A Case of Security Encryption Storage System Based on SAN Environments

Changyan Di, Kuan-Ching Li, Jason C. Hung, Qi Yu, Rui Zhou, Chao-Hung Hung, and Qingguo Zhou

Abstract SAN (storage area network) is a dedicated network that provides access to consolidated data storage and offers major advantages as simplified administration, high speed, and flexibility. This chapter proposes a security encryption storage system named ANGLE, which contains two major parts – the key management system (KMS) and the encryption engine (E-Engine). E-Engine is in charge to encrypt/decrypt storage disks under AES128 and SHA256 cryptographic algorithms, according to keys provided by KMS. These two parts communicate by IPsec protocols, and a well-defined UI (User Interface) for applications is provided. The proposed ANGLE system is implemented in both FC SAN and IP SAN, and performance tests show that the bottleneck of ANGLE's reading and writing throughput relies on data transmission speed of the storage network.

Keywords SAN • Encryption storage • Storage network

1 Introduction

SAN (storage area network) is a high-speed and dedicated network attaching servers and storage devices, offering more advantages such as better scalability, higher data throughputs, and easier management [1, 2]. It is often used in large-scale business

C. Di • Q. Yu • R. Zhou • Q. Zhou (✉)
School of Information Science and Engineering, Lanzhou University, Lanzhou, China
e-mail: zhouqg@lzu.edu.cn

K.-C. Li • C.-H. Hung
Department of Computer Science and Information Engineering (CSIE),
Providence University, Providence, Taiwan

J.C. Hung
Department of Information Management, Overseas Chinese University, Taichung, Taiwan

J. Juang and Y.-C. Huang (eds.), *Intelligent Technologies and Engineering Systems*,
Lecture Notes in Electrical Engineering 234, DOI 10.1007/978-1-4614-6747-2_4,

environment, which means that SAN systems are able to hold more critical data under severe security requirements. Besides, SAN is an open and available medium connecting servers and storage, making it vulnerable to various security threats like unauthorized access or hostile attack. Although SAN provides measures as LUN (logic unit number) and zoning schemes, it is far from enough due to malicious intrudes. In this case, encryption becomes the most direct and effective method to tackle data leaks. There is a number of software developed to secure storage units, such as BitLocker in Windows Vista/7, the open source encryption software Truecrypt, among others. Besides, SISWG (Security in Storage Working Group) under IEEE is working on the standardization project for encryption of stored data known as P1619 [3], and now P1619.1, P1619.2, and P1619.3 are issued.

In this chapter, a secured encryption storage system based on SAN named ANGLE is proposed, aimed to protect data from leaking in case of being stolen or lost in such server storage arrays. It is a kind of hardware-level encryption strategy, including two major parts – the encryption engine (E-Engine) and the key management system (KMS). ANGLE adopts FPGA as the hardware E-Engine with various cryptographic modes like XTS and CBC and cryptographic algorithms like AES (Advanced Encryption Standard) and DES (Data Encryption Algorithm) or blowfish, and encrypts data flowing in the block level. The architecture of KMS follows the standards of P1619 strictly. Finally, ANGLE is implemented in FC SAN and IP SAN. Performance evaluation shows that ANGLE's performance bottleneck lies in the data transmission speed of the storage network.

2 Design of Implementation of ANGLE

2.1 System Architecture

The schematic diagram of ANGLE is shown in Fig. 1. ANGLE adopts the hardware cryptographic mode that holds advantages as (1) the encrypting computing is processed by independent encryption hardware which does not affect the performance of SAN system and fits well in large-scale business environments and (2) the key management is tackled independently so as to provide better protection. ANGLE has embedded SHA256 and AES256 in FPGA to implement hardware encryption and, thus, increases data throughputs in SAN systems. In addition, AES256, SHA256, and random numbers are all produced by hardware that will extend system security.

The design of KMS is the most important yet difficult point in ANGLE. It is naive to say that data is secured, because it is encrypted in that this pushes the problem of securing the data to ensure that keys to decrypt or re-encrypt are only accessible in an authorized context [5]. Therefore, the design of KMS follows the P1619.3 International Standard, including key creation, destruction, usage, revocation, and update. ANGLE adopts various types of authorized schemes such as smart cards, traditional password, or biological characteristics.

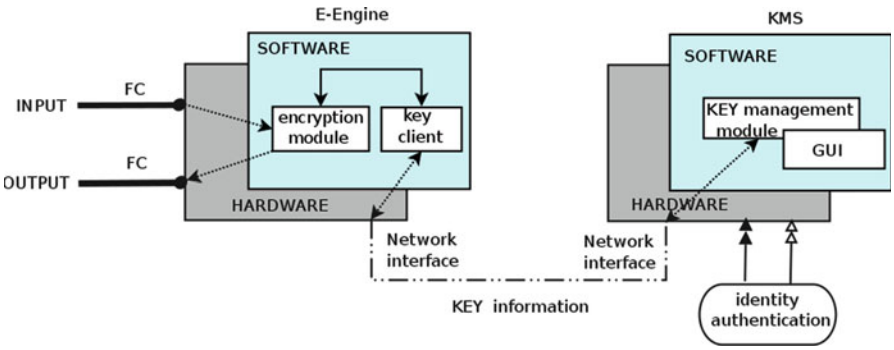

Fig. 1 Xilinx Virtex-4 FPGA device is applied as the E-Engine, which integrates cryptographic algorithms like SHA256 as IP cores [4]. A well-defined GUI provided in KMS includes system management and key management interface. E-Engine and KMS communicate with each other using IPSec protocols by PCIe ports under the slave-master mode

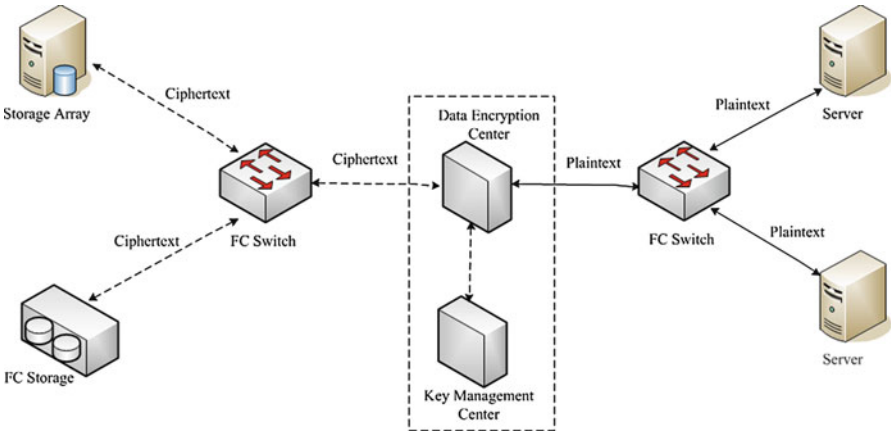

Fig. 2 In SAN, the network behind servers is usually applied to connect heterogeneous servers and storage resources. Several different components can be used in SAN's interconnection, like switches, and shown here as the implementation of ANGLE in FC SAN

2.2 Implementation of ANGLE in FC SAN and IP SAN

The term SAN is usually but not necessarily identified with block I/O services rather than file access services. Traditionally, the interconnections in SAN are based on fiber channel, whose advantages are high speed and higher level of security. Thus, FC SAN is very popular in mission-critical applications. Today, Internet Protocol (IP) has become an option to interconnect geographically separated SANs due its low cost, long distance, and also better interoperability.

As shown in Figs. 2 and 3, ANGLE is placed between storage arrays and servers and can be configurated as the initiator or the target. Storage arrays are remapped by

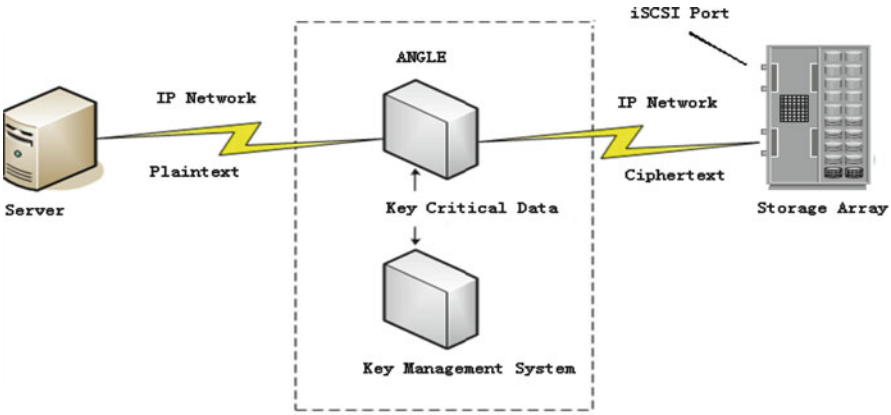

Fig. 3 IP SAN as alternative of FC SAN, it uses iSCSI protocol to encapsulate SCSI I/O over IP. As illustrated in this figure, IP traffic (*in the left of ANGLE, it is plaintext*) is routed over a network to an iSCSI storage array (*in the right of ANGLE, it is ciphertext*) that can handle the extraction and I/O natively

ANGLE and assigned to some certain servers. For every mapped disk, different keys are used to fulfill encryption and decryption requirements under some cryptographic algorithms, and applications can access the encrypted storage devices transparently. The investigations of iSCSI and FC communication protocols are fundamental in this point here, so that ANGLE can be applied in FC SAN and IP SAN seamlessly.

3 Experimental Results

As performance evaluation of ANGLE's reading and writing operations, Xilinx Virtex-4 FPGA with SHA256 IP core is used as the E-Engine with a 512-bit block size. Widely used open source software Bonnie++ [6] in UNIX is utilized to test data throughputs in different file sizes. Additionally, storage arrays are created by the *dd* command in Linux from the PC's disks. The remote encryption disks are tested in blocks of 2, 4, 8, and 16 GB at server's end with two-group comparisons, that is, (1) local non-encryption disks and (2) local encryption disks. In these tests, the server-side PC has the following configuration: one Intel Pentium Dual-core CPU E2200 2.20 GHz CPU, Linux Debian 2.6.39-dsi-new #1 i686 GNU/Linux, and 1 GB memory. After a total of over 30 tests performed, a conclusion has been drawn that the bandwidth of the storage network is the main factor affecting the performance of ANGLE, as depicted in Fig. 4.

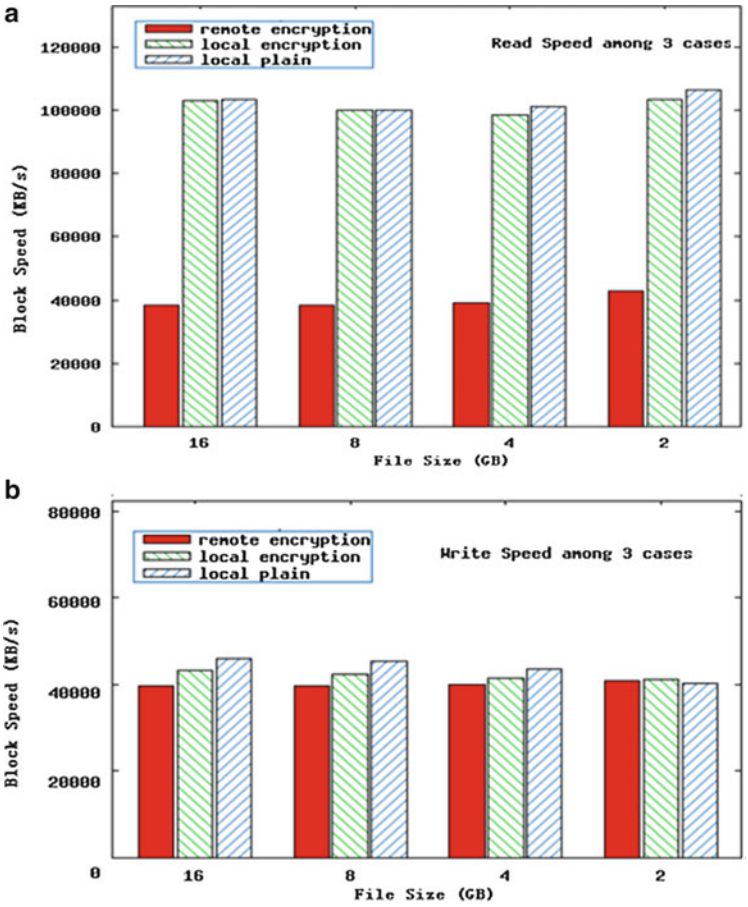

Fig. 4 *X*-axis refers to different block sizes while *Y*-axis refers to the reading or writing speed of each case in several different file block sizes. From the results shown in (**a**), reading performance between local encryption disks and non-encryption disks is almost the same when the file size is over 8 GB, but reading performance of remote encryption disks is less than 40 % of local disks and tends to be stable with the increase of the file size. Writing performance in (**b**) is smaller in remote encryption disks than that of local encryption disks, and additionally, the two are both less than that of local non-encryption disks

4 Conclusions and Future Work

In this chapter, a security storage system named ANGLE is proposed and has been implemented in FC SAN and IP SAN. The advantages of ANGLE include (1) ANGLE adopts a type of hardware encryption mode, whose encrypting speed is far higher than software encryption mode, and (2) random numbers and keys are produced by independent hardware which will provide better security. Moreover, the design of ANGLE follows P1619 International Standard.

As future work, encryption scheme at file level will be explored based on NAS. Since the concepts of Internet of Things are really popular nowadays, the way how to apply the architecture of ANGLE to intelligent mobile terminals will be investigated.

Acknowledgments This work was supported by National Natural Science Foundation of China under Grant No. 60973137, Gansu Sci.&Tech. Program under Grant No. 1104GKCA049 and the project "Cloud Storage System Based on Mobile Smart Terminal (2012)," the Fundamental Research Funds for the Central Universities under Grants No. lzujbky-2010-89 and lzujbky-2012-44, Google Faculty Award, and the National Science Council (NSC), Taiwan, under grants NSC101-2221-E-240-004- and NSC101-2221-E-126-002-.

References

1. Somasundaram G, Ahrivastava A (2009) EMC education services: information storage and management. Wiley, Hoboken
2. Osama S (2011) Storage area network implementation on an educational institute network computer networking and communication. World Comput Sci Inform Tech J 1(7):292–296
3. IEEE P1619, http://en.wikipedia.org/wiki/IEEE_P1619
4. Li CJ, Zhou QG, Liu YL, Yao Q (2011) Cost-efficient data cryptographic engine based on FPGA. In: 4th international conference on Ubi-media computing, IEEE Computer Society, Sao Paulo, 2011, pp 48–52
5. Baldwin A, Shiu S (2002) Encryption and key management in a SAN. In: 1st international IEEE security in storage workshop, IEEE Computer Society, Washington, DC, 2002, pp 35–44
6. Bonnie++, http://en.wikipedia.org/wiki/Bonnie