Amity Journal of Computational Sciences (AJCS)
ISSN: 2456-6616 (Online)
Volume 6 issue 1 July-Dec 2022

Implementing Cryptographic Techniques in Storage Area Network with respect to QoS

Ansh Agarwal
Student, MBA (tech) EXTC
NMIMS Mukesh Patel School of Technology Managementand Engineering
Mumbai, Maharashtra
ekansh.agarwal01@nmims.edu.in

Ishaan Jani
Student, MBA (tech) EXTC
NMIMS Mukesh Patel School of Technology Management and Engineering
Mumbai, Maharashtra
Shailansh.shah54@nmims.edu.in

Hem Thakar
Student, Btech EXTC
NMIMS Mukesh Patel School of Technology Managementand Engineering
Mumbai, Maharashtra
hem.thakar93@nmims.edu.in

Vishesh Mehta
Student, MBA (tech) EXTC
NMIMS Mukesh Patel School of Technology Managementand Engineering
Mumbai, Maharashtra
vishesh.mehta35@nmims.edu.in

Abstract— **The study describes how contemporary cryptographic methods are applied in storage area networks with quality of service (QOS). Modern network data storage methods include storage area networks. A SAN technology's primary goal is to give numerous servers access to a pool of data storage where any server may possibly access any storage device. Management is essential for giving security assurances as well as sequencing or serialization guarantees in this sort of environment (granting access to a particular device at certain period of time). As current cryptography is primarily influenced by mathematical theories and computer science techniques, cryptographic methods may be used in these systems to avoid data breach throughout the transit of the data. In this article, we examine the study outcomes of applying the Lustre access storage system, which aims to raise the system's quality. Llite is a new file system that Lustre adds and registers in Linux's virtual file system. Adding encryption to the front of the writing file function and adding decryption to the back of the reading file function using the various cryptographic algorithms discussed above to actualize various encryption processes and decryption processes After that, put several file-level cryptographic storage area network prototypes into use and assess their performance using IO-zone (a file system benchmark tool), which is also used to assess the performance of Lustre and other cryptographic prototypes).**

Keywords— Cryptography, Network Security, SAN and QOS.

I. INTRODUCTION

Since the fast expansion of data storage, big data storage has been regarded as one of the key concerns in the development of networks. It is evident that network storage devices may be utilized to retrieve information and share data due to their big capacity, increased I/O transfer speed, and high system accessibility. According to a poll conducted between 2005 and 2020, the size of the digital world will increase by a factor of 300, from 130 more bytes to 40,000 additional bytes to as many as 40 trillion gigabytes! It is a difficult challenge to safely transfer this enormous amount of data to the user. Data may be secured or encrypted using a variety of encryption techniques using cryptography, making the data even safer. [1] When compared to conventional backup, the amount and worth of enterprise data are growing much more quickly, and their efficacy is also rising. Major Business Enterprises are increasingly reliant on their online systems, but they are mostly dependent on the traditional, network-congested, server-attached storage systems, making it difficult for them to guarantee the availability of this data. Storage area network-related technology has entered the picture to address these issues and help businesses in considering server-less with regard to backups that have zero-time windows. New backup techniques have been used, backup data has been relocated to a secondary distant storage device, and the enterprise server is deactivated, allowing for high-performance access to both apps in the future which incorporates high data volume. The basic goal of SAN technology is to give access to a pool of data storage to several servers, allowing any server to possibly access any storage unit. Management is crucial in this sort of environment for giving security assurances as well as sequencing or serialization guarantees (granting access to a particular device at certain period of time). Due to the fact that current cryptography is mostly based on mathematical theories and computer science principles, it is possible to incorporate cryptographic methods in these systems to avoid data breaches during data transit. They are built on the premise of computational hardness in order to create algorithms that are difficult for any adversary to defeat in practical use.

II. LITERATURE REVIEW

The purpose of this document is to offer a new method of encrypting QoS parameters in Storage Area Networks. As mentioned in the Riabov Viladimir Handbook of Computer Networks, the use of Storage Area Networks would allow data to be duplicated to a remote location for specifically significantly faster disaster recovery. With SANs, data storage can be duplicated at the controller, switch, or operating system level, providing the capacity to generate multiple copies of critical data and then move those copies to other parts of the SAN or across a wide area network. For remote protection [2]. Therefore, SAN is important in modern computer architecture as well as for modern business operations. In the current scenario, strategic day-to-day business initiatives are inexorably tied to network bandwidth for storage applications; simply put, a business can grow as

soon as knowledge can be acquired, shared and acted upon. A recent study conducted at the University of California has reported that there is an estimate of about one exabyte of information generated by the human race by this date, and the second exabyte is expected to be generated within the next 3 years. By 2003, Fortune 1000 companies were projected to add more than 150 terabytes of storage capacity, and more than half of all fiber traffic in their data centers would feed storage systems. Support for storage systems is growing at more than 120% per year and is expected to be an $8 billion market by the end of 2003. Loss or even temporary unavailability of critical data is unacceptable in the event of a disaster in these primary data centers, as these large companies can easily lose millions of dollars in that time period. In today's modern environment where the need for data is a vital issue, storage area networks (SANs) have become an essential part of e-business [4]. To secure all this data between them, we can use cryptographic techniques to secure the data in the network. Cryptography can provide us with a solution to protect sensitive data at a margin when it is communicated between two points or when it is stored on a medium susceptible to physical theft. Communication security provides data protection by encrypting it at the sending point and decrypting it at the receiving point. File security provides data protection by encrypting it when it is written to storage media and decrypting it when it is retrieved from storage media. [5] As Kumar, Ravi and Singh, Namrata (2020) mentioned in his research that a combination of both (steganography and cryptography) called metamorphic cryptography which provides sealed and more secure your confidential data to be decrypted by attackers. [1] To implement such a system, we also need real-time operating system knowledge to help us achieve the goal of integrated resource allocation/dispatch planning (RAD) [6].

III. Methodology

Descriptive research is also called statistical research. The main goal of this type of research is to describe data and characteristics about what is being studied. This type of research is highly accurate, it does not collect the causes of the situation. Descriptive research is mainly done when the researcher wants to better understand the topic, for example a frozen ready meal company finds that there is a growing demand for fresh ready meals, but they don't know much about the fresh food industry so they need to do research to gain a better understanding. In this research, the facts related to the analysis of the modern solution as the implementation of cryptographic techniques in SAN through both experimental and descriptive research methodology.

IV. Implementing QOS in SAN parameter

The systematic use of security and quality of service in a data network is a basic need, despite the use of its mutual effect, engineers always try to generate a state closer to the ideal in data networks, where long service and security of both uses are at the highest level. Security may not differentiate the work with the quality of the service, or it can be said that it generates impacts on the quality of the independent and undeclared security service and vice versa. Not only are the securities not matched for free, and generally speaking, mechanisms using protection need longer processing time and a reason for the delay in operation. Real-time applications such as video conferencing, VoIP, and real-time video need special processing to achieve their goals and overcome the delays caused by adding security mechanisms. [3] There are so many network schedulers that can be developed that enable QoS guarantees. However, an integrated mechanism to provide comprehensive QoS in large network storage systems is still lacking. A new state-of-the-art framework block called RADI/O1 for end-to-end variable storage performance management, including very precise performance level guarantees, is in continuous development. It includes a real-time disk scheduler [3], a cache with QoS support, and a RADoN2 network component. RADI/O is intended for a wide range of applications, including those requiring real-time I/O requirements. Therefore, RADoN must strictly control network traffic and keep the server buffer busy so that the disk scheduler has the ability to optimize sequential accesses within and across reservations. In these areas, progress is being made on various control mechanism flows through extensive simulations based on the queuing model. Servers are given permission to send a storage reminder to the system when coupons are available. Coupons are served by a server that regularly monitors each client's cache occupancy. Network and disk are framed daily as fixed delays. In the most promising implementation, clients themselves replenish the tokens needed to achieve reserved performance based on server-allocated rates and periods, while the server directly manages tokens for unused resources.

V. Performance Study Related to CryptographicStorage Area Network

In this study, encryption is the basis and also the basic method to ensure security with respect to the storage network because it is very expensive and has many problems of outages in critical events. This paper calculates the performance of encrypted storage network with several latest updated cryptographic algorithms and hopes to contribute some useful result to help research and design security system for storage network. A method in cryptography called the DES method. It is a type of block cipher that stores data in 64-bit blocks. A 64-bit block of plaintext goes into one end of the algorithm, and a 64-bit block of cipher text comes out the other end. The total length of the key is 56 bits. DES is a combination of two basic encryption skills: obfuscation and diffusion. DES has 16 rounds. Later, in the latest permutation, one block of plaintext is split into a right half and a left half, each 32 bits long. Then there must be 16 rounds of similar operations, called Functions f, in which the data is combined with the key. Later in the sixteenth round, the right and left halves merge, and the last closed permutation completes the algorithm. In each round, the bits of the key are shifted and then 48 bits of the 56 bits of the key are selected. These four operations form the function f. The output of the function f is then combined with the left half via another XOR. The result of these operations is the new right half and the old right half the new left half. These operations are repeated 16 times, which means 16 rounds of DES. . The same block of plaintext will always be encrypted into the same block of cipher text using the same key. The main algorithms include IDEA, GOST, Blowfish and 3-way. [7] This technique is cheaper to implement and readily

available. There are two types of symmetric cryptographic algorithms: block ciphers and stream ciphers. [6]

VI. Modern Implementation of the Model

Latest updated implementation of this model could be performed using a prototype of area network named as Lustre and encrypt file data using different cryptographic algorithms. System consists of three components:

Client,

OST

MDS

It runs on one PC at a time. In order for the client to access the storage area network storage service, Luster adds a new file system called Llite and registers it in the Linux virtual file system. Using the various cryptographic algorithms mentioned above to realize different encryption process and decryption process, adding the encryption process to the front of the file write function and adding the decryption process to the back of the file read function. Then implement some file-level cryptographic storage network prototypes and evaluate their performance using IO-zone (IOzone is a file system benchmarking tool) to evaluate the performance of Luster and other cryptographic prototypes. It contains two types: write 512K and write 2048K file according to different block size. The write performance of other cryptographic storage network prototypes is lower, and it is bad to use the GOST algorithm, which has very little less than 10% of Luster's write performance. Most cryptographic algorithms require more time and space, and cryptographic storage networks are very inefficient. They are not configurable to implement the storage area network data encryption subsystem. A lightweight cryptographic algorithm is a good choice. [8] But it will reduce the security of the system. In order to ensure the security of the storage area network system, it can implement some other secure strategies such as: variable key, variable encryption strategy and so on. Analyzing the changing curve of write performance, the final finding is that most of the prototypes have the same changing curve as Luster. Its best performance appears when using a write block size of 64KB to write the file. This is because encryption consumption is directly proportional to file size. But when using the GOST algorithm, the change curve is different and its best write performance is later than Luster with the write block size change. So if the GOST algorithm is implemented to encrypt the storage network, then a large set of write block sizes when accessing the storage network.

VII. Conclusion and Future Scope

Through this paper, we conclude that the implementation of cryptographic techniques such as DES, which is mentioned in the early sections in Storage area networks with QoS, can be achieved using Luster, which adds a new file system called Llite and registers it in a virtual file system Linux system. This paper also concludes that DES is the best and most economical method for writing an encrypted file and can be implemented on a large scale and in the future this technique will support large data stores in various business enterprises.

References

[1] Kumar, Ravi and Singh, Namrata (2020), A Survey Based on Enhanced the Security of Image Using the Combined Techniques of Steganography and Cryptography (March 29, 2020). Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

[2] Riabov Viladimir (2012), Storage Area Network Fundamentals, Handbook of Computer Networks.

[3] Tim Kaldewey, Andrew Shewmaker, Richard Golding, Carlos Maltzahn, Theodore Wong, Scott Brandt Computer Science Department, RADoN: QoS in storage Networks.

[4] Casimer DeCusatis, Storage area network applications.

[5] D.K. Branstad, J. Gait, and S. Katzke, Report on the Workshop on Cryptography in Support of Computer Security.

[6] National Bureau of Standards, NBS FIPS PUB 46, Data Encryption Standards.

[7] S. A. Brandt, S. Banachowski, C. Lin, and T. Bisson, (2003). Dynamic integrated scheduling of hard real-time, soft real-time and nonreal- time processes, Dec. 2003.

[8] Nilanjna (2015). “Role of ICT and Internet in Education”, Globus Journal of Progressive Education, 5(2): 1-2.

[9] Puneet Kumar & Ruchika Gupta (2008), “Information System’s Security by using Matrices and Graphs” Conference Proceedings on Information Security and Mobile Computing, pp.62-66.

[10] Maguri, Dr. Ramesh (2015). “A Quick Review on Cloud Computing and Related Security Issues”, Cosmos An International Journal of Management, 4(2): 1-4.

[11] K.S. Mishra, Payal Dixit (2014). “Review of Web Page Clustering”, Cosmos Journal of Engineering & Technology, 4(1): 1- 3.

[12] Sharma, Dr. Seema (2017). “Technology, E-Learning and Social Media with Reference to Academic Achievement”, Cosmos an International Journal of Art & Higher Education, 6(1): 7-8.

[13] Agarwal, Nidhi and Kumar, Puneet, (2009). “Role of Information Technology in Education”, AICTE Sponsored National conference on Information Integrity & Supply chain Management Abstracts Proceeding, Book World Publisher, Dehradun Pp. 18.

[14] M, Kiruthiga Devi and Yadav, Dr. K.P., (2017). “Artificial Intelligence through Machine Learning”. Globus An International Journal of Management & IT,

9(1): 1-3.

[15] Kumar, Puneet and Kapri, Tapan, (2010). “Web Content Management System. Information and Communication Technology: Challenges and Business Opportunities, Excel Publishers, 56-62, ISBN: 978-93-81361-00-9. “

[16] K. Praveen Kumar (2014). “A Study on Cloud Computing”, Cosmos Journal of Engineering & Technology, 4(2): 1-3.

[17] Agarwal, Nidhi and Shiju P.S., (2018). “A Study on Content Generation for Internet Usage”. International Journal of Advanced Research and Development, 3(2), 1380-1382.

[18] Anuradha (2015). “Study in Technological Challenges in Digital Libraries”, Cosmos An International Journal of Art & Higher Education, 4(2): 9-11.

[19] Ruchika Gupta & Puneet Kumar (2013). “Information Technology Business Value Assessment: A Case of State Bank of India”. Globus: An International Journal of Management &; IT, 4(2): 30-34, ISSN:0975- 721X.

[20] Pandey, Satish Chandra and Kumar, Dr. Sudesh (2017). “A Study on Crash Attacks with Functions Related to Hash”, Globus An International Journal of Management & IT, 9(1): 1-3.

[21] Kumar Puneet, (2008). “A Comparative Study of Information System’s Security by using Graphs”, Enterprise Information Systems & Technology, MacMillan India Ltd., pp 222-227, ISBN 0230-63516-4.

[22] Anand Sharma (2014). “A Study of Total Quality Management: Its Legacy, Importance and Implementation in Educational Institutes”, Globus Journal of Progressive Education, 4(2): 1-5

[23] Kumar, Dushyant and Dwivedi, Dr. P.K. (2018). "A Study on In-Time-Frequency Algorithm", Cosmos An International Journal of Management, 7(2): 1-3.

[24] Navdeep Singh (2014). "A Study on Cooperative Defense Against Network Attacks", Cosmos Journal of Engineering & Technology, 4(2): 1-4.

[25] Shinde Jayesh Satish, Dr. Puneet Kumar (2016). "A Study on Queuing Problem", Cosmos Journal of Engineering & Technology, 6(1): 1-3.

[26] Gupta, Mohit and Pathak, Dr. Vibhakar (2017). "Test for Routing Algorithms in

[27] Optical Multistage Interconnection Networks", Globus An International Journal of Management & IT, 9(1): 1-3.

[28] Dr. Seema Sharma (2017). "Information System and Its Role in Uplifting of Education", Globus Journal of Progressive Education, 7(2): 1-4.

[29] Chauhan, Dr. Gandhi Singh (2016). "Criteria to Select Library Automation Software", Cosmos An International Journal of Management, 5(2): 1-5.

[30] Sayed Khasim (2014). "The Discussion On Breaching Information Security", Cosmos Journal of Engineering &; Technology, 4(2): 1-5.