Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

www.ijarcsse.com

Research Paper

Available online at: www.ijarcsse.com

Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them

Leena Khanna
IITM, JanakPuri
(I.P.University)
New Delhi, India

Prof. Anant Jaiswal
ASET, Noida
(Amity University)
U.P, India

Abstract— Cloud computing today is the latest buzzword in the software industry, an evolutionary step which encompasses elements from grid computing, utility computing and autonomic computing, into inventive deployment architecture. Although Cloud computing has achieved a great success in various industries whether it be a software industry, a Government Organization or a Healthcare sector, but this transition to Cloud computing has fuelled concerns on a critical issue for the success of information systems, communication and information security. Form the viewpoint of security, various risks and issues are identified in the area of Cloud Computing. There are various risks associated with the security but one of the major issues is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with various issues associated with Security and focus mainly on the data security and methods of providing security by data encryption. Various encryption methods of block cipher algorithms such as RSA, Blowfish are discussed for providing solutions to cloud security.

Keywords— Cloud Security, Data Security, Encryption, Encryption Algorithms, RSA, Blowfish

1. INTRODUCTION

Cloud computing is internet based computing whereby shared resources, software, and information are provided to computers and other devices on demand.

While there is a great deal of buzz surrounding cloud technologies, it's interesting to note that the term 'cloud computing' means different things to different people. The first applications to be moved to the cloud were CRM-type applications (Sales force, etc). There are four areas of pressure that are driving software development to the cloud:

1. Time, cost, and innovation –The project teams need to do more, faster within less budget, cost.
2. Distributed complex sourcing—teams are geographically dispersed.
3. Faster delivery of innovation—focus is on enabling developers to think outside the box in order to deliver business value.
4. Increasing complexity—in today's world, coding for simple project can span several million lines.

Cloud Computing is emerging approach because of the factors discussed above. In Cloud Computing, service providers provide the storage for data along with services. But due the lack of proper security policies, Cloud Computing adoption is becoming a serious issue. This paper primarily discusses various issues and possible solution to data security related issues.

2. TYPES OF CLOUDS

Public: In public cloud (also known as external cloud), the services are provided by a third party via Internet, and they are available and are for commercial purposes.

Private: This cloud consists on the hosting of private applications and services for private use (private networks) only.

Hybrid: It‘s a combination of public and private cloud. This is a better option when someone don‘t want to invest too much in infrastructure and on the other side wants the data to be secured by using private cloud deployment.

3. CLOUD SERVICES

3.1 Software as a Service (SaaS): These services are applications over Internet. Normally the user can run these applications using a web-browser. User abstract totally about the hardware and software that is using and simply access to a interface with a web browser and from there he have access to some information and functionalities. It's dedicated to current users; an example to this kind of services may be Google Docs.

3.2 Platform as a Service (PaaS): These services are focused on the deployment of applications or services online letting to the developer manage the hardware or software necessary, including also a solution stack. This service includes all the life-cycle of the deployment of application/ service such as design, implementation, testing, deployment, integrity with databases, etc

3.3 Infrastructure as a Service (IaaS): These services are focused to offer a computer infrastructure. All the servers, connections, software and other resources are offered by the providers. And the users see it like an entire infrastructure hosted in the same organization.

4. SECURITY ISSUES IN CLOUD COMPUTING

Time, cost, innovation are great benefits of cloud computing but still there are significant security concerns of cloud computing that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. Major security issues related to those faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers are discussed below:

1. Location of Data: Different organizations located in different geographical regions have different requirements and controls placed on access. Because the data is in the cloud, one may not realize that the data must reside in a physical location. The cloud provider should provide the level of security required for different customers and their needs.

2. Access to data: Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. Anyone using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals.

3. Data classification: Is the data classified? How is your data separated from other users? What is the type of Encryption mechanism?

4. Service level agreement (SLA) terms: The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

5. Security breach: If a security incident occurs, what support will be provided by the cloud provider?

6. Legal Issues: Providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

7. Authentication and authorization: Every organization has its own way to manage authentication and authorization. Every organization must determine if its current authentication system could also work in a secure and reliable way for users in a cloud environment. Apart from that what is the best way to authenticate cloud services but also be insured.

5. DATA PROTECTION IN CLOUD

In the world of cloud computing, the cloud provider will, in most cases, be the data processor, passively processing the data, for example, by storing it on its platform. Depending on the type of cloud used, the cloud provider's responsibilities could include providing infrastructure, physical security of the premises, operating system and network security.

The cloud customer, on the other hand, will be the data controller, actively processing the data for its own business purposes. Depending on the service model used, its responsibilities could include controlling the virtual infrastructure and any application security.

To make the data secure from various attacks and for the integrity of data encryption of the data should be done before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals) , geographical areas(in research) ,enemy positions (in defence), product , financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these data fall into the wrong hands, than such a breach of security could lead to declination of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement. Cryptography is a method of storing and transmitting data in a form that only those, it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. The best possible solution to deal with Security issues is Data Encryption. Various algorithms exist to encrypt the data in Cloud Computing such as DES, 3DES, blowfish, AES, etc.

6. ENCRYPTION ALGORITHMS

6.1 Blowfish Algorithm

Blowfish is a symmetric block cipher encryption algorithm meaning that it uses the same secret key to both encrypt and decrypt messages and divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. *Blowfish Algorithm* is a **Feistel**

Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits.

The basic working of a Feistal Network is:

- Split each block into halves
- Right half becomes new left half
- New right half is the final result when the left half is XOR'd with the result of applying ***f*** to the right half and the key.

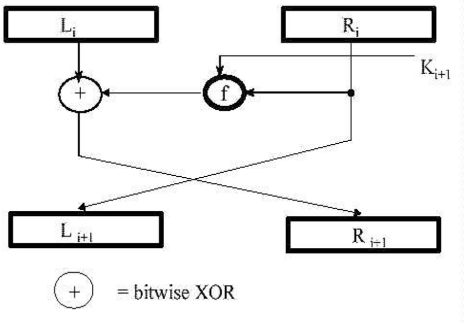


Fig 6.1 Feistel Network

6.2 AES Algorithm

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical.

The four rounds are called SubBytes, ShiftRows, MixColumns, and AddRoundKey. During SubBytes, a lookup table is used to determine what each byte is replaced with. The ShiftRows step has a certain number of rows where each row of the state is shifted cyclically by a particular offset, while leaving the first row unchanged. Each byte of the second row is shifted to the left, by an offset of one, each byte in the third row by an offset of two, and the fourth row by an offset of three. This shifting is applied to all three key lengths, though there is a variance for the 256-bit block where the first row is unchanged, the second row offset by one, the third by three, and the fourth by four.

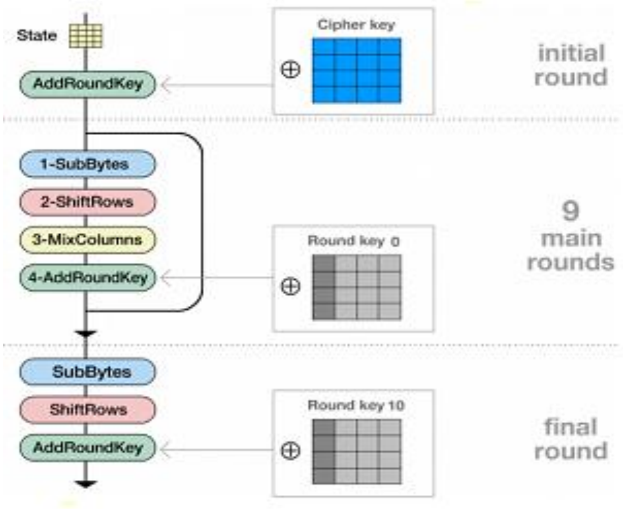


Fig 6.2 AES Encryption Process

The MixColumns step is a mixing operation using an invertible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output. In the fourth round, the AddRoundKey derives round keys from Rijndael's key schedule, and adds the round key to each byte of the state. Each round key gets added by combining each byte of the state with the corresponding byte from the round key.

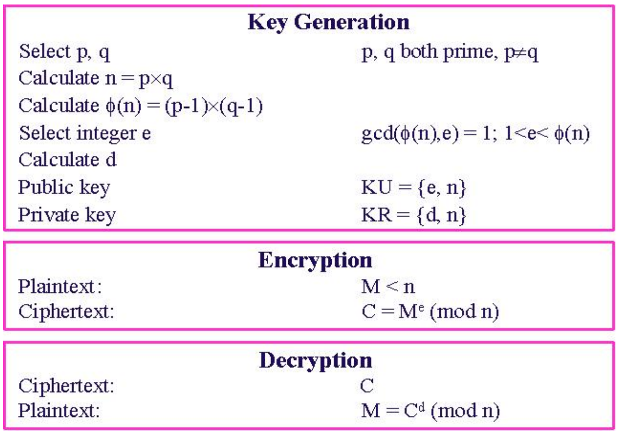
Lastly, these steps are repeated again for a fifth round, but do not include the MixColumns step.

6.3 RSA Algorithm

The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages.

The basic steps of RSA algorithm are:

- **Key Generation**
- **Encryption and**
- **Decryption**



Key Generation	
Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1$; $1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Fig 6.3 Basic Working of RSA Algorithm

The algorithm involves multiplying two large prime numbers and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key.

7. SUMMARY

Cloud computing is revolutionizing the way business is carried out in various industries (Government, Healthcare, Software etc.), use of information technology resources and services, but the revolution always comes with new problem. One of the major problems associated with Cloud computing is Security. Various Security issues and Algorithms to deal with data security issues are discussed in this paper. This paper also discusses the advantages, features, services of the cloud and the different deployment models. In future, security algorithms will be implemented producing results to justify the concepts of security for cloud computing and comparing them to find out which is the most efficient one.

REFERENCES

[1] William Stallings, "Cryptography and Network Security Principles and Practices," Prentice Hall, New Delhi.

[2] http://en.wikipedia.org/wiki/Google_App_Engine

[3] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences 2011.

[4] G. Jai Arul Jose1, C. Sajeev2, "Implementation of Data Security in Cloud, "in International Journal of P2P Network Trends and Technology- July to Aug Issue 2011.

[5] Priyanka Arora, Arun Singh, Himanshu Tyagi "Analysis of performance by using security algorithm on cloud network" in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 June, 2012

[6] Farhan Bashir Shaikh, Sajjad Haider , "Security Threats in Cloud Computing," in 6th international conference internet technology and secured transtion,11-14 december,2011,Abu Dhabi, United Arab Emirates

[7] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[8] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[9]J.L Smith, The Design of Lucifer, A Cryptographic Device for Data Communication, RC 3326, White Plains: IBM Research.

[10]M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica ―A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment, in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

[11] Gurudatt Kulkarni & Jayant Gambhir Tejswini Patil Amruta Dongare,' *A Security Aspects in Cloud Computing'*, Institute of Electrical and Electronic Engineers (IEEE), IEEE 3 rd International Conference on software engineering and service science 2012

[12] Tingyuan Nie,Chuanwang Song, Xulong Zhi,*Performance Evaluation of DES and Blowfish Algorithms',* Biomedical Engineering & computer science, 2010 International Conference.
[13] Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).
[14] Lepakshi goud.T, Dynamic routing with Security using a Blowfish Algorithm in the multiple Organizing system, IJAEST, Vol No .4, issue No 1, 2011.
[15] Simar Preet Singh, Comparison of Data Encryption Algorithm, IJCSC, Vol 2 No.1, June-2011.
[16] Irfan Abdul Gani landge, Burhannudin Contractor Tauseef Companywala, “VHDL Based Encryption and Decryption using BLOW FISH Algorithm”, International Conference on Electronics Communication and Instrumentation and Control Engineering, 2012.
[17] http://www.di-mgt.com.au/rsa_alg.html
[18] www.howstuffworks.com
[19] "4 Cloud Computing Security Policies You Must Know". CloudComputingSec. 2011. Retrieved 2011-12-13.