Securing Cloud Data using RSA Algorithm

https://doi.org/10.3991/ijes.v6i4.9910

Md Equebal Hussain (✉)
Suresh Gyan Vihar University, Jaipur, India
mdequebal.60508@mygyanvihar.com

Mohammad Rashid Hussain
King Khalid University, Abha, Saudi Arabia

Abstract—Security is one of the most important concern on cloud computing therefore institutions are hesitating to host their data over cloud. Not all data can be afforded to move on the cloud (example accounts data). The main purpose of moving data over cloud is to reduce cost (infrastructure and maintenance), faster performance, easy upgrade, storage capacity but at the same time security is major concern because cloud is not private but maintained by third party over the internet, security issues like privacy, confidentiality, authorization (what you are allowed to do), authentication (who you are) and accounting (what you actually do) will be encountered. Variety of encryption algorithms required for higher level of security. In this paper we try to provide solution for better security by proposing a combined method of key exchange algorithm with encryption technique. Data stored in cloud can be protected from hackers using proposed solution because even if transmitted key is hacked of no use without user's private key.

Keywords—cloud computing, Security, RSA

1 Introduction

Security over the cloud is one of the key requirements to use the cloud service. However, this is not a new area of research instead, many researchers, decision makers, government organization already shared their views on the concerns and obstacles in providing data confidentiality, scalability, and data leakage. The service model provided by the cloud can be SaaS (software as a service, example sales, Human Resources, Billing, CRM, sales), PaaS (Platform as a service, example Database, Business Intelligence, and integration), IaaS (Infra structure as a service, example storage, networking, servers, backup and recovery, compute) and deployment types are public, private, community and hybrid.

As name suggests public cloud is publicly accessible (less secure).

Private clouds have access level restrictions mostly used and managed by single organization (more secure).

Community cloud is formed by more than one group of organizations sharing common infrastructure.

Hybrid cloud is centrally managed private cloud linked to more than one external cloud service. It is mix of public and private cloud example virtual server, routers, firewall etc.

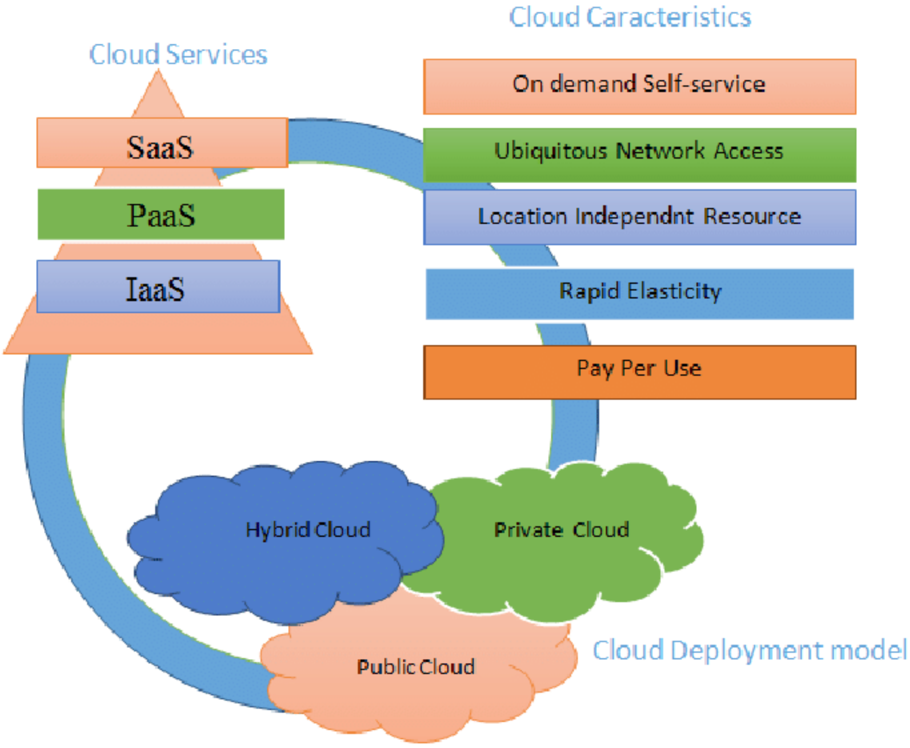

Fig. 1. Cloud computing service delivery and deployment model

2 Security issues in cloud computing (SaaS, PaaS and IaaS)

Software-as-a-Service (SaaS) applications are accessed using web browser hence browser security is very important. SaaS application can be secured using XML encryption, SSL (Secure socket layer), TLS and other available options to enforce data protections while transmitting over internet.

Platform-as-a-Service (PaaS) is set of software and development tools that developer can use to plan, design, build, deploy and test their application using virtual machines without knowing underlying service. These virtual machines can become victim of cloud malware hence need to be protected by enforcing accurate authentication check.

Infrastructure-as-a-service (IaaS) is a model where provider hosts servers, storage, networking devices, hypervisors etc. along with range of services like load balancing to maintain high availability, clustering, backup, recovery, monitoring and billing.

IaaS abstracts the underlying hardware allowing users to consume infrastructure without worrying about underlying complexities. User can create virtual machines, install operating systems, database and middleware components. Amazon Web Services (AWS) offers S3 (Simple Storage Service) and compute service EC2 (Elastic Compute Cloud) are examples of IaaS. This model is effective for temporary or experimental purpose. Long-term IaaS deployment is useful when cost is less as it is based on pay-as-you-go model hence after software is ready and tested then it can be removed from IaaS environment for in house deployment on its own data center. Challenges in cloud computing

Below are some of the major challenges in adopting cloud service.

2.1 Privacy and confidentiality

Authorized access to the client-hosted data must be guaranteed by the cloud service provider. Also the client should be assured and entrusted that his sensitive data remains safe from the cloud personnel. The cloud service provider must put in place the proper data privacy, security policies, and procedures under the confidentiality agreement to address the client's data safety concerns.

2.2 Data integrity and security

The cloud service provider must take the onus of ensuring the integrity of the data hosted on the cloud. To address compliance issues, they must draft a mechanism which records the data processing paths in order to locate the incidents of data loss at any point of time. Vital information such as the address of the public cloud on which the data is hosted, the type of the virtual memories (VM) and storage in use, the data source and custodian details must be recorded at all time to prevent data tampering or access beyond the agreed territories (Networks and Servers).

2.3 Authentication and Authorization

Most commonly used password based authentication has limitation and significant risks. Authentication (digital signature along with sender and recipient detail is also verified) and Authorization (to make sure that the message is transmitted by legitimate sender) are two key feature important to maintain in asymmetric key (public key like RSA) cryptosystem.

2.4 Data location and Relocation

Generally, the consumers are not concerned with the location of their data on the Cloud. However, the data storage location is of great importance to the enterprises as they value their sensitive information. Hence, they insist on data confidentiality agreement with the Cloud service provider, which specifies the geographic location, storage device and the server types to be used for their data. The agreement also guarantees the confidentiality of the consumer's identity as well as the security of the data. Data Mobility among the different clouds hosted by different service providers is also another serious consumer concern. To address this, Cloud service providers enter into separate mutual agreements.

2.5 Data Availability

Usually data in the cloud are kept on different servers across location due to which availability of data becomes issue.

2.6 Storage, Backup and Recovery

Cloud service provider should also provide backup options so that in case of hardware failure for cloud based application it can be rolled back to safe state.

3 Security Algorithm in cloud computing

3.1 RSA Algorithm

RSA is asymmetric cryptographic algorithm to encrypt and decrypt messages using public (known to everyone) and private key (secret, known only to user) respectively. Message encrypted using public key can only be decrypted using private key. Same key cannot be used for both encrypt and decrypt the message.

RSA algorithm consists of below three steps.

```
// Generate Key between user and cloud service provider.
begin {
        Randomly choose two large primes p and q such that $p \neq q$
        Find $n = p * q$
        Find $\varphi(n) = (p-1)(q-1)$
        Choose an e which is co prime and $1 < e < \varphi(n)$
        Find d using below formula
        $d.e \equiv 1 \bmod \varphi(n)$
        The pair (e, n) is public key (d, n) is private key.
        } while (false) /* Calculate once */
end
 // Encryption as below. Cipher text (C), message (m)
C = me (mod n).
// Decryption
m = Cd (mod n)
```

4 Conclusion

RSA algorithm for encryption of data in cloud computing between user and cloud provider is secure. Before storing data on the cloud, it is first encrypted. User places a request to cloud provided to access the data whenever required. After authenticating the user, cloud provider delivers the data. RSA is safe because large prime numbers are used. It is impossible to hack either using Brute force attack (time consuming), Dictionary attack will not work because the keys are numeric, and Frequency analysis of the character is very difficult hence, there is no way of hacking RSA cipher.

5 References

[1] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT."

[2] Parsi Kaplana, Sudha Singaraju, Data Security in Cloud Computing using RSA Algorithm, 2012

[3] Volker Fusenig and Ayush Sharma "Security Architecture for Cloud Networking" 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium. https://doi.org/10.1109/ICCNC.2012.6167464

[4] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering. https://doi.org/10.1109/ICCSEE.2012.193

[5] Zhang Xin , Lai Song-qing and Liu Nai-wen "Research on Cloud Computing Data Security Model Based on Multidimension" 2012 IEEE International symposium on information Technology in medicine and education.

[6] Farhan Bashir Shaikh and Sajjad Haider "Security Threats in Cloud Computing" 2011 IEEE 6th international conference on Internet Technology and secured transactions, 11-14 December 2011, Abu Dhabi United States of Arab Emirates.

[7] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi, "Cloud Security Issues" 2009 IEEE International Conference on Services Computing. https://doi.org/10.1109/SCC.2009.84

[8] Ayesha Malik and Muhammad Mohsin Nazir". Security Framework for Cloud Computing Environment: A Review" in Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 3, March 2012.

6 Authors

Mr. Mohammad Equebal Hussain is a Ph.D Scholar in Department of Computer Science, Suresh Gyan Vihar University, Jaipur, India. He received his Master of Technology degree from the Department of Computer Science, Indian Statistical Institute, Kolkata, India. He worked as an Assistant Professor under the Department of Computer Science and Engineering at GCET Greater Noida, India. Prior to that. He also worked as a Software Engineer with HCL Bangalore, India. He completed his Bachelor of Technology degree from NIT Patna, Bihar, India. Presently he is a Research Scholar in Gyan Vihar University, Jaipur-India. Email id: mdequebal.60508@mygyanvihar.com

Dr. Mohammad Rashid Hussain is an Assistant Professor, Department of Information Systems, College Of Computer Science, King Khalid University, Abha, Kingdom of Saudi Arabia. He received his Master of Technology degree from the Department of Computer Science & Engineering, Anna University, Chennai, India. After that, he obtained his PhD degree from Bihar University, India. He was an Associate Professor in the Department of Computer Science & Engineering, ABESIT Ghaziabad, India. He is currently working as an Assistant Professor in the department of Information Systems, King Khalid University, Abha, Saudi Arabia. His research interests include Computer Networks, Information Technology, Cloud Computind, and Operation Research. Email id: humohammad@kku.edu.sa

Article submitted 03 November 2018. Resubmitted 23 November 2018. Final acceptance 27 November 2018. Final version published as submitted by the authors.