An SLA based SaaS Security Level

Yongjing A. Li*, Jiang B. Wu
College of Information Science and Technology, Northwest University, Xi'an, China
*Corresponding author, e-mail: liyongjing315@126.com,wuj622@yahoo.com.cn

Abstract

This paper proposes a data security protection strategy of the SaaS mode ----- the SLA based SaaS Security Level. At the same time, it gives concept model and implementation architecture of the security scheme which based on the SaaS Security Level. The SLA based SaaS Security Level takes the requirements of tenants to the data security as a starting point, and it mainly relates to data security of the data center, data security of the servers and data security of the clients. This Security Level can better meet diversified users needs than the traditional security model. According to the tenants desired service number and the protection degree of data information, they can dynamically select different levels of the security strategies. Then, according to the dynamic changes of SLA, the SaaS vendors can adjust data protection strategy of the user timely. For supporting our SaaS Security Level, we build SSM (SaaS Security Model) test-bed. On the SSM test-bed, we have done some experiments, which confirmed our SaaS Security Level is feasible and easy to use.

Keywords*: data Security, SaaS Security, SaaS Model, SaaS Level, SLA, test-bed*

1. Introduction

The SaaS mode brings a favorable turn for the work and thinking mode of people. At the same time, it brings huge safety hidden troubles, which mainly dues to that it requires all the relevant data of the tenants to be stored in the data center provided by the vendors, making the exclusivity, reliability and security of enterprise data to face great risks. Worrying about the data security of the tenants has become a biggest barrier of promoting and developing the SaaS applications[1-2].

High Security means high cost. In the practical application, a SaaS system needs not provide high cost and high level security for all the tenants. So providing separated security services for the tenants to select an approving level of security services may be a solution for the SaaS security.

SLA (Service Level Agreements) is a legally binding contract signed between service providers and customers, the contract stipulates the commerce clause both sides in the service delivery process [3]. The citation [4] pointed out that SLA was main means that measures service level, and it provided a method for the service providers to attract customers. By promising to provide the determinate service level and give compensation once not meet the commitment, the providers can establish new business relationships with customers. According the service level and quality of services and other details, the service providers and service users sign the SLA contract, and the SLA contract has been widely used in cloud computing and other industries.

Therefore, using SLA into the SaaS mode to assign the responsibility, obligation and service requirements between SaaS vendors and the tenants, to solve the possible problems and contradictions of the two parties, to protect their own interests is feasible. At the same time, the SLA can facilitate the billing and payment of the SaaS mode of purchasing on-demand.

This paper's viewpoint is that SaaS operation mode is secure. Merely, at present, there is not a suited way to make the tenants be sure of that. To solve this issue, this paper studied a SLA based SaaS Security Level for the tenants to make a choice based on their security needs.

Received February 15, 2013; Revised May 2, 2013; Accepted May 15, 2013

The rest of this paper is structured as follows. Section II describes the related studies. Section III presents our SaaS security solution, which includes the SaaS Security Level based on the SLA, the SaaS Security Concept model and the key technologies of the SaaS Security Level. And then, in Section IV, we implement the SSM (SaaS Security Model)test-bed. On the SSM test-bed, we do some experiments to check our SaaS Security level in different aspects. Finally, Section V concludes the paper and introduces the future works we will do on the SaaS security.

2. Related Work

How to protect the data security of SaaS tenants has haven some research findings. The quotation [5] did a survey on security issues in service delivery models of cloud computing. The paper detailedly addressed some key security elements which should be carefully considered as an integral part of the SaaS application development and deployment process viz., Data security, Network security, Data locality, Data integrity, Data segregation, Data access, Authentication and authorization, Data confidentiality issues, Web application security, and so on.

The paper [6] proposed a scheme to ensure sensitive data safety by taking advantage of encryption and signature technique for capturing valid evidence when service provider embezzling or responsibility confirmation in management-type SaaS. And in the scheme, they used non-credible PKG of identity based signature mechanism as signature mechanism for sensitive data, so that ensures the confidentiality, integrity and non-repudiation of sensitive data.

The paper [7] adopted further separation of the users' data in SaaS mode which allowing tenants to choose another unrelated third-party to provide database services. In this solution, the simple user interface allows user to update the component code of database access through easy operation. So that service providers or software developers haven't a chance to operate the users' privacy data. Have to say, this method can protect the users' private data from being leaked by the service vendors, but the method required the user have certain fundamental programming ability, so it cannot be suitable for all of the tenants.

The paper [8] proposed a user customized data protection framework that enabled users to select the manner in which their sensitive information is protected. Their framework consisted of users, service providers, a rule repository and program conversion services. The policies for the protection of sensitive information are provided as a SaaS service; a rule repository stores protection policies; a program conversion service provides a service for creating a customized program from an original program according to a protection policy. By allowing a service provider to use their sensitive information through this program, users can protect their sensitive information according to the manner chosen by them. Although their framework based on the user selections to protect the user's information is similar with our SaaS Security Level. It focused on the rule repositories and program conversion services, which is different from the SaaS Security Level that based on the SLA.

There are also some other strategies having been proposed to protect the security of user data. The paper [9] presented a solution that store the data encrypted by the client's public Key on Server so that protected the data is abused by server administrator. An Information Systems Continuance Model was proposed by the study [10], and adopted privacy and security compliance as a new construct of interest. Based on information dispersal approach, combining with data fragmentation, the paper [11] presented an effective and flexible data obfuscation scheme DOSPA (Data Obfuscation of Single Privacy Attribute) for single attribute data privacy protection in SaaS.

The SaaS operation mode is one delivery method of Cloud Computing, so some known delivery methods of Cloud Computing which protected the user data have reference value to the SaaS model[12]. Such as, a dynamic intrusion detection system which dispatches numbers of intrusion detectors on the whole topology of the networking system [13], a mechanism for achieving maximum security by leveraging the capabilities of a processor called a cryptographic coprocessor [14], and so on.

Our SaaS Security Level is not only based on the requirements of the tenants to the data security but also the SLA, so we should not only know the data security preventive strategies of SaaS mode, but also the SLA.

Nowadays, many of SLAs are based on the SLA management manual of TMF (Telecommunication Management Forum), and different SLA realization models have different emphasis. Some SLAs center around user, focusing on the issues which the user concerned, while some others focus on the monitoring of the network. The paper [15] put forward some security issues that have to be included in SLA, so that it can help some of the enterprises to look forward in using the cloud services. Internationally, the typical SLA model which centers on users is Amdocs Service Level Agreement Blueprint, and the typical SLA models which focus on the network are Micromuse’s Netcool Suite and Orchestream’s Resolve Product Suite [16]. The paper [17] came up with the SLA model of the Cloud Computing, and then overviewed the model, and then brought in Proxy Mechanism, but the authors neither analyzed the model of SLA specifically nor mentioned how to protect the security of the user data.

The paper [18] presented a general SaaS architecture for scientific software that offers an easy-to-use web interface. Scientists define their problem description and the QoS requirements, and then they can access the results through the portal they created. They also proposed the algorithms to autonomously test the feasibility of the SLA. It main emphasized the optimization algorithm of the SLA to enhance the efficiency of the resources, but the keystone of our paper lies on the security model based on SLA to protect the user data.

The citation [19] put forward a SLA performance management model of SaaS application. The model based on the quantification of SLA parameters, and can do the real-time performance monitoring and multiple levels of performance optimization. By monitoring the tenant services quality, the model can discover abnormal state and then use scheduling algorithm to adjust situation of the resource used by the tenants dynamically, thereby effectively protect the implementation of SLA performance indicators, but the model just only meets the changes of certain SLA performance index, cannot reflect how the vendors defense the problem of data security which the tenants are most concerned about.

The paper [20] introduced an application model so that customers can model their own service level according to their individual business needs, which is different from many existing approaches that only allow the customer to choose between a small set of predefined service levels. The authors determined the QoS requirement of a component by disaggregating the QoS requirements stated in the SLA, so this is a progress towards a more business-driven provisioning of SaaS application. However, the disaggregation relies on human experience. The method doesn’t consider of the user's data security issues.

3. SLA Based Saas Security Model

Traditional security generally includes encryption, digital signatures, public key infrastructure, firewall, authorization control interview, and so on. Existing SLA application approaches mainly focus on the QoS (Quality of Service), performance management, responsibility divided, profit distribution, etc. In this paper, using SLA for security management helps to cope with the situation that the tenants want to select their satisfying service level according to their individual business needs and data security requirements in the SaaS application.

3.1. SLA Based SaaS Security Level Partition

According to the security solutions, this paper make the SaaS Security Level be divided into four levels, which are D(Public Security, the vendors must take some measures on this level), C(Fully Commissioned, in this level, we assume that the tenant completely trust the SaaS vendors), B(Partial Autonomous Control, in this level, we assume that the tenant part of trust the vendor, and it can do some work to protect their information), A(Fully Autonomous Control, the tenants just use the services provided by SaaS vendors but protect their information by themselves).

The D level only includes D. The C level is divided into four groups which are C1, C2, C3 and C4. The B level includes B1, B2 and B3. The A level is made up of A1, A2, A3 and A4.

The SaaS Security Level is described detailedly in the Table1. The reliability and confidence level of every level increases gradually from D to A as well as from A1 to A4 in A level.

Table 1 The Saas Data Security Level Based On The Sla

Security Level		Definition
A:Fully Autonomous Control	A4：	Tenant deployment
	A3：	Independent Physical Machine
	A2：	Third-part Security Services
	A1：	Tenant controlled Virtual Machine
B:Partial Autonomous Control	B3：	Client Encryption
	B2：	Tenant Encryption of the Server
	B1：	Vendor Encryption of the Server
C:Fully Commissioned（Only DBMS Technology）	C4：	DBMS Isolation
	C3：	Database Instance Isolation
	C2：	Schema Isolation
	C1：	Shared Table, DBA and Management separated authorization
D:Public Security		Others

- **D Level: Public Security——the lowest level.**

Whether traditional software or software provided by the SaaS providers, it is necessary to have the most basic security measures to ensure the safety and availability of the software. In the network, the network operators must use some security strategies to protect user information from being attacked by the hackers in the transmission process. They commonly use methods with SSL, HTTPS, etc. And as for the software maintenance personnel, adding firewall, installing antivirus software and regularly checking virus are the most basic operations. At the same time, service operators should have good communication with local government, only according with the local policies and regulations, and acquiring the approval of local government, the enterprises can operate successfully.

- **C1 Level: Shared Table, DBA and Management separated authorization**

For SaaS multitenant, many tenants using the same set of tables, and the tenant can contact its attributions with itself by the tenant ID. The paper [21] presented application level access control and DBMS level access control two kinds of mechanisms to access the shared table. Meanwhile, the DBA and the Management are authorized respectively. By using C1 Level, each database server can support the most tenants data, thus the cost of hardware and backup is lowest. However, when the data amount of shared table is too large, it will affect the speed of data query, and also the data recovery time will be longer[22]. At the same time, a number of tenants share the same database, which has many safety loopholes. For example, a tenant can easily accesses to other tenants' information in the same table, and then leaks data, so it belongs to elementary security protection measures of the data security. This scenario is suitable for not important or ostensible business information, or the tenants are willing to sacrifice data isolation so that reduce the cost.

- **C2 Level: Schema Isolation**

A number of tenants share the same database, but each tenant has its own set of tables, and each SaaS tenant's information was separated from others via the schema. This scenario is easy to implement, low cost, and also convenient for extending the data model. However, once fault occurs, regardless of whether the tenants' data have problems, the DBA must recover the data of each tenant in the database by the backup data, which increases a lot of unnecessary work, certainly will increase the data recovery time. This scenario is suitable for the applications whose database tables are relatively few, or suitable for the tenants who are willing to put their data with other tenants' data in the same database.

- **C3 Level: Database Instance Isolation**

Each tenant of the SaaS applications has its own independent database, so as to achieve the effective isolation of data, and enhance the data security of the tenants. At the same time, simplify the extension of application data. When a breakdown happened, it is convenient for recovery. However, this scenario will increase the costs of equipment maintenance, hardware and multi-tenant data backup. So the C3 Level is more suitable for particularly high data security requirements, or suitable for the enterprises that are willing to spend high maintenance costs on the commercial confidential data.

- **C4 Level: DBMS Isolation**

Different SaaS tenants respectively have a set of independent DBMS, which can achieve data isolation absolutely and is safer than Instance isolation. The DBMS Isolation is similar to the traditional software. Merely, traditionally, the enterprises deploy their DBMS in their company, and the tenants rent the DBMS and services to share computing resources and application codes. Comparing with other scenarios in the C group, the C4 Level needs the highest management cost and the biggest hard disk space. Therefore, the cost is higher than others.

- **B1 Level: Vendor Encryption of the Server**

According to the requirements of different tenants for data security, data can be transmitted from a client to a server with plaintext transmission or encrypted transmission. To transmit by a encrypted way, service providers cannot see the tenants' data, so it is relatively safe. While, in plain text transmission, service providers can see the tenants' data, so it exists certain security risks. But the service vendors can use asymmetric encryption to encrypt tenants' data, and then store the encrypted data in the database. The decryption private key is safeguarded by the tenants, which can effectively prevent database administrator of the server to peep commercial data of the tenants.

- **B2 Level: Tenant Encryption of the Server**

The tenants can encrypt their commercially sensitive data in the server-side. Although the encryption algorithm of the server-side, the encryption process was completed by the tenants, and the service providers cannot see the tenants' data, so the safety is taller than B1. However, the data is transmitted by a plaintext form from a client to a server, so the process has a potential risk that the plaintext can be intercepted by the hackers. Therefore, in the Internet transmission process, in order to ensure data security, the data should be divided into fragments [14].

- **B3 Level: Client Encryption**

The tenants encrypted data in the client, and then transmitted the data over the network to the SaaS server, and the SaaS server saved the data to the data center. In this progress, the service vendors cannot look up the tenants' data. The B3 Level can prevent data leakage in the network transmission. At the same time, this scenario effectively prevents the DBA from peeping the business data of tenants. However, this scenario is the most complex and most difficult to implement, so the technique cost is very high. And the commonly methods of the client encryption include symmetric encryption, asymmetric encryption algorithm and the hybrid encryption algorithm.

- **A1 Level: Tenant Controlled Virtual Machine**

In the SaaS applications, the tenant can rent an independent virtual machine to run their application and database, and the virtual machine should be controlled by the tenant, but the virtual machine is deployed by the service vendor.

- **A2 Level: Third-party Security Services**

In the SaaS applications, the tenants can rent or buy the third-party security services to protect their data. They can rent or buy encryption algorithms and database services. These data encryption algorithms can be delivered in the SaaS mode, an interface or other ways. By this way, the SaaS vendors don't know the specific method of the data encryption chosen by the tenants so that the vendors can't snoop the encrypted data of the tenants. Meanwhile, the third-party only provides the encryption methods so that it has not chance to access the tenants' data. By using the database services, the tenants can use the application from A vendor and store their data in B vendor to protect the data security of the tenants, just like the paper [9] has done.

- **A3 Level: Independent Physical Machine**

In the SaaS applications, the tenants can rent an independent physical machine to run their application and database and the physical machines locate in the server-side, which is similar with the A1 Level. The difference between A1 Level and A3 Level is that the tenants hold the keys of the physical Machines and physical machine is more secure but the cost is higher.

- **A4 Level: Tenant Deployment**

The tenants can rent the SaaS applications through the SaaS vendors, while, they install and deploy the independent database in their own house, and manage the DB by their own IT staffs or the service vendors. If they want to enhance the data security, they can choose the right security level strategies from C(C1, C2, C3, C4), and then create their own data security protection measures. This scenario is the safest and reliable, but the tenants should have their own server and security personnel, so the required security cost is the highest.

3.2. the Techniques distribution of the SaaS Security Level

In the SaaS Security Level, the SaaS vendors adopt different techniques for different groups to protect the security of the user information. The Figure1 shows the techniques distribution of the SaaS Security Level. The brown rounded rectangles stands for the fundamental techniques of data security, and the bright green rounded rectangles which the tenants can choose or not represent the enhanced techniques of data security.

The X axis shows where the tenants' data is located, including Data Server, Application Server and Client-side. The Y axis indicates the security of each group, which is safer and safer from D level to A level.

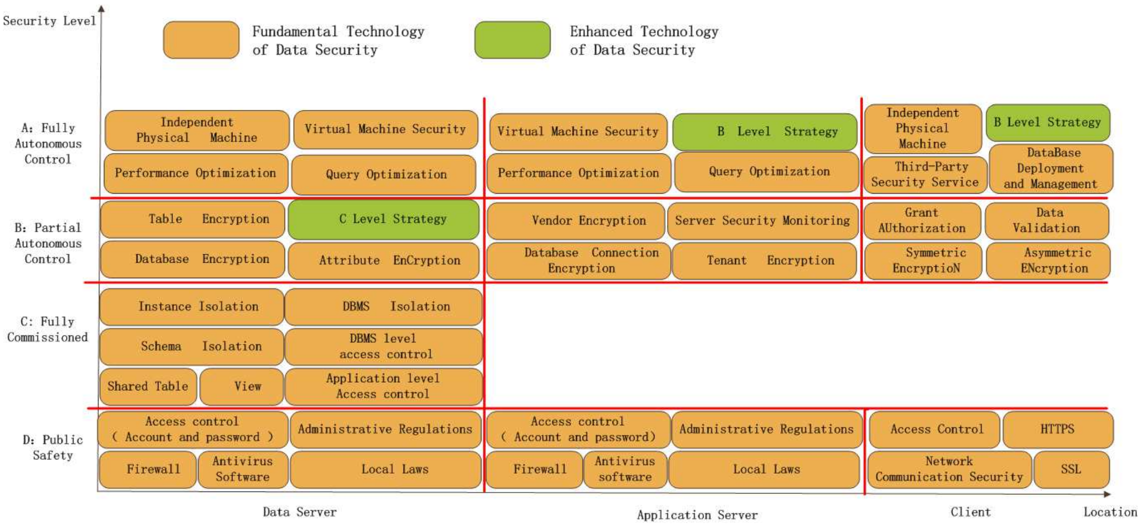


Figure 1 The Techniques Distribution of the SaaS Security Level

The D level is public safety, which only makes up of the most basic strategies, such as firewall, antivirus software, local laws, access control, administrative regulations, and so on. These have to be done not only by the Data Center, but also the server-side. Meanwhile, the Network Operators have to adopt some secure strategies, such as SSL, HTTPS, Access Control, and so on, to protect the data safety in the network transmission.

The C level is Fully Commissioned. The strategies all focus on the DBMS. The usually methods have Shared Table, View, Schema Isolation, Database Instance Isolation, DBMS Isolation, Application Level Access Control, DBMS Level Access Control, and so on. The tenants can choose the suitable methods from the C level to protect their data.

The B level is Partial Autonomous Control, which is divided into three parts. The first part is Data Server, from which the tenants can choose Table Encryption, Database Encryption and Attribute Encryption to protect their data. If the tenants want to enhance the security of their data, they can choose some strategies from the C Level. The second part is Application Server. There are many security strategies for the tenants to choose, such as Vendor Encryption of the Server, Tenant Encryption of the Server, Database Connection Encryption, and Server Security Monitoring, and so on. The third part is Client-side, including Grant Authorization, Data Validation, Asymmetric Encryption, Symmetric Encryption, and so on.

The A level is Full Autonomous Control which is similar with the B level to have three parts. The Application Server part and the Client part can choose B Level Strategies, and each part can choose different methods. For example, the Data Server can choose one or more from Virtual Machine Security, Independent Physical Machine, Query Optimization and Performance Optimization. The Application Server can choose the security strategies from Virtual Machine Security, Query Optimization, and Performance Optimization. The Client-Side can choose Independent Physical Machine, Database Deployment and Management and the Third-Party Security Service.

3.3. The SaaS Security Concept Mode

In the Figure2, the SaaS Security Concept Model is divided into five sections. Different section has different emphasis. All of them are interdependent to protect data security of the tenants.

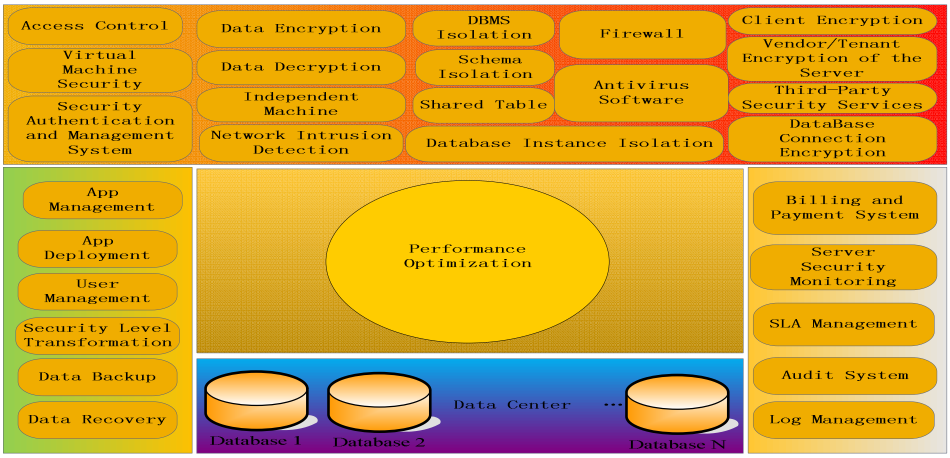


Figure 2 The SaaS Security Concept Model

The first section is Data Center which is used to store the data information of the tenants and the vendors, to record the operational logs, SLA context, the monitoring information, and so on, meanwhile, to support the other sections. The Data Center consists of many Databases.

The second section is some systems which are basic operating functions. Such as App Management for the vendors to manage the application chosen by the tenants, and App Deployment for the vendors to manage the services provided by the Service developers. User Management for the vendors to manage the SaaS services users. Meanwhile, the second section includes the Security Level Transformation for changing the security level of the tenants' data, Data Backup, Data Recovery, etc.

The third section is some strategies to enhance the data security of the tenants. These strategies mainly include Access Control, Data Encryption, Data Decryption, Virtual Machine Security, Security Authorization and Management System, Independent Machine, Data Isolation, Data Encryption and so on. Among them, the Firewall can strengthen the safety supervision, effectively record the Internet activities, refuse suspicious access, and so on.

The fourth section is some management tools to support the SaaS Security Level based on the SLA. The Billing and Payment System can be used to solve the economic problems when the tenants rent the services provided by the vendors. Third-Party Security Service can be chosen by the tenants to encrypt the tenants' data or store them in another vendor's data center so that the service vendor cannot peep the tenants' data. SLA Management for the vendors and the tenants to manage the conventions of the two parts on data security, QoS, responsibility, profit, and so on. The Network Intrusion Detection and the Security authentication and Management System can efficiently prevent hackers and illegal users access to the tenant's data lawlessly. The Security Monitoring can monitor the actions of the vendors and the tenants. Audit System can enhance the security of the SaaS services and reliability of the services.

The fifth section is certain optimized schemas to enhance the data security of the tenants. The Performance Optimization can make the server-side more reliable.

4. THE SSM TESTBED

This section describes the SSM(SaaS Security Model) test-bed we have developed for experimenting with SaaS Security Model.

For preventing the hidden troubles of the Network transmission, the tenants can firstly encrypt their data in the Client and then transmit them. When the servers receive the data, the data has been encrypted, so they cannot look up the tenants' data. The concrete realization of the process is followed by the Figure3.

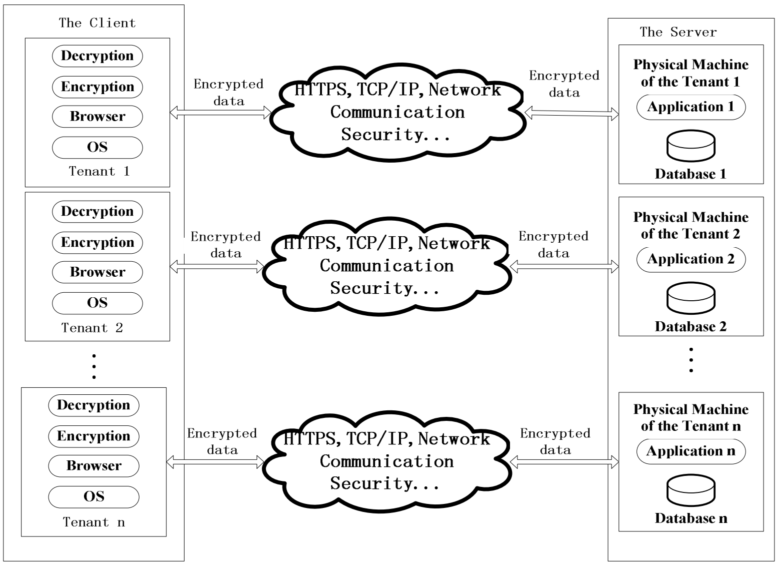


Figure 3 The Client Encryption

According the Figure3, we do a set of experiments about the Client Encryption on our SSM test-bed.

The SSM test-bed's system environment includes as follows:

1) OS: Microsoft Windows XP Professional (5.1 version 2600) ;
2) BIOS:08.00.15.LENOVO ;
3) BIO SRev: 5HKT38A01.0.2009.0505.163422;
4) Processor: Intel(R) Core(TM)2 Quad ;
5) CPU: Q8200 @ 2.33GHz(4 CPUs);
6) Memory: 3072MB RAM.

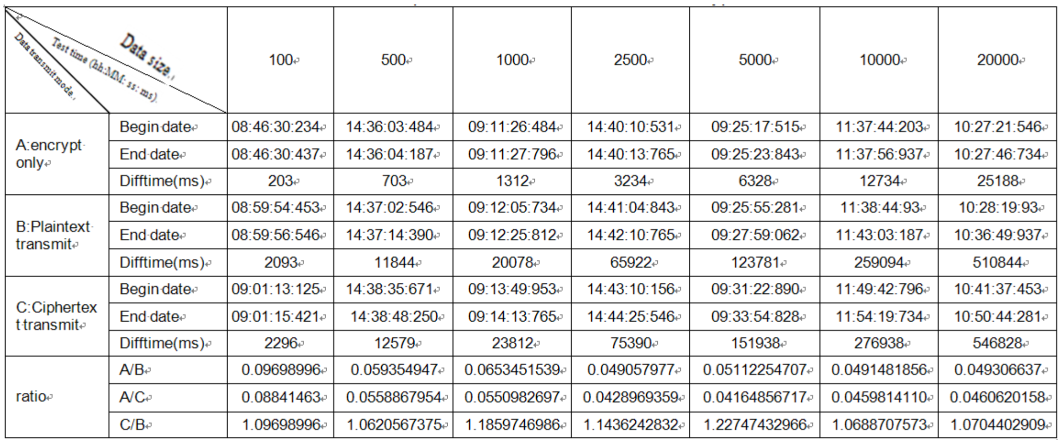
The SSM test-bed's Operating Environment includes as follows:

1) Web application server: apache-tomcat-6.0.20
2) Database: Mysql5.1
3) Myeclipse8.5, jdk1.6.0
4) Flash Builde4.6

In this experiment, we do three aspects of the test, they are respectively stated as followed:

1) Encryption only: we just get encryption time.
2) Plaintext transmition: we get transmit time of user's login accounting and password from client to the database.
3) Ciphertext transmition: we encrypt user's login accounting and password, by the way, you can encrypt other information which you think is important. And then the client transmit the ciphertext to the server and stores them. We get the time cost of the whole process. The experimental data are shown below Table 2.

Table 2 the experimental data of the Client Encryption



Data size / Test time (hh:MM: ss: ms) / Data transmit mode		100	500	1000	2500	5000	10000	20000
A:encrypt only	Begin date	08:46:30:234	14:36:03:484	09:11:26:484	14:40:10:531	09:25:17:515	11:37:44:203	10:27:21:546
	End date	08:46:30:437	14:36:04:187	09:11:27:796	14:40:13:765	09:25:23:843	11:37:56:937	10:27:46:734
	Difftime(ms)	203	703	1312	3234	6328	12734	25188
B:Plaintext transmit	Begin date	08:59:54:453	14:37:02:546	09:12:05:734	14:41:04:843	09:25:55:281	11:38:44:93	10:28:19:93
	End date	08:59:56:546	14:37:14:390	09:12:25:812	14:42:10:765	09:27:59:062	11:43:03:187	10:36:49:937
	Difftime(ms)	2093	11844	20078	65922	123781	259094	510844
C:Ciphertex t transmit	Begin date	09:01:13:125	14:38:35:671	09:13:49:953	14:43:10:156	09:31:22:890	11:49:42:796	10:41:37:453
	End date	09:01:15:421	14:38:48:250	09:14:13:765	14:44:25:546	09:33:54:828	11:54:19:734	10:50:44:281
	Difftime(ms)	2296	12579	23812	75390	151938	276938	546828
ratio	A/B	0.09698996	0.059354947	0.0653451539	0.049057977	0.05112254707	0.0491481856	0.049306637
	A/C	0.08841463	0.0558867954	0.0550982697	0.0428969359	0.04164856717	0.0459814110	0.0460620158
	C/B	1.09698996	1.0620567375	1.1859746986	1.1436242832	1.22747432966	1.0688707573	1.0704402909

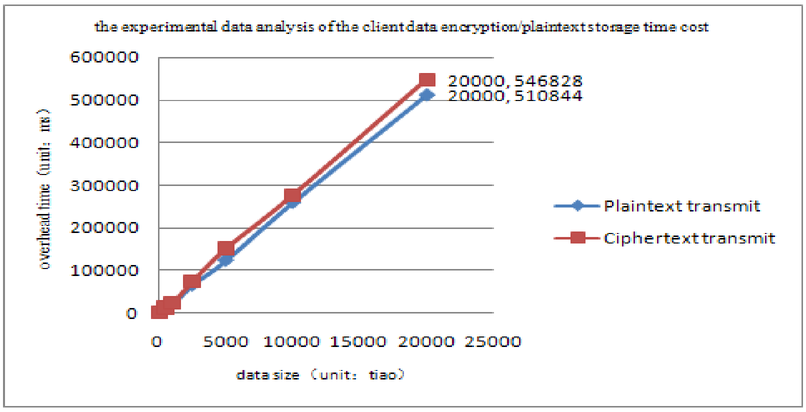


Figure 4 The experimental data analysis

With the experimental data of the Table 2, we can draw a line charts as Figure4, which analyses the client data encryption and plaintext storage time cost. According Figure4, we cannot read the information clearly between 100 and 2500, so we draw Figure6 to show the relation between plaintext transmit and ciphertext transmit from 100 to 2500. On the basis of analysing TABLE II, Figure4 and Figure5, we can gain some explicit conclutions.

Firstly, through our SSM testbed, the client encryption is feasible.

Secondly,when the data volume belows 500 record, no matter you transmit the plaintext or Ciphertext, the time cost is very close. And when the data volume is more than 1000, the time cost of Ciphertext transmit is more and more than plaintext transmit.

Thirdly, when we choose the client encryption, the time cost of the data encryption on the whole of data storage time ratio is very small. If we want our information safer, it is worth costing little time for data encryption.

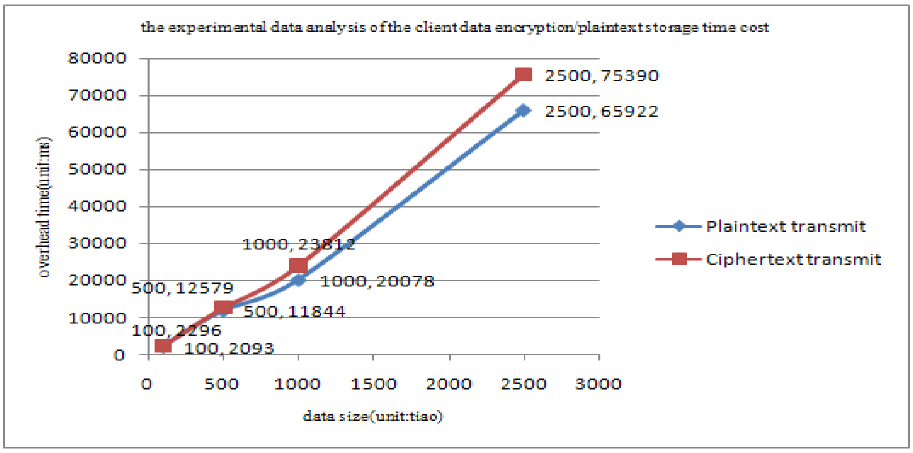


Figure 5 The detailed experiment data from 100 to 2500

5. Conclusion and Future work

Based on SaaS data security and the tenants' requirements about enterprise data security, this article studied on the traditional SLA, and then put forward SLA based SaaS Security Level, according to the tenants' requirements on the data security, this Security Level is divided into 4 levels and then refined 12 levels. Firstly, the paper detailedly described the security strategy -----the SaaS Security Level based on the SLA, the advantages and disadvantages of every level of each group, then gives some key technologies of every group in the data center, server and client, so that the tenants can choose suitable security strategies according to their actual situation. At the same time, it proposed a SaaS Security Concept Model based on the SaaS Security Level. At last, We created a SSM test-bed to do some experiments to verify validity and feasibility of the SaaS Security Level.

In the SaaS applications, the service quality committed by the SaaS vendors cannot solely insure through a SLA contract, but the SLA management mechanism to guarantee. Therefore, the next step, based on the SaaS Security Level having been proposed, our further research will focus on the SLA management mechanism of the SaaS applications.

Acknowledgments

This work is supported by grants from the key project of teaching reform plan in Northwest University.

Part technologies of this paper are applied to the project that oil Well-logging equipment and digital oilfield construction of generic technology research (Project Number: CXY1132), which is one of Xi'an technology plan (industrial application technology research and development project).

In the prophase of this work, Bin Wang, YuFei Wang, and ShengCao Han help us a lot. They all come from College of Information Science and Technology of Northwest University, and we express our heartfelt gratitude to them.

References

[1] Wang X, Jin X, Fan L, et al. *Meta-service Design and Implementation for Content Delivery Network Cloud Environments*. TELKOMNIKA Indonesian Journal of Electrical Engineering, 2012, 10(7): 1833-1842.

[2] Sun H, Chen S, Xu L, et al. *Base-on Cloud Computing A new type of distributed application server system design*. TELKOMNIKA Indonesian Journal of Electrical Engineering, 2012, 10(7): 1800-1807.

[3] John JLee, Ron BenNatan. Integrating *Service Level Agreements: Optimizing Your OSS for SLA Delivery*. Indianapolis, Wiley Publishing Inc, 2002:3-175.

[4] Zhang RuoYing, Qiu XueSong, Meng LuoMing.*SLA Representation Method and Application*. Journal of Beijing University of Posts and Telecommunications, 2003, S2:13-17.

[5] S.Subashini, V.Kavitha.*A survey on security issues in service delivery models of cloud computing*. Journal of Network and Computer Applications, 2011, 34(1):1-11.

[6] Jing Xu, Tang Jinglei, He Dongjian, Zhang Yang. *Security Scheme for Sensitive Data in Management-Type SaaS*.Information Management, Innovation Management and Industrial Engineering, 2009 International Conference on, 2009, 4:47-50.

[7] Zhang Qiang, Cui Dong.*Enhance the User Data Privacy for SAAS by Separation of Data*. Information Management, Innovation Management and Industrial Engineering, 2009 International Conference on, 2009,.3:130-132.

[8] Kenichi Takahashi, Takanori Matsuzaki, Tsunenori Mine, Takao Kawamura and Kazunori Sugahara.*Security as a Service for User Customized Data Protection*.Software Engineering and Computer Systems Communications in Computer and Information Science, 2011, 180(2):298-309.

[9] Hai Tao Song, Jing Rong Yi. *Primary Discussion on Data Security Management under SaaS Model*.Applied Mechanics and Materials , 2011, 58:441-446.

[10] YuHui Wang. *The role of SaaS privacy and security compliance for continued SaaS use* Networked Computing and Advanced Information Management (NCM), 2011 7th International Conference on, 2011:303-306.

[11] Lin Li, Qingzhong Li, Yuliang Shi and Kun Zhang. *A New Privacy-Preserving Scheme DOSPA for SaaS*. Web Information Systems and Mining Lecture Notes in Computer Science, 2011, 6987:328-335.

[12] Qingpeng Z, Shuixiu W U. *A SaaS Development Platform based on Cloud Computing*. TELKOMNIKA Indonesian Journal of Electrical Engineering, 2013, 11(3):1646 ~ 1651.

[13] ChangLung Tsai, UeiChin Lin, Chang A.Y., ChunJung Chen. *Information security issue of enterprises adopting the application of cloud computing* Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on, 2010:645-649.

[14] Ram C.P., Sreenivaasan G. *Security as a Service (SasS): Securing user data by coprocessor and distributing the data* Trendz in Information Sciences & Computing (TISC), 2010:152-155.

[15] Kandukuri B.R, Paturi V.R, Rakshit A. *Cloud Security Issues*. Services Computing, 2009. SCC '09. IEEE International Conference, 2009:517-520.

[16] ZHANG Chunfang, LI Honghui, WANG Qixian, SUN Wenhui.*SLA and Its Implementation of Model*. Application Research of Computers, 2009, v5.

[17] Deng Zhonghua, Yu Yue. *Research on the Information Service Level Agreement in the Cloud Environment*. Library and Information, 2009, v4.

[18] Niehorster O., Brinkmann A., Fels G., Kruger J., Simon J. *Enforcing SLAs in Scientific Clouds Cluster Computing*. 2010 IEEE International Conference on, 2010:178-187.

[19] Cheng Xu. *Research on Performance Management Mechanism Based on SLA in SaaS Application*. ME Thesis, Shandong: Shandong University, 2010.

[20] Tobias Unger, Ralph Mietzner and Frank Leymann. *Customer-defined service level agreements for composite applications*. Enterprise Information Systems, 2009, 3(3):369-391.

[21] ChangJie Guo, ZhiHu Wang, WenHao An, Wei Sun, Bo Gao. *The design pattern of resource sharing in the Single Instance Multitenant Application*. 2009.

[22] Padhy R P. *Big Data Processing with Hadoop-MapReduce in Cloud Systems*. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2012, 2(1):16-27.