RSA Algorithm achievement with Federal information processing Signature for Data protection in Cloud Computing

Mr. Abhishek Patial
Research Scholar

Mr. Sunny Behal
Assistant Professor
Shaheed Bhagat Singh State
Technical Campus, Ferozepur

Abstract

Cloud computing illustrates information technology as a fundamentally diverse operating model that takes advantage of the maturity of web applications, networks and the rising interoperability of computing systems to provide IT services. The Security of data is becoming a fundamental obstruction in cloud computing .There are a numbers of solutions that provide some security with model, some technology. In this paper we attempt to secure data from unauthorized access, by using RSA algorithm.For providing data security by encrypting the given data based on the KEY combinations. This data then can only be decrypted by some authorized person by using his private key. The Google application cloud has been implemented on IJCT Foundation, all data has of IJCT Foundation shifted to Google cloud and RSA security algorithm is implemented by for security data.

1. INTRODUCTION

In past three decades, the world of computation has been distorted from centralized to distributed systems and now we are getting back to the virtual centralization. Arrangement of data and processes put together differentiation in the authority of computation. An individual has been direct control on data and procedure in his/her computer [2].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[10].

As the next generation, Cloud Computing has visional architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under physical, logical and personnel controls [1]. Current cloud service is grant access to web browser or host install application directly [15]. Cloud storage space moves the user's data to large data centers database, on which user does not have any management to manage data [18]. The commercial achievement of Cloud Computing and up to date developments in Grid Computing has been create platform virtualization technology deal with high performance computing [23] by both enterprises and individuals with high service-level requirements [17].

Data security has grow to be predicament of cloud computing like file system, data security, host security. Security is a secure mode practical Internet based on the cloud computing [5]. These are security and trust issue forth, user's data has been liberating to the Cloud and safety measures sphere of the data owner [3]. The data is physically not available to the user the cloud shall provide a way for the user to check if the integrity of his data is maintain [18]. Security model based on key security considerations by looking at a number of infrastructure aspects of Cloud Computing such as SaaS, Utility, Web, Platform and Managed Services, Service commerce platforms and Internet Integration[4] with the rapid development of cloud computing [25]. But it has a negative impact on the effectiveness of caching also other parts of the equation have changed Transmission cost has dropped significantly, and so has the cost to run a cache.

1.1 RSA Algorithm

Data security has grown to be predicament of cloud computing like file system, backup, data security etc. Security is a secure mode practical Internet based on the cloud computing. RSA is an asymmetric cryptography algorithm for encrypting data with help of key which is develops by Rom Rivest, Adi Shamir, and Leonard Adleman in 1978. It is based on the presumed complicatedness of factoring large integers. An asymmetric algorithm has set of key one is public and anther 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.

1. Key generation
2. x, y (prime number)
3. n=x y
4. Ø(n)=(x-1)(y-1)
5. Select random the encryption key e
6. 1 < e <Ø (n).
7. gcd (e, Ø(n)=1)
8. Compute decryption
9. e.d=1 mod Ø (n) & 0<d<n
10. Public key (e. n)
11. Private key (d, n)
12. Encryption plain text $c=m^{e}$ mod n
13. Decryption $d=c^{d}$ mod n

Process	Sender/receiver		Key	
	Sender	Receiver	Public	Private
Send an encrypt Text		✓	✓	
Send an encrypt Sig.	✓			✓
Decrypt Text		✓		✓
Decrypt Sig	✓		✓	

Table 1: Key Management

Federal information processing standard is like digital signature which used for verification of data. FIPS specifies algorithm for data required digital signature that identity of signature. Digital signature converting string to binary digit. It used for verification of data with key .A hash function is used in signature generate process of data

1.2 Google Application Cloud

Google application is a bundle of open recourses for implementing Google application cloud. Google application is services from Google providing autonomously customizable version of several Google products under the custom domain name. It features several Web applications with comparable function to traditional office suite, including Gmail, groups, and Google calendar Talk, Docs and site. In addition to shared apps such as calendar, docs, etc there is Google Apps Market place, which is an application store for Google Apps users. It contains various apps, both free and for a fee [1].

2. RELATED WORK

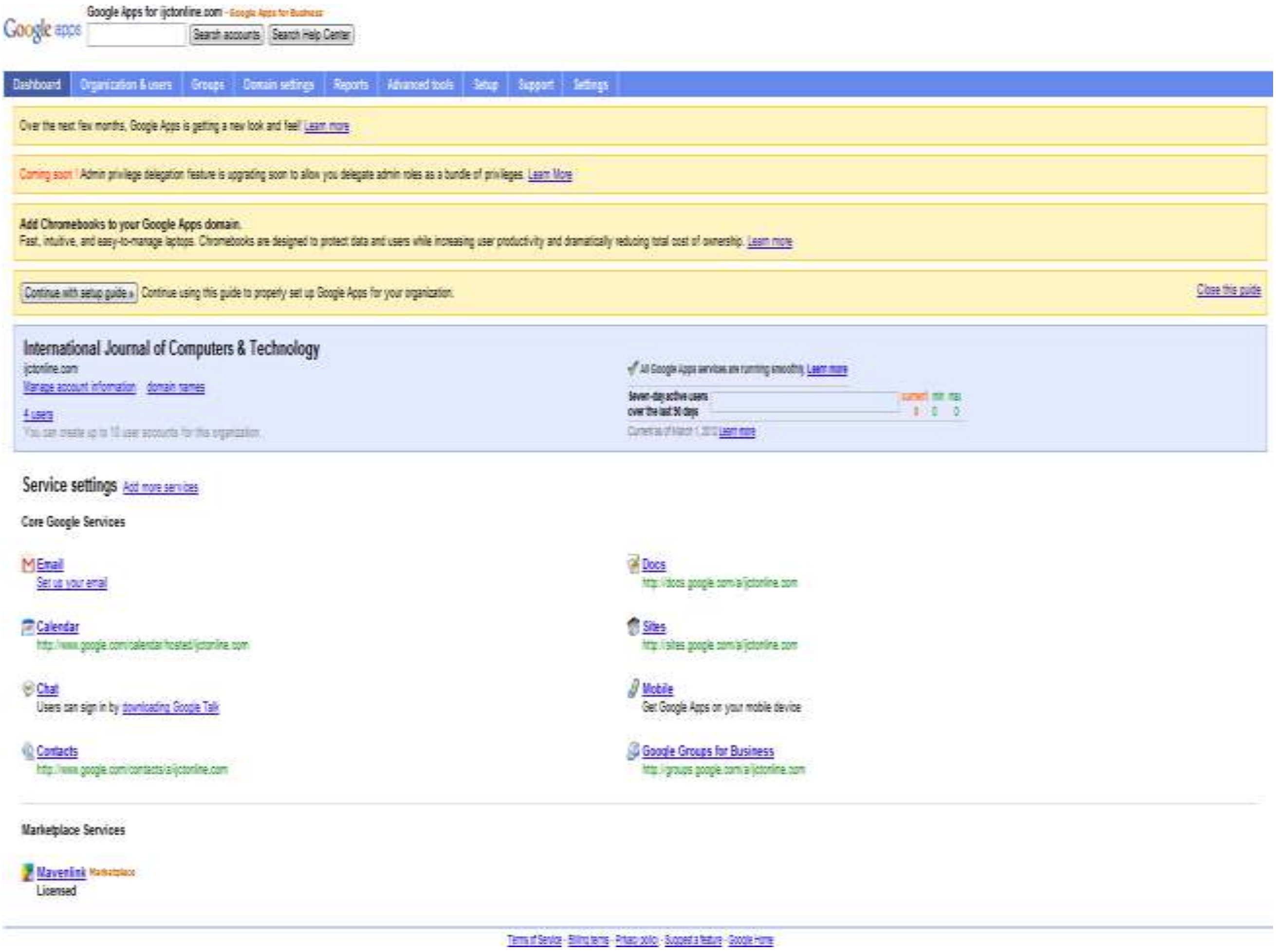
Wang et.al focuses on cloud data storage security, which has always been an important aspect of quality of service to ensure the correctness of user's data in the cloud. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server. They propose new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack [1]. Balachandra Reddy et.al has to provide some vendor assurance in service level agreements (SLA) to convince the customer on security issues. SLA has to describe different levels of security and their complexity based on the services to make the customer understand the security policies that are being implemented. It can be helpful for some enterprises to look forward in using the cloud services [2]. Meiko Jensen et.al used to build these cross-domain Internet-connected collaborations [3]. Mehmet Yildiz et.al provides layered security approach for cloud computing infrastructure macro level solution for identified common infrastructure security requirements. This model with a number of emerged patterns can be applied to infrastructure aspect of Cloud Computing as a proposed shared security approach in system development life cycle focusing on the plan-built-run scope [4]. Xiaojun Yu et.al argues that the cloud data security problem should be solved form data life cycle. After analysis of data life cycle model and data security threats, a suggested design process of data security solution is given [8]. Uma Somani et,al have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm [11]. Xiaolin Lu provides dynamically scalable geographic information technology, spatial data, and spatial applications as a web service. GIS web services were designed to provide the hosted spatial data and GIS functionality to integrate the customized GIS applications to perform basic geo-processingtasks, such as address matching, map image display, and routing, without maintaining GIS tools or the associated geographical data [13]. Mahbub Ahmed et.al have objective is served by analyzing different protocols and proposing the one in commensurate with the requirement of the security property like information or data confidentiality along the line of security in Cloud Computing Environment (CCE). To the best of our knowledge, we are the first to derive a secure protocol by successively eliminating the dangling pitfalls that remain dormant and thereby hamper confidentiality and integrity of information that is worth exchanging between the INO and the CSP. Besides, conceptually, our derived protocol is compared with the SSL from the perspectives of work flow related activities along the line of secure trusted path for information confidentiality [14]. Sang-Ho Na et.al are analyze security threats and requirements for previous researches and propose service model and security framework which include related technology for implementation and are possible to provide resource mobility [15]. Bhagyaraj Gowrigolla, et .al a data protection scheme with public auditing scheme is outlined that will address a number of these factors, by providing a mechanism to allow for data to be encrypted in the Cloud without loss of accessibility or functionality for authorized parties. This scheme is not necessarily a replacement for traditional privacy and security measures for data, but rather an enhancement which allows users greater degree of confidence in the adoption of innovative, cost saving Cloud computing technologies [17]. Wayne A. Jansen provides most acute obstacles with outsourced services. Identifies key issues, which are believed to have long-term significance in cloud computing security and privacy, based on documented problems and exhibited weaknesses [20]. Daniel Catrein et.al based telecommunication site model has been developed and parameterized with a realistic traffic and cost structure for a Western European operator [22]. Wei-Tek Tsai et.al proposed framework can ease the design of security system in cloud and reduce the complexity of system design and implementation [24]. Joshi Ashay Mukundrao et.al purposes an effective and flexible scheme with two salient features, opposing to its predecessors. Avoiding un-authorized access to user's data by signaling user by sending message to his/her mobile number at the start of transaction [26].

Cong Wang et.al utilize the public key based homomorphism authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security and finds that Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. [27]. Mr. G. A. Patil et.al emphasizes on improving existing authentication mechanism & implementing data security schemes to secure data from the data flow user Cloud Data Storage Cloud Server cloud vendor and other users of cloud [28]

3. IMPLEMENTAION OF CLOUD

Now Google application cloud has implementation on IJCT foundation, all data has of IJCT foundation sifted to Google cloud. It is powerful communication tool access anywhere. Google application clouds some services such as dashboard, group, domain name etc.

- **Dashboard**:-Dashboard is view of into data associated with your Google account. It provides management information and user information. Number of users can access cloud with some privilege. Super administrator giving right to other user can modification on cloud and also services. (Figure 1) It provides Google Application setup Wizard .it used setup of cloud.
- **Origination and user**: - help for user information and services. Which user can take which services? User has some right use those services. Administer gives right to other user for operation on cloud. It has limited number of user.
- **Group:** - we can create group for users Group of user can operate on cloud with some primitives. Function of group: - Create group, View group, delete group.
- **Domain name: -** domain name contain information of origination name, language, contact information, time zone etc.
- **Report:-**Report have represented in forms of documentation and graphics forms, audit log. It provides security for administer know information about updating.
- **Usage graphs**: - Graph's representation of Email Activity, total mail Usage, login Activity and mobile Devices.
- **Audit log**: - cloud administers knowing information related updating with event name, event description, user ID and IP address



Over the next few months, Google Apps is getting a new look and feel! Learn more

Coming soon ! Admin privilege delegation feature is upgrading soon to allow you delegate admin roles as a bundle of privileges. Learn More

Add Chromebooks to your Google Apps domain.
Fast, intuitive, and easy-to-manage laptops. Chromebooks are designed to protect data and users while increasing user productivity and dramatically reducing total cost of ownership. Learn more

Continue using this guide to properly set up Google Apps for your organization.

International Journal of Computers & Technology
ijctonline.com

You can create up to 10 user accounts for this organization.

✓ All Google Apps services are running smoothly. Learn more

Seven-day active users over the last 90 days	current	min	max
	0	0	0

Current as of March 1, 2012 Learn more

Email: Set up your email

Calendar: http://www.google.com/calendar/hosted/ijctonline.com

Chat: Users can sign in by downloading Google Talk

Contacts: http://www.google.com/contacts/a/ijctonline.com

Docs: http://docs.google.com/a/ijctonline.com

Sites: http://sites.google.com/a/ijctonline.com

Mobile: Get Google Apps on your mobile device

Google Groups for Business: http://groups.google.com/a/ijctonline.com

Mavenlink: Licensed

Figure1: Dashboard (Google Apps)

4. RESULTS

The following are the results found by the Method of data security is RSA algorithm for providing data security by encrypting the given data based on the KEY combinations. And this data then can only be decrypted by authorized person by using his private key. For the same purpose Google application cloud has been implemented on IJCT Foundation, all data has of IJCT Foundation sifted to Google cloud and RSA security algorithm is implemented by us for secure data.

The result is in two tables. Table 2 show the encryption for FIPS 186 -2 with the different parameters like MOD, signature, KEY Hash Signatures, and tells about the Encryption Key Values.

In the Table 3 the implementation of RSA on IJCT Google Cloud is shown and detail are also given that how & when the results has be computed the generated key with generated signature has been shown.

Table 2: Encryption for FIPS

Explanation Field for FIPS 186-2	
ALOG(RSA)	RSA ALGO
Generate Key	KEY Gen.
Generate SIG	Signature Gen.
Verify SIG	Signature Verification
MOD([1024], [1536], [2048])	Testing Modulus sizes
SHA([SHA-1],	Secure Hash signature supported by the RSA algorithm implementation
Encryption public Key Values([3], [17], [65537])	The valid values for encryption public Key e are 3, 17, and 65537.

Table 3: Implementation on IJCT

Sr. No.	Implementation	Operational Environment	Val. Date	Description/Notes
1	Google Cloud Application Digital library(ijct foundation)	Google cloud for IJCT foundation, c#	25/6/2012	FIPS186-2: ALGO(RSA): Key(generate)(MODLOUS: 1024 , 1536 , 2048 Encryption Public Key Values: 3 , 17 , 65537 ALGO[RSA] Signature(generate); Signature(verify); 1024 , 1536 , 2048 SHS:SHA-1 ALGO[RSA SSA-PKCS1_V1_5]: SIG(gen), SIG(verify): 1024 , 1536 , 2048 , 3072 , 4096 ALGO[RSASSA]: SIG(generate); Signature(verify); 1024 , 1536 , 2048 , 3072 , 4096

5. Conclusion and Future work

It is very problematical delineate the cloud computing. Cloud computing is a virtual amalgamating of computing. It makes available computing recourse in amalgamate for user through internet. Encryption and decryption solution to secure data confidentiality of information as well as integrity of data Future work on this research, We are known that clouds have revaluation change in internet. Future work should be in RSA cryptography to comparison of another cryptography algorithm such symmetric and asymmetric. Develop anther algorithm merge two algorithm which provide more security

6. REFERENCES

[1] Cong Wang, Qian Wang, and KuiRen, Wenjing Lou (2009) “Ensuring Data Storage Security in Cloud Computing”

[2] Balachandra Reddy Kandukuri, Rama Krishna Paturi, Dr. Atanu Rakshit (2009) “Cloud Security Issues”

[3] Meiko Jensen, Jlorg Schwenk, Nils Gruschka, Luigi Lo Iacono (2009)“On Technical Security Issues in Cloud Computing”

[4] Mehmet Yildiz, JemalAbawajy, TuncayErcan and Andrew Bernoth (2009) “A Layered Security Approach for CloudComputing Infrastructure”

[5] Jia Tiejun and Wang Xiaogang (2009) “The Construction and Realization of the IntelligentNIPS Based on the Cloud Security”

[6] Hassan Takabi, James B. D. Joshi and Gail-JoonAhn 2010 “SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments”

[7] WANG Yan- DENG Song LIN Wei-min ZHANG Tao YUYong 2010, Research of Electric Power Information Security protection on cloud security

[8]Xiaojun Yu, Qiaoyan Wen (2010) “A View about Cloud Data Security From data Life Cycle”

[9]Chenguang Wang, Huaizhi Yan2010 Study of Cloud Computing Security Based on Private Face Recognition”

[10] Jian Feng Yang, Zhibin Chen (2010) Cloud Computing Research and Security Issues”

[11] Uma Somani, Kanika Lakhani, Manish Mundra (2010)“Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”

[12] Thuy D. Nguyen, Mark A. Gondree, David J. Shifflett, Jean Khosalim, Timothy E. Levin, Cynthia E. Irvine (2010)“A Cloud-Oriented Cross-Domain Security Architecture”.

[13] Xiaolin Lu (2010) “Service and Cloud Computing Oriented Web GIS for Labor and Social Security Applications”.

[14] Mahbub Ahmed, Yang Xiang, Shawkat Ali (2010)“Above the Trust and Security in Cloud Computing: A Notion towards Innovation”.

[15] Sang-Ho Na, Jun-Young Park, Eui-Nam Huh (2010) “Personal Cloud Computing Security Framework”.

[16] Hanqian Wu Li Yao Yi Ding, Chuck Winner (2010) “Network Security for Virtual Machine in Cloud Computing”.

[17] Bhagyaraj Gowrigolla, Sathyalak shim Sivaji, M.Roberts Masillamani (2010) “Design and Auditing of Cloud Computing Security”

[18] Sravan Kumar and Ashutosh Saxena (2011) “Data Integrity Proofs in Cloud Storage”.

[19]Stephen Kaisler, SHK & Associates (2011) “Service Migration in a Cloud Architecture” Proceedings of the 44th Hawaii International Conference on System Science .

[20]Wayne A. Jansen, NIST (2011) “Cloud Hooks: Security and Privacy Issues in Cloud Computing”. [21] Brian Hay, Kara Nance, Matt Bishop (2011) “Storm Clouds Rising: Security Challenges for IaaS Cloud Computing”

[21] Brian Hay, Kara Nance, Matt Bishop 2011“Storm Clouds Rising: Security Challenges for IaaS Cloud Computing”

[22] Daniel Catrein, Bernd Lohrer, Christoph Meyer, Rene Rembarz, Thomas Weidenfeller Ericsson GmbH, Eurolab R&D (2011) IEEE An Analysis of Web Caching in Current Mobile Broadband Scenarios.

[23] Matthias Schmidt Lars Baumglartner, Pablo Graubner, David Block, Bernd Freisleb (2011) IEEE “ Malware Detection and Kernel Rootkit Prevention in Cloud Computing Environments”.

[24] Wei-Tek Tsai, Qihong Shao (2011) “Role-Based Access-Control Using Reference Ontology in Clouds”.

[25] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo (2011) “An Effective Privacy Protection Scheme for Cloud Computing”.

[26] Joshi Ashay Mukundrao, Galande Prakash Vikram (2011) “Enhancing Security in Cloud Computing”.

[27] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou (2011) “ Privacy-Preserving Public Auditing for Data StorageSecurity in Cloud Computing”.

[28] Mr. G. A. Patil, Mr. S. B. Patil (2011) “Data Security Mechanism for Cloud”.

[29] Shaik Rasool, G. Sridhar, K. Hemanth Kumar, P. Ravi Kumar (sept 2011) International Journal Of Network Security & Its Applications (JINSA)“Enhanced Secure Algorithm For message Communication”
[30]http://en.wikipedia.org/wiki/Google_Apps

[31]http://www.google.com/intl/en-B/business/ndex.html