ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secure User Data in Cloud Computing using RSA Algorithm

Abhishek Patial [*], Sunny Behal

[*] Research Scholar, CSE Department, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab,India

Assistant Professor, CSE Department, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, Inda

Abstract

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing provides customers the way to share distributed resources and services that belong to different organizations or sites. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This paper explores various security methods such as Access Control, Telecommunications and Network Security, Information security governance and risk management, Application Security, Security Architecture and Design, We proposed a method using RSA algorithm.

Keywords: Cloud Computing, Data Security, Rivest, Shamir and Adleman (RSA) Algorithm, Encryption, Decryption, Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS).

Introduction

Data Storage through Internet computing technology is known as Cloud Computing. This approach is emerging due to time, cost, distributed complex sourcing, faster delivery of innovation and increasing complexity. Cloud computing provides a computer user access to Information Technology (IT) services i.e., applications, servers, data storage, without requiring an understanding of the technology or even ownership of the infrastructure. The Cloud computing is Internet-based computing, where by shared resources, software and information, are make available to computers and devices on-demand, like the electricity grid. Cloud computing is inventiveness of the fusion of time-honored computing technology and network technology like grid computing, distributed computing parallel computing and so on. It aims to paradigm a accurate system with significant computing capability for the duration of a large number of relatively low-cost computing entity, and using the superior business models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to distribute the effectual computing capability to end users hand.

This provides the first benefit of the cloud computing (i.e.) it reduce cost of hardware that cloud have been used at end user. As there is no need to store data at end user's because it is already at some other location. So instead of buying the whole infrastructure required to run the process and save bulk of data you are just renting the assets according to your requirement.

Characterstics of Cloud Computing

- **On-demand Self-Service**
  As per demand without requiring human interaction we can use computing resources as server time, network bandwidth, storage etc.

- **Storage, Backup and Recovery**
  When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers.

- **Ubiquitous Network Access**
  Irrespective of the positioning of the system we can access the data anywhere like with laptop, mobile phones, tablets etc.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

- **Availability of Data**
  It is the data available for its storage and its location. This will ensure access to data whenever it's asked for.

- **Rapid Elasticity**
  Quick scale up or scale down of resources through elastic provisioning or the release of capabilities in near real time.

- **Data Integrity**
  Data when saved on a cloud, it is being distributed and saved on different locations. When accessing the data the service providers must ensure the data integrity while delivering back the data from their storage

- **Encryption:** The type of encryption standard that will be used will be based on the type of cloud we are using. The security of data has to be ensured by the service providers by following a set standard.

- **Data Availability**
  Data availability becomes a major issue as the availability of uninterruptible and regular provision becomes little difficult, because data is normally stored in major quantity on different servers often residing in different locations or in different Clouds.

- **Privacy and Confidentiality**
  There should be some guarantee that access to data will only be limited to authorised access. Assurances should be provided to the clients by using various Security methods. Procedures and policies should be in place to assure the cloud data safety.

- **Data Location and Relocation**
  Cloud Computing offers a high degree of data mobility. When an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location. This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information. Cloud providers have contracts with each other and they use each others' resources.

Types of Clouds

The various types of clouds are:

1. Public Cloud
The cloud infrastructure is made available to the general public or a large industry group and owned by an organization selling cloud services. The organization using public cloud does not control how those cloud services are operated, accessed or secured.

2. Private Cloud
The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party and may exist on or off-premises. While the organization does not need to physically own or operate all the assets, the key is that a shared pool of computing resources can be rapidly provisioned, dynamically allocated and operated for the benefit of a single organization.

3. Community Cloud
The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off-premises.

4. Hybrid Cloud
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

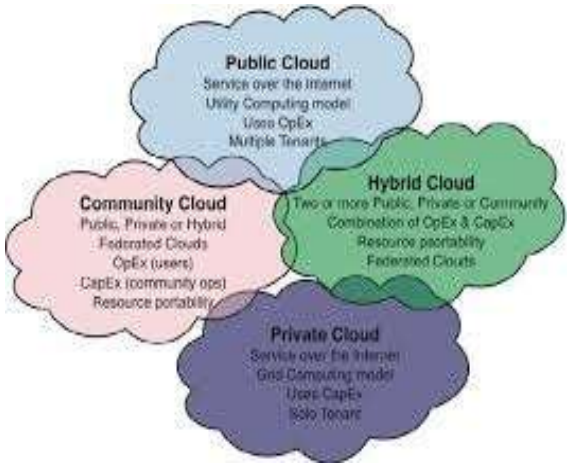

Fig1:Types of Cloud

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Categorization of Cloud Services

1. Platform as a Service (PaaS)

Cloud computing has evolved to include platforms for building and running custom applications, a concept known as Platform-as-a-Service. To develop software, you once had to buy databases, servers, networks, and a host of development tools. And then you needed the staff to install, optimize, and maintain it all. With PaaS, you can avoid those investments and focus on developing applications instead. Key characteristics of PaaS are Services to develop, test, deploy, host and maintain applications in the same integrated development environment**,** Web based user interface creation tools**,** Multi-tenant architecture**,** Integration with web services and databases**,** Support for development team collaboration**,** Utility-grade instrumentation.

2. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. Key characteristics of IaaS are Utility computing service and billing model, Automation of administrative tasks, dynamic scaling, Desktop virtualization, and Policy-based services.

3. Software as a Service (SaaS)

Software as a service (or SaaS) is a way of delivering applications over the Internet as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management. SaaS applications are sometimes called Web-based software, on-demand software, or hosted software. Key characteristics of SaaS are Scalability, Multi-tenant efficient, Configurable.

RSA Algorithm

The most commonly used asymmetric algorithm is Rivest-Shamir-Adleman (RSA). It was introduced by its three inventors, Ronald Rivest, Adi Shamir and Leonard Adleman in 1977. It is mostly used in key distribution and digital signature processes.. It is based on the presumed complicatedness of factoring large integers. An asymmetric algorithm has set of key one is public and another one private key. The RSA algorithm involves three steps Generation of key, Encryption of data, Decryption of data RSA involve a key combination such as public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Example: - we have two companies p and q. p has public cloud along with software, application and data. Company q wants to secure cloud's data from company p. We have tried to secure data of q with the help of RSA algorithm.

RSA algorithm involves three steps:
1. Key Generation
2. Encryption
3. Decryption

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.
5. Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n). Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:

1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who want to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is $C = m^e \pmod n$.
4. This cipher text or encrypted data is now stored with the Cloud service provider.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Decryption:
Decryption is the process of converting the cipher Text (data) to the original plain text(data).
Steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, $m = C^d \pmod n$.
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

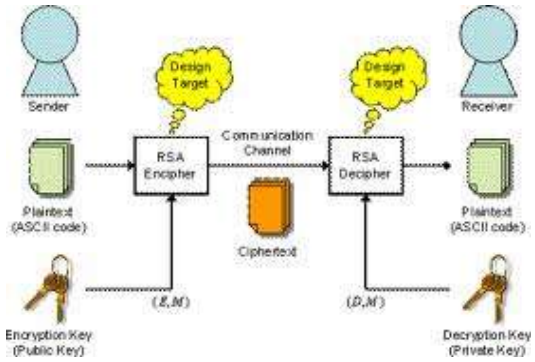

Fig.2 RSA Algorithm

Results and Discussion

Sample data for implementing RSA algorithm:

Key Generation:

1. We have chosen two distinct prime numbers p=17 and q=11.
2. Compute n=p*q, thus n=17*11=187.
3. Compute Euler's totient function, Ø(n)=(p-1)*(q-1), Thus Ø(n)=(17-1)*(11-1) =16*10 = 160
4. Chose any integer e, such that $1 < e < 160$ that is co prime to 160. Here, we chose e=7
5. Compute d ,
$d = e^{-1} \pmod{Ø(n)}$,
Thus $d=7^{-1} \pmod{160} = 23$.
6. Thus the Public-Key is (e, n) = (7, 187) and the Private- Key is (d, n) = (23,187). This Private-Key is kept secret and it is known only to the user.

Encryption:
1. The Public-Key (7, 187) is given by the Cloud service provider to the user who wishes to store the data.
2. Let us consider that the user mapped the data to an integer m=88.
3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user.
$C = 88^7 \pmod{187} = 11$
4. This encrypted data i.e., cipher text is now stored by the Cloud service provider.

Decryption:
1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
2. The cloud user decrypts the data by computing, $M = c^d \pmod n$
$M=11^{23} \pmod{187} = 65$.
3. Once the M value is obtained, user will get back the original data.

Conclusion

Cloud computing is a new evolving way where on demand computing is available. Here cloud services are easily available on pay-per-use basis. By putting the data on cloud it decreases the control on data by the organisation, thus we have to provide the new security techniques to protect that data that relies on some of the cryptography algorithms, So that only authenticated user can access the data irrespective of the number of users who can capture it. Data security is provided by implementing RSA algorithm. This paper represents implementation of RSA through encryption and decryption procedure. Future scope should be in RSA cryptography in comparison of another cryptography algorithm, and Developing another algorithm, merging two algorithms which provide more security.

References

1. *B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers", International Journal Of Engineering And Computer Science, Vol.1, pp. 63-66, 2 Nov 2012.*
2. *Shilpi Gupta and Jaya Sharma "A hybrid encryption algorithm based on RSA and diffie hellman", IEEE International Conference on Computational Intelligence and Computing Research, pp.1-4, Dec 2012.*
3. *Wuling Ren and Zhiqian Miao, "A hybrid encryption algorithm based on DES and RSA in Bluetooth communication", Second International Conference On Modeling,*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Simulation and Visualization Methods, pp. 221-225, May 2010.

4. *Mandeep Kaur, Manish Mahajan, "using encryption algorithms to enhance the data security in cloud computing, "International journal of communication and computer technologies", ISSN Number: 2278-9723.*
5. *Yan Wang, Ming Hu , Timing evaluation of the known cryptographic algorithms, College of Computer Science Wuhan University of Science and Engineering, 2009 International Conference on Computational Intelligence and Security*
6. *Abhishek Patial, Suny Behal, "RSA Algorithm achievement with Federal information processing Signature for Data protection in Cloud Computing" International Journal of Computers and Technology,2012.*
7. *Bernd Grobauer, Tobias Waloschek, and Elmar StöckerSiemens," Understanding Cloud ComputingVulnerabilties", Security & Privacy, IEEE, Vol : 9 ,Issue: 2, Pages: 50 – 57, March-April 2011.*

[8] Khaled Salah, Jose M. Alcaraz, Sherali Zeadaly,Samera Al-Mula and Mohammed Alzabi, "UsingCloud Computing to Implement a Security OverlayNetwork", security & privacy IEEE, vol. 1, Issue: 1, pages: 4 – 53, Jan.-Feb. 2013.

8. *Amazon Web Services. 2009. Amazon Web Services: Overview of Security Processes. [Online] Available from: http://aws.amazon.com/ec2/ [Accessed 26th April 2010]*
9. *Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and InformationTechnologies, Vol. 2 , 1836-1840,2011.*