Strategic Planning For Cloud Computing Architecture

Vidhi Agarwal[1], Raj Yadav[2]

Depatment of SE[1] &CSE[2], PCE[1] & KITE[2], Jaipur (Rajasthan)

Email: vidhiagarwal31@gmail.com, yadavrajc@gmail.com

Abstract - **Cloud Computing is a model for enabling convenient, on-demand, ubiquitous, network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The *National Institute of Standards and Technology's* definition of cloud computing identifies "five essential characteristics": On-demand self-service, broad network access, Resource pooling, rapid elasticity & measured service. The primary objective of this paper is to provide a basis for discussion between CSPs (Cloud Service Providers) and Cloud customers.**

Keywords- **Cloud Security, Encryption, AES, Digital Signature, Packet Sniffing.**

I. INTRODUCTION

Cloud computing is currently a buzzword in the world of computing, and a few moments of browsing the Web will soon reveal an extensive range of Cloud services and products. The reason for this great interest is that it offers what some earlier technologies have wanted to do, namely, access to processing and storage power on demand. Yet, despite its high profile, many people do not really know what it is. In essence,

Cloud computing is the outsourcing of what has been described as an unlimited range of computer resources, for instance processing power and storage capacity, by means of virtualization, i.e. It lets a private user to do the simulation of artificial intelligence tests that consume lots of resources in little time.

Cloud Computing has the long-term potential to change the way information technology is provided and used. But information security is a key factor if IT services from the cloud are to be used reliably.Cloud computing appeas to all sorts of users, from businesses to private individuals, for various reasons. Chief among the attractions is the fact that these users have the opportunity to pay as they go: pay-per-use(PPU) or pay on demand(POD). This method of paying is not new. Indeed, we have been using this business model so many years; for instance, electricity suppliers employ this method to charge for electricity used at home, where households pay for as much as they use, instead of paying monthly. Another example would be for pay-as-you-go for mobile phones. What the PPU system offers, however, is flexibility: we only pay for what we use and when we use it. Cloud computing may seem to offer great benefits, and both, individuals and organizations are adopting it rapidly.

However, there are problems associated with this system/environment. The main problem according to Ian Foster, Yong Zhao, Ioan Raicu and Shiyong Lu[3] is that, everytime a company wants to provide a service, there arises a common need to use and manage large facilities. This kind of managing of systems is used for using and requesting resources that are provided by central facilities like datacentres. Highly parallel computations are implemented in these environments and executed through thes distributed resources. What has happened is that we have created a new environment in which vast amounts of information,etc. are being distributed through a large number of computers. One consequence of this is the issue of security. The large and extensive scale of Cloud computing activities requires effective security.

II. SECURITY ISSUES IN CLOUD COMPUTING

As with every distributed system, Cloud Computing has lots of problems. We have to take care of the network infrastructure, which is not always in our control, and be very careful with the data in order to avoid third parties from capturing it. Some security solutions and problems have been proposed by ArmMichael Halton[2]:

• Web application vulnerabilities: Cross scripting, SQL injections. **Solution:** Develop a security oriented framework that teaches the best programming practices.

• Vulnerabilities inherent to the TCP/IP stack and/or the operating systems: DoS, and DDos (Distributed denial of service). **Solution:** Deactivate unused services, update applications and control rights.

• Authentication problems: IP spoofing, RIP attacks, ARP poisoning. **Solution:** Use encrypted protocols if possible prevents IP spoofing, controlling rights to access ARP tables etc.

• The verification, tampering and loss of data. **Solution:** encrypted data would be a solution, but, 'since the unencrypted data must reside in the memory of the host running the computation', this must be encrypted in order to avoid memory copies [9].

• Physical access. **Solution:** Control rights and log actions when accessing the hardware.

• Privacy control of data. **Solution:** Use Service-level agreements.

III. EXISTING METHODS FOR CLOUD ENVIRONMENT

Common methods for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission. These protection methods normally require cryptography algorithms and digital signature techniques, as explained below:

Common data encryption methods include symmetric and asymmetric cryptography algorithms. Symmetric cryptography is used in the U.S. Federal Information Processing Standard's (FIPS) 46-3 Triple Data Encryption Algorithm (TDEA, also known as Triple-DES or 3DES) or 197 Advanced Encryption Standard (AES) and others. This type of encryption and decryption process uses a secret key. Asymmetric cryptography, on the other hand, uses two different keys, a "public key" for encryption, and a "private key" for decryption. Examples include RSA cryptography and Elliptic Curve Cryptography (ECC). Generally speaking, symmetric cryptography is more efficient, and is suitable for encrypting large volumes of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography.

The use of passwords as an authentication process is more familiar to general users, but messages sent by the user are vulnerable to surreptitious recording by hackers who can then use the data in the message to log into the service as the user. In more advanced authentication systems, the system side will generate a random number to send the user a challenge message, requesting the user to transmit an encrypted response message in reply to the challenge message, thus authenticating that the user has the correct encryption key. Without this key, the user will not be allowed access. In the process of challenge and response the client's encrypted key uses the client's password to convert a derived value and. In this program, each communication between the client and server is unique, and a hacker using an old message would fail to access the system. In addition, the One-Time Password (OTP) authentication system differs from most peoples' conception of a password. Most people understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP, however is the single-use nature of the password.

After receiving authentication from the user, the system side must create a secure transmission channel to exchange information with the user. The Secure Sockets Layer (SSL) is a common method of building secure channels, primarily using RSA encryption to transmit the secret keys needed for the both sides to encrypt and decrypt data transmitted between them. When using cryptographic technology to protect user data, the keys used for encryption and decryption of that data must be securely stored. In particular, cloud computing service providers must have specific methods for constraining internal system management personnel to prevent them from obtaining both encrypted data and their decryption keys – this is critical to protecting user data. Operator policies for protecting user data must be clearly laid out in the Service Level Agreement (SLA) and must explain how special privilege users are prevented from improperly accessing user data.

Kandukuri, Paturi and Rakshit offer six recommendations for SLA content, including (1) special privilege user data access must be controlled to prevent unauthorized storage or retrieval, (2) cloud computing services must comply with relevant laws, (3) user data must be properly stored and encrypted, (4) a reset mechanism must be provided in case of service disruption or system crash, (5) service must be sustainable and guaranteed against service discontinuation due to change or dissolution of the provider and (6) if cloud computing services are used for illegal purposes, the provider must be able to provide records to assist with investigations.

IV. PROPOSED SECURE ARCHITECTURE

In our proposed system, the Authorization for the Storage and Encryption/Decryption of User Data must be vested with two different service providers[1]. As our Encryption/Decryption as Service provider includes management of the key required for the encryption/decryption of user data, but not the storage of decrypted or encrypted user data. In this Propose Solution, user data in the Storage Service System is all saved encrypted. Without the decryption key, there is no way for the service provider to access the user data. Within the Encryption/Decryption Service System there is no stored user data, thus eliminating the possibility that user data might be improperly disclosed.

Following are the Steps:

1) User login through web App. into CRM Service.
2) CRM stores Data in Encrypted form using Digital Signature. (In Earlier Approach, Unencrypted data transmits due to which chances are more for Packet Sniffing)
3) Now, Encrypted data will transfer to Encrypt/Decrypt Service for Double Encryption, Here we are using AES (ADVANCED ENCRYPTION STANDARDS) for Cryptography. This service will also Manage Keys and Generate Unique ID for Each Users.
4) Once, Data is Encrypted in above Service Module, it will transfer to Storage Service module where Encrypted form is stored for future purpose.

Once we move the data from One Service Module to another, it's no more Exist in Previous Module. Cloud Computing tries to share only the user interface while the resource interfaces are hiddent. That's the reason it's known as SOA (Service Oriented Architecture).

Encryption/Decryption Service Module:

AES provides plaintext length should be 128bit, its key length has three optional values: the first value is 128bit, the second value is 192bit, and the third value is 256bit. According to the secret key length, AES algorithm completed Nr iterations. The relationship of Nr times and key length is in the Table I as shown below.

Table I
Relationship of Nr Times and Key Length

Key length	128	192	256
Nr times	10	12	14

The 128-bit input plaintext is divided into 16 bytes, usually represented as a 4 * 4 matrix; each matrix element is 8 bits (one byte). The plaintext sequence from left to right is S00, S10, S20, S30,S01, S11, S21, S31, S02, S12, S22, S32, S03, S13, S23, S33. The plaintext block of any stage in the wheel transform is named "state"[5] .

The initial plaintexts block M:
s00 s01 s02 s03
s10 s11 s11 s13
s20 s21 s12 s23
s30 s31 s13 s33

AES encryption has the following steps:

1) Conducted a round of secret key plus operator first.
2) Conducted Nr-1 iterations. Use S block to substitute each byte; do the displacement for the substitution result, then do the mix column transform operation. After these, a round of secret key plus operator is conducted.

3) Final round transform include byte substitution, line transformation and key processing operation.

Application of AES algorithm:

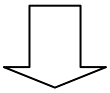
File encryption and decryption was respectively used in the (file upload & download) Encryption/decryption modules.

Encryption process

1) Bytes transformation: AES defines an S-box matrix composed with a 16 * 16 bytes array. Take the high 4 bit of 8 matrix elements as the row value and low 4 bit of 8 matrix elements as the column value searching S-box table, and the corresponding value obtained is the result of the transformation matrix elements.
2) Row displacement: displace a row of the State matrix.
3) Column mix: AES selected a fixed polynomial which is facilitating to calculate. The polynomial is c(x)=03x3+01x2+01x+02

02	03	01	01
01	02	03	01

S00	S01	S02	S03
S10	S11	S11	S13



Result matrix of column mix

4) Key plus

$$\begin{array}{|c|c|c|c|}\hline \mathrm{B2} & 10 & \mathrm{C1} & \mathrm{AC} \\ \hline 38 & 62 & \mathrm{6E} & \mathrm{E7} \\ \hline 75 & 80 & \mathrm{2C} & \mathrm{5B} \\ \hline \mathrm{4A} & \mathrm{9C} & 23 & 80 \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|}\hline 88 & \mathrm{8D} & \mathrm{FE} & \mathrm{FE} \\ \hline 34 & 55 & 37 & 62 \\ \hline 48 & 71 & 74 & \mathrm{7D} \\ \hline \mathrm{FA} & \mathrm{AC} & \mathrm{9D} & \mathrm{AF} \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline \mathrm{3A} & \mathrm{9D} & \mathrm{3F} & 52 \\ \hline \mathrm{0C} & 37 & 59 & 85 \\ \hline \mathrm{3D} & \mathrm{F1} & 58 & 26 \\ \hline \mathrm{B0} & 30 & \mathrm{BE} & \mathrm{2F} \\ \hline \end{array}$$

5) Key Expansion: the key to be calculated as the basic unit of bytes is expressed by a matrix of four lines.
   Round key length=block length *(Round Nr+1)

Decryption process:

1) Inverse byte substitution: Like the byte substitution, Inverse byte substitution search each byte though the table.
2) Inverse row displacement: In contrast with Row displacement operation.
3) Inverse column mix: almost the same as column mix operation, but inverse column mix has its own polynomial. The polynomial is d(x)=0Bx3+0Dx2+09x+0E.
4) Key plus: the same as key plus operation in encryption process.

V. CONCLUSION

Cloud computing is revolutionizing the way business is carried out in various industries (Government, Public, 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.

VI. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino,J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, pp. 50-55, January 2009.

[2] ArmMichael Halton. *Security Issues and Solution in Cloud Computing*. June 2010. http://wolfhalton.info/2010/06/25/ security-issues-and-solutions-in-cloud-computing/.

[3] David Linthicum. *Cloud Computing, Deep Dive*. 2009. MPI-SWS http: //www.scribd.com/doc/26495704/ Cloud-Computing-Deep-Dive-Report.

[4] A. Parakh and S. Kak, “Online data storage using implicit security”, Information Sciences, vol. 179, issue 19, pp. 3323-3333, September 2009.

[5] V. Miller, “Uses of elliptic curves in cryptography,” Advances in Cryptology -

CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986.

[6] Simar Preet Singh, Comparison of Data Encryption Algorithm, IJCSC, Vol 2 No.1, June-2011.

[7] "4 Cloud Computing Security Policies You Must Know". Cloud Computing Sec. 2011. Retrieved 2011-12-13.

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

[9] Nuno Santos,Krishna P., Gummadi Rodrigo Rodrigue. *Towards Trusted Cloud Computing.* May 2009. MPI-SWS http://www.usenix.org/events/ hotcloud09/tech/ full_papers/santos.pdf.