NETWORK SECURITY IN CLOUD COMPUTING

V. Shrividhya, P. Manimegalai

Dept. of ECE, Karpagam Academy of Higher Education, Coimbatore, India. manimegalai.vairavan@gmail.com

ABSTRACT

Cloud Computing Security architecture using Rijndael as the standard symmetric key encryption algorithm. Data security has become the vital issue of cloud computing security. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. So in this we focused on client side security In our proposed system, only the authorized user can access the data. Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally, he will not be able to decrypt it. Also it is proposed that encryption must be done by the user to provide better security. Henceforth, security is provided using Rijndael.

Keywords — Network, Cloud, Security, Rijndael

1. Introduction

Cloud computing security or, more simply, cloud security is an evolving sub-domain3, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls.

Deterrent controls these controls Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. The Cloud computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure. In order for this to become reality, however, there are still some challenges to be solved. Most important among these are security and trust issues, since the user data has to be released to the Cloud and thus leaves the protection sphere of the data owner. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. Security is to save data from danger and vulnerability. There are so many dangers and vulnerabilities to be handled. Various security issues and some of their solution are explained and are concentrating mainly on public cloud security issues and their solutions.

Data should always be encrypted when stored using separate symmetric encryption keys and transmitted. If this is implemented appropriately, even if another tenant can access the data, all that will appear is gibberish. So a method is proposed such that we are encrypting the whole data along with the cryptographic key, intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

2. Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address. The System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

3. Encryption techniques in Cloud Computing

Data security issues in the cloud Securing data is always of vital importance and because of the critical nature of cloud computing and large amounts of complex data it carries, the need is even important. Therefore, data privacy and security are issues that need to be resolved as they are acting as a major obstacle in the adoption of cloud computing services Cloud Computing Concerns The major security issues with cloud are: 1. Privacy and Confidentiality Once the clients outsource data to the cloud there must be some assurance that data is accessible to only authorized users. The cloud user should be assured that data stored on the cloud will be confidential.

Security and Data Integrity Data security can be provided using various encryption and decryption techniques. With providing the security of the data, cloud service provider should also implement mechanism to monitor integrity of the data at the cloud.

4. Rijndael encryption Algorithm

Rijndael as the standard symmetric key encryption algorithm to be used to encrypt sensitive information. Rijndael is an iterated block cipher, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). As input, Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks. The plaintext is input and then mapped onto state bytes. The cipher key is also a one-dimensional 8-bit byte array. With an iterated

block cipher, the different transformations operate in sequence on intermediate cipher results (states).

steps of the methodology are given below:

1. User sends the authentication request to the Cloud Service Provider (CSP).
2. CSP checks the authorization using EAP-CHAP and sends the acknowledgement back to the user.
3. User first encrypts his data and then outsources it to the server.
4. When the user downloads his data from CSP, it is received in the encrypted form.
5. To use the data user can decrypt it using same key used for encryption. A. Authentication Protocol EAP will implement on Cloud environment for authentication purpose. However different categories EAP are classified by authentication method.

In our purposed model, we use Challenge-Handshake Authentication Protocol (CHAP) for authentication. When client demands data or any service of cloud computing. Service Provider Authenticator (SPA) first requests for client identity. Implementation of CHAP in Cloud Computing Authentication of CHAP performs in three steps:

1. When client demands a service, Service Provider Authentication sends a "challenge" message to client.
2. Client responds with a value that is calculated by using one way hash function on the challenge.
3. Authenticator verifies the response value against its own calculated hash value. If the values match, the Cloud provider will give service, otherwise it should terminate the connection. Implementation of EAP-CHAP in Cloud Computing will solve the authentication and authorization problems

Rijndael Encryption Algorithm Implementation Encryption: The code for encryption process is given Rijndael (State, Cipher Key) {Key Expansion (Cipher Key, Expanded Key); Add Round Key (State, Expanded Key); for (i=1; I Final Round (State, Expanded Key + Nb*Nr);}

and the round function is defined as:

Round (State, Round Key) {Byte Sub (State); Shift Row (State); Mix Column (State); Add Round Key (State, Round Key);}

Rijndael Encryption Code the User data is encrypted by using Rijndeal Encryption. Symmetric key is used for encryption. The Rijndeal can be implemented easily and it is one of the most secure algorithms in the world. Rijndeal implementation has 128,192or 256bit key lengths. Size of data blocks to be encrypted with Rijndeal is always 128 bits. Initial round of Rijndeal is Add Round Key, this is followed by four iterative round including sub Bytes, shift Rows, mix Columns and add round key. Rijndeal with 128bit key length has 10 rounds, 192 bit has 12 rounds and 256 bit has 14 rounds.

Each round consists of the following steps.

1. Initial Add Round Key
2. Sub Bytes () Transformation
3. Substitutional Box Created For Sub bytes
4. Mix Columns () Transformation
5. Add Round Key () transformation The inverse process of encryption gives decryption text [4].

Rijndael Algorithm: Encryption/Decryption Process for Rijndael Algorithm is as follows:

1)Sub Byte step is a non-linear byte substitution that operates on each of the 'state' bytes independently, where a state is an intermediate cipher result. Here each byte in the state matrix is replaced with a Sub Byte using an 8-bit substitution box, the Rijndael S-box.

2) The Shift Rows step The Shift Rows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes

3) The Mix Columns step During this operation, each column is multiplied by the known matrix that for the 128-bit key is: The multiplication operation is defined as: multiplication by 1 means no change, multiplication by 2 means shifting to the left, and multiplication by 3 means shifting to the left and then performing xor with the initial unshifted value. After shifting, a conditional xor with 0x11B should be performed if the shifted value is larger than 0xFF. In more general sense, each column is treated as a polynomial over GF (28) and is then multiplied modulo x4+1 with a fixed polynomial $c(x) = 0x03 \cdot x3 + x2 + x + 0x02$

4) The Add Round Key step In the Add Round Key step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR [3].

I. CONCLUSION

Data security has become the vital issue of cloud computing security. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. So in this we focused on client side security In our proposed system, only the authorized user can access the data. Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally, he will not be able to decrypt it. Also, it is proposed that encryption must be done by the user to provide better security. Henceforth, security is provided using Rijndael.

REFERENCES

[1] Tejas P.Bhatt, Ashish Maheta, Security in Cloud Computing using File Encryption. International Journal of Engineering Research and Technology 1(9): (2012).

[2] Pratiyush Guleria, Vikas Sharma, Development and Usage of Software as a Service for a Cloud and Non-Cloud based Enviroment-An Empirical Study. International Journal of Cloud Computing and Services Sciences (IJ-CLOSER) 2(1): (2013).

[3] Sanjoli Singla, Jasmeet Singh, Survey on Enhancing Cloud Data Security using EAP with Rijn-

dael Encryption Algorithm", Global Journal of Computer Science and Technology (GJCST) 13(5): (2013).

[4] G.Jai Arul Jose, C.Sajeev, Implementation of Data Security in Cloud Computing. International Journals of P2P Network Trends and Technology 1(1): (2011).

[5] Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham, Mirza Aamir Mehmood, Implementation of EAP with RSA for enhancing the security of cloud computing. International Journal of Basics and Applied Sciences 1(3): 177-183 (2012).

[6] Prashant Rewagad, Yogita Pawar, Use of Digital Signature and Rijndael encryption Algorithm to Enhanced Security of data in Cloud computing Services, Proceeding published in International Journal of Computer Applications (IJCA) (2012).

[7] http://thegadgetsquare.com/1552/what-is-cloud-computing/

[8] http://en.wikipedia.org/wiki/Cloud_computing

[9] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[10] https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol