A Review Paper on Data Security in Cloud Computing

Gopal Krishn Tholambia

Student of PGI, Jaipur, India

Ms. Neeraj Bhardwaj

Assistant Professor at PIET,Jaipur,India

**Abstract**:

In cloud computing, security is a core concern because an organization or users trust for their critical information on cloud which is geographically dispersed and not under control of that user. Therefore security procedures and design of security architecture must be specific for cloud environment different to conventional technical system.

Data security very important part of our life and it became a broad issue for information technology. In the cloud computing network environment, security more serious foe the user’s information is available in various locations and worldwide. Data security protection is main concerns of the user about cloud technology. Although many cloud computing strategies have been investigated in both industry, academia and data protection privacy protection have been central to the development of cloud computing technologies in government, industry and business. In cloud Architecture, Data security and privacy protection are useful both Hardware and software. This study of reviews paper to have different strategies and challenges from both software and Hardware aspects of data protection in the cloud and aims to improve data security and environmental protection in a trusted cloud environment. In this paper, we perform a comparable empirical comparative study of existing research on data security and privacy protection techniques used in computer in the cloud.

In this paper I discuss about general data security issues and brief about cloud computing.

***Keywords – Cloud, Computing, Security***

**Introduction:**

CC provides storage facility and a online applications. Many companies uses cloud’s service model of cloud and types of cloud.

Two Categories are their in the security : Challenges are faced by Service provider (organization provide 3 facilities : Software as a service, Platform as a service, Infrastructure as a service) and Privacy & Security challenges faced by user (Organization those are uses cloud to store data and hosting application). Service providers must ensure that their cloud’s Infrastructure and data of client must be secured and applications are safe , while the user must take measures to fortify their services and use strongest passwords and authentication method.

The security of cloud computing includes a number of policies, digital technologies, software and controls that are used to protect the virtualization of Internet, protocols for content, customers, content, applications, services, and cloud's associated infrastructure. It is a sub-domain of computers, networks and more broadly the protection of information security. In Cloud Computing we study cloud security models and Privacy challenges & their solutions.

Traditional data protection models often focus on network-centric and perimeter security, often with devices such as firewalls and access control systems. But this method does not provide sufficient protection for APTs, privileged users, or other types of security attacks. Many businesses use document audit and protection (DAP) and Security Information and Field Management (SIEM) solutions to gather information together about what is happening. But monitoring and event relatedness alone does not translate into data protection.

**Cloud Computing:**

Cloud computing is defined as a mode for enabling convenient, on-demand network access to a shared pool of flexible and reliable computing resources, such as servers, storage, applications, services, etc., with minimal allocation and release speed. Or service provider interaction. Cloud is a platform where user can upload and maintain data. And user can able to access his/her data anywhere. Many big organizations/companies like Google, Amazon, Salesforce and Interest (use Amazon’s web service) use cloud platform to store the users data and they also provide security to their data by using encryption techniques.

Cloud computing provides low cost services, provides facility to use services from anywhere at anytime.

Cloud computing provides following facilities Scalability on demand, improving business process, storage facility, manipulations capability, accessing server, networking facility and software/application access facility.

**Ethical Issues in Cloud computing:-**

Data Privacy:- All major organizations provides privacy facilities to users data. Before uploading data on cloud it is necessary to encrypt the users data.

Data Security:- Data must be secured by taking backup before migrations on other data center.

Data Backup:- A good data backup policy ensures the security and consistency of data. Data backup is performed on regular basis so that user’s data is not lost.

Phishing & social attack

Insufficient Backup

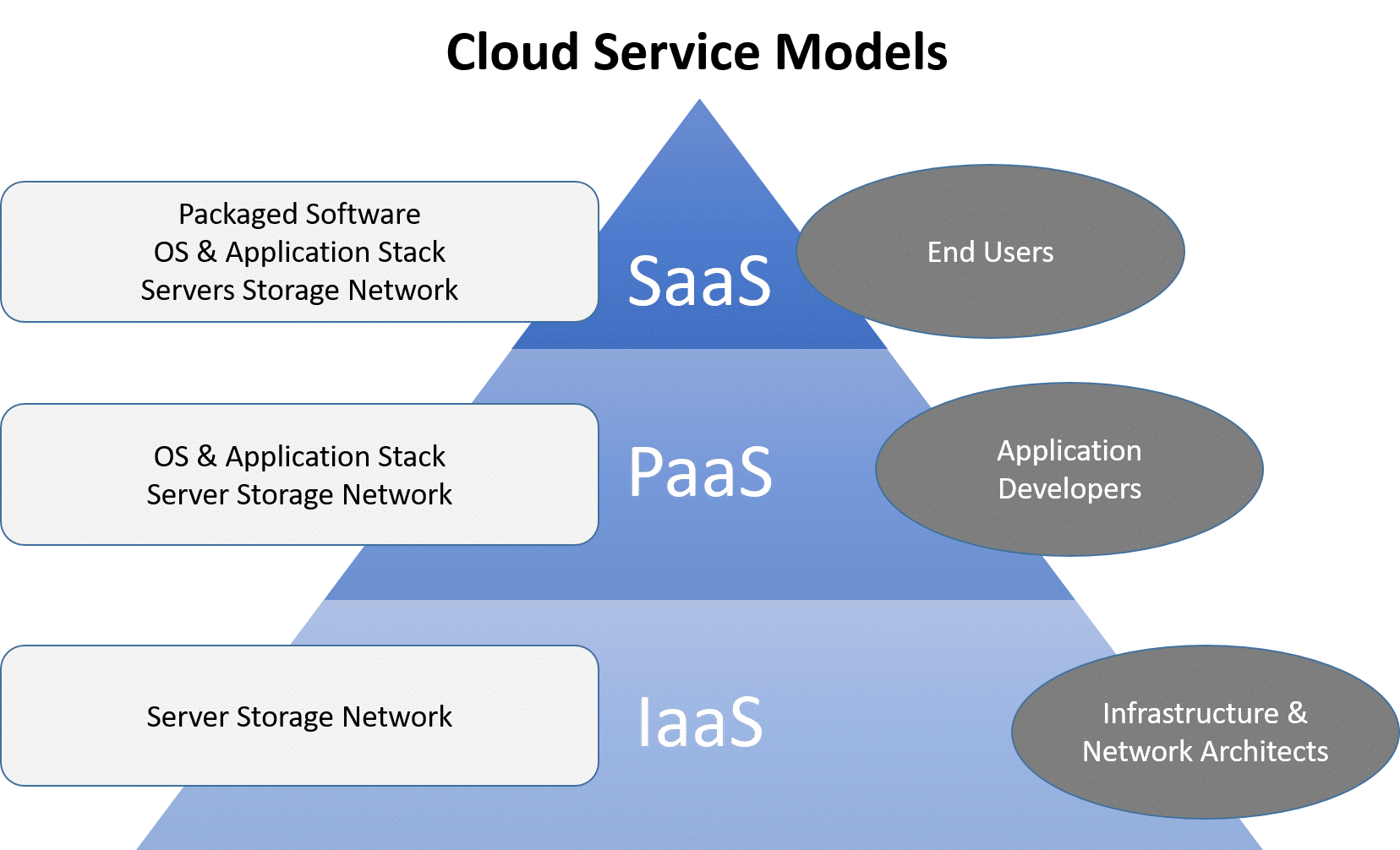
System penetrability

**Cloud Computing model:-**

-SAAS (Software as a service)

-PAAS (Platform as a service)

-IAAS (Infrastructure as a service)



**Cloud Security Algorithms:-**

**Data Encryption Standard:-**

Another name of DES (Data Encryption Standard algorithm) is symmetric key block cipher algorithm issued by NIST. Uses a single key (private key) in dual encryption and decryption. It works on 64 bits of data. 48 bit is the size of round key.

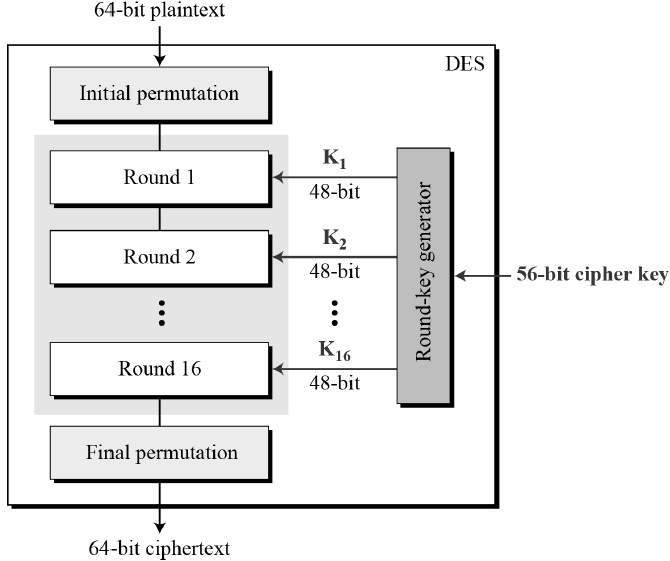
Into blocks of 64 bit size whole segment is divided; if necessary then the last block is attached. More permits and replacements are used everywhere to increase the complexity of the process crypt analysis in the cipher. The DES algorithm contains 2 P boxes (permutations) and 16 F(Feistily) rounds. The whole operation can be divided into three sections. The first category is Initial permutation and the last category is final permissions.

1. The original permutation resets 64-bit fragments. It doesn't work any buttons, it works on the specified form.

2. There are 16 fiestel rounds or cycle. Each cycle uses a different 48-bit rotation key applies to full containers to produce 64 products, produced according to a predefined set algorithm. The circular generator makes 16 48-bit keys in a 56-bit key.

3. Finally the final stage performs the final approval, the concurrent operation of the initial acknowledgment and the result is a 64-bit cipher script.

**General Structure of DES:**



**Advance Encryption Algorithm:**

Another name of Advance Encryption algorithm is Rijindael, it is developed after DES by NIST. Till now there is only one activate attack is possible on AES known as Brute force attack, if when attackers try all combinations of character to active encryption. AES and DES both are example of block cipher. Here Maximum variable length is 128, 192, or 256 but 256 is default. 128 blocks of data are Encrypted in bits (10,12,14 bits) depend on the size of key. AES encryption is rapid and elastic and it can be able to run on various platform mainly on smaller machines. And, this algorithm is closely monitored for multiple safety applications.

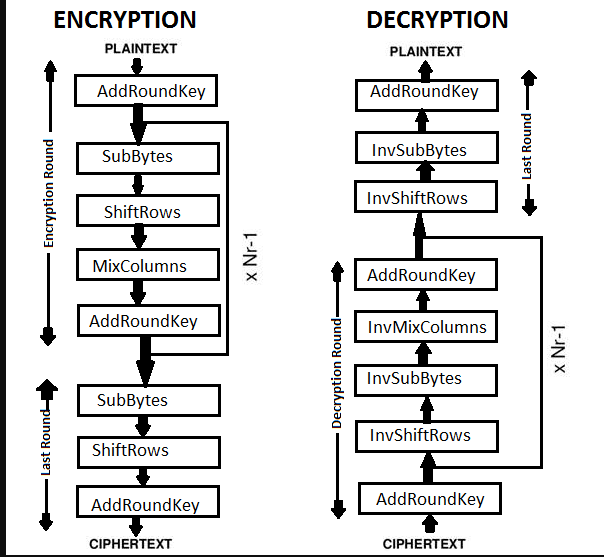
AES software implementable in C and JAVA.

AES dependent on substitutions-permutation network. Speed of AES in 6 time faster then Triple DES.

**General Structure of.AES :**

****

**Encryption and Decryption process of AES:-**

****

**Advantages of AES:-**

-Because it is implemented in both hardware and software, it is a very strong security protocol.

-It is one of the most widely used open source marketing solutions in the world.

-No one can access your personal information.

**Conclusion**:

So here I discussed about the algorithms of cloud, implementation of those algorithms. In future I will try to find more attack which may affect AES algorithm.

**References:-**

1. Ahmadi, M. and Moghaddam, F.F.; Jam, A.J.; Gholizadeh, S.; Eslami, M. A 3-level re-encryption model to ensure data protection in cloud computing environments. In Proceedings of the IEEE Conference on System, Process & Control , Kuala Lumpur, Malaysia, 12–14 December 2014.
2. Anitha Y, ―Security Issues in cloud computing‖, ―International Journal of Thesis Projects and Dissertations ―(IJTPD) Vol. 1, Issue 1, PP :( 1-6), Month: October 2013.
3. Oluyinka. I. Omotosho -- A Review on Cloud Computing
4. Arockiam, L. and Monikandan, S. Efficient cloud storage confidentiality to ensure data security. In Proceedings of the International Conference on Computer Communication and Informatics, Coimbatore, India, 3–5 January 2014; pp. 1–5.
5. Balamurugan, S.; Sathyanarayana, S. and Manikandasaran, S.S. ESSAO: Enhanced security service algorithm using data obfuscation technique to protect data in public cloud storage. Indian J. Sci. Technol. 2016.
6. Cloud Computing. Available online: https://en.wikipedia.org/wiki/Cloud\_computing#Security\_and\_ privacy (accessed on 8 February 2017).
7. Abdul D. S. and Elminaam, H. M. Abdul Kader and M. M. Hadhoud, ―Performance Evaluation of Symmetric Encryption Algorithms‖, Communications of the IBIMA Volume 8, 2009.
8. Gurpreet S. and Supriya K. ―Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security‖ International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
9. Garima S. and Gurgaon N. S., ―Triple Security of Data in Cloud Computing‖. Garima Saini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5 (4).2014,
10. Jaeger, B. Security as a Service Working Group, Defined Categories of Security as a Service (Preview)—Continuous Monitoring as a Service. Cloud Security Alliance 2016. Available online: <https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categoriessecurities-prep.pdf> (accessed on 10 August 2016).
11. Li, M. On the Confidentiality of Information Dispersal Algorithms and Their Erasure Codes. arXiv 2013, arXiv:1206.4123v2.
12. Mar, K. K.; Law, C. Y. and Chin, V. Secure personal cloud storage. InProceedingsofthe10thInternationalConference for Internet Technology and Secured Transactions (ICITST-2015), London, UK,14–16December2015.
13. Mask Sensitive Data. Available online: https://dataapps.io/redact.html (accessed on 12 January 2017).
14. Microsoft azure. http://www.windowsazure.com/; 2013.
15. Amazon s3. http://aws.amazon.com/s3; 2013.
16. Dropbox - your stuff, anywhere. https://www.dropbox.com/; 2013.
17. Varia, J., Mathew, S.. Overview of amazon web services. http://aws.amazon.com/whitepapers; March 2013.
18. Amazon web services: Overview of security processes. http://aws.amazon.com/security/; June 2013.
19. Google, “Browser security handbook,” 2009. [Online].Available: <http://code.google.com/p/browsersec/>
20. P. Karl Rexer. 2010 data miner survey highlights the views of 735 data miners, 2010.