Components Based Key Management Algorithm for Storage Area Networks

P.Mahalingam
System Administrator, Caledonian College of Engineering,
Muscat, Sultanate of Oman.
Email: mahalingam@caledonian.edu.om

Dr.N.Jayaprakash
Professor and Dean, School of Computer Applications
Professional Group of Institutions, Coimbatore, India.
Email: njayaprakash_46@yahoo.com

Dr.S.Karthikeyan
Assistant Professor, Dept. of Information Technology,
College of Applied Sciences,
Sohar, Sultanate of Oman.
Email: skaarthi@gmail.com

Abstract— **Data sharing and file distributions are the two primary functions of network attached storages. Fibre Channel based Storage Area Networks (FC-SAN) has become a more popular solution for the enterprise storage requirements and provides high speed data transfer with high availability, scalability and reliable storage solutions. As SAN keeps and shares entire organizations critical information, it is considered to be more vulnerable to the attackers who gain a single point of access. In most of the data sharing operations among network users, uses encrypted data transfer with proper key management. Securing the SAN data with public key algorithm like RSA is the least less discussed topic and generating keys is a difficult task in distributed environment like Storage Area networks. SAN, considered to be a heterogeneous network, needs distributed key management for the scalability which is one of the important advantages of using SAN. This research paper explores the deployment of RSA algorithm with component based key generation without a key server. This paper also uses compression algorithm ALDC to compress the data during transmission for faster data transfer. The SAN performance was analyzed after the implementation RSA and ALDC algorithm in a customized testing SAN scenario and throughput analysis done for the effectiveness of cryptographic key management.**

Index Terms— **Storage Area Networks; FC-SAN; Fibre Channel Protocol (FCP); RSA; Public Key; Secret Key; Key Management; Key Distribution**

I. Introduction

Securing data during transmission has become a difficult task, in particular when the data is traversing through heterogeneous networks like Storage Area Networks (SAN). Applying cryptographic algorithms to secure the data during its transmission in conventional networks such as LAN, WAN, WLAN are much discussed topics and the SAN is one area where focus needs to be given. Group communication needs a secured way of transmitting information and in the last twenty years group based security and key management has become one of the most discussed and researched areas [2][1]. It is important to protect information transmitted through network from various attacks, both internally and externally either by sending encrypted forms or using some other methods. During the transmission, if an unauthorized user intercepts and gains access to the data then it is difficult get the original information since the information is encrypted and needs the proper key to decrypt it and read the data [7]. Most of the data transfer happens in the group of users among networks and many users will join and leave during the sessions. So, generating a new set of keys for freshly joined members of the group and revoking the left users is the job of the key management. RSA is one of the oldest cryptographic algorithm maintain the public key and secret key in an effective manner [8]. Identity, group identity and component identity based key management is more efficient when compared to the normal cryptographic key management [24]. The basic requirements of cryptographic system such as confidentiality of information, proper authentication and integrity of stored data are achieved using the group key agreement protocol using the well managed key management. The growth of digital information has become very rapid in the last few years due to the use of modern gadgets, internet and automation of various manual works. The sources of digital contents are widening day-by-day. The digital contents are managed by various storage models such as Direct-Attached-Storage (DAS), Network-Attached Storage (NAS) and Storage Area Networks (SAN). SAN is a specialized network as described in "Fig. 1" whose primary purpose is to the transfer of data between computer systems and storage elements and vice versa [3][4].

doi:10.4304/jait.2.2.72-79

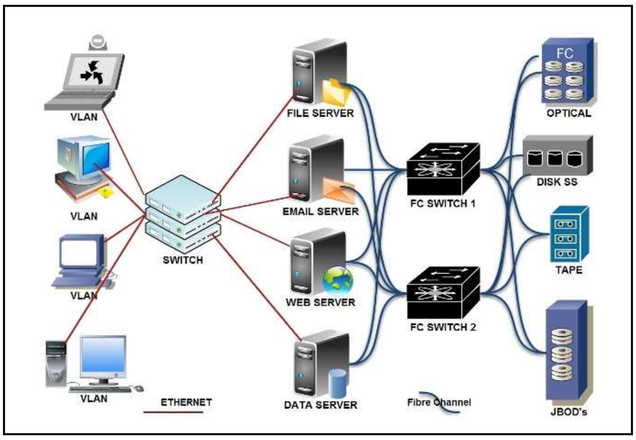


Figure 1. Storage Area Networks

The major benefits of SAN includes, increased disk usage, improved sharing among users, high speed data transmission over the network using fibre channel, centralized backup, storage consolidation, reduced TCO, enhanced manageability, better disaster recovery and high availability. SAN uses its storages in an external environment is one of the unique characteristic which make SAN as top of the enterprise storage solution. SAN is an isolated network from the conventional network and its users and still the attacker's gains control of stored or transmitted data [6].

II. Cryptographic Key Management

Key management mainly focuses on key generation, distribution, use and destroys for the encryption and decryption of data. There are two types of key management in place such as, i) centralized group key management with centralized key server which can be used for the distribution of keys and ii) decentralized group key management without the key server where in the key distribution is taken care by the smaller sub groups. The benefit of decentralized group key management without the key server provides the scalability which is the primary requirement for storage area networks. Scalability will help the users to get dynamic storage allocation. This paper uses decentralized group key management to get the scalability without a key server. Key management system for the SAN combines the devices, people and operations required to create, maintain and control keys used in encryption and decryption of information either at data-at-rest or data-at-transit. Key generation is the process of generating an entity which is not known to unauthorized users and can be known only to the owner and will be used to encrypt and decrypt the data to facilitate cryptography techniques [8]. The major functions of key management illustrated in "Fig. 2", are but not limited to:

i. Key initialization and generation
ii. Store the keys in a database to be compared with each new key generated to avoid the repetition of keys
iii. Distribution of keying materials among group as public and secret keys
iv. Use of keying material over the network
v. Terminate, update, revoke and destroy of keying material
vi. Storage, backup/recovery and archiving of keying material

Why is key management very important to focus more on? The simple answer is, key management will open a path to the attacker to read all the keys which are used by various users so that the attacker can use the keys to interpret the data. Good key management practices start right from the generation of the keys. The key generation should be tough enough to generate and not the same generated twice. The objective of better key management is to maintain the keys such a way so that any threats and risks for the keys will be addressed appropriately. The most common threat to the key management was:

i. Threat to the confidentiality of secret keys
ii. Originality of public keys
iii. Unauthorized use of public or private keys

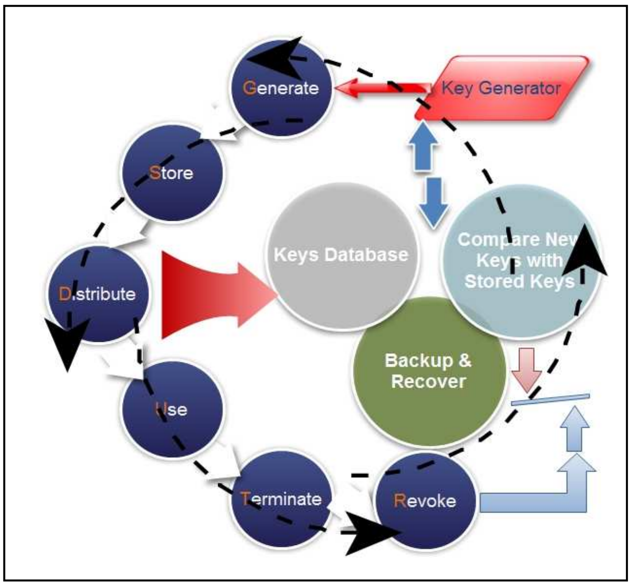


Figure 2. Key Management Life-Cycle

In cryptography, there are a number of threats to the keys where an attacker would like to gain control over the mission critical information's. The prime requirements of data are confidentiality, integrity and availability risked by key exposure, key modification by attackers and the denial of access once the attacker gains the control of data which can lead to a business outbreak [11].

III. San Data Security

To protect the organization information's stored in SAN involves the implementation of appropriate security methods [5] and encryption is one of the techniques to protect it. Conventional networks such as LAN, WAN, MAN, WLAN and other ad hoc networks heavily use the encryption algorithms [10] such as DES, 3DES, AES, RSA etc. SAN uses Fibre Channel Protocol (FCP) for its data transmission and it also uses Fibre Channel Secure Protocol (FCSP) to transport encrypted data from one place to another and vice versa. The application of encryption algorithm over FCSP is less focused area so far. These days, research is conducted at various levels the research is aimed to use encryption algorithm to protect the data during transit. The Storage Area Network data can be protected in two ways, Data-at-Rest (DAR) and Data-at-Transit (DAT). Set of specialized security techniques applied to protect the data-at-rest includes Disk Encryption, Secured File System (SFS), and Cryptographic File System (CFS) etc and applying such techniques is not the scope of this paper. This paper mainly focuses on the data-at-transit by applying the appropriate algorithm to protect SAN data while it is transmitted over the network. SAN send and receives the data over Fibre Channel, LAN and WLAN, etc. The methods involved in a comprehensive security in storage area networks are,

i. Authentication
ii. Access Control
iii. Encryption

Authentication involves recognizing the genuine users and allowing them to use the data and de-recognize the unauthorized users (eg. RADIUS, CHAP etc.). Access control involves to level of access to the authorized users i.e. which user to access what data (eg. Zoning and LUN masking). Encryption involves applying appropriate techniques to convert the readable format to unreadable with the help of secret keys so that one cannot read the data without the key used during encryption [16]. Unlike other networks, the use of encryption methods do not affect the performance of data transfer because the SAN uses high speed fibre channel which is much higher than the conventional networks [5]. There are several methods employed to encrypt the data and the commonly used method is, Advanced Encryption Standards (AES). The some of the encryption techniques involved in data protection are, Full Disk Encryption (FDE), AES, DES, 3DES, Serpent, Two fish and many more[12]. To implement the encryption techniques, there are various types of encryption methods are involved, such as Symmetric and Asymmetric. Symmetric algorithms uses single key for both encryption and decryption whereas asymmetric uses public and private keys makes more secured than symmetric key algorithms.

In general, most of the encryption methods use symmetric cryptography, there is a big risk of key exposure in a network during the transit and if anyone reads the key can easily decrypt the data. To avoid the 'key exposure', a public key concept was introduced [8]. The public key removes the feature of using the same key to encrypt and decrypt it. The public key as its name implies, sends to public wherein the private key is kept secret in the source itself. So, the public and secret keys are used to encrypt and decrypt the information that is to transmit over the network, safely.

IV. Proposed Components Based Key Management

The proposed SAN data security uses the modified RSA algorithm which is used to protect the data from attackers during the transmission of data with improved components based key generation. The compression algorithm is also used along with RSA algorithm for the better performance of high volume data transfer. The use of compression algorithm is to increase the speed of the data transmission. The compression algorithm used in the work is Adaptive Lossless Compression Algorithm (ALDC) from ECMA [13]. The storage area network test scenario divided in to 3 physical parts "Fig. 3".

1. Clients with TCP/IP
2. Servers with TCP/IP & Key Generation
3. SAN with Fibre Channel

The Fibre Channel based storage area network along with storage devices is one part and the servers connected to the SAN with Fibre channel is second part. The third part is a user level LAN.

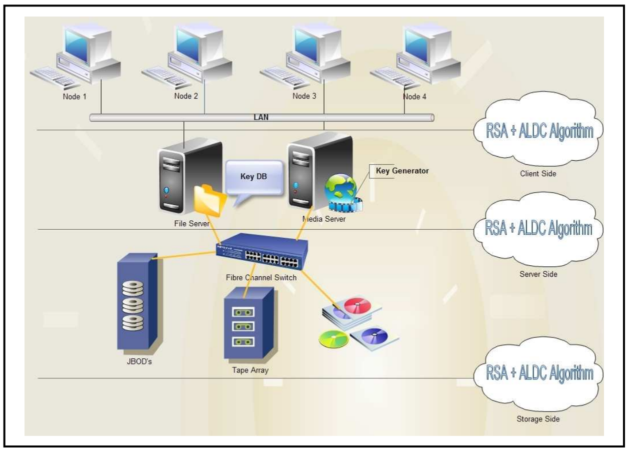
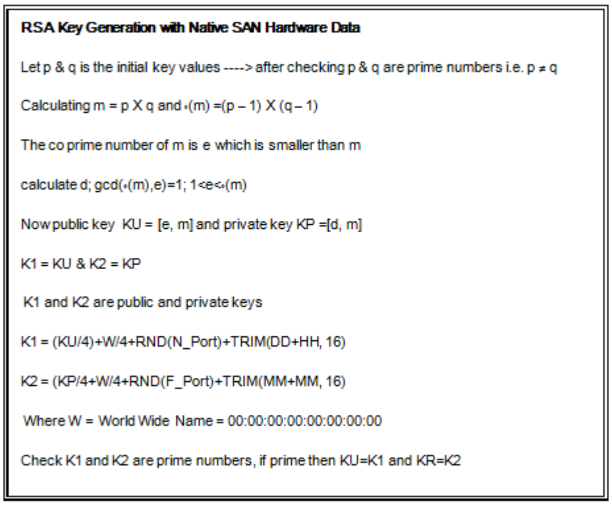


Figure 3. SAN Test Scenario

A. The Key Generation Algorithm

RSA refers to Rivest, Shamir and Adleman, the names of three inventors who invented this public key algorithm in 1977 which named first commercial algorithm. RSA algorithm key generation is one of the fewest algorithm used widely today to protect the information and for the secured communication [14]. The RSA algorithm supports lengthier keys which make the data more secured. RSA algorithm is considered to be a public key algorithm which operates a public key for encryption and a private key for decryption [21][6][20]. The RSA algorithm's key generation incorporated with the SAN native component addresses for key generation is explained below:

If the K1 and K2 are not prime numbers, then the next lowest prime number will be calculated each time. The World Wide Name or WWN is a 64 bit address used in fibre channel networks to uniquely identify each element in FC network [17].



RSA Key Generation with Native SAN Hardware Data

Let p & q is the initial key values ----> after checking p & q are prime numbers i.e. p ≠ q

Calculating m = p X q and ϕ(m) =(p – 1) X (q – 1)

The co prime number of m is e which is smaller than m

calculate d; gcd(ϕ(m),e)=1; 1<e<ϕ(m)

Now public key KU = [e, m] and private key KP =[d, m]

K1 = KU & K2 = KP

K1 and K2 are public and private keys

K1 = (KU/4)+W/4+RND(N_Port)+TRIM(DD+HH, 16)

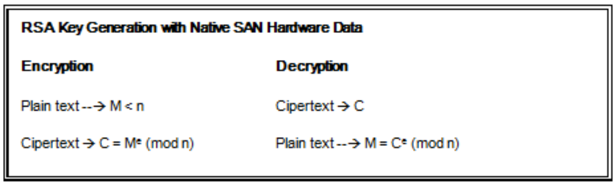
K2 = (KP/4+W/4+RND(F_Port)+TRIM(MM+MM, 16)

Where W = World Wide Name = 00:00:00:00:00:00:00:00

Check K1 and K2 are prime numbers, if prime then KU=K1 and KR=K2

WWNs are 64 bits in length, grouped into 8 hexadecimal pairs, separated by colons, for example, 00:00:00:00:00:00:00:00. The format of the WWN is determined by the first four bits (effectively the first digit) which specifies the Network Address Authority [18]. Each time the 'p' and 'q' are generated, they are stored in the database and checked for checked whether these are prime numbers and its repetition. If the generated key is already used, the two prime numbers 'p' and 'q' will be regenerated or added with next prime number which gives a fresh set of keys.

The RSA algorithm modified as explained above to incorporate the key generation portion based on the SAN components information such as WWN, Port address, device ID and time of transmission along with random number generation module to get the strong public and private keys. As per the above procedure the encryption and decryption takes place as mentioned below:



RSA Key Generation with Native SAN Hardware Data

Encryption	**Decryption**
Plain text --→ M < n	Cipertext → C
Cipertext → C = M^e (mod n)	Plain text --→ M = C^e (mod n)

The above procedure and algorithm implemneted in server side by JAVA code developed [22][23]. The first 8 bits of keys 'p' and 'q' given input to the ALDC algorithm.

B. ALDC Compression Algorithm

The Adaptive Lossless Compression (ALDC) algorithm accepts input in 8-bit data bytes and outputs a bit stream representing data in compressed form [8]. The ALDC algorithm is implemented based on Lempel-Ziv (LZ1) class of data compression algorithms. The ALDC algorithm will increase data transmission speed over the network dramatically [19]. The 8-bit input was selected from the RSA key generator implemented in JAVA [22][23] explained above. The 8 bit input for the ALDC is,

Ai = first_8_bits(p); Bi = first_8_bits(q)

wherein,

Ai will be given 1st time and
Bi will be given 2nd time and so on.

Each time the 8-bit input to the compression algorithm will change as per the above explained procedure.

C. Key Management

Providing key management for large networks connected to the Storage Area Networks is always a challenging task. In a scenario, a network of 200 users may require generation of 10000 keys for a single session, when used symmetric cryptography and the network or user grows, the number of keys increases accordingly. In order to generate and handle the keys effectively we need a better key management protocol which takes care of key growth and its security. The key management adapted in this SAN environment to effectively manage the is explained in the flow chat "Fig. 4".

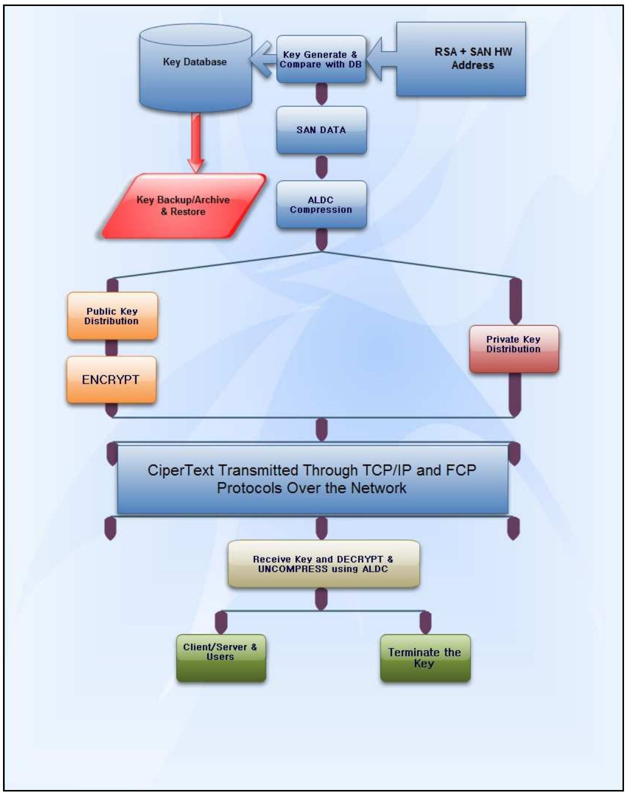

Key Database
Key Generate & Compare with DB
RSA + SAN HW Address
SAN DATA
Key Backup/Archive & Restore
ALDC Compression
Public Key Distribution
ENCRYPT
Private Key Distribution
CiperText Transmitted Through TCP/IP and FCP Protocols Over the Network
Receive Key and DECRYPT & UNCOMPRESS using ALDC
Client/Server & Users
Terminate the Key

Figure 4. SAN Key Management Process

Effective key management needs the control of keys traversing through the network. The key should not be exposed which could lead the attackers to gain the access of keys and get the information over the network. The "Fig. 5" shows how the key is traversing over the network in both IP as well as FC storage area networks.

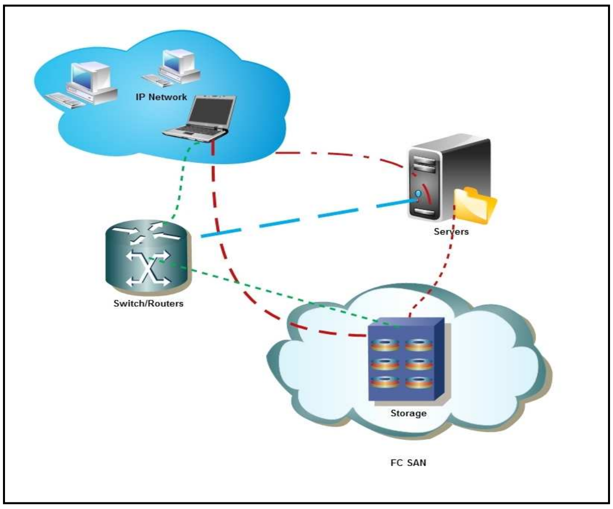


Figure 5. SAN Key Distribution

IV. SAN PERFORMANCE ANALYSIS

The SAN test scenario consists of the following hardware for the implementation of the proposed distributed key management system for the storage area networks. These servers, clients and storage components are interconnected as a network to form a TCP/IP network as well as isolated SAN.

1. Two Servers
2. Four clients
3. One FC-Switch
4. One Network Switch
5. Fibre Optic Cables
6. CAT6 Cables
7. JBOD's
8. Tape drive
9. Optical Disk Drive

The specifications of servers, clients and other components used in this work are listed in the Table I. The client used in this test are identical in specification.

TABLE I.
SAN TESTING HARDWARE SPECIFICATIONS

Description	Specifications
Servers	Pentium 4/4GB RAM with NIC & HBA's
Clients	Pentium 4/2GB RAM & NIC's
FC Switch	3Com Switch 8800, 360 Gbps Fabric Module
Network Switch	3Com OfficeConnect Gigabit Switch 16
JBOD's	Ataptec SANbloc 2GB JBOD, 3 U, upto 14 drives
Tape Library	HP StorageWorks MSL 4048 2 LTO-4 Ultrium 1840 tape library
Compact Disc	Fujitsu Compact Disc Array GR710 RAID 0, 1, 0+1, 5
Host Bus Adaptors	HP FCA2210 2 Gb 64-Bit/133 MHz

The RSA algorithm with component based key generation JAVA program was running in the server side and the keys database was also stored in a database. The test was conducted in 20 sec and 30 sec duration with variable block sizes 100 KB to 1000 KB "Table II"). The performance was analysis conducted and measured after the implementation of modified RSA key generation algorithm and ALDC compression algorithm. The following three types of tests were conducted as below:

1. Between the server to client
2. Between the server to storage
3. Between client to storage

TABLE II.
SAN TESTING HARDWARE SPECIFICATIONS

Test Parameters	
Block Size	Start: 100 KB End: 1000 KB Step: 8 and 14 KB
Time	20 Sec. 30 Sec.

In order to decide whether the performance will be affected due to the implementation of the components based key generation using RSA algorithm, above three types of tests were conducted. The performance test output is taken as graphs as Kilo Bytes versus Sec.). The server to client and clients to server data transfer uses TCP/IP protocol. The average data sent and received between the clients and server performance is not affected due to the implementation of both algorithms from server side as well as client side. However, there was a small delay and a drop in 15th sec. indicates the key regeneration and compression with the key database. The server to client data transfer performance clearly shows that, the use of compression algorithm increased the where is server to storage is decreased because of high speed fibre channel.

The performance analysis "Fig. 4, 5" graph is measured between server to client, uses TCP/IP as its protocol before and after the implementation of RSA algorithm and ALDC compression. The results shows there are no significant end-to-end delay in time. However, the data transfer rate was slightly dropped and slight variation observed in sending the data due to the running of both the algorithm from the server side. The results of data transfer between the server to storage "Fig. 6, 7" uses FCP as protocol uses high speed fibre channel as a transport medium sends and receives the data higher rate when compared to the TCP/IP. However the data transfer between clients "Fig. 8, 9" to storage uses both the protocols TCP/IP and FCP, because it first contacts the server for any transfer request using TCP/IP and the server sends the request to the storage as per the client requests. In these results, one common significant observation is the drop in data transfer rate especially from the recipient side which indicates the transfer load after the implementation of algorithms. The throughput analysis also showed clearly there is no load from storage side instead the clients are having low data transfer rate due to the use of two protocols TCP/IP and FCP. Also the data needs to traverse from storage to server and then to the clients. Since server and storage communicate with only FCP protocol has fewer burdens which provides a high rate of data transfer "Fig. 10".

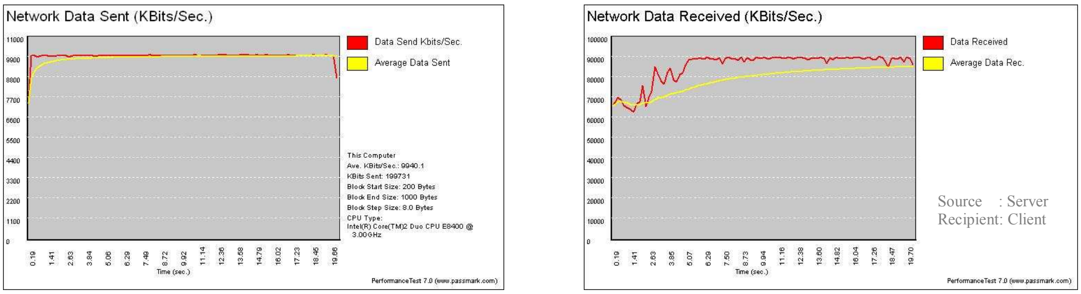


Figure 4. Data transfer between Server to Client before running Algorithm

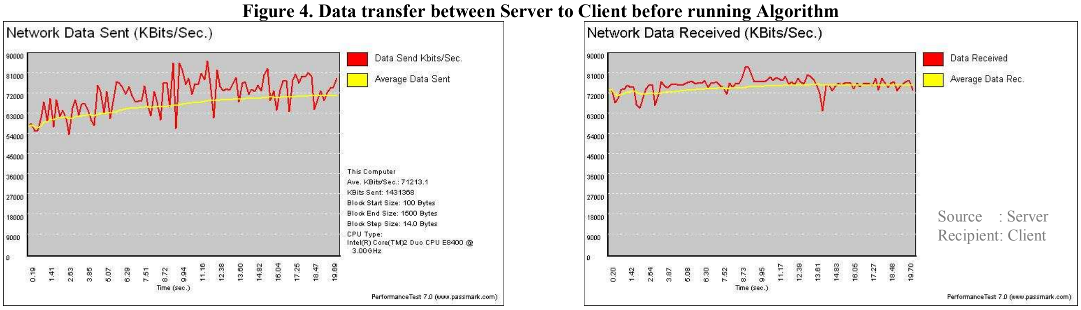


Figure 5. Data transfer between Server to Client after running Algorithm

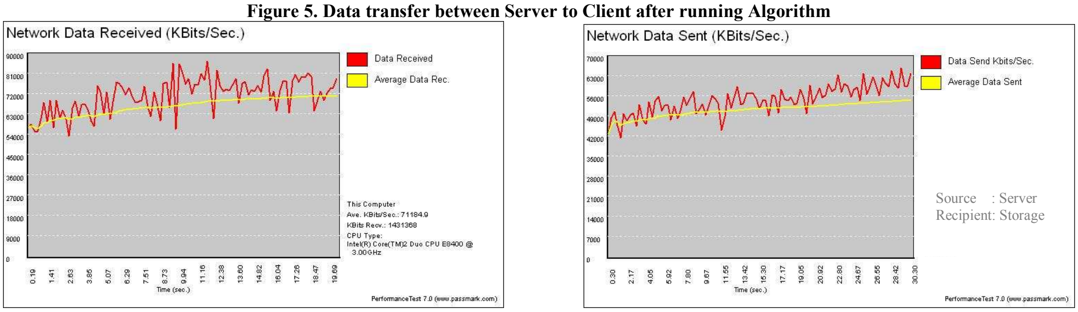


Figure 6. Data transfer between Server to Storage before running Algorithm

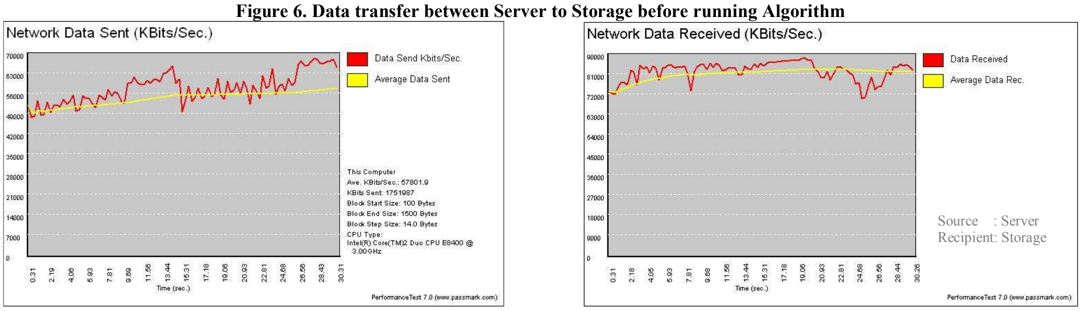


Figure 7. Data transfer between Server to Storage after running Algorithm

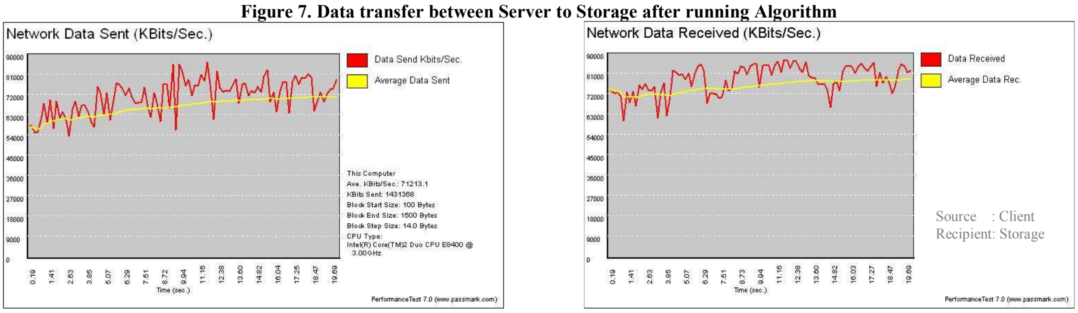


Figure 8. Data transfer between Clients to Storage before running Algorithm

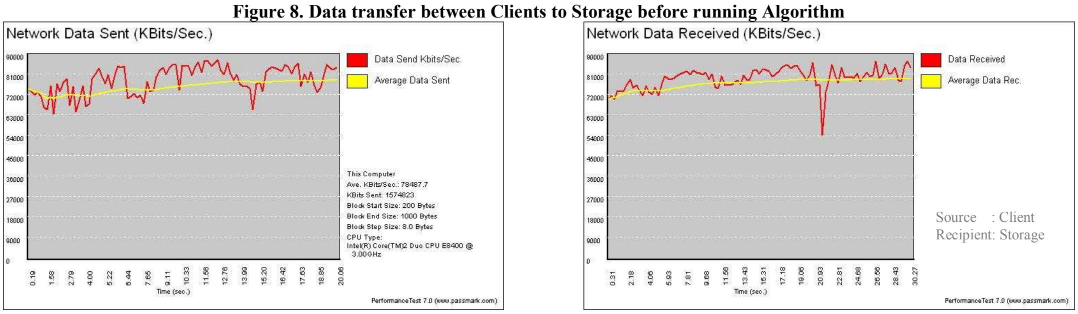


Figure 9. Data transfer between Clients to Storage after running Algorithm

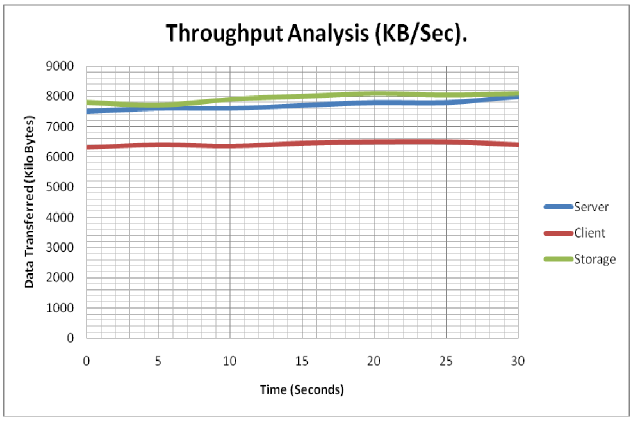


Figure 10. Throughput Analysis of Data Transfer

I. Conclusions and Future Work

In this paper, the general architecture of SAN and its security was taken into consideration to protect its data especially when it is transmitted over the network. The focus is given to evaluate an idea of using the SAN's native hardware information incorporated while generating the key for its encryption and decryption. The RSA public key algorithm incorporated with distributed key management is the summary of work evaluated in this paper and the results obtained after the tests. It is clear that, the impact of this algorithm implementation does not affect the performance of storage as well as the data transfer between the clients and server. It is proved that the data traversed in a secured manner without affecting the performance. The scalability is also taken care by not keeping the key server and the key generation remains in the server side. Storage Area Networks play a vital role for the integrity of information which is very important to meet the customer demand and be a leader in the industry. Hence, the proposed system will efficiently protect the SAN's data when it is transmitted and at the same time, the performance data transfer will not be affected since the compression algorithm is also used. Future work will be carried out from this work by applying different sizes of data with various time durations and also by the application of different key exchange protocols along with existing RSA algorithm incorporating the components based key generator. It is also planned to use encrypted file system from storage side to protect the data-at-rest which is presently not the scope of this paper.

Acknowledgment

This paper is a part of PhD work of the first author and the author places a sincere thanks to the Management of Caledonian College of Engineering for their support of this work.

References

[1] E. Bresson and D. Catalano, Constant round authenticated group key agreement via distributed computation. In Proceedings of Public Key Cryptography - Pkc'04, Vol. 2947, 2004, pp. 115-129.

[2] Harney, H., and C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification", RFC 2093, July 1997.

[3] G. A. Gibson, D. F. Nagle, K. Amiri, J. Butler, F. W. Chang, H. Gobioff, C. Hardin, E. Riedel, D. Rochberg, and J. Zelenka, "A cost-effective, high-bandwidth storage architecture," in ASPLOS-VIII: Proc. of 18th Int. Conf. on Architectural support for programming languages and OS, vol. 32, no. 5. New York, NY, USA: ACM Press, December 1998, pp. 92-103.

[4] Jiwu Shu, Bigang Li, Weimin Zheng, "Design and Implementation of an SAN System Based on the Fiber Channel Protocol," IEEE Transactions on Computers, pp. 439-448, April, 2005.

[5] P. Mahalingam, N. Jayaprakash, S. Karthikeyan, "Enhanced Data Security Framework for Storage Area Networks," ICECS, pp.105-110, 2009 Second International Conference on Env. And Computer Science, 2009.

[6] "Storage Area Networks Design Reference Guide", Hewlett-Packard, pp.26. Sep 2003. Available: http://www.ost-india.com/services/san/understanding%20sans.pdf.

[7] K.Fu. "Group Sharing and random access in cryptographic storage file systems". Master Thesis. Massachusetts Institute of Technology, June 1999.

[8] William Stallings. "Cryptography and Network Security, Principles and Practices", Fourth Edition, Prentice Hall, November 2005.

[9] Daniel Augot , Raghav Bhaskar , Valerie Issarny , Daniele Sacchetti, "An Efficient Group Key Agreement Protocol for Ad Hoc Networks", Proceedings of the First International IEEE WoWMoM Workshop on Trust, Security and Privacy for Ubiquitous Computing, p.576-580, June 13-16, 2005.

[10] Yuling He. Yun Pan, Ping Pan, Lichen Wang. "Simulation of Key Management Protocol in Wireless Sensor Networks", IJCCSO, IEEE, 978-0-7695-3605-7/09, p.333-335, 2009.

[11] Yingwu Zhu; Yiming Hu. "SNARE: a strong security scheme for network-attached storage". IEEExplore, Proc. Reliable Distributed Systems, 2003. Proceedings. 22nd International Symposium on, pp.250-259, 2003.

[12] Tao Cai Shiguang, Ju JunJie Zhao and Wei Zhong. "Performance study of Cryptographic Storage Area Network". Workshop on Network and Parallel Computing. NPC Workshops, IFIP Pp.561-565. Sep 2007.

[13] Standard ECMA-222, "Adaptive Lossless Data Compression Algorithm". June 1995. http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-222.pdf.

[14] Lu, C., dos Santos, A. L., and Pimentel, F. R. 2002. "Implementation of fast RSA key generation on smart cards". In *Proceedings of the 2002 ACM Symposium on Applied Computing* (Madrid, Spain, March 11 - 14, 2002). SAC '02. ACM, New York, NY, 214-220. DOI= http://doi.acm.org/10.1145/508791.508837.

[15] Performance Test, Passmark, Software, USA. http://www.passmark.com/support/performancetest/index.htm.

[16] M. Blaze. "Key Management in an Encrypting File System". USENIX Summer 1994 Technical Conference, Boston, MA, June 1994.

[17] http://www.tech-faq.com/world-wide-name-wwn.html.

[18] http://www.sanduel.com/SAN-Storage-FAQs/What-is-WWN-and-WWN-Zoning.html.

[19] ALDC in wireless communications, aha Products Group, http://www.aha.com/show_page.php?tag=ALDC.

[20] Jing Lu, Wan Qian. Implementing a 1024-bit RSA on FPGA, Reconfigurable Network Group, Applied Research Lab, Department of Computer Science and Engineering, Washington University in St. Louis, Project Report, 2003.

[21] RSA Algorithm, RSA-based Cryptographic Schemes, RSA Labs, USA. http://www.rsa.com/rsalabs/node.asp?id=2146.

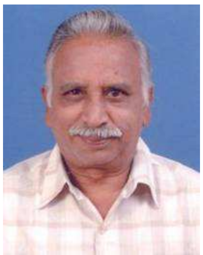
[22] JAVA 6 SE SDK and JAVA 6 SE Documentation. http://www.oracle.com/technetwork/java/javase/downloads/index.html and http://download.oracle.com/javase/6/docs.

[23] Bruce Schneier, "Applied Cryptocraphy: Protocols, Algorithms, and Source Code in C." 2nd edition, 1996.

[24] C.J.Cao and J.F.Ma. “Identity-based constant round group key exchange protocol via secret-share”, WSEAS Transactions on Systems, Volume 7, Issue 1, pp.7-16, Jan, 2008.

P.Mahalingam was born in Madurai city, Tamil Nadu, India, in June, 1970; received Bachelor of Computer Applications from University of Madras, Chennai, India; received M.Sc. in Information Technology from Karnataka University, Mysore, India; received M.Phil. in Computer Science from Periyar University, Salem, India. His research interests include networking, information security, Storage Area Networks.

Mahalingam worked as a Sr.Programmer/IT In charge in International Institute of Biotechnology and Toxicology (IIBAT) from Aug 1994 to Oct 2003 in Chennai, India. Presently he works as System Engineer & Administrator at Caledonian College of Engineering, Muscat, Oman since November 2003, and doing his PhD in Storage Area Network Security from Vinayaka Mission University, Salem, Tamil Nadu, India. His work was supported by PhD Program Staff Development Fund at CCEO, Muscat. He is a SNIA Certified Storage Professional (SCSP 2008) and also IEEE professional member, IACSIT senior member, ACEEE senior member and member of SNIA. He has attended several national and international conferences in the area of IT, networking and information security.



Dr.N.Jayaprakash presently working as Dean and Professor at School of Computer Science, Professional Group of Institutions, Coimbatore, India. Previously he was a Head of Master of Computer Applications at Sri Muthukumaran Institute of Technology, Mangadu, Chennai, India and also he was Assistant Professor, Professor, Head of Computer Science at various educational institutions in India. He has total of 33 years of teachings and research experience. He was awarded his PhD at IIT, Chennai, India during 1982. He has published various books in the area of Physics, Mathematics, and Computer Networks. He has guided 3 PhD scholars, 4 M.Phil Computer Science students and presently he is guiding 2 PhD research scholars.

Dr.S.Karthikeyan presently working as Assistant Professor, College of Applied Sciences, Oman and previously he was a Senior Lecturer at Caledonian College of Engineering, Oman. He was a Professor & Director at Karpagam University, School of Computer Science and Application, Coimbatore. He has total of 13 years of teaching and research experience. Dr.Karthikeyan completed his PhD at Alagappa University, Karaikudi, India in the area of Network Security, Computer Science and Engineering by Feb 2008. He has 28 research papers and guiding 11 PhD research scholars from various universities in India and he has also guided 19 M.Phil students. He is Chief and guest editor of various national and international journals. He has chaired many conference sessions and served as Technical Committee member of various boards at various colleges, universities and conferences.