
SL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DRC4_ASM -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DMD5_ASM -DAES_
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
aes-256-gcm     281202.84k   775299.26k  1625945.93k  2060247.04k  2413682.69k
```

Fig. 11: Speed test of AES-256-GCM.

In general, an OpenVPN server must handle many numbers of VPN client connections, then because of that cryptographic cipher was a proper choice, [18].

B. Benefit and OpenVPN Mechanism over GlusterFS.

The OpenVPN was running over TCP by using port number 443, so the bunch of traffic was distinguishable from the general way of TLS traffic. The Deep Packet Inspection process can be used to filter out OpenVPN traffic.

In addition, the major difference between Browser-based TLS and OpenVPN TLS was the way packets were signed. OpenVPN has been offered to mitigate security attacks from DoS attacks by using special signing packets using the method over the control channel by using a static key generated randomly called TLS auth Key, [19].

A type of hardware token and smart cards were typically very small devices that could be embedded into a chip. Also, it was highly responsible for securely generating, storing, and managing SSL-based private keys. Additionally, that feature was validated certificates and private key pairs were securely stored in a portable single device, [20].

C. Sampling Calculation and Process

Table 1. Morgan Table

Confidence = 95.0%

Population Size	Degree of Accuracy/Margin of Error			
	0.097	0.035	0.025	0.01
10	9	10	10	10
20	17	20	20	20
30	23	29	29	30
50	34	47	48	50
75	43	69	72	74
100	51	89	94	99
150	61	126	137	148
200	68	160	177	196

Table 1 shows that the questions have been asked to obtain information about the occupational pattern, potential members of the team, critical assets with priority under the area of concern, and identification, and security requirements on critical assets, [21].

D. Conceptual Framework

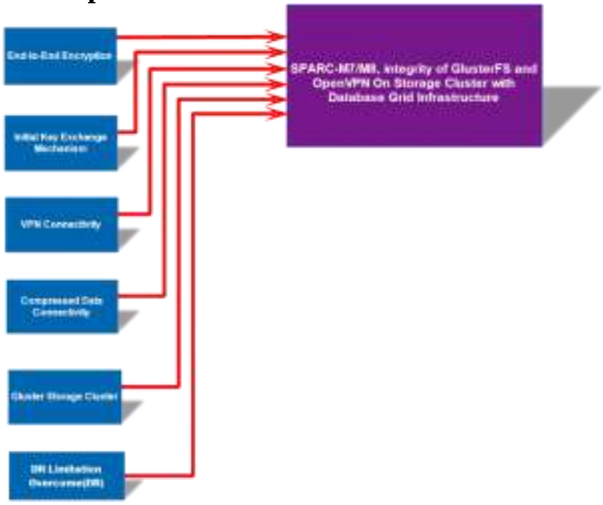

End-to-End Encryption
Initial Key Exchange Mechanism
VPN Connectivity
Compressed Data Connectivity
Cluster Storage Cluster
DB Limitation Overcome(DB)
SPARC-M7/M8, integrity of GlusterFS and OpenVPN On Storage Cluster with Database Grid Infrastructure

Fig. 12: The Conceptual Framework.

Figure 12 shows the theoretical framework that structures the sections of the study that need to be covered and it can help to determine the problem area.

Research questions have been addressed and methodology to find the solution for this problem.

E. Analysis Stages.

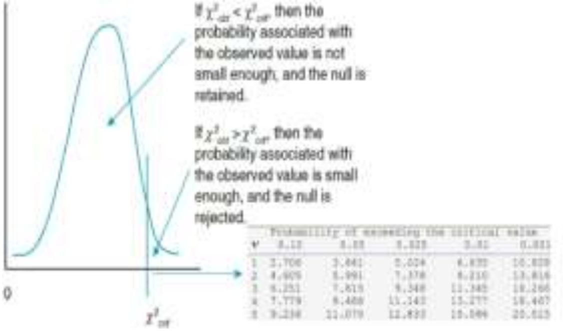


Fig. 13: Critical Value Identification.

Figure 13 shows that the CSQ was used to effectively test hypotheses regarding the distribution of certain observations between different categories, [22].

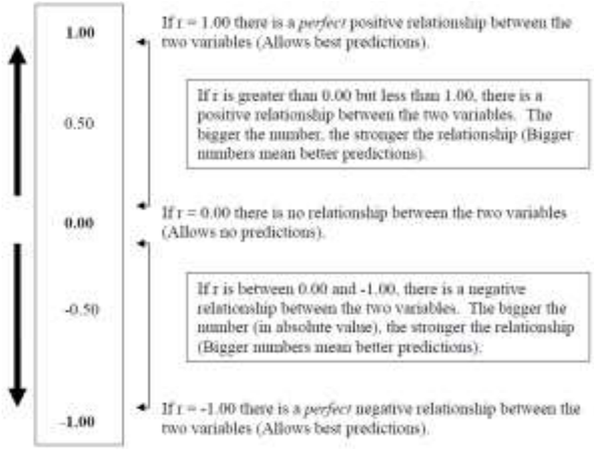

1.00
0.50
0.00
-0.50
-1.00
If r = 1.00 there is a *perfect* positive relationship between the two variables (Allows best predictions).
If r is greater than 0.00 but less than 1.00, there is a positive relationship between the two variables. The bigger the number, the stronger the relationship (Bigger numbers mean better predictions).
If r = 0.00 there is no relationship between the two variables (Allows no predictions).
If r is between 0.00 and -1.00, there is a negative relationship between the two variables. The bigger the number (in absolute value), the stronger the relationship (Bigger numbers mean better predictions).
If r = -1.00 there is a *perfect* negative relationship between the two variables (Allows best predictions).

Fig. 14: The Illustration of Correlation Coefficient.

Figure 14 shows that the Correlation Analysis method was developed to properly assess the direct and indirect relationship between variables. Also, the affected side of the Correlation analysis process has been mentioned as the strength of the correlation, [23].

F. NMAP Scan over GlusterFS Nodes

Illustrates the resultant of the NMAP scan using the techniques of TCP SYN scan. It was initiated using different scanning principles such as ARP Ping Scan, SYN Stealth Scan, Service Scan, and RPC Bind Scan against each node among Storage GlusterFS.

The Next step was to attack both Oracle RAC and GlsuterFS Cluster using the Armitage Application has been powered by Metasploit Framework as an automated attack method that was already generated by Pen Test. It failed to exploit the required server nodes by using known and discovered mid-range level vulnerabilities due to a recent Linux OS update that was made over the cluster. As a result of the overall Pen Test, it failed to attack any single Node of the Server due to the patch management process with the latest OS Update and Upgrade of the rest of the Application behind the cluster node in the Oracle RAC.

4 Conclusion

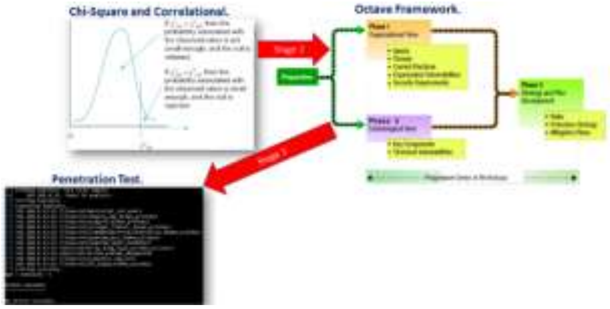


Fig. 15: Statistical, Octave, and Pen test integration.

Figure 15 shows that the validation process was illustrated in the six hypothesis statements due to various affected sizes among the independent variable according to the dependent variable. The X2 > 0 conditions have proved the validation of the objects which was involved in the data collection and analysis phase.

The output has been directly inherited into the Octave Framework for the further technical level of vulnerability assessment with organizational risk factors in the particle way and a proven good level of security strength regarding the provided solution.

After the OS, Kernel, and application update process, it was reduced up to 98%. Also, the organizational vulnerabilities were reduced with the Security Policy of ABC LTD after the embedded with Octave stage with existing ABC LTD's security policy as well.

The penetration test occurred to attack the IT assets after an anonymous way of the test method and got the sufficient level of the good security level of the provided solution with the above stages.

4.1 Proposed Solution and Future Research

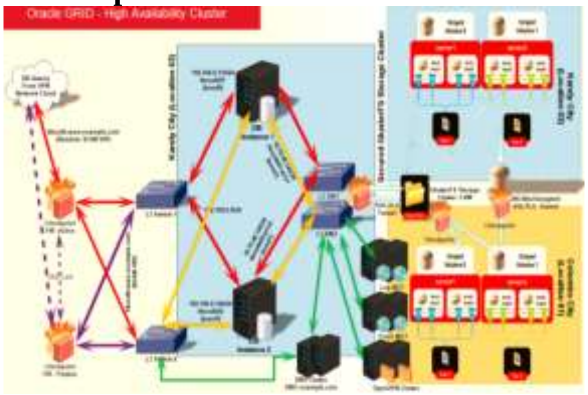


Fig. 16: The Solution with Enhancements.

Figure 16 shows that must be very adaptive and important to propose a system for the monitoring purpose of storage volumes when ABC LTD plans to establish capacity planning or performance tuning scheduled activities over the GlusterFS OGISC. Also, that can monitor Gluster storage volumes using different customizable parameters and can reuse those outputs to identify and clear understanding of troubleshooting issues. The Zabbix monitoring system could enable information gathering such as CPU, physical memory, Raid disk, Network Interfaces, Swap memory, cluster, cluster volume, brick over nodes, LVM host, Glusterd quota, geo-replication, self-heal so on using https secured management web interface.

However, the proactive analysis mechanism can enable detection processes and events that are not specifically highlighted by an automated IDS system and it should cause to use to limit the broader range of impact as well as the cost of an incident.

The requirement of correlation of logs and events over a variety of devices was a very critical area of secured storage cluster over Oracle grid incident response activity such that assists an organization in the assessment process over the possibility of the impact of a network compromise. Also, that must be informed toward the Security team of ABC LTD to necessary for mitigation. The security hardware or software-based product should have identified when an intruder randomly performed an anonymous remote attack against ABC LTD's OpenVPN and GlsuterFS applications, but sometimes it does not have the alert rules to identify the attacker's random penetration through the ABC LTD's network from the initial stage of compromise. By correlating the original alert event with log files from the GlusterFS storage cluster, OpenVPN, Syslog, access log, Oracle database, and authentication servers, as well as events, were generated on the server nodes, greatened visibility of the extent of the compromise which must be established.

References:

[1] Y. Wei, R. Ye and X. Chen, "Oracle RAC performance analysis on VMware Virtual SAN," *2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS)*, Beijing, China, 2019, pp. 562-565, doi: 10.1109/ICIS46139.2019.8940347.

[2] Y. Gong, Y. Wu, K. Pan, J. Chang and J. Xu, "Research and application of distributed storage technology in power grid enterprise database," *2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)*, Chengdu, China, 2019, pp. 1706-1710, doi: 10.1109/ISGT-Asia.2019.8881152.

[3] Oracle LTD, "Oracle's SPARC M7 Processor–Based Servers," oracle.com, [Online]. http://www.oracle.com/technetwork/server-storage/hardware-solutions/oos-for-secure-oracle-database-2736047.pdf (Accessed Date: November 22, 2023).

[4] Oracle LTD, "Enhanced data centre security with Oracle SPARC and Oracle Solaris," oracle.com, [Online]. http://www.oracle.com/us/products/servers-storage/sparc-your-power-wp-3033447.pdf (Accessed Date: November 22, 2023).

[5] S. Pendse, V. Krishnaswamy, K. Kulkarni, Y. Li, T. Lahiri, V. Raja, J. Zheng, M. Girkar, A. Kulkarni, "Oracle Database In-Memory on Active Data Guard: Real-time Analytics on a Standby Database," *2020 IEEE 36th International Conference on Data Engineering (ICDE)*, Dallas, TX, USA, 2020, pp. 1570-1578, doi: 10.1109/ICDE48307.2020.00139.

[6] J. Stuecheli, S. Willenborg and W. Starke, "IBM's Next Generation POWER Processor," *2019 IEEE Hot Chips 31 Symposium (HCS)*, Cupertino, CA, USA, 2019, pp. 1-19, doi: 10.1109/HOTCHIPS.2019.8875663.

[7] D. Chen, G. Jacques-Silva, Z. Kalbarczyk, R. K. Iyer and B. Mealey, "Error Behavior

Comparison of Multiple Computing Systems: A Case Study Using Linux on Pentium, Solaris on SPARC, and AIX on POWER," *2008 14th IEEE Pacific Rim International Symposium on Dependable Computing*, Taipei, Taiwan, 2008, pp. 339-346, doi: 10.1109/PRDC.2008.35.

[8] S. Menaka, K. Navaneethakrishna, J. A. Blesswin Geo Sam, V. K. Hariharasuthan, S. Murugesan, N. Bharathiraja, "Cyber Security Tool for Combat Remote Work Vulnerability," *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Erode, India, 2023, pp.1-4, doi: 10.1109/ICECCT56650.2023.10179806.

[9] Gluster Community, "Distributed Striped Volume," glusterdocs-beta.readthedocs.io, [Online]. http://glusterdocs-beta.readthedocs.io/en/latest/overview-concepts/volume_types.html (Accessed Date: November 22, 2023).

[10] S. Y. Pan, T. Morris, and U. Adhikari, Developing a hybrid intrusion detection system using data mining for power systems, *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015.

[11] Gluster Inc, "Distributed Striped Glusterfs Volume," docs.gluster.org, para, [Online]. https://docs.gluster.org/en/v3/Quick-Start-Guide/Architecture/. (Accessed Date: November 22, 2023).

[12] Azure Inc, "Gluster storage architecture" azure.microsoft.com, [Online]. https://azure.microsoft.com/mediahandler/files/resourcefiles/771b82cd-8b2a-4466-886d-43abf80b14c2/Implement_GlusterFS_on_Azure.pdf (Accessed Date: November 22, 2023)

[13] Gluster Inc, "DHT (Distributed Hash Table) Translator," docs.gluster.org, [Online]. https://docs.gluster.org/en/v3/Quick-Start-Guide/Architecture/ (Accessed Date: November 22, 2023).

[14] RedHat Inc, "Workload-Optimized Distributed File System Clusters., "redhat.com, [Online]. https://www.redhat.com/cms/managed-files/st-RHGS-QCT-config-size-guide-technology-detail-INC0436676-201608-en.pdf (Accessed Date: November 22, 2023).

[15] Sudarshan D. "Simple Application of GlusterFs: Distributed file system for Academics", *International Journal of Computer Science and Information Technologies*, Vol. 6 (3), 2015, 2972-2974.

[16] RedHat Inc, "No Metadata with The Elastic Hashing Algorithm., "access.redhat.com, [Online] https://access.redhat.com/documentation/en-us/red_hat_gluster_storage/3.1/html/administration_guide/no_metadata_with_the_elastic_hashing_algorithm (Accessed Date: November 22, 2023).

[17] Gluster Inc, "On-Wire Compression + Decompression, "staged-gluster-docs.readthedocs.io, [Online]. https://staged-gluster-docs.readthedocs.io/en/release3.7.0beta1/Developer-guide/network_compression/ (Accessed Date: November 22, 2023).

[18] Gluster Community, "Setting up GlusterFS with SSL/TLS," docs.gluster.org, [Online]. https://docs.gluster.org/en/latest/Administrator%20Guide/SSL/#setting-up-glusterfs-with-ssltls (Accessed Date: November 22, 2023).

[19] Packt LTD, "OpenVPN Cookbook. Birmingham", UK.: *Packt Publishing Ltd.*, 2017, pp. 279-282.

[20] Packt LTD, "OpenVPN Cookbook. Birmingham", UK.: P*ackt Publishing Ltd.*, 2017, pp. 19-90.

[21] MaCorr Research Inc, "Sample Size Terminology., "macorr.com, [Online]. http://www.macorr.com/sample-size-methodology.htm (Accessed Date: November 22, 2023).

[22] S. Tsumoto and S. Hirano, "Degree of freedom and numbers of subdeterminants in contingency table," *2012 IEEE International Conference on Granular Computing*, Hangzhou, China, 2012, pp. 481-486, doi: 10.1109/GrC.2012.6468603.

[23] DJS Research Inc, "Sample Size Terminology., "djsresearch.co.uk, [Online]. https://www.djsresearch.co.uk/glossary/item/correlation-analysis-market-research. (Accessed Date: November 22, 2023).

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0
https://creativecommons.org/licenses/by/4.0/deed.en_US