CRYPTO AS A SERVICE

Mengzhen Wang
Tianjin University
School of Elec.& Info. Eng.
Tianjin, China
wangmz1223@126.com

Li Liu
Tianjin University
School of Elec.& Info. Eng.
Tianjin, China
lliu@tju.edu.cn

Abstract—**Cloud security is one of the most important issues in practice of cloud computing. In this paper, we proposed a crypto cloud infrastructure which is inherently constructed using asymmetric cryptography. Different to the prevalent public key infrastructure (PKI) system, the crypto cloud is based on a self-authentication key system. Every component in the crypto-cloud has its own identity for data encryption and decryption. Such cipher functions can be provided to users as a service, or Crypto as a Service.**

Keywords-Cloud computing; Internet security; Asymmetric cryptography

I. INTRODUCTION

In the past three decades, with the development of computer science, the world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the virtual centralization (cloud computing). The cloud computing model provides convenience for the sharing of resources and the interacting of information. At the same time, cloud security has become the most significant barrier to the application of the cloud computing. There are many threatens for the cloud computing applications. There are seven specific security issues: privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, long-term viability [1]. In general, these problems can be divided into three categories: Data Security, Data Storage Security and Hostile Attack [10].

Many approaches have been studied for security of cloud computing. However, no method has been found that can provide intrinsic protection against all practical threatens. Thus, security of cloud computing cannot be guaranteed.

In this paper, we proposed a new type of computing, Crypto Cloud Computing, for security of cloud computing. Under the framework of crypto cloud computing, all components are integrated with cryptography functions. Besides, every components are labeled with a self-authentication key. The structure of the paper is as follows: the Cloud Computing and its potential dangers are reviewed in Section 2, crypto cloud computing and Self-authentication Key are discussed in Section 3. An application of crypto cloud computing, Crypto as a Service, is introduce in Section 4. We conclude the paper in Section 5.

II. CLOUD COMPUTING

A. *Defining Cloud Computing*

There is little consensus on how to define the Cloud. Here, we use our own definition to the already saturated list of definitions for cloud computing: Cloud computing is a large-scale distributed computing model that is driven by economies of scale. It integrates a set of abstracted, virtualized, dynamically-scalable, and managed resources, such as computing power, storage, platforms, and services. External users can access to resources over the Internet using terminals, especially mobile terminals. Cloud architectures are developed in on-demand fashion. That is, customers can reduce expenditure on resources like software licenses, hardware and other services (e.g., email) as they can obtain all these things from one source, the cloud services provider. The resources are dynamically assigned to a user according to his request, and relinquished after the job is done [4]. According to the scale of the customers which cloud computing provides to, the cloud computing includes three types: public cloud, private cloud and their mixture.

Cloud computing is a pool of services including the hardware and operating system infrastructure, the formation of systems and management platform including management software, virtualization components and cloud computing management system. According to the level of its resources, cloud computing services can be divided into three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). IaaS provides services such as storage and computing, the application of the service is EC2 of the Amazon. The mainly application of the PaaS is the APP Engine of the Google, because of its strong platform environment and capabilities. Besides, SaaS provides a set of applications on the cloud computing, such as Facebook and webpage games and so on. Figure 1 shows the layers of the cloud.

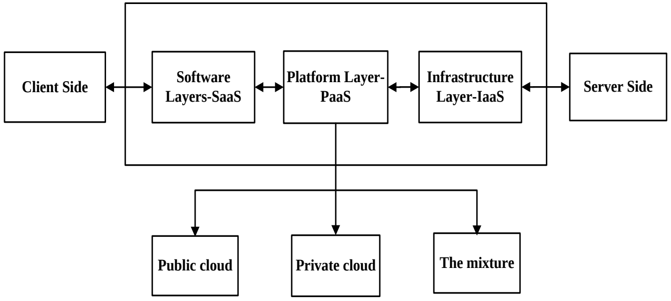

Figure 1: The layer of the cloud

B. The potential dangers of the Cloud computing

While enjoying the convenience of cloud computing, network security risks cannot be ignored. A customer's data security relies on security service from cloud computing providers, however, current structure of cloud computing services are provided by independent operators. In the cloud computing environment, important data, files and records are entrusted to a third party, which enables data security to become the main security issue of cloud computing [5]. First, the user's information security provides commerce and management. Second, the information leakage can be caused by technology flows of providers. Here, network security refers to the protection of the data and application in the cloud environment, not applying the cloud technology to the systems like 360. This security mainly applies to the virtualization, data transmission and management, platform and infrastructure, terminal. Cloud computing is an opening environment, any weakness will cause information security risks of the whole system. Its feature makes the information leakage be possible by the technology flows of providers, so the security will be our care.

III. CRYPTO CLOUD COMPUTING

To make up the short of the previous methods which is using to solve the potential dangers of the network, a new concept –Crypto Cloud Computing is proposed.

Cloud computing is a combination of IaaS, PaaS, SaaS. To construct a secure cloud computing system, security at infrastructure, service platforms and application software levels have to be studied for a secure cloud computing system. Information encryption is one of effective means to achieve cloud computing information security. Traditionally, information encryption focuses on specified stages and operations, such as data encryption. For cloud computing, a system level design has to be implemented.

In the cloud computing, we are daily witnessing various problems – infection of computers by malware, distribution of E–mail spam, phishing of Web pages, penetrations by hackers, software bugs, stolen industrial secrets and credit cards, disclosure of sensitive documents, and so on. To solve these questions, we have considered two approaches. One approach is to enforce isolation of users, network resources, and applications. The second approach is to apply methodology, tools and security solutions already in the process of creating network applications. However, current experience clearly shows that both approaches failed to provide an adequate level of security, where users would be guaranteed to deploy and use secure, reliable and trusted network applications [8].

Crypto cloud computing is a new secure cloud computing architecture. It can provide protection of information security at the system level, and allows users access to shared services conveniently and accurately. Crypto cloud computing protects individual's connections with the outside world. It can protect the personal privacy without any delay of information exchange.

A. Self- authentication Key

The cryptographic method includes two types: asymmetric and symmetric encryption algorithm. For perspective, the reader should keep in mind that all current cryptosystems are symmetric in the sense that either the same key is held by both communications, so this mechanism leads to problem that if a key is compromised, further secure communications are impossible with that key. To solve it, the concept of asymmetric is proposed which the transmitter and receiver hold different keys at least one of which it is computationally infeasible to derive from the other [6]. The most popular algorithm of the asymmetric is RSA whose principle is the decomposition of large prime number, the result is the couple keys: public key and private key. The principle of the asymmetric is showed in the Figure 2.

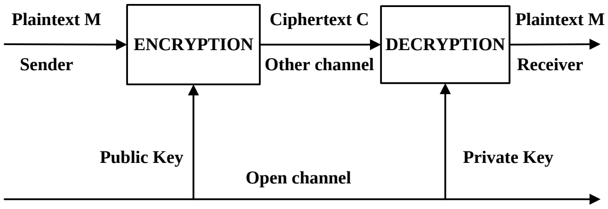

Figure 2: The principle of the asymmetric

Asymmetric key mechanism has been proved to be an effective means of information protection in the network environment. In this mechanism, data authentication and encryption are implemented. Firstly, to achieve data authentication, senders send the data that are encrypted by their private keys and receivers decrypted the data by their original owner's public keys; Secondly, opposite to the authentication, the function of encryption of the data can be achieved. The safe use of the key is based on the reliable of the public-private key mechanism so that a reasonable and efficient key management is the core problem of security cloud computing.

Public Key Infrastructure (PKI) [9] is increasingly popular as the asymmetrical key system in corporate information systems and cloud computing. Generally, the role of the PKI is to provide the necessary mechanisms to establish trust relationship and obtain security services [7]. The access of the public key in the PKI system requires the support of the third-party Certification Authority (CA) and databases online. For example, if Alice wants to send data to Bob, Alice first sends her request to the CA, CA receives her requests and sends Bob's public key to her, so she can encrypt the data and send it to Bob. Figure 3 shows the process of the PKI. At the same time, Bob can decrypt the data use his own private key. However, if CA itself is not reliable, such as its internal staff sell it or it is hijacked. So it is unwise to rely on the third parties to access the public key.

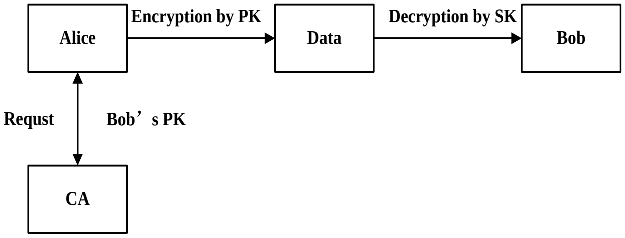

Figure 3: The process of the PKI

To solve the above question, a new concept which is namely self-authentication key is proposed. The function of the self-authentication is that when exchange the key in the process of the authentication and encryption, the third party like CA is not needed, it is happened only between the two sides of the event. That namely, if Alice wants to send data to Bob, Alice can encrypt the data by her private key only, Bob decrypts the data by Alice’s public key which is stored in Bob’s database. Above all process, none of the public key obtained through a third party to achieve, thereby reducing the consumption of network resources, and improving the security of data encryption and authentication.

The process of data certification which is based on the self-certification asymmetric key system can be seen from the Figure 4.(1)Alice encrypt the information M by its private key and identification ID, so the signature by Alice is formed;(2)The signature of Alice can be transmitted to Bob through Internet, then Bob can query Alice's public key based on Alice's unique ID and complete the certification process;(3)If the certification can recover the information M, we can think the certification is successful, otherwise it is failure.

B. Procedure

Crypto cloud computing is based on the Quantum Direct Key system. The Quantum Direct Key (QDK) is a set of advanced asymmetric offline key mechanism. In this mechanism, all entities get public and private key pair according to their ID. Each entity only holds its own private key, but has a public key generator to generate any public key. In this system, an entity can produce the public key of any other entities offline, no any third-party agency (such as CA) is necessary. It provides a method for smart identity management. Crypto cloud computing based on QDK can avoid network traffic congestion, and other drawbacks using current encryption system.

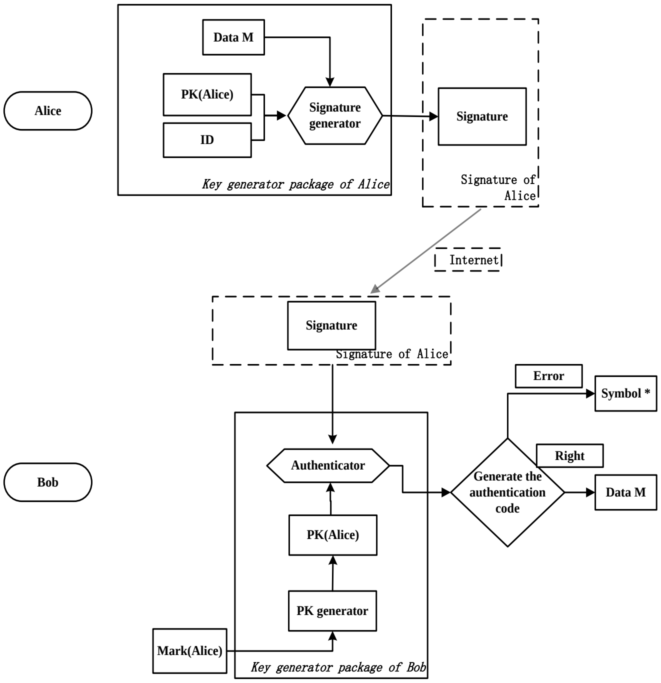

Figure 4: The process of the data certification

In the crypto cloud computing system, each entity encrypts data using his/her own private key. All elements in the system such as cloud computing infrastructure units, platform, virtualization tools and all involved entities have their own keys. While fulfilling their own functions of information exchange and processing, all these elements will use the public key and private key to perform authentication first. What’s more, events occur in the cloud computing are also assigned a unique key. In this way, crypto cloud system guarantees the security and credibility of information exchange.

Current cloud computing structure is developed for data and computing sharing. Security is not priority of system. On the contrary, encryption and security are inherently integrated in the crypto cloud computing based on the QDK. QDK authorized function units are bricks of crypto cloud computing. Besides primary function of data en/decryption, crypto cloud computing also provides many security related functions. For example, all channels sign transmit data using with their own keys, and the receiving terminals can avoid hijacking by verifying signature. What’s more, the exact position of security leakage can be identified determined by analyzing digital signatures of forged data. .

Crypto cloud computing is not only the advances in information technology, but also innovation of logical relationship. In crypto cloud computing system, non-system data is not allowed to store and transmit. Private Key and offline public key, play a role of identification and certification in the process of information exchange. In this way, the cloud establishes a relationship of trust with a customer. Data identification depends on the logical relationship of mutual trust or need, and the logical relationship depends on the cloud customer.

Crypto cloud contributes to establish a new framework for resource sharing, when a customer accesses to cloud computing resources conveniently and clearly, his privacy security is protected. Through this mechanism, first, it can guarantee the security and integrity of all aspects of cloud computing applications; second, a customer can access to the traceability of data by analyzing the signature information, finally we can manage cloud computing; moreover, the customer can access to his information with QDK key.

In the current cloud service architecture, privacy is a luxury. However, with the establishment of Crypto Cloud, we can resolve the conflict between services data sharing and privacy security. It opens up new prospects for the development of information sharing technology.

IV. Crypto as a Service

To solve the security question in the cloud computing, we have key labels affixed on each node, which is owned by every user. For example, when cloud 1 communicates with the user A, cloud 1 will encrypt the information by user's public key and add an identity tag of cloud 1. Moreover, the identity tag of cloud 1 will be added in all aspect of the transmission. Therefore, the user A could decrypt the information by his/her own private key, then, according to the label, the users will determine whether the information is from the cloud 1. By this way of encryption and labeling, hijacked data during the transmission will be avoided. This cloud computing, in which all data will be encrypted and all steps will be labeled, is called crypto cloud.

In the crypto cloud computing environment, any interactions are required within a confidential environment to achieve, crypto cloud environment integrates encryption and decryption which help realizing data and computing and offered as a service to the users. Besides, the service of the crypto cloud can protect the data and information through transferring. For example, when user accesses the mail service of the terminal, the user terminal and server will authenticate their own key, if they are right, the cloud server can provide an encrypted channel and data to the user automatically. On the other hand, the mail information on the cloud will encrypt and decrypt the user's key through server. If the key of users is missing, server cannot process and save the data because server itself only offers the service of encryption and decryption. Users can enjoy 'Crypto Service' for the combining soft platform, infrastructure and authentication with encryption, decryption. Crypto service provided by the cloud according to the needs of customers, it includes the encryption of data, the user's operation and the presence of the user, so born a new concept-'Crypto as a service'. The risks of the cloud computing reduce because users can establish mutual trust with the cloud, without worrying about the invasion of non-authenticated users.

CaaS has many benefits, for example, the safety system of the crypto computing environment is improved, the information of the user can be protected systematic, the incidence of the online fraud is reduced. In this sense, CaaS is an effective solution to solve the safety of the cloud computing. However, CaaS need to combine with the law and network to format an effective cloud computing security system.

V. Conclusion

Since the concept of cloud computing was proposed in 2006, cloud security has become the most significant barrier to the application of the cloud computing. There three types of cloud security: Data Security, Data Storage Security and Hostile Attack. To solve these problems, we proposed the crypto cloud computing which is based on a self-authentication key method. Under the framework of crypto cloud computing, all participant components are armed with crypto functions, and can provide to customers as a service--crypto as a service.

References

[1] J. Brodkin. Gartner: Seven cloud-computing security risks. Infoworld, 2008.

[2] Meyer, C.H. Cryptography-a state of the art review, CompEuro '89.,'VLSI and Computer Peripherals,pp,1989,150-154

[3] Q.Wang, H.Su, K.Ren, K.Kim. Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks, INFOCOM,Proceedings IEEE, 2011,1422-1430

[4] I. Foster , Y. Zhao, I Raicu, S Lu, "Cloud Computing and Grid Computing 360-Degree Compared" Grid Computing Environments. , 2008,pp.1–10.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou. "Ensuring data storage security in cloud computing," In Quality of Service, IWQoS. 17th International Workshop on, 2009,pp.19.

[6] GJ Simmons, "Symmetric and Asymmetric Encryption,"ACM Computing Surveys(CSUR),vol. 11,1979,pp. 305-330.

[7] H EI Bakkali, BI Kaitouni, " A Predicate Calculus Logic for the PKI Trust Model Analysis," Network Computing and Applications, , 2001, pp. 368-371.

[8] Abdul Ghafoor Abbasi ,"CryptoNet: Generic Security Framework for Cloud Computing Environments," School of Information and Communication Technologies (ICT), 2011

[9] Kumar, S.; Prajapati, R.K.; Singh, M.;De,A.;Security enforcement using PKI in Semantic Web,CISIM, ,2010,pp.392-397

[10] Shaikh,F.B.;Haider,S.;Security threats in cloud computing; Internet Technology and Secured Transactions (ICITST) ,2011,pp:214-219