International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Ensuring Data Integrity and Security in Cloud Storage

Dharmesh Dhablia[1], Shruti Timande[2],
Mtech (CSE)[1], Mtech (WCC)[2]
Email: dharmeshdhabliya@gmail.com[1],shruti14591@rediff.com[2]

Abstract- As with the Internet, on-demand applications have grown so ubiquitous that almost every business user interacts with at least one, whether it's an email service, a Web conferencing application, or a file hosting system. This model is already quite common for consumer apps like email and photo sharing, and for certain business applications. In this paper we present a way to secure the data using different compression and encryption algorithms and to hide its location from the users that stores and retrieves it. The data is stored at multiple places over the information space (over the Internet). It sounds similar to file hosting websites which stores the data that is being uploaded by different users and can be retrieved using proper authentication. The only difference is that the system for which paper is presented is a application based system like which will run on the clients own system. This application will allow users to upload file of different formats with security features including Encryption and Compression. The uploaded files can be accessed from anywhere using the application which is provided. We believe this system serves as a foundation for future work in integrating and securing information sources across the WWW.

Keywords
IaaS, SaaS, PaaS, Encryption, Decryption, Compression, Decompression, File hosting services.

1. INTRODUCTION

Typically, the applications used for file transfers and storage is web based and hence requires web browsers to upload the files on servers. But the problem arises the time required and the limits of a browser to run properly till the file is transferred.

This application will allow the uploading of files without disturbing other processes and at the same time user may be able to work in web browsers without hanging up the uploads. The file size varies according the premium or free users. The application uses compression as well as encryption algorithms for file security and therefore takes more time to upload a file. The key to encryption can be taken by user or a default key for users can be taken according to the design of application.

After the implementation of the application, it needs to be hosted so that it is available to the end user. For this purpose various hosting services including cloud are available.

1.1 CLOUD COMPUTING

Software, Platform, and Infrastructure as a Service are the three main service delivery models for Cloud Computing. Those models are accessible as a service over the Internet. The Cloud services are made available as pay-as-you-go where users pay only for the resources they actually use for a specific time, unlike traditional services, e.g., web hosting. Furthermore, The pricing for cloud services generally varies according to QoS requirements [1]. The cloud deployment models, based on their relationship to the enterprise, are classified to private, public, and hybrid.

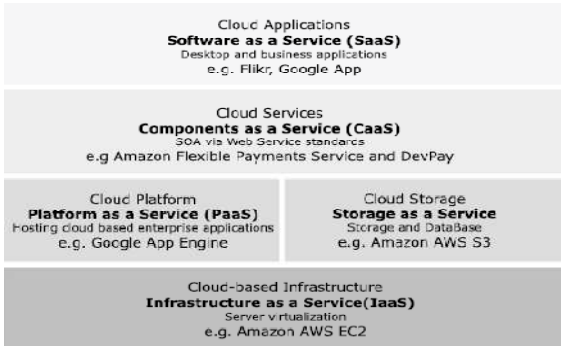

Figure 1 : Cloud Architecture

Examples of emerging Cloud Computing Platforms include Microsoft Azure1, Amazon EC22, and Google App Engine3. The confusion between Cloud and Service Oriented Architecture (SOA) has prompted us to discuss this issue and offer a brief comparison between them. SOA and Cloud Computing can be considered complementary services sharing common characteristics. Hence, if SOA is a set of principles and methodologies designed to facilitate systems integration and communication regardless of development languages and platforms, Cloud Computing, on the other hand, is designed to enable companies to utilize massive capacities instantly without having to invest into new infrastructure, train new staff, or license new software. Cloud Computing allows small and medium-sized businesses to completely outsource their datacenter infrastructure, as well as large companies that need huge load capacities without building larger expensive datacenters internally. Cloud Computing employs the virtualization technology to offer a secure, scalable, shared, and manageable environment. In short, regardless of the difference in designing purposes and the dependency of Cloud Computing on virtualization technology, Cloud Computing might intersect with SOA in Components as a Service, e.g., SOA via Web Service standards. Therefore, Cloud Computing and SOA can be pursued independently, or concurrently as complementary activities to provide an outstanding business.

This paper presents a detailed and precise study of IaaS security and privacy concerns. We have investigated security for each IaaS component: Service Level Agreement (SLA), Utility Computing (UC), Platform Virtualization, Networks & Internet Connectivity, and Computer Hardware. Furthermore, Cloud software's security that impact on IaaS and on the whole Cloud Computing is presented. We are interested in the IaaS delivery model because it is the foundation of all other delivery models, and a lack of security in this layer affects the other delivery models that are built upon IaaS layer.

2. SECURITY MECHANISMS

Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered and sending the in splitted format is most secured way to transfer the data through the network.

2.1 AES ENCRYPTION

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits.

The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

2.2 Working of AES:

Advanced Encryption Standard or AES was invented by Joan Daemen and Vincent

Rijmen, and accepted by the US federal government in 2001 for top secret approved encryption algorithms. It is also referred to as Rijndael, as it is based off the Rijndael algorithm. Reportedly, this standard has never been cracked.

AES has three approved key length: 128 bits, 192 bits, and 256 bits. To try to explain the process in simple terms, an algorithm starts with a random number, in which the key and data encrypted with it are scrambled though four rounds of mathematical processes. The key that is used to encrypt the number must also be used to decrypt it.

The four rounds are called SubBytes, ShiftRows, MixColumns, and AddRoundKey. During SubBytes, a lookup table is used to determine what each byte is replaced with. The ShiftRows step has a certain number of rows where each row of the state is shifted cyclically by a particular offset, while leaving the

first row unchanged. Each byte of the second row is shifted to the left, by an offset of one, each byte in the third row by an offset of two, and the fourth row by an offset of three. This shifting is applied to all three key lengths, though there is a variance for the 256-bit block where the first row is unchanged, the second row offset by one, the third by three, and the fourth by four. The MixColumns step is a mixing operation using an invertible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output.

In the fourth round, the AddRoundKey derives round keys from Rijndael's key schedule, and adds the round key to each byte of the state. Each round key gets added by combining each byte of the state with the corresponding byte from the round key. Lastly, these steps are repeated again for a fifth round, but do not include the MixColumns step.

These algorithms essentially take basic data and change it into a code known as cipher text. The larger the key, the greater number of potential patterns that can be created. This makes it extremely difficult to descramble the contents, which is why AES has been Teflon-coated.

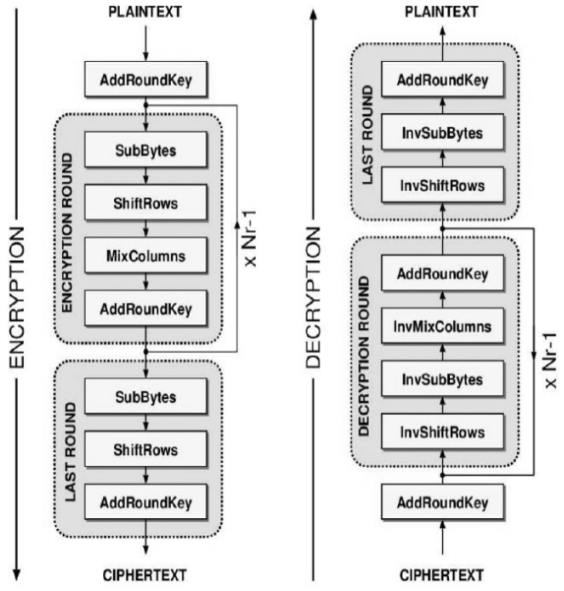

Figure 2 : Working of AES

2.3 CRITERIA OF A CRYPTOGRAPHIC ALGORITHM

The security of the model has been analysis on the basis of their encryption algorithm and the key management. It has been observed that the encryption algorithm have their own characteristics; one algorithm provides security at the cost of hardware, other is reliable but uses more number of keys, one takes more processing time. This section shows the various parameters which plays an important role while selecting the cryptographic algorithm. The Algorithm found most promising is AES Algorithm with 256 bit key size (256k).

3. Design

As application developers, our job now is to figure out which platform components are going to allow us to build all of these features.

The system architecture shows the core design of the application. The system serves the purpose of file hosting and hence requires a server that holds data. Multiple clients can logged in to the server and share files. The system should work in the flow as shown below:

- User should register on website and download the application and install it.
- User has to log in through the application and performs operation user wants.

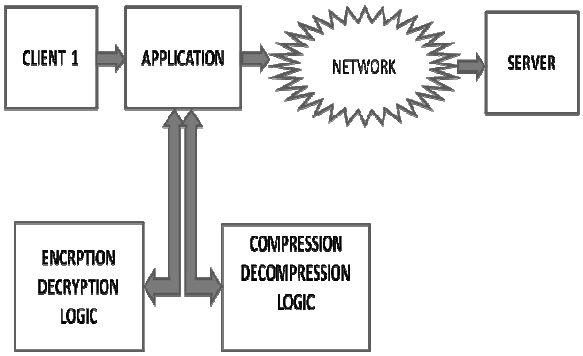

Figure 3 : System Architecture

4. CONCLUSION AND FUTURE WORK

IaaS is the foundation layer of the Cloud Computing delivery model that consists of multiple components and technologies. Each component in Cloud infrastructure has its vulnerability which might impact the whole Cloud's computing security. Cloud Computing business grows rapidly despite security concerns, so collaborations between Cloud parties would assist in overcoming security challenges and promote secure Cloud Computing services.

In this paper, we investigated the security challenges that associated with IaaS implementation and deployment. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions. Our future research vision will focus on two directions to provide confidentiality, integrity, and secure Infrastructure management for IaaS service. First, extending techniques such as proposed in TCCP into IaaS layer to improve confidentiality and integrity of VMs. Second, integrating TCCP with secure resources management schemes to get more controlled isolation environment. Finally, a prototype will be implemented to demonstrate the system feasibility and performance.

REFERENCES

[1] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, p. 9, August 2008. [Online]. Available: http://arxiv.org/abs/0808.3558

[2] SLA Management Team, SLA Management Handbook, 4th ed. Enterprise Perspective, 2004.

[3] G. Frankova, Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.

[4] P. Patel, A. Ranabahu, and A. Sheth, "Service Level Agreement in Cloud Computing," Cloud Workshops at OOPSLA09, 2009. [Online]. Available:

http://knoesis.wright.edu/aboutus/visitors/summer2009/PatelReport.pdf

[5] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud- Computing System," Cluster Computing and the Grid, IEEE International Symposium on, vol. 0, pp. 124–131, 2009.

[6] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, 1st ed., 2009. [Online]. Available:

http://books.google.com/books?id=BHazecOuDLYC&pgis=1

[7] R. Kanneganti and P. Chodavarapu, SOA Security. Manning Publications, 2008. [Online]. Available: http://www.amazon.com/SOASecurity-Ramarao-Kanneganti/dp/1932394680

[8] M. McIntosh and P. Austel, "XML signature element wrapping attacks and countermeasures," Workshop On Secure Web Services, 2005.

[9] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.

[10] B. D. Payne, "Xenaccess." [Online]. Available: http://doc.xenaccess.org/

[11] J. Kirch, "Virtual machine security guidelines," 2007. [Online]. Available: http://www.cisecurity.org/tools2/vm/ CISn VMn Benchmarkn v1.0.pdf

[12] T. G. Ben, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A Virtual Machine-Based Platform for Trusted Computing." ACM Press, 2003, pp. 193–206.

[13] S. Berger, R. C´aceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "TVDc: Managing security in the trusted

virtual datacenter," ACM SIGOPS Operating Systems Review, vol. 42, no. 1, p. 7, 2008.