ISSN 2395-1621

Securing Software as a Service Model for Cloud Computing

[#1]Smita D. Patil, [#2]Pushpa B. Didwagh, [#3]Tanvi V. Mhaske, [#4]Trupti B. Yadav, [#5]Prof. Archana Patil

[1]sdpatil1595@gmail.com
[2]pushpadidwagh215@gmail.com
[3]Mhasketanvi12@gmail.com
[4] Truptiyadav149@gmail.com

[#123]Department of Computer Engg,
JSPM NTC, Pune, Maharashtra, India

ABSTRACT

Cloud computingndoubtedly, has become the buzzword in the IT industry today. Looking at the potential impact it has on numerous business applications as well as in our everyday life, it can certainly be said that this disruptive technology is here to stay. Many of the features that make cloud computing attractive, have not just challenged the existing security system, but have also revealed new security issues. This paper provides an insightful analysis of the existing status on cloud computing security issues based on a detailed survey carried by the author. It also makes an attempt to describe the security challenges in Software as a Service (SaaS) model of cloud computing and also endeavors to provide future security research directions.

Keywords— **Cloud security, Security architecture, Security, Privacy.**

ARTICLE INFO

Article History

Received :28th December 2015

Received in revised form :

29th December 2015

Accepted : 30th December , 2015

Published online :

4th January 2016

I. INTRODUCTION

Cloud computing has become an important technology where cloud services providers provide computing resources to their customers (tenants) to host their data or perform their computing tasks. Cloud computing can be categorized into different service deliver models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Virtualization is one of the key technologies used in the IaaS cloud infrastructures. For instance, virtualization is used by some of the major cloud service providers such as Amazon and Microsoft in the provision of cloud services. We will use the term tenant to refer to cloud customers who wish to access services from cloud providers. Tenants can themselves be using their virtual machines to provide services to their own customers; we will refer to customers as those who use the services of the tenants. Hence customers in our architecture are the customers of the tenants.

Project Area

Area of our project is Cloud computing. Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet.

Working of cloud:The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive online computer games. To do this, cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Related Work

In existing system an effective reputation management system with associated trust establishment through multiple

© 2015, IERJ All Rights Reserved

scoring functions and implemented the security service on a realistic application scenario in distributed environments. There are depicted several privacy as well as security issues that arise in a cloud computing framework.Yanetal had proposed a nice scheme for handling data protection in terms of confidentiality through amalgamation of identity management with hierarchical identity-based cryptography for distribution of the key as well as mutual authentication in the cloud infrastructure.In trust and reputation based scheme in collaborative computing is presented. In the super-peer to handle queries for consumers and clients. The law-aware super-peer acts as a guardian providing data integration as well as protection. presented the pay-as-you-go business model of cloud infrastructure and put forward the urge of providing high security for cloud computing as this is going over publicly accessible internet domain.

II. Existing System

In the existing system the operating systems and applications of the tenants can be potentially large and complex. The existing system contains security vulnerabilities .The data are stored without compression in the cloud which lead to large space utilization .In the existing system the cloud service providers do not generally offer security as a service to their tenants. Tenants need to make their own arrangements for securing their virtual machines that are hosted in the cloud. There are several significant challenges in securing infrastructure from different types of attacks.

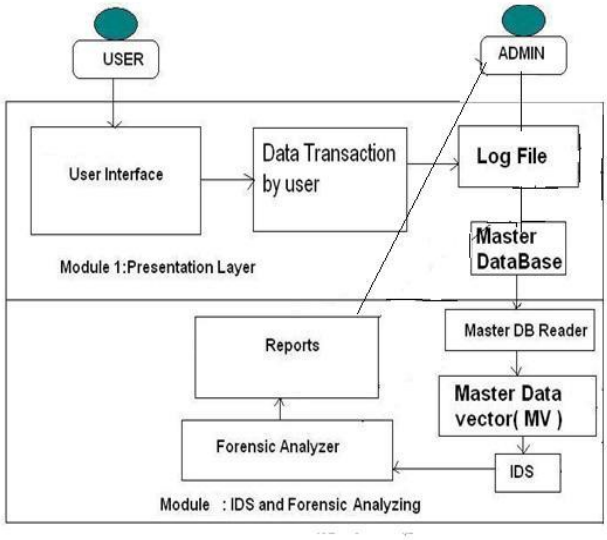

Fig 2.1 Existing System

III. PROPOSED SYSTEM:

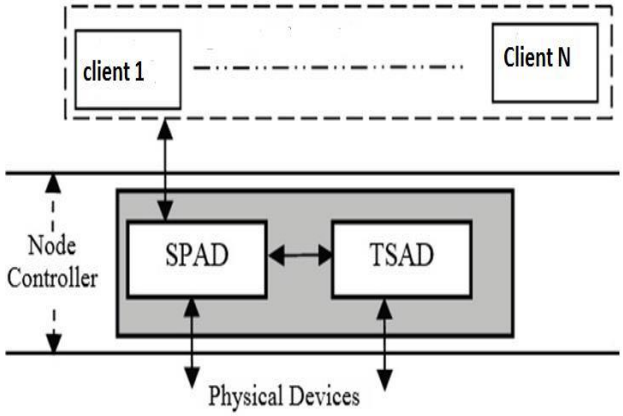

Fig 3.1 Basic block diagram

The data are stored after compression in the cloud that lead to less space utilization. The data storage is allowed only after the ip verification of the user is authorized. The authentication is included at the time of node creation rather that storage and retrieval of the data. The node controller control capability is extended to provide services to large number of user with a single link. The storage controllers first compress the data before storing into the cloud. The data can be retrieved by the user after the IP address verification.

IV. SYSTEM ARCHITECTURE

The data are stored after compression in the cloud that lead to less space utilization. The data storage is allowed only after the ip verification of the user is authorized. The authentication is included at the time of node creation rather that storage and retrieval of the data. The node controller control capability is extended to provide services to large number of user with a single link. The storage controller first compresses the data before storing into the cloud. The data can be retrieved by the user after the ip address verification

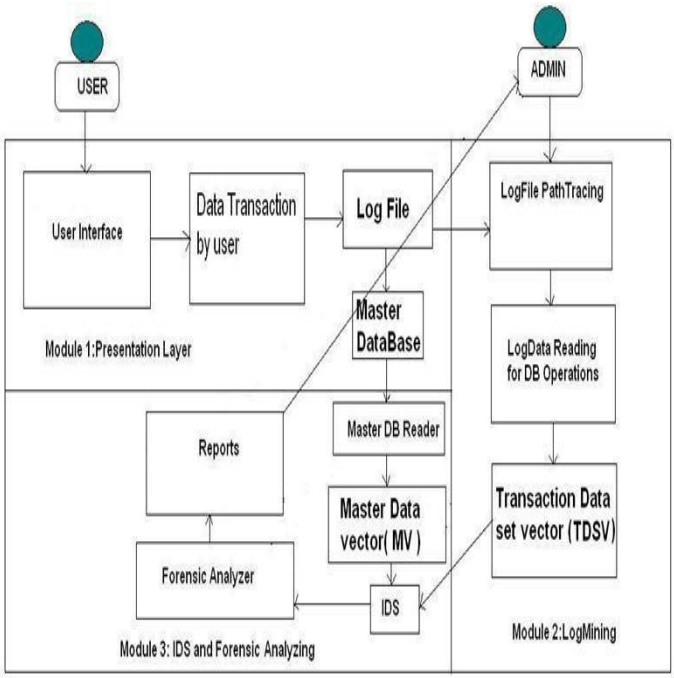

Fig 4.1: System Architecture

© 2015, IERJ All Rights Reserved

V. CONCLUSION

Though there are numerous advantages in using a cloud based system, there are yet many practical issues which have to be sorted. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service level agreements (SLA), security and privacy, and power efficiency. As described in the paper, currently security has lot of loose ends which scares away several potential users. Until a proper security module is not in place, potential users will not be able to leverage the true benefits of this technology.

VI. REFRENCES

[1] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", October 7, 2009, version 15, National Institute of Standards and Technology (NIST).(www.csrc.nist.gov)

[2] Kevin Curran, Sean Carlin and Mervyn Adams "Security issues in cloud computing", publishedin August 2011, Elixir Network Engg.(www.elixirjournal.org)

[3] Kevin Hemalen, Murat Kantarcioglu, Latifur Khan,and Bhavani Thuraisingham, The University of Texas at Dallas, USA, "Security Issues for cloud computing", April-June 2010,international Journal of Information Security and Privacy.

[4] "Security Guidance for Critical Areas of Focus in Cloud Computing", April 2009, presented by Cloud Security Alliance (CSA).

[5]Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, VasanthBala and PengNing, "Managing security of virtual machine images in a cloud environment", November 2009, Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96.

[6] Miranda Mowbray and Siani Pearson, "A Client-Based Privacy Manager for Cloud computing", June 2009,Proceedings of the Fourth International ICST Conference on communication system software and middleware.

[7] Flavio Lombardi and Roberto Di Pietro, "Transparent Security for Cloud", March 2010, Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415.

© 2015, IERJ All Rights Reserved