 ISSN: 2321-8169
3297 – 3300

Accelerating Security on Cloud Based Data

Anandteerth Gopal Onkar
ME Research Scholar
JSPM Imperial College of Engineering,
Pune, Maharashtra, India.
anandteerthonkar@gmail.com

Dyaneshwar Rokade
Asst. Professor
JSPM Imperial College of Engineering,
Pune, Maharashtra, India.
drokade2006@gmail.com

Abstract — The rapid emergence of cloud computing is transforming the way organizations promoting their IT resources. Studying the diversified security aspects, data security can be contemplated as one of the challenging factor to organizations retaining cloud infrastructure. This paper reviews the data security challenges. Based on which we propose a model for storing confidential data over cloud, using enhanced public key cryptographic scheme of RSA. This model proposes a strong and fast cryptography along with user access control.

Keywords- *Cloud Computing, Data Security, Public Key Cryptography, RSA.*

*****

I. INTRODUCTION

Cloud computing being an evolving paradigm, characterizes important aspects of cloud computing which intends to compare of cloud services and deployment strategies and provides a baseline how efficiently cloud computing can be used.

The NIST cloud computing definition [1] is universally accepted which provides a clear understanding of cloud computing technologies and cloud services. It provides a univocal taxonomy of three service models available to cloud consumers: Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). It also summarizes four deployment models describing how the computing infrastructure that delivers these services can be shared: private cloud, community cloud, public cloud, and hybrid cloud. Finally, the NIST definition provides five essential characteristics that all cloud services exhibit: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

The NIST cloud computing reference architecture [2], identifies the major actors, their activities and functions in cloud computing. The diagram depicts a generic high-level architecture that helps to understand the role of each entity in cloud computing.

Market insight for Cloud Computing

With evolution of Cloud Computing, there has been a rapid growth for adoption of various cloud services, creating a high growth curve for the segment [6]. Conventionally the public cloud services industry is to show an annual growth rate of 17.7% in next five years (Refer Figure 2). The IaaS subdomain can showcase exponential growth at a rate 41.3%.

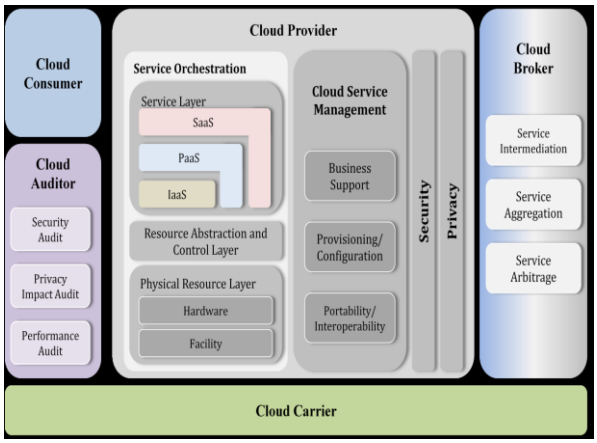


Figure 1: The Conceptual Reference Model

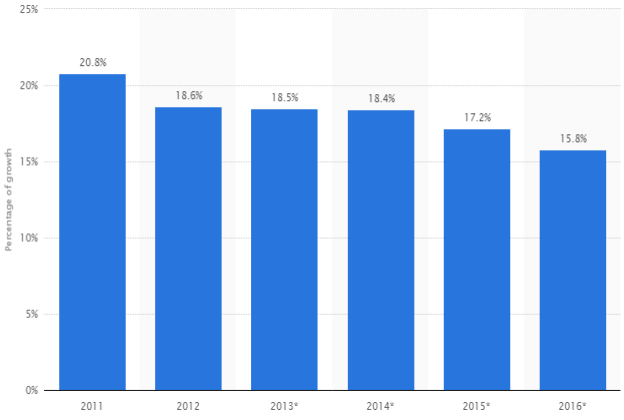
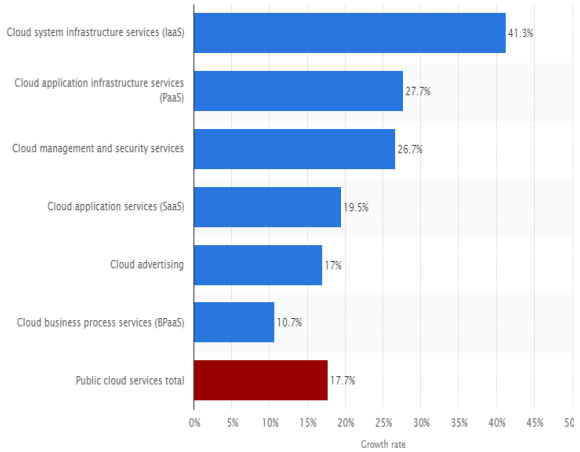


Figure 2 – Growth Rate of Public Cloud Service.

The forecast (Refer Figure 2) of public IT cloud services from 2011 to 2016 depicts the IT cloud services of the global market [7]. In 2012, the market was bullish at the rate of 18.6%. A durable growth rate is expected in coming years.



The Indian market has managed witnessed a desirable movements in cloud technology in the course of time. The cloud services market growth rate in India has shown at 32.2% in 2014 to total USD 556.8 million, as per a Gartner report [4]. The total cloud market of the country in 2013 was USD 421 million and is expected to reach USD 1.7 billion in 2018 [5].

Data in Cloud

Adoption of cloud does not mean mere replacement of data centers. It is completely a new IT delivery model and lot of business both within IT and Business needs revitalization. Cloud computing usually is served by a third-party known as cloud service provider (CSP). The CSP have their own network of remote servers which are hosted on the internet to store and manage data. In simple words, cloud services enables consumers to own a secured private hard drive in the cloud. The demand public cloud services is growing as it is easily affordable to all types of consumers, convenient to use and the storage capacity is high. Apparently the biggest concern of these services is the accessibility; as consumers can access their data from any device with internet access, due to which consumers can access their data from anywhere, with compatible smart devices.

Many giant IT firms have launched cloud services viz. Apple, Amazon EC2, Google, Microsoft, Rackspace etc., who provide several storage tier plans tailored for both consumers and businesses. Some firms may proclaim themselves as cloud services, but ironically they tend to serve online backup or file sharing services. Though they sound to be akin, but certainly there are discrepancy between each of these services, cloud services stands to be unique as they allow to view, edit and share files saved in the cloud. With some services, consumers
can even sync content across all your computers and devices. For this reason the consumer forecast their cloud service providers on Integrity and Availability of data. Downtrend of Amazon S3 [3], is one of such cases occurred.

II. PROBLEM STATEMENT

With emerging trends in cloud, Information Security becomes one of the critical issue, as there is lack of data transparency, wherein the consumers are unfamiliar about the storage location of data, over geographically distributed datacenters. This feature of cloud computing raises several concerns with respect to consumer's authentication, information integrity and confidentiality. Ultimately this influences to propose an enhanced security model in order to optimize the information security triad CIA – Confidentiality, Integrity and Authentication to store and access data from and to data centers with user access rights.

III. RELATED WORK

In [8], they analyze the security challenges in cloud based data along with the possible solutions to overcome these challenges. The data may exist in several phases in its complete lifecycle, from the time it is created, stored, used, archived or shared till its destruction. They address the security for data in cloud related to its form viz. in-transit, at-rest, at process etc. depending on which appropriate security measure that must be taken into consideration is depicted.

In [9] insights the security issues associated with cloud data storage. A data is vulnerable while it's been uploaded on cloud across distributed data centers, during which the user verification is carried out by misconducting nodes. They firmly believe that their scheme is effective to handle certain failures, malicious data modification attack, and even server colluding attacks. This scheme loopholes to new security challenges, leading to unexpected ironies in research areas that are yet to be diagnosed and worked upon.

In [10] an overview of considerable privacy issues within cloud computing is described. They also contribute a detailed analysis on privacy threat, hinged on the type of cloud implemented based on which, the severity of threat diverge conferring to the area of application. Their work describes the necessary guidelines that should be taken into consideration for software engineers while scheming cloud services, ensuring that the privacy is not weakened. The main aim of their under laid scheme focuses on the risks, threats, design patterns and accountability with in cloud computing scenario.

In [11] they provide an overview of security mechanism along with the issues faced while choosing a security mechanisms in the context of cloud. Apparently they describe various threats, its potential impact and relevance to real-world cloud environment. From their research and investigation, we can conclude that to improve data security in cloud it is necessary to exaggerate the security capability for web applications and frameworks.

In [12] they describe issues related to storage of data in cloud along with its sustainability in virtualized environment, to which they have proposed a method to store data further the security to data is accomplished using public key cryptography algorithm RSA. Though using RSA would guarantee high security, but simultaneously would arise issues related to performance.

IV. PROPOSED WORK

Studying the above research works by scholars, we tend to propose a secure system with elevated performance.

PROPOSED ARCHITECTURE

In this section we schematically propose our security model for cloud computing, which focus on accelerated security and performance. The proposed architecture is as shown in Figure 3, which has three major entitles – the

organization network, a front-end encryption tool and cloud storage provider.

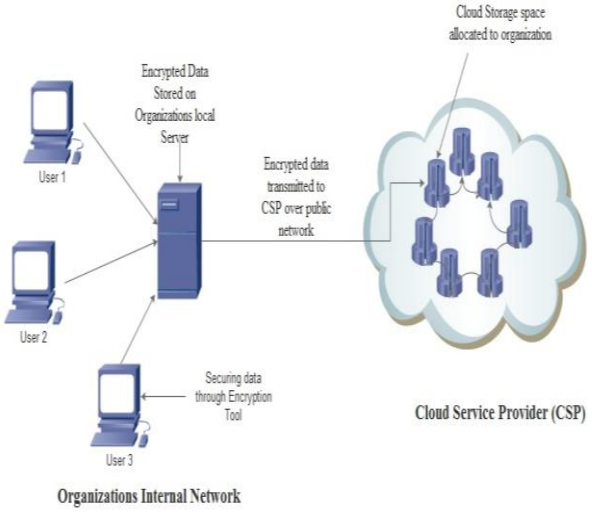


Figure 3: Proposed Architecture

PUBLIC KEY CRYPTOGRAPHY - RSA

RSA's mechanism is based on a mathematical theory, which encodes data using defined algorithms. RSA being a Public-key encryption algorithm it proves to be highly secured encryption systems other than the traditional ones, which uses a single "key" to encode and decode data.

RSA has three major steps:-

- Key Generation
- Encryption
- Decryption

RSA key generation is the initial stage wherein two keys are generated using various methods that would be further used for encryption and decryption purpose. RSA's encryption products use two keys.

For Example: - Consider a person 'A' who possess public key and a private key that is associated with an encryption algorithm, if he wished to send/receive encrypted data, he needs to share his public key with the person he wants to send/receive encrypted information. The key is sent publically, so it can fall into wrong hands, therefore a private key is used by person 'A', to decode the encrypted information.

Alternately, person 'A' can encrypt the information using his private key and send it to the people who are aware of person 'A' public key. Using person 'A' public key, the recipient can decode the encrypted message. The proof of authenticated information is accomplished when other person are able to decrypt the message. In addition person 'A' could send two pieces of information, one original and other scrambled. When these information are decrypted and they match, it guarantees that the information is genuine and has not been tampered while in flight. Thus RSA not only secures the data, but also authenticates the sender's identity, which verifies the integrity of received data.

ENHANCED RSA ALGORITHM:

The RSA encryption mechanism we propose will have-

- Key generation using BigInteger Library.
- Encryption
- Fast Decryption using Chinese Remainder Theorem (CRT).

BigInteger Library

The BigInteger class [14] operations are similar to integer operators, along with other operations such as GCD calculation, prime generation, modular arithmetic, primarily testing, bit manipulation, and other miscellaneous operations. All operations in BigInteger's are represented in two's-complement form. To generate public and private keys using BigInteger Library, it is important to understand the mathematical calculations underneath RSA algorithm.

RSA Algorithm:

Key Generation:

- Select two prime numbers p and q randomly.
- Calculate N=p * q;
- Calculate ϕ (N) = (p-1) * (q-1)
- Choose an integer 'e' such that GCD (e, ϕ (N)) =1
- Find out'd' such that d ≡ e-1 (mod (ϕ (N))
- Pair of Public Key => {e ,N}
- Pair of Private Key => {d, N}

Encryption:

- First modify the original text into integer value M.
- Then find the cipher text using the equation

C=Me mod N.

Decryption:

- To decrypt the encrypted/cipher text use the following equation

M = Cd mod N.

Fast Decryption using Chinese Remainder Theorem (CRT):

The core concept of CRT is to split the huge decryption data into two smaller and faster exponentiations [13].

Steps for RSA using CRT:-

- Calculate 'e' &'d'.
- Evaluate dp = d mod p-1.
- Evaluate dq = d mod q-1.
- Therefore the keys are generated with following pairs:
  Pair of Public key {e, N},
  Pair of Private Key {p, q, dp, dq}.
- Encryption is done in similar fashion as that of normal RSA.
- Decryption is accomplished by splitting the encrypted information into two computations.
  First Computation: Mp = Cdp mod p
  Second Computation: Mq = Cdq mod q.
- Calculate

M = (Mpq (q-1 mod p) + Mqp (p-1mod q)) mod N based on CRT.

V. CONCLUSION AND FUTURE WORK

Today world is moving towards cloud computing, but the security concerns at various levels have grown which must be addressed. In this paper, we reviewed several security challenges in cloud computing and propose a security tool for secure cloud computing environment.

We have provisioned the faster implementation algorithms of RSA using the BigInteger library and CRT to implement in software at a faster rate. Research is currently under progress to make RSA implementation faster without compromising on the security of the algorithm.

On future work would be focused on developing a complete security framework that would cover all security aspects related to data. We assume that this pilot project would tend to benefit the institutions/organizations to migrate to Cloud environment and build robust IT infrastructure.

VI. ACKNOWLEDGMENT

First of all we are thankful to International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC) for providing us a platform to publish our research papers. I would like to thank Prof. Dyaneshwar Rokade, Asst. Professor Faculty of Computer Department at JSMP's Imperial College of Engineering for supporting at various stages while working on this project and Prof. S.R. Todmal, H.O.D of Computer Department at JSMP's Imperial College of Engineering for providing the necessary facilities for the preparation of the paper. Lastly I would like to thank Mr. Shailesh Saple, Sr. Developer at John Deer for his extensive support to overcome the hurdles.

REFERENCES

[1] NIST SP 800-145, "A NIST definition of cloud computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[2] NIST SP 500-292, "NIST Cloud Computing Reference Architecture" http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

[3] N. Gohring, "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/142549/amazon s S3 down for several hours.html, 2008.

[4] "Gartner Says Indian Public Cloud Services Market on Pace to Total $557 Million In 2014", http://www.gartner.com/newsroom/id/2721517, Mumbai, India, April 28, 2014.

[5] "Forecast Analysis: Public Cloud Services, Q14-Update 2012-18", http://www.gartner.com/document/2696318. October 1, 2014.

[6] "Public cloud services five year compound annual growth rate from 2011 to 2016, by segment". http://www.statista.com/statistics/258718/market-growth-forecast-of-public-it-cloud-services-worldwide/. October 2, 2014.

[7] "Market growth forecast for public IT cloud services worldwide from 2011 to 2016", http://www.statista.com/statistics/203578/global-forecast-of-cloud-computing-services-growth/. October 2, 2014.

[8] T V Sathyanarayana and Dr. L. Mary Immaculate Sheela "Data Security in Cloud Computing", International Conference on Green Computing, Communication and Conservation of Energy (ICGCE) 2013, pp 810-813, 14362505/2013.

[9] Cong Wang, Qian Wang and Kui Ren,"Ensuring Data Storage Security in Cloud Computing" 978-1- 4244 -3876-1/2009 IEEE.

[10] Siani Pearson "Taking account of Privacy when Designing Cloud computing Services CLOUD'09", May 23, 2009, Vancouver, Canada, 2009 IEEE.

[11] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On technical security issues in cloud computing" 2009, IEEE Computer Society.

[12] Pachipala Yellamma, Challa Narasimham, Velagapudi Sreenivas, "DATA SECURITY IN CLOUD USING RSA" Computing,Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference, pp.1-6, 978-1-4799-3925-1/2013.

[13] Cetin Kaya Koc, "High-Speed RSA Implementation" Version 2.0, November 1994.

[14] Chew Keong TAN, "C# BigInteger Class", http://www.codeproject.com/Articles/2728/C-BigInteger-Class, October 8, 2014.