INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 10(4):579-592, August, 2015.

A Trusted-based Cloud Computing Virtual Storage System and Key Technologies

K.H. Wu, L. Chen, Y. Li

Kehe Wu, Long Chen*, Yi Li
School of Control and Computer Engineering
North China Electric Power University
NO.2 Beinong Road, Changping District, Beijing 102206, China
lw_ncepu@163.com, easy_cl@163.com, somethingnew1989@163.com
*Corresponding author: easy_cl@163.com

Abstract: With the popularity of Cloud Computing, people become incresingly concern about security problems, especially the data security, which has become the biggest obstacle for the development of Cloud Computing. In order to protect confidentiality and integrity of user data in Cloud Computing, this paper firstly studies the relevant research works in fields of trusted computing and Cloud Computing data protection and secondly introduces the concept of trusted into Cloud Computing data protection, presents the concept of Trusted Virtual Block Storage Device (TVBSD) and designs the Trusted Cloud Computing Virtual Storage System (TCCVSS). And then, the key technologies such as isolation, block device encryption and two-way authentication are expounded in this paper. Finally, the result of experiments shows that the system and the related technologies can not only effectively ensure the security of user data, but also control the consequent performance overhead in a proper range.
Keywords: trusted, Cloud Computing, virtual storage, cloud storage, encryption, authentication.

1 Introduction

Cloud Computing is an extension of distributed computing and grid computing technology, which offers a variety of services to customers through the network, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [1, 2]. Compared with the traditional PC service model, the Cloud Computing model provides almost limitless resources for users, which means inexhaustible, taken on demand and pay per use, and for the companies it can reduce the IT infrastructure investment and operation & support costs, so that the companies can gain the maximum economic profits.

Admittedly, cloud computing owns many merits, but it also has defects. As the computing tasks are performed in the cloud and all user data must be stored in the cloud, so the problems, such as where and how the data would be stored, are transparent to the user, which means that the user loses the absolute control over the data. Therefore, the service agreement signed between service providers becomes the only guarantee, and the confidentiality and integrity of data become the primary issues that should be considered [3, 4], and also become the biggest obstacle for the development of Cloud Computing.

In Cloud Computing there are two main data storage modes. One is distributed file system, which regard the virtual machine as a client for system storage the typical representative include GFS(Google File System) [5],Hadoop [6] and Amazon S3 [7]; and the other is virtual block storage device, the typical representative is Amazon EC2. Both have their advantages and disadvantages. The former, as its own application software must derectly minipulate user data, is difficult to guarantee the consistency of data; and the latter is more flexible, which is transparent, so that the customers can use it just as they usually use local disk, and thus the users can build their own

file systems and databases according to different needs. It not only can meet the requirements of massive digital information storage and improve the utilization of storage space, but also can shield the heterogeneity of operating system to realize storage management of automation and intelligentce, so as to better improve the quality of Cloud Computing services. Therefore, it is very significant to provide a safe and reliable data storage system and protection technologies for Cloud Computing.

Many existing data storage system has good reliability, flexibility, efficiency and ease of management performance, but it still need to be improved for ensuring data security. Though the exsiting storage system has used protecting strategies and technologies, including encryption, firewalls and rights management, it only has solved part of the security problems, which has a degree of limitation [8]. So there are still existing following problems in terms of ensuring the data safety and credibility:

(i) The problems of internal attack. using the traditional technologies such as encryption and firewalls can only defend the illegal intrusion from outer, but it is incapable to defend the internal attack. In the cloud computing model, the cloud services administrator (simply administrator for short) has many authority, if the insiders obtain the administrator privileges, he can attack the system from inside by an "legal" method, and then destroy the user data and the system. The administrator has all control permissions on the data, services, network and other important resources, so it can access to user data at any time or change the configuration file of the storage devices. Therefore, we must balance distribution of authority between the ordinary users and administrator or restrict administrators access to user data. Only in this way can we solve the problems of internal attack, and ensure the confidentiality of user data.

(ii) The problems of device management. As the characteristics of Cloud Computing, all user data are stored in the cloud, and in order to protect the confidentiality of the data, it will be stored with encrypted mode and be decrypted when using. However, as the storage device has no protection, the intruders can attack the device to obtain any data they want, and thus use attack technique the brute force attack to get the data that available to them, resulting in leakage of user data and destruction the confidentiality and integrity of data. Therefore, there is a must to practice rational management to storage device, for increasing protection measure of devices, which means to prevent attacks to the devices, so as to better prevent user data from unauthorized intrusion and tampering.

(iii) The problems of secure authentication. The following two situations can lead to the disclosure of user data: one is the storage device is remapped to the illegal users or accessed directly by the administrator; and the other is legitimate users stored their confidential data to a non-credible (illegal) storage device. In order to prevent the above situations from occurring, we must provide security authentication, through which, we can bind the storage device with legitimate user, making the legitimate users can not store data on a non-certified storage device, while the trusted storage devices can not be accessed by the unauthenticated user, that means user can only access the storage device belonging to its own. Only in this way can we completely prevent the above situations from occurring and thus can prevent data leakage.

In order to solve the above problems, this paper presents a trusted cloud computing virtual storage system based on the research of trusted computing and virtual storage technology, and the key techniques is researched and achieved. The main contributions are shown as follows:

(i) Through the study and research of trusted computing [9] and virtual storage technologies, this paper presents the concept of trusted virtual block storage devices, and then design a trusted cloud computing virtual storage systems , so as to better ensure the confidentiality and the integrity of data.

(ii) As for the problems of internal attack, this paper proposes the isolation technology, which separate the management section in user-level and the executive section in kernel of the storage

system, and then place them in different virtual machine, so that even the administrator cannot access the data directorly, only through the interfaces provided by the storage system can he manage the trusted virtual block storage device Thus, in this way it can solve the data security problems caused by administrator's overmuch operating authorities.

(iii) As for the problems of device management, this paper puts forward the block device encryption technology, which not only can encrypt the data stored in the trusted virtual block storage device, but also can encrypt the block storage device, so that only the user with the private key of the block storage device can access the device and obtain the data, while the unauthorized user cannot access it. In this way, it can avoid the illegal users obtain user data through attacking the storage devices, and thus well-ensured the security of the data.

(iv) As for the problems of secure authentication, this paper raises a two-way authentication technology, namely the user needs to authenticate the storage device whether it is a trusted one, and at the same time, the device also needs to authenticate the user whether it has access, and thus combine the user and device, making the legitimate user can only access the device belongs to its own. That is, the legitimate users can not store data on a non-certified storage device, and the trusted storage devices can not be accessed by the unauthenticated user.

(v) The effectiveness and performance of the system has been tested and analyzed, the result shows that the system and the related technologies not only can effectively ensure the security of user data, but also can control the consequent performance overhead in a proper range.

The paper is organized as follows. In section 1, we study the relevant research works in fields of trusted computing and cloud computing data protection. In section 2, we introduce the concept of trusted into cloud computing virtual storage, propose the concept of Trusted Virtual Block Storage Device (TVBSD) and design the Trusted Cloud Computing Virtual Storage System (TCCVSS), and then provide highlights of the key technologies, such as isolation, block device encryption and two-way authentication. In section 3 , we conduct test and analyze the effectiveness and performance of the system. The last section is the conclusion of the paper and gives lights to our future work.

2 Related Work

In recent years, as cloud computing technology gradually become mature, there are more and more studies on it., among which the data security become one of the crucial researches.

Some studies focus on the integrity of software load time and run time, enhancing system security by software integrity verification, so as to ensure the data security. For instance, the Seshadri [10] through memory virtualization technology can ensure that only validated code can execute in kernel mode, so as to withstand the attack to the integrity of the kemel caused by code injection and ensure system security. Xu et al. [11] propose a method based on the virtual machine monitor to detect and prevent the integrity of kemel, and hence prevent system from illeagal operating intrusion.

In addition, some studies mainly through the key management to protect the security of data. For example, Pearson et al. [12] use the anti-attack ability of TPM(Trusted Platform Module) and the hardware encryption technology to protect data encryption key, and combine the key with platform, making the key incapable to be used on the other platforms ,so as to protect the confidentiality of the data. Wang et al. [13] propose a management approach to key-used times based on trusted platform module in cloud storage, it can also control the times of using key while ensuring the safe storage of key, making the use of the key in user client controlled. Cheng et al. [14] present a novel key management scheme based on global logical hierarchical graph (GLHG), which is used to enforce correctly the global authorization policies of all users.

It can eliminates the redundant to minimize the amount of keys transferred and stored, and to maximum reduce the costs and risks of user key management.

As the trusted technology widely used in data security and platform security, there are also some research work applied the trusted technology to cloud computing to solve the credibility problem in virtual storage. Liu et al. [15] propose a new storage process of object-oriented properties in trusted storage, which can verify the QoS attributes of storage to resist a potential threat to the security and integrity of storage. However, this process only solve the trusted storage problem of physical storage device in single platform. Wang et al. [16] present a method to solve the security of data storage in virtualization platform, which is a data encapsulation method based on the properties of component and achieved by using the Trusted Platform Module (TPM). Yang et al. [17] design an architecture of cloud storage system based on TPM. This architecture used the symmetric key to encrypt data, and then used the asymmetric key to encrypt symmetric key, and finally used TPM to protect the asymmetric key. Only in this way can we manage the process of key storage, backup and share effectively.

Based on the above studies and inspirations, this paper introduce the trusted technology into the virtual storage of cloud computing, design a trusted cloud computing virtual storage system (TCCVSS), and put forward the isolation, block device encryption and two-way authentication technologies. Meanwhile, by testing and analyzing its effectiveness and performance of the system, the result shows that the system and the related technologies can effectively ensure the security of user data. The following sections describe the system architecture and key technologies in detail.

3 TCCVSS and Key Technologies

3.1 The Architecture of TCCVSS

Based on the research of trusted and storage technologies, this paper designs a Trusted Cloud Computing Virtual Storage System (TCCVSS) applied to IaaS. Each trusted virtual block storage devices (TVBSD) of the system are built on the storage resources based on hard disk and iSCSI, which can be used by multiple users but only one owner. TVBSD is a virtualization of the trusted physical storage device, which its storage space can be divided into two parts: one is a private storage space, which mainly used to store the confidential information of TVBSD, such as the key of TVBSD, the integrity measurement value, the access control list and so on; and the other is a user storage space, which mainly used to store the user data. TCCVSS is a trusted virtual storage system based on the virtualization platform framework of Xen, which inherits the functions in traditional storage system including snapshot and mirroring, and also joins the isolation, block device encryption and two-way authentication technologies, making the protection of system data more safe and reliable. Fig.1 shows the system architecture diagram of TCCVSS.

Among these, the main components are listed as follows:

(1) The TVBSD Manager Tool: Implementation of this section is based on Logical Volume Manager (LVM2), and it is mainly used to manage the logical volume, such as creating, deleting, snapshotting, mirroring and dynamic extension capabilities.

(2) The TVBSD Master: This section can be achieved on the basis of Device Mapper, which is the new component of Linux2.6 kernel and the later versions. Device Mapper provides a method to unify the ways for creating the virtual layer of block device, so it can facilitate realizes the functions including striping, tandem, mirroring and snapshots in virtual layer for users. This paper use the isolation technology, which will be discussed in later chapters, to separate this section into two parts: TVBSD Master front-end and TVBSD Master back-end, so that it can

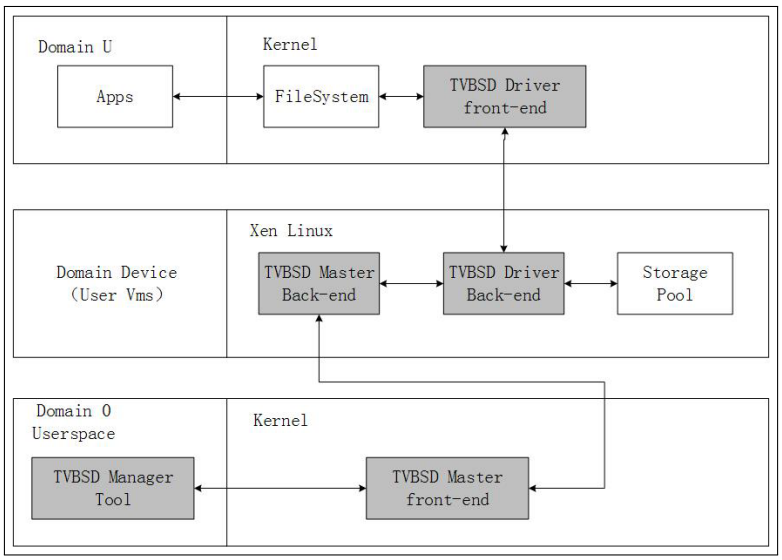


Figure 1: System Architecture Diagram of TCCVSS

effectively prevent the illegal access to data.

(3) The TVBSD Driver: This section mainly provides system security functions including access control, data encryption and user authentication, which can guarantee the confidentiality and integrity of data. The encryption and user authentication technologies will be discussed in more detail in later chapters.

3.2 Isolation Technology

In the traditional cloud computing model, the administrator has so many authority that if the insiders obtain the administrator privileges, it can attack the system from within, and then destroy the user data and the system. The administrator has all control permissions to the data, services, network and other important resources, so it can access to user data at any time and change the configuration file of the storage devices. Therefore, we must balance distribution of authority between the ordinary users and administrator or restrict administrators access to user data. Only then can we solve the problems of internal attack, and ensure the confidentiality of user data.

In the traditional virtual storage system, such as in Xen, the virtual block device (VBD) and its management tool are in the same operating system, as shown in Fig.2 by dotted box. In this way, the administrator can access the VBD directly through VBD Master Tool while the system is running, and then illegal intrude or tamper with the data stored in VBD to destroy the confidentiality and integrity of data.

In order to protect the security of user data, there is a need to prevent administrator to access the user data directly, so this paper present the isolation technology to solve this problem. That is, to divide the VBD Master into VBD Master front-end and VBD Master back-end, as shown in Fig.3. And then place the VBD Master front-end and VBD Master Tool in the same virtual machine to provide VBD management interface for VBD Master Tool; and place the VBD Master back-end in another virtual machine to receive the orders from VBD Master front-end and execute them, as shown in Fig.4 by dotted box. In this way, the executing section of VBD is separated from VBD Master Tool, so the administrator does not have permission to access the virtual machine where the VBD Master back-end resides. Therefore, the administrator can only access VBD through the interface provided by VBD Master front-end instead of accessing

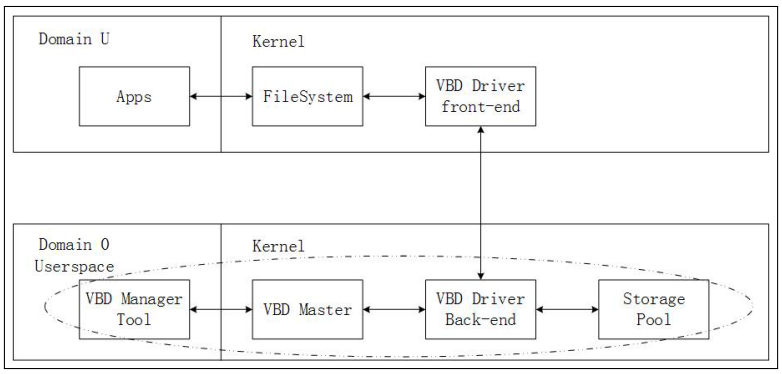


Figure 2: The Organization Chart of VBD in Xen

directly, thus ensuring the confidentiality and integrity of data.

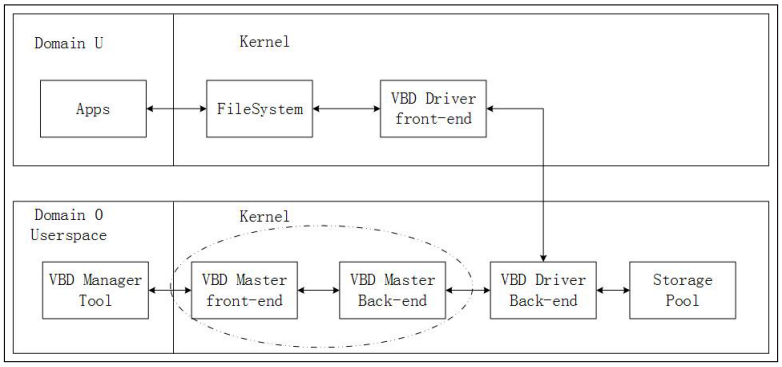


Figure 3: VBD Master Divide Into VBD Master Front-end and VBD Master Back-end

3.3 Block Device Encryption Technology

Since the characteristics of Cloud Computing, all user data is stored in the cloud, and in order to protect the confidentiality of the data, it will be stored with encrypted mode and be decrypted when using. However, due to the storage device does not make any protection, the intruders can attack the device to obtain any data they want, resulting in leakage of user data and destruction of data confidentiality and integrity. Therefore, there is a need for rational management of storage devices, to increase protection measure of devices, which means to prevent attacks on the devices, so as to better protect user data from unauthorized intrusion and tampering.

To this end, this paper presents a block device encryption technology, which means assigning a Block Device Encryption Key (BDEK) for each trusted virtual block storage device(TVBSD). During the initializing phase, the system generates a BDEK for each user, which is an asymmetric key consisted of two keys–a public key and a private key. The users own the private key themselves to protect the key from exposure to any other entity; and when the user need to store data, the system creates TVBSD according to user needs, and then the public key certificate issued to each TVBSD. The relationship between user and TVBSD is shown in Fig.5 as follows:

It can be seen from the figure that there is a one-to-many relationship between the user and the TVBSD, that is each user can have multiple TVBSD and each TVBSD corresponds to only one user. And meanwhile, each TVBSD has just one Block Device Encryption Key (BDEK), which is used to sign the data information rather than encrypt it. If we used K_{pri} and K_{pub} to

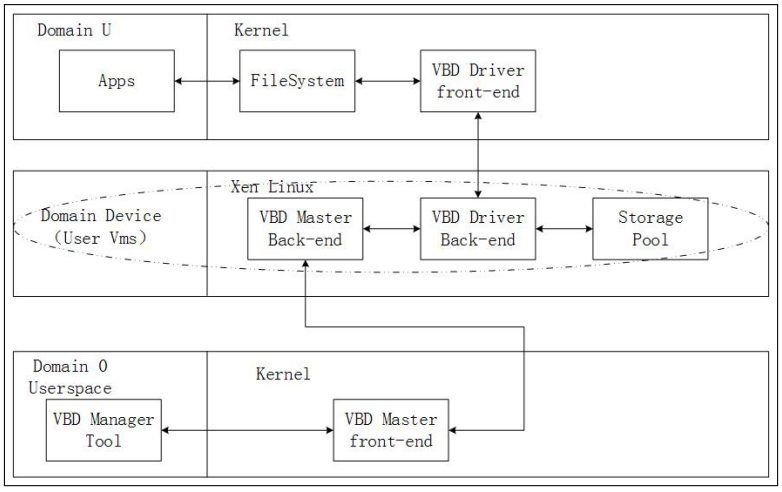


Figure 4: The Isolation Technology in TCCVSS

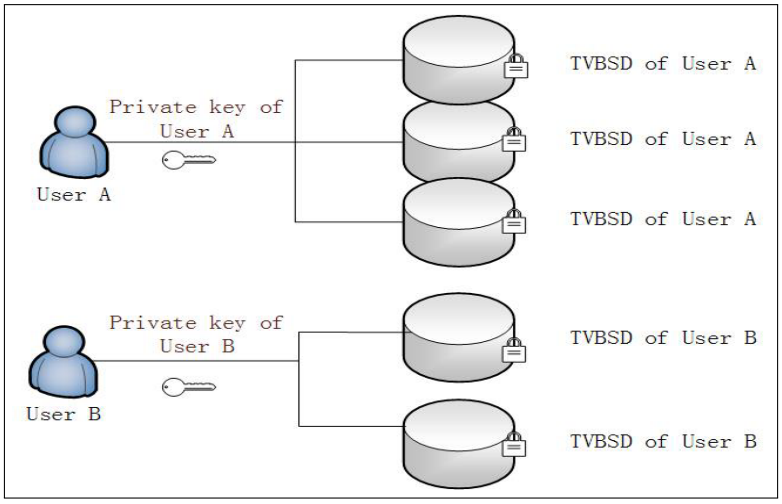


Figure 5: The Relationship Between TVBSD and User

represent private key and public key of BDEK, and used the Data to represent the ciphertext, then the data read and write operations using BDEK as shown below:

(1) Data write operation: use the public key of BDEK to sign the data, which is expressed as follows:

$$Data_1 = E(Data, K_{pub}) \tag{1}$$

where the $E(Data, K_{pub})$ means using the public key K_{pub} to sign the data $Data$, the $Data$ means the ciphertext and the $Data_1$ means the actual stored information in the block device, which is signed using the public key, and only the one who has the corresponding private key can decrypt the ciphertext to get the useful information.

(2) Data read operation: we need to isolate the information $Data$ from the signed data, which is expressed as follows:

$$Data = D(Data_1, K_{pri}) \tag{2}$$

where the $D(Data_1, K_{pri})$ means using the private key to decrypt the signed data $Data_1 = E(Data, K_{pub})$, and the $Data$ means the ciphertext. Thus it can be seen that only the one who has the corresponding private key can decrypt the data signed by the public key, so as to protect the data from obtaining by the unauthorized entities.

In summary, using the BDEK technology can prevent the unauthorized entities from accessing the TVBSD, even under the condition of the device be attacked or lost, so as to ensure the security and credibility of TVBSD and Protect the data from being invaded and abused.

3.4 Two-way Authentication Technology

The following two situations can lead to the disclosure of user data: one is the storage device is remapped to the illegal users or accessed directly by the administrator; and the other is legitimate users stored their confidential data to a non-credible (illegal) storage device. In order to prevent the above situations from occurring, we must provide security authentication, through which, we can bind the storage device with legitimate user, making the legitimate users can not store data on a non-certified storage device, while the trusted storage devices can not be accessed by the unauthenticated user, that means user can only access the storage device belonging to its own. This paper proposed the two-way authentication technology to solve the above problems, which is mainly shown in the following two aspects:

(1) Can block the storage requests initiated by the user who does not have the access to trusted virtual block storage device.

(2) Can reject the unauthorized virtual block storage device as users storage device.

In order to better complete the two-way authentication process, this paper proposed a Trusted Authentication Module (TAM) and designed three tables, namely: the user information table User_list, the trusted virtual block storage device table Tvbsd_list and the corresponding relation table of user and TVBSD is User_Tvbsd_list. Among this, the User_list is used to store the information of all authenticated users, while the Tvbsd_list is used to store the information of all trusted devices, and the User_Tvbsd_list is used to store the mapping relationship between the users and their corresponding TVBSD. The specific authentication steps are as follows:

The process of two-way authentication is shown in the following Fig.6:

(1) The user send a data storage request to TAM, including the information of user information ID_{user}, device information ID_{tvbsd} and so on.

(2) When the TAM received the data storage request:

(a) To search the user information table User_list based on the user information ID_{user}, determining whether the user is an authenticated one. If so, then go to next step; if not, then reject the user's data storage request and feedback to the user.

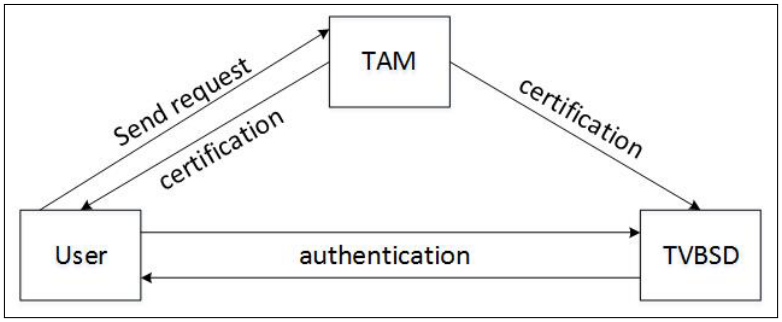


Figure 6: The Two-way Authentication

(b) To search the TVBSD table Tvbsd_list based on the device information ID_{tvbsd}, determining whether the device is an authenticated one. If so, then go to next step; if not, then reject the user's data storage request and feedback to the user.

(c) If the user and the device are both authenticated, then continue to search the corresponding relation table of user and TVBSD User_Tvbsd_list, determining whether the block storage devices users applied to belongs to users themselves. If so, then allow the data storage request and issue the certificate to the user and the TVBSD user applied to; if not, then reject the user's data storage request and feedback to the user.

(3) To establish a connection between user and TVBSD to complete the two-way authentication:

(a) User creates a timestamp T_1 and then sent it with user's certificate to the TVBDS.

(b) TVBDS creates another timestamp T_2 and calculate

$$M_1 = E(T_2||H(Data)||E(ID_{user}||T_1||T_2, K_{pubU}), K_{priT}) \tag{3}$$

then sent its certificate with timestamp T_2 and M_1 to the user. Among this, $H(Data)$ means the hash value of information in this communication, K_{pubU} means the user's public key, K_{priT} means the TVBDS's private key, and $E(Data, K)$ means encrypting the information $Data$ with the key K.

(c) To verify the TVBSD. Firstly, to decrypt the M_1 with the public key of TVBSD K_{pubT} to get the information including T_2, $H(Data)$ and $E(ID_{user}||T_1||T_2, K_{pubU})$. And then, to decrypt the $E(ID_{user}||T_1||T_2, K_{pubU})$ with private key of user K_{priU} to get the information including ID_{user} and T_1, determining whether the information we got matched the original one. If so, the user accept the TVBSD; if not, the user reject the TVBSD.

$$Verity(ID_{user}||T_1||T_2, M_1) = True \tag{4}$$

(d) The user calculate

$$M_2 = E(H(Data)||E(ID_{tvbsd}||T_2, K_{priU}), K_{pubT}) \tag{5}$$

and then sent it to TVBSD.

(e) To verity the user. Firstly, to decrypt the M_2 with the private key of TVBSD K_{priT} to get the information including $H(Data)$ and $E(ID_{tvbsd}||T_2, K_{priU})$. And then, to decrypt the $E(ID_{tvbsd}||T_2, K_{priU})$ with public key of user K_{pubU} to get the information including ID_{tvbsd} and T_2, determining whether the information we got matched the original one. If so, the TVBSD accept the user; if not, the TVBSD reject the user.

$$Verity(ID_{tvbsd}||T_2, M_2) = True \tag{6}$$

The whole procedure of two-way authentication is finished after the above steps, which can implement the binding between user and TVBSD, so as to better ensure the data confidentiality and integrity.

4 Experiments and Analysis

4.1 Validity Analysis

In this paper, we designed four experiments to evaluate the effectiveness of the system, from the perspective of the kind of attack, it can be divided into the following tests: unauthorized user access attack test, illegal equipment mount attack test, data monitoring attack test and physical device attack test.

(1) For the unauthorized user access attack test: the access of unauthorized user can be sorted into the following two situations: one is the access of illegal user without authorization; and the other is the access to the storage device, which does not belong to the authenticated user. However, in traditional virtual storage systems, take Xen for example, as administrators have too much operating authority, so both of the above users can use the administrator privileges to access to the users storage device directly, or remap the storage device to the unauthorized users, so as to obtain the users' data. While in the TCCVSS proposed in this paper, owning to the use of isolation technology, the administrator can only use the interface provided by the TVBSD Master front-end to access to the TVBSD, which prevent the administrator from accessing to the virtual block storage devices directly. Meanwhile, the Trusted Authentication Module (TAM) in two-way authentication technology can verify the identity of a user when the user initiate the request for accessing. The experiments result indicates that only the users, who can pass the validation of TAM, can establish a connection with the TVBSD, while the illegal users, who can not pass the validation of TAM, can not access to the TVBSD, so that it ensure the security of user data.

(2) For the illegal equipment mount attack test: Similar to the unauthorized user access, the access of illegal device mounts can also be divided into the following two situations: the first is the mount of equipment without authentication; the second is the authorized device mounted to the user who does not have the access to the device. In the TCCVSS, the Trusted Authentication Module (TAM) in two-way authentication technology can verify the identity of a user when user initiate request for mounting. The experiment suggests that only authenticated devices can establish a connection with user, while the illegal device would be denied by TAM, and thus ensure the security of user data.

(3) For the data monitoring attack test: In traditional storage systems, VBD management tools and VBD are in the same system, the system administrator can monitor the device's memory by installing and running various software, and can steal user data by attacking the memory. In the TCCVSS, with the use of isolation technology, the management section of TVBSD and the actual operation section of TVBSD can be isolated, so that the administrator can only access to the TVBSD through the interface provided by the TVBSD Master front-end. The result of testing indicates that the administrator is unable to install monitoring software in the equipment area where the perform section of TVBSD stayed, thereby, he cannot carry out monitoring attack to the device's memory, and thus ensure the security of the data.

(4) For the physical device attack test: In the traditional storage systems, both the attack on a physical storage device and the loss of the physical storage device may cause damage to user data. In the TCCVSS, with the use of block device encryption technology, the security of the device can be ensured. After testing, the results shows that it is difficult to steal user data by attacking the physical device in the absence of private key, and thus ensure the security of data.

The above experiments indicates that the system can perfectly ensure the confidentiality and integrity of data by using various technologies, such as the isolation, block device encryption and tw-way authentication, etc. Compared with the traditional virtual storage system, the TCCVSS has a higher level of security and reliability.

4.2 Performance Analysis

The experimental environment in this paper is as follows:
CPU: Inter Core 2 @2.7 GHz
RAM: 2GB
System: CentOS 6.4, the kernel version is 2.6.32
Platform: Xen v4.2.2
Hash function: SHA-1
Encryption algorithm: AES in OpenSSL0.9.8
Test tools: IOMeter, IOzone

In order to test the performance of the system designed in this paper, we use the test tools IOMeter and IOzone to measure the effects of this system on the performance of Xen virtualization platform.

Iometer is an I/O subsystem measurement and characterization tool for single and clustered systems. Its main functions include testing the performance of the disk and the network controllers, bandwidth and delay capacity of the bus, the throughput of the network, the performance of the shared bus, the performance of the hard drive in system level and the performance of the network in system level, etc [18]. Therefore, it can be used as a benchmark and troubleshooting tool and is easily configured to replicate the behavior of many popular applications.

IOzone is a file system benchmark tool, which can test the read/write performance of file system in different operating system. The benchmark generates and measures a variety of file operations,such as Read, write, re-read, re-write, read backwards, read strided, fread, fwrite, random read, pread, mmap, aio_read, aio_write,etc. Iozone has been ported to many machines and runs under many operating systems.

In order to better measure the performance of this system designed in this paper, we access the following three types of disk in Xen: the disk with eCryptfs, the disk with dm-crypt and the disk with TVBSD. The eCryptfs is the enterprise file encryption system in Linux; And the dm-crypt is a target driver developed based on the Device-Mapper, which mainly offers transparent encryption of block devices.

First, we use IOMeter tool to do three experiments under the same operating environment, to compare the throughput of the disk under three cases. The test parameters set as follows:

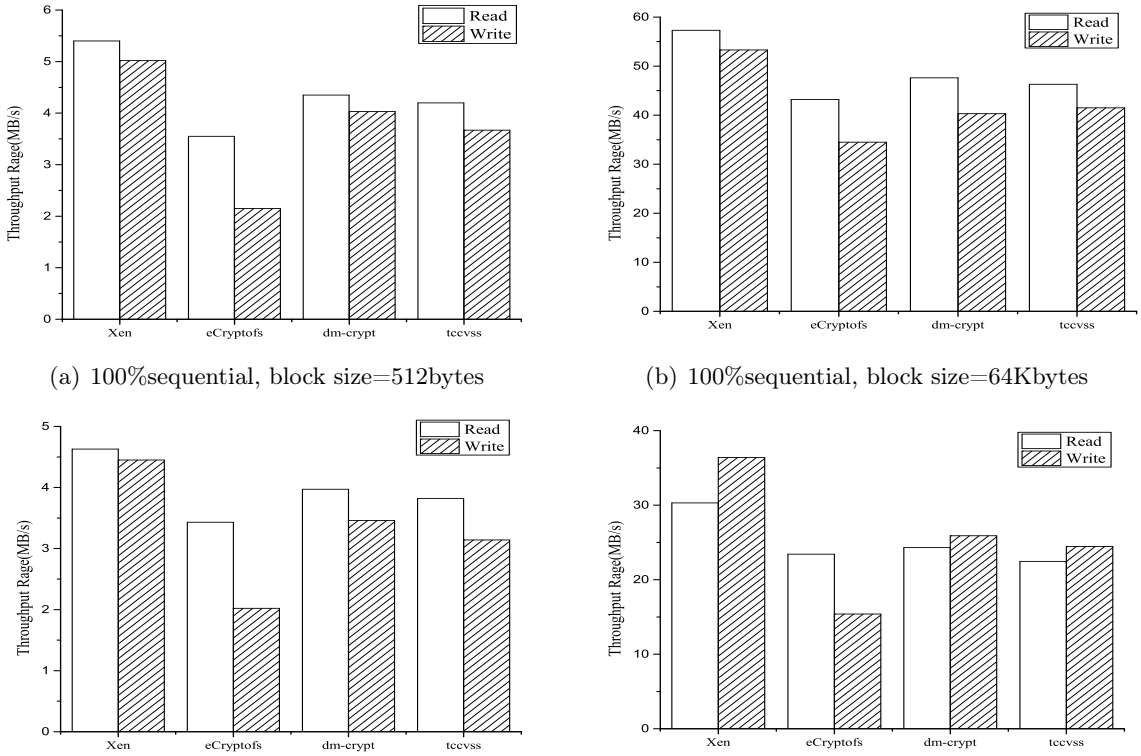
(1) The size of data block: transfer request size is set to two cases: 512bytes and 64Kbytes;

(2) The method of read and write: percent random/sequential distribution is set to two cases: 100% sequential and 100% random;

(3) The percentage of read and write: percent read/write distribution is set to two cases: 100% read and 100% write .

The result is shown in Fig.7, which is the average of multiple measurement experiments:

It can be seen that, compared with Xen system without encryption function, the read and write performance of the other three disks has a certain loss, which is caused by adding the encryption function, and thus increase the system overhead. Compared with the disk of dm-crypt, the TCCVSS only has a small portion of performance lost, which is not obvious. But compared with the disk of eCryptfs, the performance improved significantly. Meanwhile, in the case of the same block size, the throughput of sequential read and write is higher than that of random read and write.



(a) 100%sequential, block size=512bytes

(b) 100%sequential, block size=64Kbytes

(c) 100%random, block size=512bytes

(d) 100%random, block size=64Kbytes

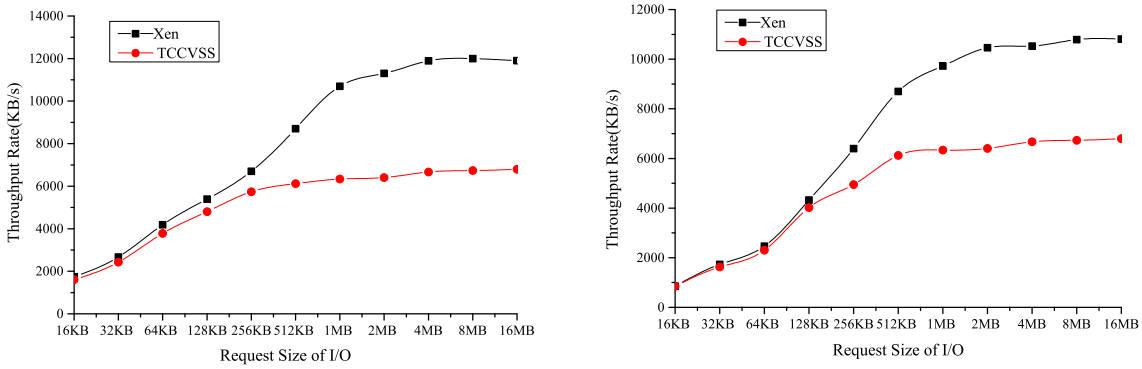
Figure 7: Throughout Evaluation

Then we use IOzone tool to measure its I/O performance being a file system server. The experiment focus on comparing the change of throughout rate of the original Xen system with that of this system under the circumstance of different I/O request size, the requested block size change from 16KB to 16MB. The results show in Fig.8:

As is shown in this Figure, with the increase of I/O requests, the system's performance gap also increase. This is because with the increase in I/O request, the time system spent in locating the file location and reading the document properties increases small, but the proportion of encryption and certification in the entire operation increases because of joining some technologies, such as the isolation, block device encryption and two-way authentication, so the CPU processing speed of encryption and authentication operations become the bottleneck of system performance, which is not obvious when the I/O request is very small.

5 Conclusion

Based on the research of the trusted computing and storage technologies, this paper introduces the concept of trusted into cloud computing virtual storage, defines the concept of Trusted Virtual Block Storage Device (TVBSD) and designs the Trusted Cloud Computing Virtual Storage System (TCCVSS), and then provides highlights of the key technologies, such as isolation, block device encryption and two-way authentication, with which can we ensure the safety of the user data in the system. We use the simulation experiments to test its effectiveness, the results show that the system can well protect the confidentiality and integrity of the user data. And



(a) The performance comparison of write operations (b) The performance comparison of read operations

Figure 8: Performance Comparison Between Xen and TCCVSS at Different I/O Request Size

the test tools, such as IOMeter and IOzone have been used to test its performance, the results show that this system, compared with other storage systems, has improved to some extent in protecting the confidentiality and the integrity of user data. However, the system loss increased due to use the technologies, such as isolation, block device encryption and two-way authentication, resulting in a performance degradation within a reasonable range. In addition, because the system is designed in an ideal experiment environment, there are many problems need to be solved in the practical application, so the further work is to improve the performance of the system under the condition of ensuring the confidentiality and integrity of user data, and to implement a more safe and reliable cloud computing virtual storage system, which can be suitable for practical application scenes.

Bibliography

[1] B. Tograph, Y.R. Morgens (2008), Cloud computing, *Communications of the ACM*, 51(7): 9-11.

[2] A. Weiss (2007), Computing in the clouds, *Network of ACM*, 11(4): 16-25.

[3] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica (2009), Above the clouds: A Berkeley view of cloud computing. *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS 28, 13. 2009.*

[4] J. Heiser, M. Nicolett (2008), Assessing the security risks of cloud computing. *Gartner Report.*

[5] http://labs.google.com/papers/gfs.html.

[6] http://hadoop.apache.org/.

[7] http://aws.amazon.com/s3/.

[8] U. Kűhn, K. Kursawe, S. Lucks, A.R. Sadeghi, C. Stűble (2005), Secure data management in trusted computing, *In: Cryptographic Hardware and Embedded SystemsCHES 2005: Springer*, 324-338.

[9] C. Shen, H. Zhang, H. Wang, J. Wang, B. Zhao, F. Yan, F. Yu, L. Zhang, M. Xu (2010), Research on trusted computing and its development. *Science China Information Sciences*, 53(3): 405-433.

[10] A. Seshadri, M. Luk, N. Qu, A. Perrig (2007), SecVisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity OSes, *ACM SIGOPS Operating Systems Review*, 41(3): 335-350.

[11] M. Xu, X. Jiang, R. Sandhu, X. Zhang (2007), Towards a VMM-based usage control framework for OS kernel integrity protection. *In: Proceedings of the 12th ACM symposium on Access control models and technologies: ACM*, 71-80.

[12] S. Pearson, Y. Shen, M. Mowbray (2009), A privacy manager for cloud computing. *In: Cloud Computing: Springer*, 90-106.

[13] L. Wang, Z. Ren, Y. Dong, R. Yu, R. Deng (2013), A management approach to key-used times based on trusted platform module in cloud storage. *Jisuanji Yanjiu yu Fazhan/Computer Research and Development*, 50(8): 1628-1636.

[14] F. Cheng, Z. Peng, W. Song, S. Wang, Y. Cui (2013), Key management for access control in trusted cloud storages, *Jisuanji Yanjiu yu Fazhan/Computer Research and Development*,50(8): 1613-1627.

[15] L. Zhaobin, Q. Wenyu, L. Keqiu, F. Ruoyu (2009), Object oriented property attestation for trusted storage. *In: IEEE 9th International Conference on Computer and Information Technology, CIT 2009, October 11, 2009 - October 14, 2009 Xiamen, China: IEEE Computer Society*, 93-97.

[16] D. Wang, D. Feng (2010), A hypervisor-based secure storage scheme. *In: 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC 2010, April 24, 2010 - April 25, 2010 Wuhan, Hubei, China: IEEE Computer Society*, 81-86.

[17] X. Yang, Q. Shen, Y. Yang, S. Qing (2011), A way of key management in cloud storage based on trusted computing. *In: 8th IFIP International Conference on Network and Parallel Computing, NPC 2011, October 21, 2011 - October 23, 2011 Changsha, China: Springer Verlag*, 135-145.

[18] J. Chen (2011), Design and Implementation Volume-Based Hierarchical Storage System. *Huazhong University of Science & Technology.*