Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Computing: Multi-Level Security Using AES and RC4

Priya Sharma
Research Scholar, M. Tech.,
Computer Science & Engineering,
Uttar Pradesh Technical University, India

Dr. Rajesh Pathak
Head of Department,
Computer Science & Engineering,
Uttar Pradesh Technical University, India

Abstract—Cloud Computing is a platform for expanding capabilities and developing potentialities dynamically without employing new infrastructure, personnel, or software system. Information Technology infrastructure continues to grow with growing technology. The use of mobile devices and computer has increased due to the innovation of the Internet. Every Internet user is accessing cloud services either directly or indirectly without aware of security aspects Cloud computing is not just a service of computing or how the computing service is delivered. Security is the most challenges aspects in the internet and network application .Internet and network application are growing very fast, so the importance and the value of the exchanged data over the internet or other media types are increasing. Hence the search for the best solution to offer the necessary protection against the data intruders attacks along with providing these services in time is one of the most interesting subjects in the security related communities .Cryptography is one of the main category of computer security that converts information from its normal form into unreadable form. In this paper we discussed the AES and RC4 algorithm that we will apply in securing cloud.

Keywords— Cloud Computing, Threats, Security in cloud, Cryptography, AES, RC4.

I. INTRODUCTION

Internet was introduced in 1982 after TCP/IP was standardized and consequently, the concept of TCP/IP network announced. Internet started to make huge impact on world with electronic mail, instant messaging, VoIP, video calls and especially World Wide Web with its social networking, blogs, online shopping sites and discussion forums. Increasing amount of data is transmitted at high speeds due to networking developments (fiber optics). In the year 1993, only 1% of information flows through two-way telecommunication networks. It increased to 57% by 2000 and 97% by 2007 [1].

Nowadays, the Internet continues to grow and greater amount of information is being transferred. Adding smart phones and tablet pc's to this environment. As a result, data and application in Internet and mobile have continuously increased. Thus, data must be stored and achieved. All these technological developments provide new business model which is cloud computing. Cloud computing is an important solution and cost effective model in order to facilitate companies' computing needs and accomplish business objectives [2].

Cloud Computing Introduction:

CLOUD(Common Location independent Online Utility on Demand) is a broad solution that delivers IT as a solution. Cloud computing is a new computing model, which comes from the concept of grid computing, distributed computing, virtualization technology and other computing technologies[3]. The cloud computing changes the style of software .The data can be stored in the cloud environment can be accessed from anywhere anytime due to the distributed architecture of cloud environment. Now a day most of the small and medium business organisation tending towards the cloud platform and putting their application and data in to the cloud.

NIST (National Institute Of Standard & Technology) [7] defines Cloud Computing as a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources such as (network, servers, storage, applications and services) that can be rapidly provisioned and reduced with minimal management effort or service provider interaction.

NIST [7], defines cloud computing by describing five essential characteristics, three cloud service models & four deployment model as explained below:

The Cloud Computing model can be seen as a combination of three service delivery models and three deployment models [8].

The deployment models are:

- **Private cloud:** a cloud platform that is committed for explicit organization,
- **Public cloud:** it's openly available to public users to register and use the infrastructure in accordance to their utility, and

- **Hybrid cloud:** It's an arrangement of private cloud that can extend to use resources in public clouds. Among all these, the most vulnerable deployment models are public models because they are available for public users to host their services and they may be malicious users.

The cloud service delivery models, include:

- **Infrastructure-as-a-service (IaaS):** where cloud providers deliver computation resources, storage and network as an internet-based services. This service model is based on the virtualization technology. The most familiar IaaS provider is Amazon EC2.
- **Platform-as-a-service (PaaS):** where cloud providers deliver platforms, tools and other business services that gives the ability to customers to develop their own applications, and they can also manage the applications by themselves, removing the need of installing any platforms or support tools on their devices. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. The most known PaaS provider are Google Apps and Microsoft Windows Azure[9].
- **Software-as-a-service (SaaS):** where cloud providers deliver applications hosted on the cloud infrastructure as internet based service for end users, without requiring installing the applications on the customers' computers. This model may be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. An example of the SaaS provider is SalesForce[9].

Characteristics of Cloud Computing

a. Broad network access: Various client platforms like laptops, tablets, mobile phones can be used to access these capabilities that are available over the network.
b. On-demand self-service: Without the human interaction with each service provider a consumer can provision computing capabilities automatically as and when required.
c. Rapid Elasticity: A user can quickly acquire more resources from the cloud by scaling out . They can scale backing by releasing those resources once they are no longer required[8].
d. Resource pooling: Multiple consumers are served with the providers pooled computing resources using a model, with different virtual and physical resources dynamically assigned and reassigned depending on the demand of consumer[8].
e. Measured Service: Resources usage is metered using suitable metrics such as monitoring storage usage, CPU hours, bandwidth usage etc.

Cloud Computing has advantages and disadvantages. Disadvantages of cloud computing are security threats for cloud computing customer. Disadvantages are generally about security.

II. SECURITY THREATS IN CLOUD COMPUTING

Those threats compromise the CIA of the resources provided. Currently, we may consider seven different threats:

- Abuse and Nefarious Use of Cloud Computing,
- Insecure Interfaces and APIs,
- Malicious Insiders,
- Shared Technology Issues,
- Data Loss or Leakage,
- Account or Service Hijacking and
- Unknown Risk Profile [5].

One of the reasons why those threats are quite challenging is because in Cloud Computing the computational resources are the result of homogeneous data centres. This characteristic means that there is not an individual and proper management for each data centre, making harder the adoption of an efficient security model that fulfils the specifications of the security policies [8].

A. Abuse and Nefarious Use of Cloud Computing

Cloud service provider provides various types of services including unlimited bandwidth and storage capacity. Free limited trial periods are offered by various cloud service provider that gives an opportunity for hackers to access the cloud immorally, their impact includes launching potential attack points, decoding and cracking of passwords and executing malicious commands. As cloud service providers are targeted for their weak registration systems and limited fraud detection capabilities, Spammers, malicious code authors and other cyber criminals can conduct their activities with relative impunity. The consequence of this Threat helps the growth of plagues such as botnets, from which come problems like Distributed Denial of Service (DDoS), solves of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), storage of malicious files and botnet networks [5].

B. Insecure Interfaces and APIs

To access and manage the cloud services cloud users are using software APIs and interfaces. These APIs need to be protected because they play a vital part during provisioning, organization and monitoring of the processes running in a cloud

environment. The availability and security of cloud services is reliant upon the security of these APIs so they should include features of verification, access control, encryption and activity monitoring[9]. APIs must be intended to defend against both accidental and malicious attempts to avoid threats. If cloud service provider depends on weak set of APIs, diversity of security issues will be raised related to privacy, integrity, availability and accountability such as malicious or anonymous access, API dependencies, limited monitoring/logging capabilities, inflexible access controls, mysterious access, reusable tokens/passwords and inappropriate authorizations.

C. Malicious Insiders

Insider attacks can be performed by malicious employees at the provider's or user's site. Malicious insider can steal confidential data of cloud. This type of threat can shatter the expectation of cloud users on provider. Cryptographic keys, files and password can be easily obtained by malicious insider. These attacks may involve various types of scam, spoil or stealing of information and misuse of IT resources. Due to lack of transparency in cloud provider's processes and procedures the threat of malicious attacks has increased [4]. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analysed . The financial value as well as brand reputation of an organization can be damage by malicious insider attacks.

D. Shared Technology Issues

Iaas is based on shared infrastructure, which is often not designed to accommodate multitenant architecture. Overlooked flaws have allowed guest operating system to gain unauthorized level of control and influence on the platform [8].

E. Data Loss or Leakage

Due to operational failures, untrustworthy data storage and inconsistent use of encryption keys data loss can occur. Deletion or variation of records without a backup of the original content that can take place intentionally or unintentionally is refer to operational failure. Unreliable data storage refers to saving of data on unreliable media that will be unrecoverable if data is lost [8]. The inconsistent use of encryption keys will result into loss and unauthorized accesses of data that will lead to the destruction of confidential and sensitive information. Twitter hack is an example of data loss. Compromise in one's intellectual property can lead to financial implications as well as legal consequences.

F. Account or Service Hijacking

Unauthorized access gained by attackers to control the users' accounts, such as fraud, phishing and exploitation of software vulnerabilities is called account or service hijacking .For example if an attacker gains access to users' credentials, they can manipulate their data, spy on their activities/transactions, return falsified information and redirect them to illegitimate sites[9].

A usual approach to maintain access control when using web-browsers to access cloud computing systems are authentication and authorization through the use of roles and password protecting. However, to secure sensitive and critical data this method is not sufficient enough.

G. Unknown Risk Profile

Users should be acquainted with software versions, security practices, code updates and invasion attempts. Most often, these functionally are well advertised while the details about compliance of the internal security procedures remain unnoticed. Users must know how and where their data and related logs are stored.

III. ENSURING DATA SECURITY WITH ENCRYPTION ALGORITHM

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. According to key characteristics, modern cryptosystem can be classified [11] into symmetric cryptosystem and asymmetric cryptosystem. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key.

RC4

RC4 i.e. Rivest Cipher 4 also known as **ARC4** or **ARCFOUR** meaning Alleged RC4 . In cryptography this algorithm is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software. This stream cipher was invented in 1987 by Ron Rivest, one of the inventors of the RSA public key cryptography algorithm and co-founders of RSA security. Even though the RC4 cipher is officially named "Rivest Cipher 4", it is also known as "Ron's Code 4"[13].

The trade secret behind RC4 was revealed in September 1994 when the description of the cipher was sent to the Cypherpunks mailing list (group of people interested in privacy and cryptography who used this mailing list to communicate). After that, the description was posted on many website and the genuineness of the information was confirmed as the resulting outputs of the described cipher were matching the outputs of licensed RC4[13]. Thanks to its simplicity and efficiency due to which RC4 had a really large success . It was used in many popular standards and protocols such as WEP, WPA, SSL or TLS.

Principle Of RC 4:

The RC4 algorithm generates a pseudo-random key stream that is then used to generate the cipher text (by XORing it with the plaintext). It is called pseudorandom because it generates a sequence of numbers that only approximates the properties of random numbers. Since the output is always the same for a given input so sequence of bytes generated is not random but it has to approximate random properties to make it harder to crack. From a variable length key the key stream is generated using an internal state composed of the following elements:

- A 256 bytes array (denoted S) containing a permutation of these 256 bytes
- Two indexes x and y, used to point elements in the S array (only 8 bits are necessary for each index since the array only have 256 elements)
- Once the S array has been initialized and ”shuffled” with the key-scheduling algorithm (KSA), it is used and modified in the pseudo-random generation algorithm (PRGA) to generate the key stream.

AES

In 1997 the National Institute of Standards and Technology (NIST), started a process to identify a replacement for the Data Encryption Standard (DES). It was commonly recognized that DES was not safe because of advances in computer processing power. The main objective of NIST was to discover a replacement for DES that could be used for non-military information security applications by US government agencies[12]. Certainly, it was recognized that commercial and other non-government users would benefit from the work of NIST and that the work would be generally accepted as a commercial standard. From all over the world the NIST invited cryptography and data security specialists to participate in the discussion and selection process. Five encryption algorithms were adopted for further study. Through a process of accord the encryption algorithm proposed by the Belgium cryptographers Joan Daeman and Vincent Rijmen was selected. Preceding to assortment Daeman and Rijmen used the name Rijndael (derived from their names) for the algorithm. After approval the encryption algorithm was given the name Advanced Encryption Standard (AES) which is in common use today.

AES Working [10]:

- Rijndael produces 10 keys of 128 bits each, from the 128-bit key.
- Then these keys are placed into 4x4 arrays.
- The plain text is further divided into 4x4 arrays (128 bits each).
- In 10 rounds each of the 128-bit plain-text items is processed (10 rounds for 128-bit-keys, 12 for 192, 14 for 256).
- After the 10th round the code is produced. Each single byte is substituted in an S box and replaced by the reciprocal on GF (2 8).
- Then a bit-wise modulo-2 matrix is applied, followed by an XOR operation with 63.
- Cyclically the lines of the matrices are sorted.
- The columns of the matrix multiplication are interchanged on GF (2 8).
- The sub keys of each round are subjected to an XOR operation.

IV. CONCLUSIONS

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. But to best utilize the model we need to block the existing security holes. In this paper the purpose is to tell about various security threats in cloud computing and how can can we overcome that. Also this paper is intended to provide good security to cloud using cryptographic algorithm so that we can efficiently use cloud computing services.

ACKNOWLEDGMENT

I take the opportunity to thanks all those, who have contributed to the completion of this work and helped me with valuable suggestions for improvement .

I express my deep gratitude to my guide, Dr Rajesh Pathak (HOD) for their valuable support, help and guidance during the project work and providing me with best facilities and atmosphere for the work and encouragement.

REFERENCES

[1] History of The Internet, http://en.wikipedia.orglwiki/HistorLoCthe_Internet/,2013. (Access date:15.08.2013).

[2] "The benefits and challenges of cloud computing", http://www.moorestephens.com/cloud_computing_benefits_ch allenges.aspxl, 2013. (Access date: 21.08.2013).

[3] Wentao Liu,"Research on cloud computing security problem strategy ", IEEE, ISBN 978-1-4577-1415-3112.

[4] Networkworld,"Gartner Cloud Putting Crimp in traditional software,hardware sales",July 2012 , Available from http://www.networkworld.com/news/2012/071312-gartner-cloud-260882.html

[5] Cloud Security Alliance, “Top Threats to Cloud Computing V1.0“, March 2010, Avaliable from: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "Above the Clouds: A Berkeley View of Cloud", Electrical Engineering and Computer Sciences, University of California at Berkeley, February 10, 2009.
[7] Security guidance for Critical Areas of Focus In Cloud Computing V3.0,Cloud Security Alliance 2011.
[8] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf, Accessed April 2010
[9] Dr. Rajesh Pathak and Priya Sharma.2015, Security Issues at different levels in cloud computing, International Journal of Advanced Research in Computer science and Software Engineering, Volume 5, Issues 4, April 2015 .
[10] http://www.password-depot.com/know-how/blowfish_and_rijndael.htm
[11] Mengmeng Wang, Guiliang Zhu, Xiaoqiang Zhang, "General Survey on Massive Data Encryption", P. 150-155.
[12] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[13] https://en.wikipedia.org/wiki/RC4

