ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Implementing Multiprime RSA Algorithm to Enhance the Data Security in Cloud Computing

Suganya .N[1], N.Boopal M.E[2], Naveena .M[3]

Assistant Professor, Department of CSE, N.S.N. College of Engineering and Technology, Karur, Tamilnadu, India[1]

Assistant Professor, Coimbatore Institute of Engineering and Technology, Coimbatore, Tamilnadu, India[2]

Assistant Professor, Department of CSE, N.S.N. College of Engineering and Technology, Karur, Tamilnadu, India[3]

ABSTRACT: Cloud computing is an internet based technology where a large amount of resources are shared as a service. It is a Payment-based model where the users can pay for what they can use. The resources available in the cloud can be shared "as-a-service". Many business organizations have fear in storing their data in cloud due to the negative impacts in cloud. Different encryption strategies have been carried out for attaining the secure data storage and access security. In this work, we implement Multi-prime RSA algorithm in the middle layer before the data is stored in the cloud environment. When an authorized user requests the data, then the data is decrypted and provided to the user.

KEYWORDS: Cloud computing, Multi prime RSA, Encryption

I. INTRODUCTION

In cloud, the stored documents and the applications can be accessed from anywhere in the world. So many of the users can access the resources in cloud systems. The resources are provided as a service to the user such as SAAS(software as a service) where the internet based applications are offered as a service, PAAS(Platform as a service) where the platforms are used to design, deploy and test the applications, IAAS(Infrastructure as a service) where the servers, storage systems, datacenter are provided for storage. These service models are referred to as **SPI** models [2].

The resources provided in the cloud may shrink down and wrap up depending on the needs of the customers. In cloud there exists a legal agreement between the customer and the cloud service provider known as service level agreement (SLA).Cloud computing is flexible, cost-effective and it also increases the efficiency of computing. Based on the services available in the cloud, the architecture of the cloud may vary.

II. CHARACTERISTICS

ON-DEMAND SELF-SERVICE

Cloud computing allows their users to control their own virtual resources without any service providers intervention such as server time and network storage. Through a self-service portal the consumers use cloud templates to move applications between clouds[12].

DYNAMIC PROVISIONING

Cloud capabilities are elastically provisioned. Automatic shrink and wrapping of the capabilities based on the users demand and the user can pay for what they use. At peak time, the capabilities can be expanded to handle the workloads.

BROAD NETWORK ACCESS

Cloud capabilities are accessed over the network from a wide range of devices such as PCS, mobile devices, laptops [2]. The cloud can be approached by standard mechanisms that use heterogeneous thick and thin client.

MANAGED METERING
Cloud environment is a subscription-based model. The billing depends on what the users use and pay for it. It reduces the infrastructure implementation cost and maintenance cost.

HIGH AVAILABILITY
Cloud computing use multiple copies to manage the data. If any single [13] point of failure occurs then the application will be managed by other resource**.**

III. SECURITY ISSUES IN CLOUD COMPUTING

Though cloud offers different advantages but we cannot say it is hundred percent reliable. Security in cloud is consistently increasing when the applications and data are moving to the cloud because [9] the individual loss of control over their data. Despite from the potential benefits it has lots of open issues such as virtualization, multi-tenancy, vendor lock-in, data security, cloud secure federation [1], insecure application programming interface, lack of standards.

IV. PROBLEM STATEMENT

Cloud provides prominent advantages from small businesses to large-scale industries but when data is moved to cloud the customer loss the control of their own data. The loss of control outside the secure corporate parameter increases the risk of compromise. To ensure the data integrity, the data needs to be protected by using strong encryption. In certain circumstances, the user data will be progressed by the third party auditor where the security gets lag, because of implementing encryption techniques at the provider’s environment alone.

V. RELATED WORK

The paper is mostly related to works in security of the user’s data. Some of the works are listed below.
In [7] third party auditor and auditing mechanisms are proposed. Auditing is the process of tracing and logging the system events that happen during the run time. A third party auditor who has resources can audit the user’s data in cloud. Privacy preserving public auditing and challenge-response protocols were implemented to ensure data integrity by auditing. In addition with auditing, master checklist is used implemented for correctness of the data in all stages of the service models.

In [4] stated that inside threats are possible still having advance firewall and security. The security issue occurs when external customers can store their data in cloud in which any employee in the cloud could manage the misuse of the data. The data stored in the cloud will exhibit a high level of availability. The data stored in the cloud can be accessible only to the user who owns the data. The authorization and authentication, password protecting are maintained for access control.

If a customer is dissatisfied with any one of the computing service provider, then they can make a move to another one. During this, the company needs to reformat the data and applications and then transfer them to the new provider. Open standards are used to resolve the issues. The hypervisor in the virtualization technique is modified on the host operating system so that the attacker can access it and install the rootkit. Modified versions of the virtualization product are used to prevent this attack.

The host operating system can be maintained properly. If an attacker can get the control of the operating system [4] then they control all the host operating system functions. To protect the host operating system from the attacker, the minimal operating system is chosen to be stripped for all unnecessary service.

The customer in the cloud can create and modify their own virtual private servers. This results in many operating systems, running in a single system and it is easy for the attacker to find vulnerability in one of the system. Isolation between the systems is necessary to prevent from attack. Transferring data from and out the cloud have security issues.

Since some one can listen the network and intercept the information. Encryption techniques are used to prevent these security issues.

The data should be backed up as well as appropriate level of data mirroring is implemented. Firewalls are implemented to prevent information which resides in the cloud from DDos and Dos attacks [6].

In [14] stated that symmetric and asymmetric key encryption methodologies are used to improve the security. Before storing the data at the cloud server the data will be encrypted using the encryption strategies. The symmetric encryption uses single key for both encryption and decryption while the asymmetric method uses separate key for encryption and decryption. Data integrity is verified because only the authorized person who knows the key can decrypt and modify the data.

In [1] discusses the security issues in cloud and the methods to resolve those issues. Multi-tenancy arises due to sharing of physical, logical and other resources in cloud, creates confidentiality issues. To overcome these shortcomings isolation process is maintained among the tenant data and that should be arise in VM's, storage, Processing, memory, running services, API's as well as in operating system. The consumers scale up and down the resources based on the demand. Due the scale up and down of the need the same resource will be used by some other tenant. Placement Engines are used to maintain a list of available resources. This list is used to allocate resources to the users based on the demand. Cloud secure federation occurs when a customer uses different services from different clouds; it will need to maintain its security requirements enforced by both cloud providers. User identity, authorization and authentication, single-signon will resolve federation issues.

VI. PROPOSED FRAMEWORK

To improve the security of the user's data RSA algorithm is implemented as a middle secure layer of web services. Whenever the user wants to store their data in cloud, the user could login into the system and access the web service to encrypt their data. The Multi-prime RSA algorithm generates a public and a private key with the help of randomly chosen prime numbers. The user's data will be encrypted by using public key and send to the cloud environment. The private key is kept as secret. Whenever the user wants to access the data, it will be retrieved from the cloud as an encrypted format and decryption is done at the user's environment using the private key.

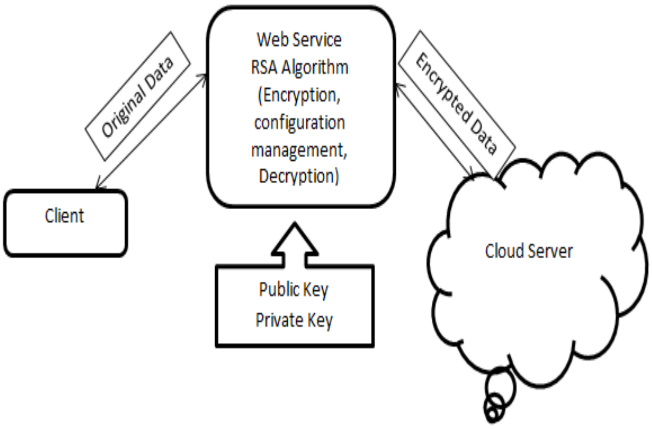

Figure:1 Architecture Diagram

VII. MULTI PRIME RSA ALGORITHM

Multi-prime RSA is an isolated version of RSA cryptosystem. In Multi-prime the modulus consists of more than two prime numbers and the decryption will be speed-up by using Chinese remainder theorem.
Multi-prime RSA is composed of three phases

i)Key Generation
ii)Encryption
iii)Decryption

For any integer, r>= 2, r-prime RSA consists of the following three algorithms.

Key Generation:

Let N be the product of r, randomly chosen distinct primes $p_{1.....}p_r$. Compute Euler's Totient function of N:$\varphi(N) = \Pi_{i=1}^{r}(p_i-1)$. Choose an integer e, $1 < e < \varphi(N)$, such that gcd(e,φ(N)) =1. The pair (N; e) is the public key. Compute the integer d € Z_N such that ed ≡ 1 mod φ(N), here d is the private key[11].

Encryption:

For any message M € Z_N, the cipher text is computed as $C \equiv m^e$ mod N[5]

Decryption:

Decryption is done using the Chinese remainder theorem. Let di ≡d mod (p_i-1). To decrypt the cipher text C, one can first computes $M_i \equiv$ ´ $C^d{}_i$ mod p_i for each i, 1<= i<=· r, then combines the M_i's using the CRT to obtain $M \equiv C^d$ mod N.

VIII. EXAMPLE FOR MULTI PRIME RSA

1. Let us choose an integer r as 15,such that 15>=2.
2.Let N be the product of randomly chosen prime numbers as 2,3,5,7,11 and 13.So we get N as 30030
3.The Euler's totient function is computed such that φ(N)=5760
4.Choose e, such that e is not a factor of 5460
5460=2*2*2*2*2*2*2*2*3*5
So e can be either 7 or 11 or 13….
Let it be 7
5.Compute d such that ed≡l mod φ(N)
d= 823
Public key(30030,7)
Private key(30030,823)
6.Encryption:
If the message is M, then the value of the message M<N.Let us choose M=5[8]

$C \equiv m^e$ mod N
$C \equiv 5^7$ mod 30030
C=18065

7.Decryption:
By using chinese remainder theorem we combine M_i. After that we find M.

$M \equiv C^d$ mod N
$M \equiv 18065^{823}$ mod 30030
M=5

IX. METHODOLOGY
X.

In completing these objectives, our work will provide the following contributions:

In client phase, the client sends the query to the server. Depends on the query the server responds to the client with the corresponding file. Before this process, the client authorization step is involved. In the server side [10], it checks the client name and its password for security process. If it is satisfied, the queries are received from the client and the corresponding files are searched in the database. Finally, the corresponding file is retrieved which will be send to the client [3].

In the second phase, virtual setup is configured. Since virtual machines are dynamic, they can quickly be reverted to previous instances, paused and restarted, relatively easily. Virtualization technology allows the user to run multiple operating systems simultaneously on a single physical machine sharing the underlying resources. The user's subscribed applications are stored in the datacenters which is a collection of servers.

In third phase, encryption strategy will be implemented. Encryption is done on the endpoint before being sent across the network or is already stored in a suitable encrypted format. Stored object is used as the back end for an application, data gets encrypted by using an encryption engine, which is embedded in the application or client. Multi prime RSA is an asymmetric algorithm in which different keys are used for both encryption and decryption.

It is an efficient and independent examination of data, records of an enterprise for a stated purpose. It is maintained and reviewed properly to overcome security issues. Whenever the client login and updates or request for the any activity it is recorded and reviewed properly.

XI. CONCLUSION AND FUTURE WORK

Security is the major concern in all the emerging technology because users often work with sensitive data. The cloud computing is a hopeful technology, but to better use of technology we need to block the security holes. The users can keep their data secret only if they are having proper security policies. To achieve this we implement the technique at the client side in the cloud. Encryption plays a vital tool in preventing threats to preserve the data integrity. Even encryption is implemented there exists a lot of security problems.

In future, we will try to concentrate on more confidentiality issues in cloud computing and give some better solutions to achieve robust security using cryptographic techniques in data security. Some hybrid algorithms may be proposed to achieve better security with security-as- a-layer in cloud.

REFERENCES

[1] Akhil Bhel and Kanika Bhel (2012) “An Analysis of Cloud Computing security issues” World Congress on Information and Communication Technologies.

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

[3] Cong Wang, Qian Wang, and Kui Ren and Wenjing Lou (2011) “Ensuring Data Storage Security in Cloud Computing”- IEEE Transaction on Parallel and Distributed Systems, Vol. 22, No. 5.

[4] Eystein Mathisen (2011) “Security challenges & solutions in cloud computing” 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST), Daejeon, Korea.

[5] Esh Narayan,Mohit Malik,Aman preet singh and Prem Narain “To Enhance the Data Security of Cloud in Cloud Computing using RSA Algorithm” International Journal of Software Engineering vol.1 No.1 sep 2012.

[6] Gurudatt Kulkarni & Jayant Gambhir, Tejswini Patil, Amruta Dongare (2012) “A security aspect in cloud computing” 3rd IEEE International Conference on Software Engineering and Service Science (ICSESS).

[77] Irfan Gul, Atiq ur Rehman and M Hasan Islam (2011) “Cloud computing security Auditing”, 2nd International Conference on Next Generation Information Technology (ICNIT).

[8] Navaneet Ojha and Sahadeo Padhye “Cryptanalysis of Multi Prime RSA with Secret Key Greater than Public Key” International Journal of Network Security, Vol.16, No.1, PP.53-57, Jan. 2014

[9] Rashmi Rao & Pawan Prakash “Improving security for data migration in cloud computing using randomized encryption technique” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 6 (May. - Jun. 2013), PP 39-42.

[10] N.Saravanan, A.Mahendrian, N.Venkata Subramanian and N.sriram “An Implementation of RSA Algorithm in Google Cloud using Cloud SQL” Research Journal of Applied Sciences,Engineering and Technology mar 2012.

[11] P.Saveetha & S.Arumugam “Study on improvement in RSA algorithm and its implementation” International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3, Issue-6, 7, 8, 2012.

[12] Shivlal Mewada , Umesh Kumar Singh and Pradeep Sharma (2011)“Security Based Model for Cloud Computing”, IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1.

[13] Wang Jun-jie & MuSen (2011) “Security Issues and Countermeasures in Cloud Computing” IEEE Conference on Grey Systems and Intelligent Services (GSIS).

[14] Wentao Liu (2012) ”Research on Cloud Computing Security Problem and strategy” 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).