International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 36-39
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

A NOVEL APPROACH TO CLOUD COMPUTING: INFRASTRUCTURE AS A SERVICE SECURITY

Sukrit Sehgal
Student
Department of Electronics and Communications
Amity University, Noida

Michail Papoutsidakis, MEng, MPhil, PhD
Assistant Professor
Dept. of Automation Engineering
Piraeus University of Applied Sciences
P.Ralli & Thivon 250, 12244, Athens, Greece

Abhishek Srivastava
Assistant Professor
Department of Information Technology
Amity University, Noida

Kriti Bansal
Student
Department of Electronics and Communications
Amity University, Noida

***Abstract*-Organizations bringing cloud usage onto their business in greater urge of sustaining, and gaining cost efficiency has enabled utilization of pay-per-use pattern of service and optimized use of other alternative methodologies. In order to prevent trade-off of data critical to business, organizations are obliged to hold the insight into what type of cloud suits their business best. Cryptography hit upon as the quick fix to storage of data along with its legitimate and proper access. This paper put forward a new method for Infrastructure as a service security to the already existing solution.**

***Keywords*- Public cloud, Private Cloud, Hybrid Cloud, Data Integrity, Data Privacy**

I. INTRODUCTION

Cloud computing is a modern hypothesis acknowledged of making sharing resources available to the user as a service on demand. In a short span of time, this feature provides the web based infrastructure for data storage regardless of user's location all over the world with pay-per-use criterion. IT assets incorporate system, server, stockpiling, applications, switches, administrations. Consequently, they can be dealt, and administered with much greater ease, and cooperation from administrative suppliers [1]. The availability of internet has turned cost effective sharing and store of data – customary. As a rule, the physical location of stored data remains anonymous from the end user of cloud computing [2]. Technology is reformed in a way to maintain data and associated applications through the services of internet and central remote servers.

There are various **clouds computing services (Fig. 1)** which are as follow:

1) Infrastructure As A Service(IAAS)
2) Platform As A Service(PAAS)
3) Software As A Service(SAAS)
4) Database As A Service(DAAS)

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 36-39
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

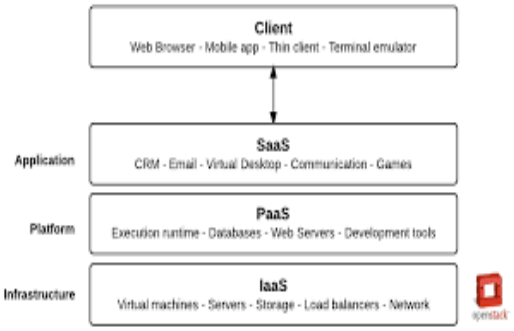

Fig. 1: Cloud computing services

Infrastructure as a Service: IAAS Model allows organizations narrow out the devices which are used to strengthen operations including: capacity, equipment, servers, and organizing segments. Foundation as an administration is otherwise called Hardware as an administration (HAAS). The association allows an organization pay as per requirement. It is now and again circumvented as utility figuring. The well-known Infrastructure as a service provider is Amazon web services [3].

Platform as a Service: PAAS allows transmission of both: figuring stage, and arrangement compartment as an administration without programming downloads or establishments for designers, IT supervisor and end-client. The application lets engineers build and run their product arrangement on a cloud regardless of expense incurred in purchasing products and equipment. Illustrations of Platform as an administration are force.com, Google App Engine and so forth.

Programming as a Service: The programming is conducted over the web to remain operative behind a firewall in the neighbourhood, PC, laptops, tabs, etc. The user has to "pay-as-you-go" model which is mainly deployed for Customer Relationship Management (CRM) and Sales Force Automation (SFA) [4] that reduces the cost of software by eliminating the need of technical staff to manage: install, software upgrades, and reduce the cost of licensing software.

Database as a Service: In cloud computing another model referred to as database as a server (DAAS) is illustrated for keeping up the information [5]. The model permits pay per utilization. The DAAS model has its own distinct arrangement of constraints differing from conventional databases. The assurance of Information Security is a principle challenge to DAAS model is. The model arranges a service provided by the service provider to the clients over internet. Contrary, the drawback is uncertainty in efficient execution of query at the cloud resident server so as to not compromise data security

To crack the data security problem, a new framework - Phantom DB has been introduced. Phantom DB maintains data security by encrypting data prior to storage at server with every data item encryption under multiple encryption schemes. The encryption have some special characteristics allowing server perform certain operations on the cipher text itself.

The storage of data in a private data centre turns out to be problematic that can be overcome by modern concept of cloud used. There are mainly four **types of cloud or model** (Fig 2) available which are as follows:

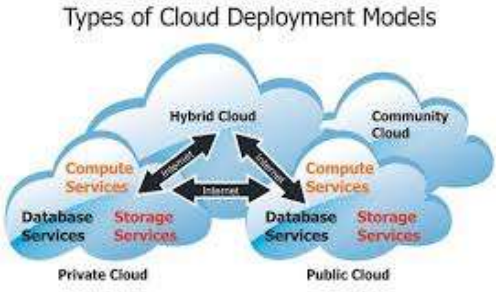

Fig. 2: Types of cloud

1) Public Cloud: The distributed computing model having administrator making assets. For instance, applications accessible to all over the web publically can be made free by administration with user paying as per the amount usage of data/space. It is also called as external cloud.

2) Private Cloud: Private cloud can be defined as the cloud computing model, which is owned or managed by the organization or a third party with inbound or, outbound of organization which is more expensive than public cloud [6]. It is also regarded as internal cloud and corporate cloud. For example, eucalyptus system.

3) Community Cloud: Community cloud can be characterized as distributed computing model having base shared by a few associations for a common cause monitored by them, or administered by third party. For example, Amazon's elastic compute cloud (EC2) and simple Storage Service (S3) [6].

4) Hybrid Cloud: Hybrid cloud is composed of chunk of two or more cloud organization model which are connected in a way allowing exchange of information without interrupting each other [1]. A settled hybrid cloud can be esteemed for providing

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 36-39
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

secure administration, for instance, accepting client instalments, and instalments that are in reserve to the business. for example, representative finance handling.

II. RELATED WORK

In 2010 Farrell [7] addressed the following issues: potential security, privacy, and related GRC. The paper spotlights highly perceived technological benefits asking prioritization. In 2011, Hori et. al reported about various security features for internal challenge on cloud computing [8]. In 2011, Khorshed et. al performed a survey focusing on lacunae along with challenges of crime with bringing out an approach to preventions of attacks [9]. In 2012, Ayala et. al defined the problem and advised on the basis of guidance from National Institute of Standard Technology [10]. In 2012, Yeluri worked about the experiences of Intel team with the challenges to security and control on resources in cloud computing [11]. In 2014, D. kanchana suggested the intrusion detection and elimination architecture in virtual network systems to develop a defense-in –depth intrusion detection framework. Issues and challenges associated with secure QoS aware routing in MANETs are discussed in [12-13].

III. SECURITY ISSUES

From last few years, cloud computing is a segment rising unprecedentedly. Information security includes scrambling the information and giving the right approaches which are authorized for information sharing. Some of the different security issues in infrastructure as a service security are:

Data Privacy: Information in the cloud take off in all directions which raises concern for the security of data or information.

Data Integrity: Data integrity assures data remain unchanged at all level because data is vulnerable at any level of storage.

Data Segregation: Data in the cloud is imparted together to information from other customer. In order to prevent unauthorized access, security is a concern.

Securing Data Storage: Securing the information is highly critical security-issue in distributed computing. How to anticipate information misfortune and planting innovations accordingly.

III. PROPOSED WORK

This paper proposes a solution for infrastructure as a Service Security based on the results and inferences from the research papers published in past defining cloud computing, types of cloud services, types of cloud model, Infrastructure as a Service in various journals and conferences etc.

About Infrastructure As A Service: Infrastructure is the base for alternate administrations which are accessible in distributed computing. Versatile distributed computing highly alludes to a base where both capacity of information and the handling on the information happens out of mobile device [2]. Security and privacy features must be embedded in the cloud computing adoption.

The data can be encrypted using cryptography. Fig. 3.Cryptography is the technique of storing and transmitting a data in another form - 'encrypted' form with authorised person having access or transmit the data using public or private key. As in traditional database data are distributed in different system but we can apply this approach to save our data more efficiently.

RSA utilizes open and private key for encryption/unscrambling, open key is utilized to encode information that is kept confidential. Information hashed with open key must be decoded with private key. The decision of choosing key size is most basic criterion since it marks the security level. For all intents and purposes picking key size of 2048 piece or 4096 bit is not pre-decided and it can be adjusted with scope of some other choice like key lifetime, devoted application some backing 2048 key and some backing 4096 key size, that is versatile based application. For instance, let information is scrambled by utilizing keys and assume an assault is found allowing a 2048 piece key get hacked in 200 hours. Now it won't imply 4096 piece key getting hacked in 400 hours, in fact it might at present need numerous years to break a solitary 4096 key.

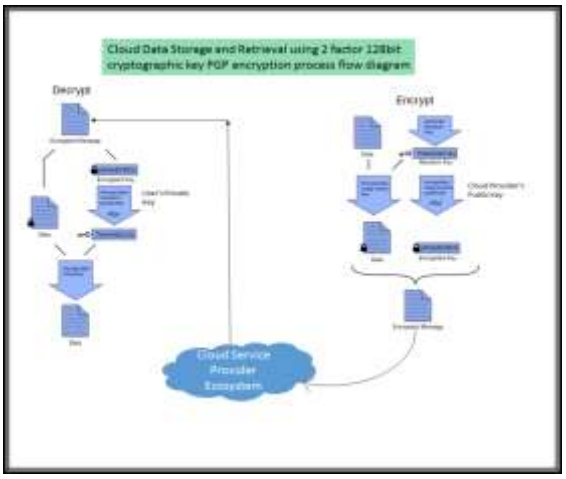

Fig. 3: Proposed Architecture

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 36-39
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

Pseudo Code of the algorithm:

a) Encryption and data Storage algorithm :

Step 1: Login to the system utilizing the username and password - (1st factor security)
Step 2: Generate random key
Step 3: Encrypt the random key using the cloud service provider's 128bit primary number based public key
Step 4: New Key = Encrypted random key
Step 5: Encrypt data using random key – (2nd Factor security)
Step 6: Combine the encrypted data and the "New Key" from Step no 4
Step 7: Save data to the Cloud Storage Service using the user credentials and unique account number.

b) Decryption and data Retrieval algorithm:

Step 1: Login to the system utilizing the username and password - (1st factor security)
Step 2: Acquire the encrypted key
Step 3: Decrypt the key using combined key using the User's Private Key to get the "New Key"
Step 4: Decrypt the data using the "New Key"
Step 5: Retrieve the data from the cloud
Step 6: Revalidate the user credentials for 2 factor authentication
Step 7: Showcase the data

IV. CONCLUSION

There are various possible solutions to address vulnerabilities in the security of infrastructure. Organizations have to wisely adopt cloud related system without compromising the data security. This work has proposed several security issues concerned with infrastructure as a service component, Fig 3.

The approach proposed is ensuring the information offer confirmation to client. This framework gives ideal arrangement about information security in cloud on the grounds that in the event, anyone can access client information from cloud. Consequently they can't comprehend the substance of information. As the information is in scrambled structure, the framework is executed in light of easing information assurance to the cloud client; moreover, framework guarantee security of information, which is most vital requisite for enabling client enjoy benefits of cloud.

In this paper, various layer of Infrastructure as a service has been outlined. We also proposed security adding by having cryptography technology having cipher text, public key and private key infrastructure included.

V. REFERENCES

1. B. D. Chung, H. Jeon, and K.-K. Seo, "A framework of cloud service quality evaluation system - focusing on security quality evaluation," Int. J. Software Eng. Applicat., vol. 8, no. 4, pp. 41–46, May 2014.
2. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, March 2012.
3. R. Tempo, G. Calafiore, and F. Dabbene, Randomized Algorithms for Analysis and Control of Uncertain Systems, with Applications, 2nd ed. London: Springer-Verlag, 2013.
4. J. Yao, X. Liu, X. Chen, X. Wang, and J. Li, "Online decentralized adaptive optimal controller design of cpu utilization for distributed real-time embedded systems," in Amer. Control Conf. ACC'10, Baltimore, MD, 2010, pp. 283–288
5. H. Hoffmann, J. Eastep, M. D. Santambrogio, J. E. Miller, and A. Agarwal, "Application heartbeats: A generic for expressing performance goals and progress in self-tunning systems," in 4th Workshop on Statistical Mach. Learning Approaches Architecture Compilation SMART'10, Pisa, Italy, January 2010, pp. 1–15.
6. M. Maggio, H. Hoffmann, M. D. Santambrogio, A. Agarwal, and A. Leva, "Controlling software applications via resource allocation within the heartbeats framework," in IEEE Conf. Decision and Control CDC'10, Atlanta, GA, December 2010, pp. 3736–3741.
7. J. Hellerstein, Y. Diao, S. Parekh, and D. M. Tilbury, Feedback Control of Computing Systems. Hoboken, NJ: John Wiley & Sons, 2004.
8. R. Kulhavy, "Restricted exponential forgetting in real-time identi- ´ fication," Automatica, vol. 25, no. 5, pp. 589–600, September 1987.
9. S. Haykin, Adaptive Filter Theory, 5th ed. Upper Saddle River, NJ: Prentice Hall, 2013.