International Journal of Engineering & Technology, 7 (1.5) (2018) 253-257

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Multilevel classification of security threats in cloud computing

N. Srinivasu *, O. Sree Priyanka, M. Prudhvi, G. Meghana

Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur,Andhra Pradesh, India-522502
**Corresponding author E-mail: srinivasu28@kluniversity.in*

Abstract

Cloud Security was provided for the services such as storage, network, applications and software through internet. The Security was given at each layer (Saas, Paas, and Iaas), in each layer, there are some security threats which became the major problem in cloud computing. In Saas, the security issues are mainly present in Web Application services and this issue can be overcome by web application scanners and service level agreement(SLA). In Paas, the major problem is Data Transmission. During transmission of data, some data may be lost or modified. The PaaS environment accomplishes proficiency to some extent through duplication of information. The duplication of information makes high accessibility of information for engineers and clients. However, data is never fully deleted instead the pointers to the data are deleted. In order to overcome this problem the techniques that used are encryption[12], data backup. In Iaas the security threat that occurs in is virtualization and the techniques that are used to overcome the threats are Dynamic Security Provisioning(DSC), operational security procedure, for which Cloud Software is available in the market, for e.g. Eucalyptus, Nimbus 6.

***Keywords**: Saas, Paas, Iaas, data backup, encryption, DSC, SLA, Virtualization, data transmission.*

1. Introduction

Cloud computing is one of the most used technology in today's world. Cloud computing simply describes that it is a hard disk that provided to the user by some user credentials, which the user can access the data and store the data through internet. In the cloud the user can increase the capacity of the storage, so that large amount of data can be stored. Cloud systems consist of three different layers Saas, Paas, Iaas which provides different kinds of services [14]. But while providing these services by cloud some security issues [3] arise. So, in this, we discuss the issues that occur in different layers and solutions to overcome the issues.

1.1 Software as a service

SaaS is a software delivery strategy that gives access to programming and its capacities remotely as a Web-based service. Saas uses the internet to deliver theapplications that can be accessed by the client. It is the most familiar service for cloud clients. It provides the services such as Google apps, workday, Cisco WebEx, sales force, Criti x go to the meeting. The services include email, customer relationship management, and healthcare-related applications. As the service is provided with the help of the internet there is no need of installing and running the applications on individual systems. The main security threats[3][7] in this layer are risks in data accessing and web applications services and the solutions to overcome these issues is service level agreement[4], web application scanners between the attributes and classify the same into sub attributes groups are also a notable work by Dromey et al. [6].

1.2 Platform as a service

Platform as a service which, provides platform and environment make the client build applications and services through internet. Paas is used for application and development while providing the components to the software. It makes the development, deployment, and testing of application easy, simple and cost-effective. The applications in Paas inherit some of the cloud characteristics such as scalability, high availability, multi-tenancy etc. [2] ... The services that are provided in this layer are .Net, Python, Java etc. Apprenda is one of the most used providers of private cloud Paas for.Net and java. In Paas, the major security issues that we are facing in is data transmission. Data transmission means transferring of data from source to the destination. The major problem that we are facing in data transmission [3] [13] is data may get attacked i.e., the data getting lost or modified by the third party [2] [11]. The solutions for this attack during data transmission is encryption [9] [12] and data backup [4].

1.3 Infrastructure as a service

Infrastructure as a Service (IaaS), are self-service models that which provides an operating system, for managing memory and processes along with a systems administration, and servers for growing such applications, services, and for deploying development tools, databases, etc… Iaas model allows automated deployment of servers, processing storage and networking. It can build a virtual data center in the cloud which means a collection of cloud resources specifically designed for business needs. Some of the services provided by Iaas are Amazon Web Service (AWS) [7] [12], Microsoft Azure, Cisco Metapod etc. The major security threats that occur in Iaas is in virtualization [3]. Virtualization is a technique in which an image of the total operating system of original one can be seen in another operating system. The security threat in virtualization is if the hypervisor gets to attack the system will also get attack and hence the data also gets attacked [1] [12] [14]. Another security threat in virtualization is allocation and deallocation of resources i.e. if the VM [7] operation data is written to the memory and is not cleared before reallocation of memory to next VM, then there is a chance of the data getting exposed to the next VM, but this should not have happened [11] [14]. The solutions for these issues are proper authentication and dynamic security provisioning [4].

2. Literature survey

1. Syed AsadHussai, Mehwish Fatima, Atid Saeed and Imran Raja who discuss about the dynamic security for each cloud layer. [1] [14]
2. Jeena Jha and JalakPansuriya who discuss the multi-level authenticate to generate password multiple level to access the cloud services. [1] [11]
3. R. Chaitanya, K. Mohan, S. Nithya who discuss about the levels such as application level host level and network level. [12]
4. LugiCappoliano, Salvatore, GuienniMazero who discuss the problems occurred in Denial of Services and Data Breaches. [7] [12]

2.1 Security threats analysis on cloud service layer

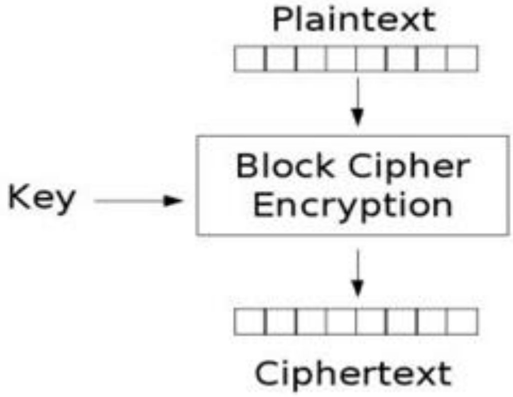
a) Data Transmission:

Data Transmission is one of the services provided at Platform as a service (Paas) [1] [4] [12]. It means transferring data between the client and the server and vice versa. The data transmission can be done in two different types of cloud environments they are public cloud and private cloud [11] [12] [14].]. Public cloud means the data in this type of cloud can be accessed byall the users of the cloud whereas private cloud means the data that can be used by the limited number of the users [11] [12] [14]. The data in the private cloud can be accessed only by the users who are provided the access by the cloud service provider(CSP) [7] [12] [14]. The CSP provides the key to access the private data in the cloud to the users who are eligible to access that data[7][12]. During these data transmissions from a sender to the receiver the data may get attacked i.e., the data may either get lost or modified [2] [11]. So, some of the solutions are provided which helps in stopping the attackers to attack the data.

In order to stop the modification of data by the third parties the solution that is provided is encryption technique. Encryption means converting the plaintext to cipher text [2]. The source should encrypt the plaintext by using some encryption technique and send it to the destination. The destination receives the cipher text and should use the same encryption technique which is used by the source and decrypt the data. Thus, the encryption can be done using many techniques. Some of them are cryptographic techniques like a stream cipher, block cipher and hash function [2]. In this paper, we discuss these cryptographic techniques in detail.

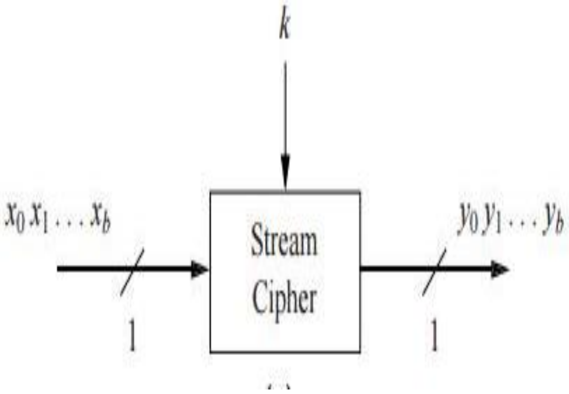
b)Block cipher

In block cipher encryption is done for the group of bits or group of bytes at a time. The size of the block that we encrypt may be either 64-bit or 128-bit [2]. In this method the cryptographic key is applied for the block of data and encryption, decryption is done at source and destination respectively. In this technique, we must make sure that the encryption key we are using must be different for the similar blocks of data. The solution for this is the cipher text which is obtained from the previous encrypted block of data should be used as an encryption key in order to encrypt the next block of data. By encrypting the blocks of data like this there is no way that the encryption key gets repeated. If the encryption key doesn't repeat, then the corresponding cipher text will also not repeat.



c) Stream Cipher

A stream cipher is sometimes also called as state cipher. In this method, encryption is done either bit by bit or byte by byte [2]. The performance of stream cipher is much faster and better when compared to the block cipher because the data that has to get encrypted is very less in stream cipher when compared to the block cipher. However, this method becomes a more complex and difficult one to perform for a large amount of data.



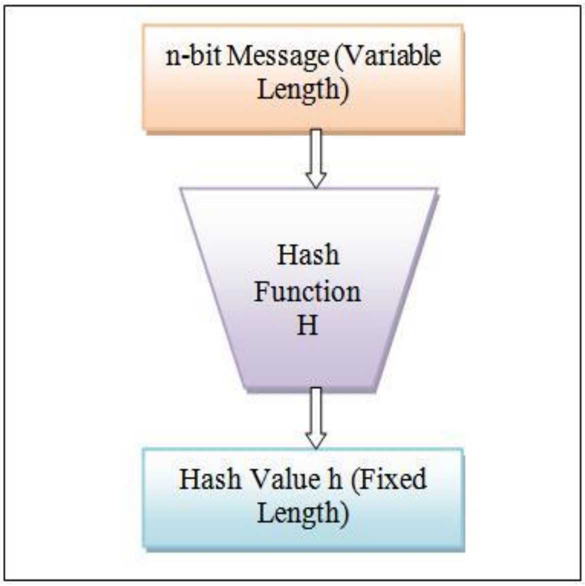
d) Hash Function:

A hash function is any function which is used to map data or arbitrary size to memory or data of fixed size. The values returned by this hash functions are called hash values, hash codes, simply hashes. In this method, encryption is done using a function called hash function [11]. The hash function is nothing, but a mathematical equation as shown below

$$F(x)=x \bmod 10$$

Where x is the plain text or the input on which the encryption must be performed.With the help of this hash function, the plain text can be converted into an alphanumeric string. The output that is obtained will be of fixed size. This technique makes sure that the encryption is done in such a way that no two inputs or plaintexts will produce the same outputs. Even if there is a slight difference in the plain texts the cipher texts that are obtained will have a large difference.

All the above-mentioned methods will help in providing data security. The usage of these techniques varies from one scenario to the other. Whatever the technique we use we must make sure that it applies for providing the security for the data which is present in both public and as well as private environments of the cloud.



e) Virtualization:

Iaas can build a virtual data center(VDC) in the cloud which means a collection of cloud resources which is specifically designed for specific needs [12] [14]. Virtualization is a technique in which an image of the total operating system of original one can be seen in another operating system so that it can utilize the resources of the real operating system fully [1] [14]. For capturing the functionalities of one operating system and transfer to the other operating system we require some medium. The medium that is used is a hypervisor [1] [12] [14]. A hypervisor is nothing but a special function which is required to run the guest operating system as a virtual machine [4] [11]. We can also say that virtualization is an component of cloud computing which helps in conveying the center estimations of cloud computing. However, because of virtualization sometimes we may face many risks [14]. In this paper, we discuss some of these risks and some solutions to overcome those risks.

One of the risks is that attacking the hypervisor[3]. If the attacker attacks the hypervisor the whole system gets attacked and hence the data will also get attacked[14]. Another risk that is associated with virtualization is allocation and de-allocation of resources. Suppose if one virtual machine operation data is written to the memory and the data is not cleared before the memory is allocated to the next virtual machine i.e. before reallocation then there is a scope that the data can be accessed by next virtual machine which should not happen. The solution for these two kinds of attacks is should have proper planning regarding the using of virtualization [2]. The resources should be used in a proper manner by the virtual machines. The data must be properly authenticated before deallocation of resources is done.

Another attack that can be done in virtualization is sniffing attack [12][14]. The sniffing attack is done by the sniffers. Sniffers are also called as network protocol analyzers [14]. These sniffers attack virtual network and capture the sensitive information such as passwords, account information etc[14]… The sniffers not only attack the sensitive information but sometimes hack the whole system and capture all the data which is present in the system. Different types ofsniffing attacks are MAC attack, DNS poisoning [12][14], ARP poisoning attacks[12]. The attacker attacks the IP address using these different kinds of sniffing attacks. There is a free sniffing tool called Wire Shark which helps in attacking the whole system. The solution provided to overcome thesesniffing attacks is dynamic security [15] provisioning[1]. Dynamic security contract(DSC)[1] identifies what is the type of attack that has occurred and in which service model the attack has occurred and provides security based on the type of the attack that has occurred and risk level associated with that attack. The mathematical equation that has been used for dynamic security contract(DSC)[1] is

DSC(X,S,A)--->R

Where X is service type.

S is security that has to be provided

A is type of attack that has occurred

R is level of risk because of attack

f) Web application service:

In Saas instead of installing and running the applications in an individual system, we use a service called as web application service. In this web application service, many services are provided such as accessing the data, modifying the data, administrative access etc.. The problem in this service is that the cloud service provider should not allow all the users to provide all the operations. So, we should restrict the users from performing all the operations one solution for this problem is authentication must be done i.e., verification must be done whether the cloud user is accessing the data in the right way or not.

Another solution for this kind of issues is service level agreement(SLA)[1][12].service level agreement is nothing but a contract between the cloud service provider and the user. In this, the user who wants to perform some operations in this web application is not directly allowed to perform the operations. The user must keep the request to the cloud service[15] provider by asking him to allow to access and perform the operation providing some details. If the cloud service provider is satisfied with the details provided by the user then he can allow that user to access the data. With the help of the service level agreement, multi-authentication is achieved[2].

Another few problems in this service are cookie poisoning, Backdoor and debug options, Denial of Service Attack(DOS attack)[7][12][14], Google hacking etc.. cookie poisoning means the content of the cookies can be modified or changed by an unauthorized user[14]. The solution for this cookie poisoning is cookies should be avoided or regular clean-up of the cookies is necessary. Backdoor and debug options means debug options provide an easy entry to the hacker into the website and let him make changes at the website level. The entry is easy to the hacker because the debug options are left unnoticed. So, the solution is we should scan the system periodically. Denial of service attack means the service that can be used by an authorized user is unable to be used by them. The solution for this attack is Intrusion Detection [14] System(IDS) is the most popular method. Preventive tools like firewalls, switches are used in this system. Google hacking means Google search engine is the best option for the hacker to access the sensitive information. The solution for this prevents sharing of all the sensitive information [1].

3. Advantages and disadvantages

Service	Advantages	Disadvantages
Data Transmission	1. Protecting data from unauthorized access. 2. Confidentiality [9], protecting data by keeping it private or secrete. 3. Authenticate [9], verifying the identity of the user. 4. Data integrity, the accuracy and consistency of data.	1. Very complex technique to implement. 2. Difficult to keep the key Secure. 3. Man in the middle attack.
Web Application Service	1. Guarantees better service and satisfied customer. 2. Information can be should and reported in a manner.	1. Some time’s it is different for the CSP’s to evaluate the SLA’s of cloud vendor
Virtualization	1. Easier backup and disaster recovery. 2. Better business continuity 3. More efficient	1. More Cost. 2. Implementing and managing is most difficult task.
Stream Encryption	1. Speed of transformation, algorithms is linear in time and constant in space. 2. Low error propagation, an error in encrypting one symbolically will not affect subsequent symbols.	1. Low transmission of all information, of a plaintext symbol is contained in a single cipher text symbol. 2. Susceptibility, to insertions/ modification of an active interceptor who breaks the algorithm might insert spurious text that looks authentic.
Block Encryption	1. High transmission, information from one plaintext symbol is diffused into several cipher text symbols. 2. Insusceptibility will be tampering was troublesome to embed symbols without identification.	1. Slowness of encryption, an entire block must be accumulated before encryption/decryption can begin. 2. Error propagation, an error in one symbol can make entire block untrustworthy

4. Conclusion

A novel Multilevel classification of Security threats in cloud computing survey the effect of different security attacks on different cloud layer is discussed some on this paper. This multilevel classification provides anewdimensiontoaddresssecurityconcernsonmultiplelevelsandminimization of their effects. The attack is also assessed slow, medium and high across different security concerns. The security requirements for different cloud services are also outlined for the secure cloud computing. These security requirements include data encryption [2][12], confidentiality, dataintegrity[9],dataprivacy,authenticationandauthorization. These security requirements are mapped to different cloud services to achieve integrity and coherence in the cloud system.

References

[1] King Saud University. Production and hosting by Elsevier B.V.This is an open access article under the CC BY-NC-ND license.

[2] Fifth International Conference on Future Generation Communication Tecnlogies(FGCT 2016).

[3] Luigi Coppolino Salvatore D’Antonio , GiovanniMazzeo , Luigi Romano Cloud security: Emerging threats and current solutions, 2016 Elsevie.

[4] Ashish Singh, Kakali Chatterjee, Cloud security issues and challenges: a survey, 2016.

[5] Minhai Ahmad Khan, A survey on security issues on Cloud Computing, 2016.

[6] International Journal of Scientific & Engineering Research, Volume 7, Issue 5, May-2016 149 ISSN 2229-5518.

[7] Brian Cusack, Evaluating single sign on security failure in cloud services, 2015.

[8] (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, 2015.

[9] ICCMIT- M. El-Kafrawya, Azza A. Abdoa, Amr. F. Shawish, Security Issues Over Some Cloud Models,2015.

[10] Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.

[11] Farzad Sabahi, Cloud Computing Security Threats and Responses,2011.

[12] IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[13] D. Fox, “Open web application security project,”Datenschutz und Datensicherheit-DuD, vol. 30, no. 10, pp. 636–636, 2006.

[14] R. Charanya et al./International Journal of Engineering and Technology (IJET).

[15] Yong Yu, Cloud computing security and privacy : Standards and regulations,2016.

[16] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.

[17] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.

[18] N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.

[19] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.

[20] Mahesh Mudavath, K Hari Kishore "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Inte-

grating FPGAs” Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.

[21] P Bala Gopal, K Hari Kishore, B.Praveen Kittu “An FPGA Implementation of On Chip UART Testing with BIST Techniques”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015

[22] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.

[23] N Bala Gopal, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.