ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 11, November 2015

A Survey on Security Issues in Cloud Computing and its Solutions

Densy John V[1], Dr. X. Agnise Kala Rani[2]

Research Scholar, Karpagam Academy of Higher Education, Coimbatore, India[1]

Professor, Dept. of Computer Applications, Karpagam Academy of Higher Education, Coimbatore, India[2]

Abstract: Cloud computing is becoming a popular tool for storing data both by individuals and corporate sectors. The cloud provides many services which are accessible and economical for its users over the Globe. The main concern of the data storage in the cloud is its security. Many security attacks can happen when transferring and keeping the data over the network. This paper studies about the various network security issues and its solutions. Cryptography plays an important role in the security solution of cloud data. The paper discuss about DES, AES, and BLOWFISH to find the faster Cryptographic algorithm.

Keywords: Security, passive and active attacks, cryptography, symmetric and asymmetric encryption, DES, AES, RSA, BLOWFISH, CryptDB.

I INTRODUCTION

Cloud computing is considered as an innovative way of information systems architecture. It is a cost-effective way of computing where resources and services are managed in a remote location away from the geographical location of the actual business. This makes the cloud architecture more risky and prone to uncertainty at all levels of network, host, application and data. The cloud can be defined as "a shared pool of resources like network, storage, server, applications and services that can be provisioned with minimal management effort" [1]. There are so many characteristics and benefits for cloud computing that makes the people and business to migrate to this technology.

Some of the characteristics are defined below [2]:

Flexibility: The users can quickly add–on the resources whenever they want.

Elasticity: The cloud consumers can expand the resources when they need more and release them once they finish.

Resource pooling: All computing resources from the cloud service provider are pooled together to serve the cloud consumers using either the multi-tenancy or virtualization [3]. In this, the resources are assigned and reassigned according to the need of the customers.

Broad network access: The cloud resources are available on the network through internet by heterogeneous devices like mobile phones, laptops, PDA's.

There are different service models available in computing. They are given in the following:

Software as a Service (SaaS): Cloud consumers can choose any applications running the site. The applications are accessible from different client's devices which can be considered as the different instances of the same software. Examples are: Google Docs, SalesForce.com, ERP, CRM, SCM. SaaS gives the customers less control over the infrastructure but has optimization in terms of availability, disaster recovery and maintenance.

Platform as a Service (PaaS): Using this cloud consumer can deploy their own applications in the cloud without having the underlying platform needed for it in their client system. PaaS is a development platform for the SaaS like cloud services and applications. Therefore, the security requirement for both SaaS and PaaS are inter-related. Example is: Google Apps Engine, Microsoft Azure, Amazon Map Reduce [4].

Infrastructure as a Service (IaaS): Infrastructure gives the consumers storage, hardware, servers and networking components. This provides the cloud users to run any software, which may include operation systems and applications. The user has a control over the cloud infrastructure including network, storage, and operating system [2]. Infrastructure can be dynamically expanded and shrunk as and when needed. Example: Amazon Elastic Cloud Computing and Simple Storage Services (S3) [4].

Data Storage as a Service (DaaS): [3] Data storage is one of the main service that cloud offers to its customers. It helps the users to pay only for what they actually use rather than the software license, infrastructure and the platform they are using. Daas offers a table structure that may be much easier and faster than the traditional RDBMS. Examples include: Amazon S3, Google BigTable, Apache HBase.

The four types of cloud implementation are the following:

Private cloud: A private cloud is implemented and operated by a company in its premises or off premises or by a third party [2] [3]. There are several factors behind implementing the private cloud. The organization will get a full control of the cloud which will in turn make the cloud more reliable and secure over the activities within its network. The cloud computing will utilize the IT resources in the organization in its full extend. The data transfer cost from a local IT structure to a Public cloud is also considerable. [3]

Community cloud: The cloud is shared by several organization of same characteristics, security requirements and policies. It may be controlled by the organization on premise or off premise or by a third party [2] [3].

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 11, November 2015

Public cloud: This type of cloud architecture is available to the public by an organization providing cloud services. Its policies, value, profit and costing are solely determined by the service provider. The data will reside in the datacenter of the cloud service provider and the maintenance and security is the responsibility of the service provider [3].
Hybrid cloud: The infrastructure is the combination of two or more of the above architecture (like private, community, public). The organizations will optimize the core competencies by giving out peripheral business functions onto public cloud while controlling the core activities on-premise through private cloud.

II SECURITY ISSUES IN CLOUD

The security issues has an important effect in the cloud computing. The cloud offers data to store in a remote location. It is the modern way of accessing the computing resources over the internet and hence more susceptible to the security issues and vulnerabilities posed by the traditional internet. Moving and storing information in the cloud has the possibility to store information in different servers residing in remote countries which has different regulations. [5] Moreover, multi-tenancy and resource pooling will make the information of the organization unsecure. The basic factors of security are availability, integrity and confidentiality.

Security Criteria

Availability: The data, software and hardware residing in the remote location should be available to the authorized persons on demand. The cloud service providers have the big risk of providing the requirements of their clients whatever they need. It should safe-guard the information and software of its customers.
Integrity: Integrity means Information assets can be modified by only by authorized parties [2]. Data Integrity refers to the protection of data against deletion or modification. The cloud service providers will make sure of any unauthorized users are gaining access to the system and may alter or delete users data and there by affect the integrity of the system.
Confidentiality and privacy: It refers that only authorized parties can access secured or protected information in the cloud. Since the parties using the cloud are increasing day by day the chances of accessing the secured information of the organization will be higher. Confidentiality can be achieved by providing a strong authentication. The cloud provider is responsible for ensuring user's privacy. The data stored in cloud server means that it may be located in any geographical area like Asia or Europe. Any dispute in the privacy disclosure may be affected by the local regulations of the region where the actual cloud server resides. [2]
Authentication: it is the technique to prove that the participants in the conversation are genuine. Digital Signature is an example for such Authentication. They are also used to ensure the non-repudiation of the digital documents or transactions done by the participants in the communication. The non-repudiation ensures preventing a sender from denying the authenticity of a document he produced or send.

Attack Types in Networks

There are two categories of attacks: Passive attacks and Active attacks. [14] The **release of message contents** and **traffic analysis** are the two types of passive attacks. In the release of message contents the intruder reads the content transmitted through the network between the participants whereas in traffic analysis the pattern and frequency of the message between the sender and receiver is observed.
Passive attacks are Denial of Service (DoS), Masquerade, replay and modification of messages. In **DoS** (Denial of Service) the attacker tampers the data in the physical channel and will not allow the user to access the information they need.
Masquerading happens when the intruder takes the place of one the entity in the conversation. In **replay** the intruder takes the information transmitted between the participants earlier and resends it on behalf of one of the participant. **Modification** of message means that the attacker takes information in the network and alters them and sends it through the network.

III SECURITY SOLUTIONS FOR CLOUD COMPUTING

Many techniques are needed to protect data in a cloud. Some of the efficient methods are access control, Digital Signature and Cryptography. [13] Cryptography is one of them that secure the data while transmitting across the network. It can prevent the both passive and active attacks. The encryption algorithm uses the combination of public and private keys to protect the sensitive data. By suitably choosing the encryption keys and implementing the digital signature we can minimize the network security issues. There are many cryptographic algorithms available and widely used for network security.

Cryptography can be divided into two types- symmetric and asymmetric. Symmetric encryption uses only one key for encryption and decryption and asymmetric encryption use two keys- public and private, one for encryption and other for decryption. In this study we discuss about various encryption algorithms and compare their performance.

In [7], authors explain that encryption can keep the data safe in the network and also in database where we store them for information safe. In this paper they suggest the use of encryption and genetic algorithm to encode crossover and decode the information sent through the network. The receiving end will do the reverse process of crossover and decoding and encoding of octal sequence. There will be a sequence of iterations depending on the need of security of the data encrypted. Implementation of genetic algorithm provides the security in the method of encoding, crossover type, length of data, and key used for encoding. The concept of encrypting the data even when they are stored makes it more secure. CryptDB[8] is where the data stored encrypted and the query runs on the encrypted data. [9]The database proxy running in the cloud will performs the encryption and decryption of the query that may run on the modified database management system. The encrypted result will be given back to the user as plain text using the key to decrypt database proxy.

In [9] authors explain about the secure architecture for mobile database. There are three levels of security is needed when we think about the mobile computing. One of them is the security of the device. The theft of the device, attack on mobile OS, confidentiality of data residing in the device. The second one is the security of mobile database. Encryption plays an important role in protecting the sensitive data while carrying the mobile device outside the physical boundary of the organization. The third one is the secured network provided for the mobile data when transmitted across the network in order to synchronize with the mobile server.

In [6] the authors have chosen DES, AES and RSA for comparison. DES consists of single key for both encryption and decryption. AES is good in security and also in speed while RSA secures data so that only the concerned users can access it. From the experiments done they proved that AES decryption is faster when comparing the DES and RSA encryption algorithm and the RSA takes more time to encrypt and decrypt back to the original text.

Whenever the network contains the malicious nodes the security can be provided by the encryption algorithm. [10]The Diffie-Hellman algorithm will enable the parties to send both keys safely in an unsecured network.

In [11] the authors study AES and BLOWFISH the two symmetric key encryption algorithms commonly used for network security. The paper reveals that BLOWFISH algorithm has a better performance when comparing with AES. It takes less memory space and faster encryption and decryption. AES consumes more space and resources if the data encrypted is bigger in size.

The need of better security leads to the implementation of double encryption algorithms. The paper [12] explains one such method in which the authors implemented the binary addition operation and circular shift operations which is hardly broken by any cryptanalyst. This content-based algorithm needs to transfer the key for decryption secure along with the message. This becomes the harder part since the key to decipher the message should be send safely. Without the key it is impossible to decipher.

IV CONCLUSION

In this paper, we studied about the importance of cloud computing and its security issues. We found that the security can be implemented by suitable encryption methods and key interchange. Authorization and authentication can be done with Digital Signature which also uses the encrypted digital value. While comparing the encryption algorithm studies reveal that AES is faster than DES and RSA while BLOWFISH is more efficient than AES.

REFERENCES

[1] P. Mell and T. Grance,"The NIST definition of cloud computing", NIST special Publication, 2011. [online]. Available: http:// csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2]Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues" journal home page: www. Elsevier.com/locate/fgcs available online: 22 December 2010

[3] Tharam Dillon, Chen Wu, Elizabeth Chang "Cloud Computing: Issues and challenges" 2010 4th IEEE International conference on Advanced Information Networking and Applications

[4]Hoanh T. Dinh, ChonhoLee, Dusit Niyato and Ping Wang "A survey of mobile cloud computing: architecture, application and approaches" Published online 11October 2011 in Wiley Online Library Wireless Communication and mobile computing 2013

[5] Younis a Younis, Madjid Merabti and Kashif Kifayat "Secure cloud Computing for Critical Infrastructure: A Survey" MYA Younis, K Kifayat - Liverpool John Moores University, United Kingdom, 2013 - cms.livjm.ac.uk

[6] Dr. Prerna Mahajan& Abhishek Sachdeva "A study of Encryption algorithms AES, DES and RSA for Security" Global Journal of Computer Science and Technology network, Web & Security vol.13, issue 15 version 1.0 Year 2013

[7] Sabareesan M, Gobinathan N, "Network Database Security issues and Defense" International Journal of Engineering Research and Applications Vol. 3, Issue1, January- February 2013, pp1748-1752

[8] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan " Crypt DB: Protecting Confidentiality with Encrypted Query prcessing" International Journal of Engineering Research Applications SOSP '11, October 23–26, 2011, Cascais, Portugal. Copyright 2011 ACM 978-1-4503-0977-6/11/10

[9] D. Roselin Selvarani, Dr. T N Ravi "A Review on the role of Encryption in Mobile Database Security" International Journal of Application or Innovation in Engineering & Management, www. Ijaiem.org Vol.3, Issue 12, December2014

[10] Basant Kumar Verma, Binod Kumar "An improved Weighted Clustering for Ad-hoc Network Security" International journal of Computer Sciences and Engineering, Vol. – 3.(3), PP(51-55) Mar2015, E-ISSN: 2347-2693.

[11] K. Lakshmi Narayanan, P. Kannan, S. Esakki Rajavel, "A Comparative Study and Performance Evaluation of Cryptographic Algorithms: AES and Blowfish", International Journal of Advanced Research Trends in Engineering and Technology, Vol.1 , Issue 3, November 2014.

[12] Sourabh Chandra, Bidisha Mandal, Sk. Safikul Alam, Siddhartha Bhattacharyya, " Content based double encryption algorithm using Symmetric key cryptography", International Conference on Recent Trends in Computing, Procedia Computer Science 57 (2015) 1228-1234. Available online at www. Sciencedirect.com

[13] M. Madhurya, B. Ananda Krishna, T. Subhashini, " Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks", International Journal of Computer Network and Information Security, 2014, 2 30-37

[14] William Stallings., Cryptography and Network Security- Principles and Practice, 5th Edition. Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall.

BIOGRAPHIES

Ms. Densy John V is a research Scholar of Karpagam University. She is working as Lecturer in Computer Science for Bachelor of Science Business Informatics in AMA International University Bahrain. She holds Masters Degree in Computer Applications from Madurai Kamaraj University.

Dr. X. Agnise Kala Rani is a Professor in the Department of Computer Applications at Karpagam University, Coimbatore. She received her Ph.D. in 2011 from Mother Teresa University. She holds the Master of Engineering degree from VMKV University and Master of Computer Applications degree from Madras University. She has several publications including scientific journals and top-tier networking conferences to her credit.