Cloud Computing Model for MyGRANTs Project

Mohammed Adam Ibrahim Fakhreldin[a], Jasni Mohamed Zain[a], Ahmed N Abdalla, Mohamad Fadli Zolkipli[a], Ramdan Razali

[a]Faculty of Computer System and Software Engineering,
University Malaysia Pahang,
Kuantan, Malaysia.
mohfakhrdeen@gmail.com, jasni@ump.edu, ahmed@ump.edu.my, fadli@ump.edu.my, ramdan@ump.edu.my

Abstract. Key management is the most complex part of any security system dealing with encryption of data. Using cloud computing reduces not only pressure on IT cost but it provides satisfactory performance. However, a very fundamental issue on cloud computing is the loss of hands-on control of system, application, and data security. In viewing of current cloud-computing environment, there is an issue of a comprehensive key management scheme. This paper analyzes the special security requirements of key management under the cloud-computing environment. The study involves analyzing a cloud-computing key management framework based on the XML key management specification and designs the cloud-computing key management framework and module function for MyGRANTs. XML key management specification establishes an abstraction layer between the application program and PKI, which solves the interoperability problem between different PKI systems. As a result, the improved interoperabilty of cloud computing key management with three working modules based on different trust relationship for MyGRANTs is outlined.

Keywords: Cloud-Computing; Key Management; XML Key Management Specification.

1 Introduction

Cloud computing links a large number of computing resources, storage resources and software resources together, forming a virtual IT resource sharing pool at a large scale to provide IT services for the remote computer users which seems to possess an infinite power at users' disposal [1]. However, cloud computing has become critical implementation dark due to security and privacy considerations [2]. It features a super-large scale, virtualization and generality and so on, meanwhile also brings a tremendous impact and challenges for the realization of user information security and privacy protection. Cryptography is one of effective methods to solve the security problems, while key management is its core problem, so the key management has become an important technology to insure the cloud-computing security.

Public key infrastructure (PKI) is one of the main methods of traditional public key management, whose core is composed of certificate authority (CA), by issuing a public key certificate for the user's public key to guarantee its authenticity and validity in the system. Public key certificate works out the issue of the authenticity and effectiveness of the public key, allowing PKI to provide a good security service for Internet users. But for cloud computing, PKI cannot be directly deployed because of two reasons: a) cloud computing covers a wide range, and has a large number of users, which result in the requirement of a unified, standard key management service, while PKI has a poor interoperability because of the technical standard differences in various countries and regions and the differences existing in the data formats and the transport protocols; b) it is required to install a complex toolkit in the client side where all operations will be performed, which will cost a huge amount of resources and have a difficult deployment and appliance, so the efficiency of the cloud-computing server will seriously be affected.

XKMS (XML key management specification,) establishes an abstraction layer between the application program and PKI, which blocks the underlying technologies of PKI, to allow the user to make use of the different PKI solutions, which solves the interoperability problem between different PKI systems. The literature [3] discusses the security problems of XKMS and puts forward by adding a sequence number in each message to prevent replay attacks. The literature [4] proposes two methods to ensure the security of XKMS message transmission: a) introducing the security service provided by boundary transmission protocol; b) introducing a transport layer protocol without security features. The literature [5] compares the protections for the denial of service attack from the two phase protocols, and puts forward to achieve the authentication of the client and the trust service respectively by the signature of message, identification code, revoke code and restoring the authorization code. The literature [6] gives the analysis on the XKMS security channel problems, and puts forward three approaches to establish a secure channel mode, namely, XML signature, transport layer security (such as SSL, TLS etc.) and network layer security (such as IPSec). However, the XKMS has not been studied under the cloud-computing environment. Through a research on the characteristics of the cloud-computing environment, this paper, based on improved XKMS, establishes a four-layer cloud-computing key management framework, designs the module of each part, presents a working mode based on the trust domain and finally analyzes the requirements to meet the cloud-computing key management needs.

2 Cloud-Computing Key Management Framework

2.1 The Characteristics of the Cloud-Computing Key Management

Virtualization is one of the key technologies of cloud computing, which allows running multiple virtual machines simultaneously on the same physical server. Because of the different needs of each user, the cloud-computing has the following characteristics: a) there are different operating systems in the virtual machines; b) a virtual machine may possess several identities, and each identity has a different security level; c) different services as well as customized service have different qualities. At the same time, cloud computing also features a rapid deployment and dynamic migration.

These characteristics of cloud computing different from those ordinary networks also impose some higher requirements on the key management: a) cloud providers need to provide key management client sides suitable to different operating systems and different key management technology standards and able to install and configure quickly. B) The security and usability of key in the process and after the completion of the virtual machine migration should be ensured. C) The key control among different levels should be more complex.

2.2 General of XKMS

The XKMS protocol is composed of two parts, namely XML key information service specification (XKISS) and XML key registration service specification (X-KRSS). Both X-KISS and XKRSS are defined according to the structured language of XML Schema, running the message-based communication based on the simple object access protocol (SOAP), and the services they provide and the syntax definition of messages both are abiding by the Web service definition language (WSDL) [7]. X-KISS defines the key information service specifications and provides key information services to key users, a kind service any client-side entity can use. XKISS offers two kinds of services, the query one and the verification one. X-KRSS defines the key management service specifications and provides key management services to key administrators, but each client-side entity has to go through the trust service authentication prior to utilizing such service. XKRSS provides registration service, redistribution service, undo service and recovery service.

2.3 Cloud-Computing Key Management Framework

Because cloud computing is the fusion and development of distributed computing, Internet technologies, large-scale resource management and other technologies, its key security is subjected to a higher requirement and a more difficult management. The literature [8] holds that the problems and challenges the cloud-computing key management is facing include the storage of the safe key, key access, key backup and recovery. It suggests separating the key management from the cloud service providers, which can exempt the cloud service provider and cloud users from conflicts when a need authorized by law occurs to provide data. The cloud-computing key management framework proposed in literature [9][10] consists of the cloud-computing key client side and cloud-computing key management server, providing the comprehensive and effective cloud-computing key management services based on the unified management framework and mechanism.

At present, the cloud-computing, in the way of computing center, spreads all over the world, yet the existing PKI obviously has the regional and industry characteristics, so the cloud-computing can capitalize on the existing PKI providers to provide the key management services.

Currently, the cloud-computing, in the way of computing center, spreads all over the world, yet the existing PKI obviously has the regional and industry characteristics. Therefore, the cloud-computing can capitalize on the existing PKI providers to provide the key management services. According to the cloud-computing deployment model, this paper designs a four-layer cloud-computing key management framework, namely, key management client, trust service, key management service center and PKI providers, in Fig 1. This framework covers four management levels, ranging from the small to the large, including virtual machine, cloud-computing physical server, cloud-computing center and the whole cloud.

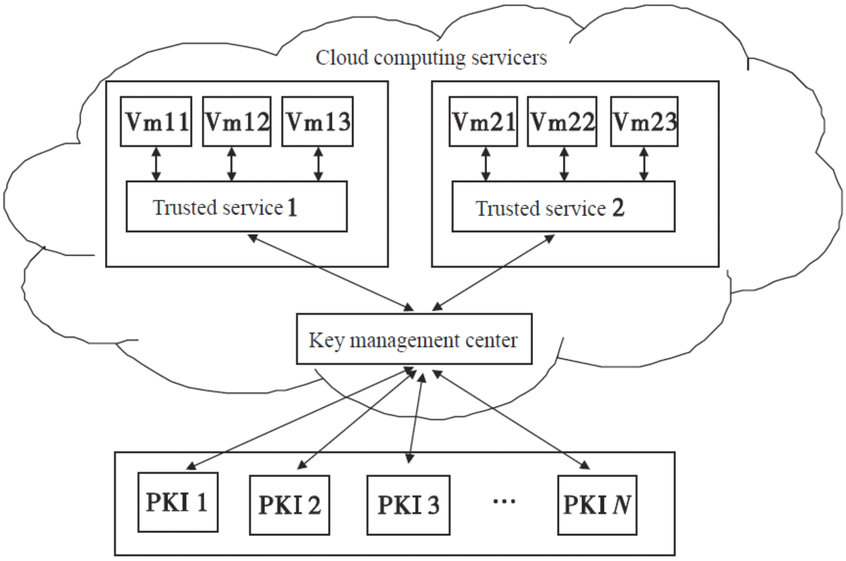

Fig 1. Cloud computing key management framework

3 Module Design

The cloud-computing key management framework has been discussed above, and next we will take about the module components of each part. a) Key management client side is deployed in the cloud user’s virtual machine, responsible for delivering the trust services required by user’s application programs in the SOAP message format to the trust server, receiving and analyzing the response messages from the trust server, and offering the response to the request message to the application program. It includes client application interface, message structure/analysis module, encryption / decryption algorithm module, XML signature module, trusted attestation module and trust services interface, as shown in Fig 2. Trust server side deployed in the cloud-computing application server, is an independent virtual domain in charge of receiving the client's request and reply, and communicating with the key management center. Trust service embodies an idea "transforming software into service", as the agent of the PKI provider, it undertakes many key/certificate operations originally completed by the PKI users, such as, certificate analysis, LDAP directory access, CRL and so on. Cloud users no longer need to install and run the complicated PKI client software, but only need to use the single client-side software before enjoying the service mode to obtain the information of key/certificate. Trust server side includes the client-side interface, message parsing/structure module, certificate authentication module, XML signature module and key management center interface, as shown in Fig 3. Key management center in the logical boundary of cloud is a management center linking the cloud-computing and the external PKI, responsible for the integration, scheduling and then transmitting to the PKI of the key management request in the in cloud computing. It includes trust service interface, message structure / analysis module, task scheduling module, trusted attestation module and PKI interface, as shown in Fig 4.

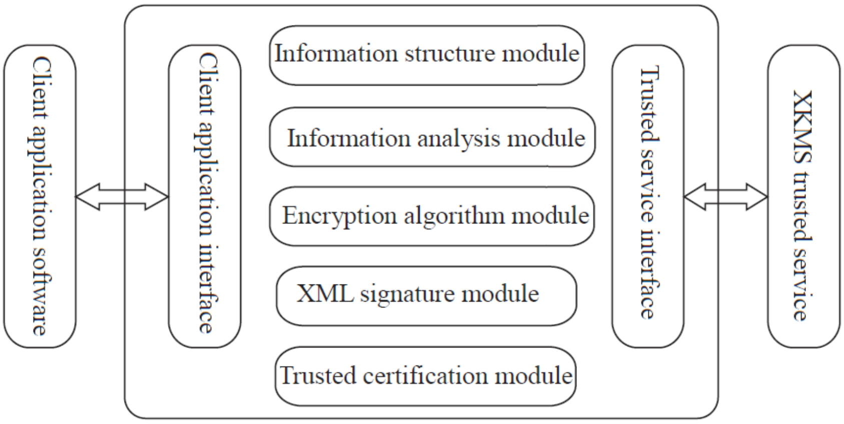
Client application software
Client application interface
Information structure module
Information analysis module
Encryption algorithm module
XML signature module
Trusted certification module
Trusted service interface
XKMS trusted service

Fig 2. Key management client

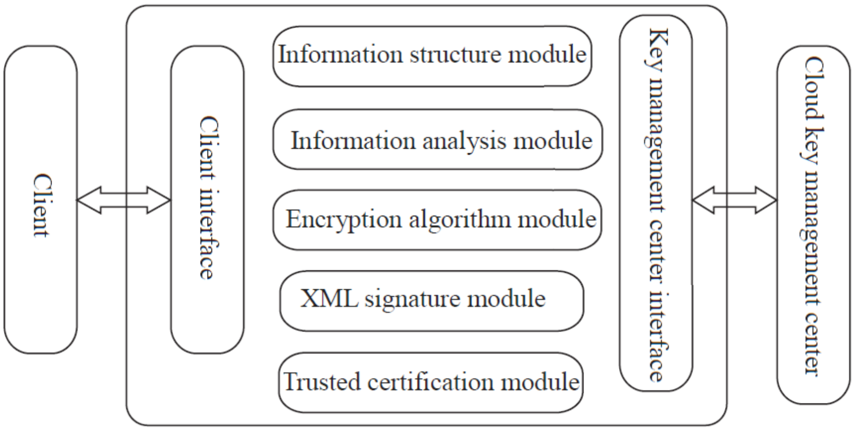
Client
Client interface
Information structure module
Information analysis module
Encryption algorithm module
XML signature module
Trusted certification module
Key management center interface
Cloud key management center

Fig 3. Key management trusted service

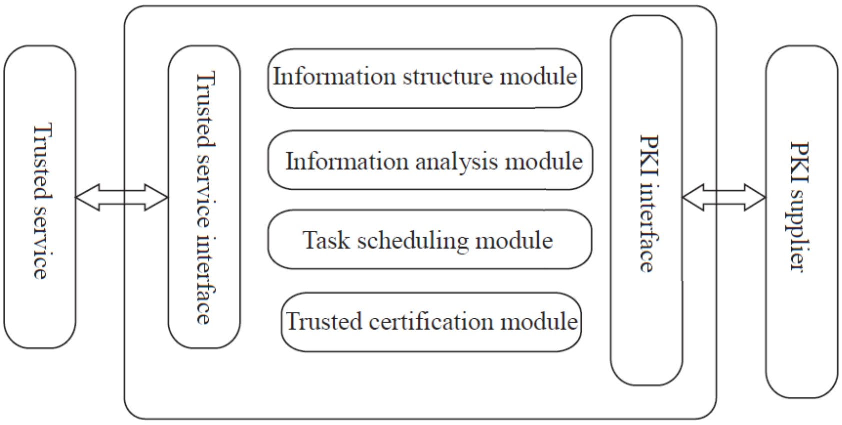
Trusted service
Trusted service interface
Information structure module
Information analysis module
Task scheduling module
Trusted certification module
PKI interface
PKI supplier

Fig 4. Cloud key management center

3.1 Cloud-Computing Key Management Scheme

System initialization: System initialization covers user side, server side, key management center and the confirmation of the PKI key parameters. The registration of user key: After receiving the login request from the user side, the trust server will analyze the message and verify it by a digital signature, then to submit to the key management center; the key management center will request the distribution to the corresponding underlying PKI, finally, which will release a digital certificate to the user. And the trust server will save user’s digital certificate in the local certificate repository for later query. Key query: User side will send the 'ds: KeyInfo' elements request to the trust server which will send back the 'ds: KeyInfo' elements covering public key to meet the client’s demand according to whether the queried key exists the trust server or not: trust service can analyze the 'ds: KeyInfo' elements locally, or also can transfer the client request to other PKI servers. Key migration: With the migration of the user's virtual machine, the user's key will also be on its' heel. Key management center notifies the trust service A in the place where the virtual machine was of migrating to the trust service B in the place where the virtual machine is. Firstly, trust services A and B will have a identity authentication and trusted attestation; and then trust service A will go through a key encryption for the user key making use of the public key of the trust service B, and transmit the encrypted key to B. after receiving it B will decrypt the encrypted key by its private key, then the key migration finishes its course. Thus, the transmission of the user's key between trust services can avoid the bottleneck problems generated by the key migration between the key management centers.

4 Conclusion

In view of the present cloud-computing still short of a complete and unified key management scheme, this paper puts forward the four-layer cloud-computing key management framework based on the XKMS. Including trust service client side, trust server, key management service center and PKI provider, the framework, taking the traditional PKI as the underlying server of the cloud-computing key management service and capitalizing on the abstraction layer between the PKI and the XKMS as an application program, shields the difference of PKI's underlying technology, and improves the interoperability of the cloud-computing key management. Aiming at the framework, this paper also designed the module function of each part, and conceives three working modes based on different trust relationship.

Acknowledgments. The authors would like to thank the members in the Malaysia Greater Research Network System (MyGRANTs) Project especially Cloud & Security Research Group for their helpful discussions and suggestions. This work was supported by MyGRANTs Project, Ministry of Higher Education (MOSTI), Malaysia.

References

1. S. Carlin, andK. Curran, "Cloud computing security", International Journal of Ambient Computing and Intelligence (IJACI), 2011, 3(1), 14-19.
2. M. Bamiah, S. Brohi, S. Chuprat, and M. N. Brohi, "Cloud implementation security challenges", International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), 2013, vol., no., pp.174,178.
3. R. Zicari,"XML data management: native XML and XML-enabled database systems", Addison-Wesley Professional, 2003.
4. T. Chen, J. Jiang, B. Chen, and W. Li, " Research on XML-Based Key Management Service for Identity-Based Cryptography", InMultimedia Information Networking and Security (MINES), 2010, International Conference on (pp. 468-472). IEEE.

5. M. Marković, and G. Đorđević, “One Possible Model of Secure e/m-Government System. Information Systems Management”, 2010, 27(4), 320-333.
6. E. Bertino, L. Martino, F. Paci, and A. Squicciarini, “Security for Web Services and Service-Oriented Architectures”, Springer Publishing Company, Incorporated, 2009.
7. HALLAM-BAKER P, “XML key management specification (XKMS 2. 0) W3C working draft”, (2005). http://www. w3. org /TR/2005 /REC-x kms2-20050628 /.
8. J. ARCHER, “Security guidance for critical areas of focus in cloud computing v2.1. cloud security alliance”m(2009) .http: //www.cloudsecurityalliance. org/ guidance.
9. S. Ramgovind, M. M. Eloff, and E. Smith, “The management of security in cloud computing”. In Information Security for South Africa (ISSA), August 2010, (pp. 1-7). IEEE.
10. S. Lei, D. Zishan, and G. Jindi , “Research on Key Management Infrastructure in Cloud Computing Environment”, 9th International Conference on Grid and Cooperative Computing (GCC), 2010, vol., no., pp.404,407.