Data Security in Cloud using RSA

Dhaval Jha[1] Vishva Tanna[2] Ripal Patel[3]
[1]Department of Computer Science [2, 3] Department of IT
[1, 2, 3] Nirma University

Abstract--- The security of cloud computing has always been an important aspect of quality of service from cloud service providers. However, cloud computing poses many new security challenges which have not been well investigated .The prevalent problem associated with cloud computing is data privacy, security, anonymity and reliability etc. But the most important between them is security and how cloud provider assures it. The proposed work plan is to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud as per different perspective of cloud customers. This paper focuses on issues relating to the cloud data storage methods and security in virtual environment. We propose a method for providing data storage and security in cloud using public key cryptosystem RSA. Further, describes the security services includes key generation, encryption and decryption in virtual environment.

Keywords: - RSA algorithm, Data Encryption, Cloud Computing, Data Security, Data Decryption

I. INTRODUCTION

Cloud computing proposes new model for computing and related issues like compute, storage, software. It provides development environment, allocation and reallocation of resources when needed, storage and networking facility virtually. It is almost everywhere. It promises to cut operational costs and more importantly let IT departments focus on strategic projects instead of keeping datacenters running. It satisfies the on-demand Needs of the user. It facilitates the sharable resources "as a-service" model. Cloud Service Providers maintains Computing resources and data automatically via software. The concept of Cloud computing is associated with those of IaaS ,PaaS and SaaS. Cloud computing has five attributes: elasticity, massive scalabilty ,multi-tenancy, ty, pay as you go, and self-provisioning of resources, it makes new advances in processors, Virtualization technology, disk storage, broadband Internet connection, and fast, inexpensive servers have combined to make the cloud a more compelling solution. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services. Data security is an important aspect of quality of service as a result, Security must be imposed on data by using encryption strategies to achieve secured data storage and access. In this work, we implement RSA algorithm before storing the sensitive data in cloud. When the authorized user request the data for usage then data decrypted and provided to the user. This paper propose a method for Cloud Computing system by providing data storage and securing Cloud Computing system using RSA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system.

II. BASIC SERVICE MODELS

According to service model, cloud computing can be categorized into three main categories :

A. Platform-as-a-Service (PaaS)

PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install software. PaaS services include application design, development, testing, deployment, and
hosting. Other services include team collaboration,web service integration, database
integration, security, scalability, storage, state management, and versioning.

B. Sotfware-as-a-Service (SaaS)

Cloud applications can be built as compositions of other services from the same or different providers. Services such user authentication, e-mail, payroll management, and calendars are
examples of building blocks that can be reused and combined in a business solution in case a single, ready-made system does not provide all those features.

C. Infrastructure-as-a-Service (IaaS)

Public Infrastructure as a Service providers commonly offer virtual servers containing one or more CPUs, running several choices of operating systems and a customized software stack. In addition, storage space and communication
facilities are often provided.

III. TYPES OF CLOUDS

There are basically four types of clouds, which are as below :

A. Public cloud:

This is the one of the cloud in which cloud services are being available to users via a service provider over the Internet. It provides a control mechanism for them. The services may be free or offered on a pay-per-usage model.

B. Private Cloud :

This provides many of the benefits of public, but the main difference among two is that the data is managed properly within the organization only, without the limits of network bandwidth.

C. Community Cloud :

This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud.

D. Hybrid Cloud :

This is the combination of public as well as private cloud. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one system to another.

IV. DATA SECURITY ISSUES IN THE CLOUD

A. Data Availability:

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

B. Privacy and Confidentiality:

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

C. Governance

Governance implies management and oversight by the organization over procedures, standards and policies for application development and data technology service acquirement, also because the style, implementation, testing, use, and watching of deployed or engaged services.

D. Compliance

Compliance refers to an association's responsibility to work in agreement with established laws, specifications and standards. One with all the foremost common compliance problems facing a company is an information location means storage of data or information.

E. Malicious Insiders

'Malicious insiders' impact on the organization is considerable. Malicious insiders are the threat which has access to the data or information about the organization being a member of the organization. As cloud consumers application data is stored on cloud storage provided by cloud provider which also has the access to that data.

F. Account or service Hijacking

This threat occurs due to phishing, fraud and software vulnerabilities. In this type attacker can get access to critical areas onto the cloud from where he can take permit and steeling important information leading to compromise of the availability, integrity, and also confidentiality to the services.

G. Cross Site Scripting (XSS)

This occurs when the application accepts untrusted data and sends it to the browser without proper validation. Attackers can execute scripts to hijack the user's session, steal cookies, deface websites and redirect users to malicious web sites. The 3 types of XSS attacks are stored, reflected and DOM.API's pose a huge problem as a data security issue in the cloud.

V. PROBLEMS DEFINITION

Cloud Storage system provides the user for safe and consistent place to save valuable data and documents. However, user's files are not encrypted on some open source cloud storage systems, such as Hadoop and Sector. In the past, there is no known way to completely handle encrypted data, unless the cloud data is only used for simple storage .The storage service provider can easily access the user's files. This brings a big concern about user's privacy. The user has no supreme control over the software applications including secret data. User has to depend on the provider's action, maintenance and admin it. The user does not have direct access to the software to fix the problems while something goes wrong in any application and its valuable data.

VI. PROPOSED WORK- RSA ALGORITHM

RSA is widely used Public-Key algorithm.RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it .User data is encrypted first and then it is stored in the Cloud. When required, user places are quest for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public -Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Thus with the use of this algorithm we can prove that once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only and thus keeps the data secure thus solving the problem.

A. RSA algorithm: involves three steps:

A. Key Generation
B .Encryption
C..Decryption

VII. IMPLEMENTATION

A. Key Generation Steps

1. We have to choose two distinct prime numbers p and q. The integers p and q should be chosen at random for security purposes, and should be of similar bit-length.
2. Next we compute $n = pq$.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime. e is released as the public key exponent.
5. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$). d is kept as the private key exponent.

B. Encryption Steps

1. Input : integers k, n, M is integer representation of plaintext message
2. Computation : let C be integer representation of cipher text C = (Mk)%n
3. Output : integer C

C. Decryption Steps

1. Input : integers d, n, C is integer representation of cipher text message

2. Computation : let D be integer representation of decrypted cipher text D = (Cd)%n
3. Output: integer D

D. A Simple Worked Example

1. Choose two distinct prime numbers, such as $p = 61$ and $q = 53$
2. Compute $n = pq$ giving $n = 61 \times 53 = 3233$
3. Compute the totient of the product as $\varphi(n) = (p - 1)(q - 1)$ giving $\varphi(3233) = (61 - 1)(53 - 1) = 3120$
4. Choose any number $1 < e < 3120$ that is co prime to 3120. Choosing a prime number for e leaves us only to check that e is not a divisor of 3120. Let $e = 17$
5. Compute d, the modular multiplicative inverse of e (mod $\varphi(n)$) yielding $d = 2753$
6. The **public key** is (n = 3233, e = 17). For a padded plaintext message m, the encryption function is $c(m) = m^{17} \bmod 3233$
7. The **private key** is (n = 3233, d = 2753). For an encrypted cipher text c, the decryption function is $m(c) = c^{2753} \bmod 3233$.
8. For instance, in order to encrypt m = 65, we calculate $c = 65^{17} \bmod 3233 = 2790.$
9. To decrypt c = 2790, we calculate $m = 2790^{2753} \bmod 3233 = 65$

VIII. Conclusion

Cloud computing is a technology that keep up data and its application by using internet and central remote servers . Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at lower cost. Because of this, cloud computing has been receiving a good amount of attention lately and many people have been shifting to the cloud solution . Cloud computing is an Internet-based computing solution where shared resources are provided like electricity distributed on the electrical grid. Computers in the cloud are configured to work together and the various applications use the collective computing power as if they are running on a single system. The RSA provides the high security in high potential data encryption methodology.

IX. References

[1] Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh, A survey of cryptographic algorithm for cloud computing.
[2] Pachipala Yellamma, C h a lla Narasimham, Velagapudi sreenivas, Data Security in cloud using RSA.
[3] Jay Singh, Brajesh Kumar, Asha Khatri, Improving Stored Data Security In Cloud Using Rc5 Algorithm.
[4] Ashutosh Kumar Dubey , Animesh Kumar Dubey , Mayank Namdev, Shiv Shakti Shrivastava, Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment.

