International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 20th April 2018. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-4

Title: SECURITY IN CLOUD COMPUTING – A SURVEY PAPER.

Volume 07, Issue 04, Page No: 76-84.

Paper Authors

***MALLEREDDY. SOWJANYA REDDY, SOMANABOINA. RAJESWARI.**

* Siddahartha Institute of Technology and Sciences.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SECURITY IN CLOUD COMPUTING – A SURVEY PAPER

[1]MALLEREDDY. SOWJANYA REDDY, [2]SOMANABOINA. RAJESWARI

[1,2] Assistant Professor, Dept of CSE, Siddahartha Institute of Technology and Sciences, Narapally,Hyderabad,Telangana,India

ABSTRACT: Cloud computing will be mainly giving many users a very flexible way of transferring the data through a network. By using the cloud computing we can be connected to a group of people in a small area like an office and many others. In this cloud computing there will be security issues that will occur to the users that are connected in a network. So to overcome this security issues natively trusted computing platform is used to overcome these security issues. By using these there won't be complete security provided. So to give the complete security to the cloud computing we will be introducing our proposed system that is Shamir's secret sharing algorithm. This will be examining each every security aspect very much in a detailed manner and giving the maximum security to the people in the network who are using cloud computing.

KEY WORDS: Security in Cloud Computing, Trusted Computing, Shamir's Secret Sharing algorithm.

I. INTRODUCTION

Cloud computing is computing that includes a large number of computers associated through a communication network such as the Internet, similar to utility computing [4]. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. Network-based services, which appear to be delivered by real server hardware and are in fact served up by virtual hardware simulated by software running on one or more real machines, is often called cloud computing. Such simulated servers do not physically exist and can therefore be relocated around and scaled up or down on the fly without disturbing the end user, somewhat like a cloud becoming larger or smaller without being a physical object [3].

In common usage, the term "the cloud" is fundamentally a metaphor for the Internet [5]. Marketers have further made popular the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service", i.e. remotely through the Internet.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Typically, the seller has actual energy-consuming servers which host products and services from a remote location, so end-users don't have to; they can simply log on to the network without installing anything. The major models of cloud computing service are known as software as a service, platform as a service, and infrastructure as a service [3].

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network [6]. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users.

Security in cloud computing:

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model [4] [7]. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures [8]. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security [9].

Cloud computing offers many benefits, but is vulnerable to threats. As cloud computing uses increase, it is likely that more criminals find new ways to exploit system vulnerabilities. Many underlying challenges and risks in cloud computing increase the threat of data compromise. To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology.

II. RELATED WORK

Mikkilineni, Rao stated that The skyrocketing demand for a new generation of cloud-based consumer and business applications is driving the need for next

generation of data centers that must be massively scalable, efficient, agile, reliable and secure. The authors see a parallel between the state of the data centers today and the evolution of the Intelligent Network (IN) infrastructure in telecommunication. The telecommunications networks have for many years, demonstrated their ability to reliably enable network (voice) services creation, assurance and delivery on a massive scale. Based on an analysis of the Intelligent Networks in telecommunications to identify proven concepts and key lessons that can be applied to enable next generation IT datacenters experience this paper asserts that:

1. In order to scale cloud services reliably to millions of service developers and billions of end users the next generation cloud computing and datacenter infrastructure will have to follow an evolution similar to the one that led to the creation of scalable telecommunication networks.

2. In the future network-based cloud service providers will leverage virtualization technologies to be able to allocate just the right levels of virtualized compute, network and storage resources to individual applications based on real-time business demand while also providing full service level assurance of availability, performance and security at a reasonable cost.

3. A key component - identified in this paper as the Virtual Resource Mediation Layer (VRML), must be developed through industry collaboration to enable interoperability of various public and private clouds. This layer will form the basis for ensuring massive scalability of cloud infrastructure by enabling distributed service creation, service delivery and service assurance without any single vendor domination.

4. The next generation virtualization technologies must allow applications to dynamically access CPU, memory, bandwidth and storage (capacity, I/O and - throughput) in a manner similar to that of the telecommunications 800 Service Call Model with one level of indirection and mediation. The authors believe that the next generation cloud evolution is a fundamental transformation - and not just an evolutionary stack of XaaS

implementations, which will enable global service collaboration networks utilizing optimally distributed and managed computing, network and storage resources driven in real-time by business priorities.

Jensen, M. stated that The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure (CapEx) and operational expenditure (OpEx). In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection-sphere of the data owner. Most of the discussions on this topics are mainly driven by arguments related to organizational means. This paper focuses on technical security issues arising from the usage of Cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations

Anirban Kundu, Guanxiong Xu, Ruopeng Liu stated that a load balancing strategy in heterogeneous environment of a Cloud is going to be developed. It consists of several high-end servers and cluster computers. A set of Web servers is to be utilized to create the effect of Web based scenario. Load balancers are being used to control the propagation of the user oriented requests towards a specific sub-network of proposed Cloud. Exhaustive experimentations are to be exhibited in the paper to demonstrate systems' high performance. The goal of setting up the overall system network is to meet the high demand of services from the clients' devices in a concurrent manner. Experimental results have been demonstrated using proposed Cloud architecture based on space, CPU, disk, memory, and network. Test results of Windows clients are generated using freeware "Jmeter" for maximum of 2000 concurrent users. In case of Linux clients, test results are generated using freeware "ab" for maximum of 1000 concurrent users. Maximum 2000 users are used for the sake of showing the results in a concise way.

III. EXISTING SYSTEM

Trusted cloud computing platform (TCCP) that provides a closed box execution environment by extending the concept of trusted platform to an entire IaaS backend. The TCCP guarantees the confidentiality and the

integrity of a user's VM, and allows a user to determine up front whether or not the IaaS enforces these properties.

The model of trusted computing is originally designed to provide the privacy and trust in the personal platform and the trusted computing platform is the base of the trusted computing. Since the internet computing or network computing has been the main computing from the end of the last century, the model of trusted computing is being developed to the network computing, especially the distributed systems environment. The cloud computing is a promising distributed system model and will act as an important role in the e-business or research environments. As web service technology have developed quickly and have been used broadly, cloud computing system could evolve to cloud computing service, which integrates the cloud computing with web service technology. So we could extend the trusted computing mechanism to cloud computing service systems by integrating the TCP into cloud computing system.

In cloud computing environment, different entities can appeal to join the CLOUD. Then the first step is to prove their identities to the cloud computing system administration.

Because cloud computing should involve a large mount of entities, such as users and resources from different sources, the authentication is important and complicated. Considering these, we use the TCP to aid to process the authentication in cloud computing.

The TCP is based on the TPM. The TPM is a logic independent hardware. It can resist the attack from software, and even the hardware attack. The TPM contain a private master key which can provide protect for other information store in cloud computing system. Because the hardware certificate can store in TPM, it is hard to attack it. So TPM can provide the trust root for users.

Since the users have full information about their identity, the cloud computing system can use some mechanism to trace the users and get their origin. Because in the TCP the user's identity is proved by user's personal key and this mechanism is integrated in the hardware, such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information. Each site in the cloud computing system will record the visitor's information. So by using the TCP mechanism in cloud computing, the trace of participants can be known by the cloud computing trace mechanism.

IV. PROPOSED SYSTEM

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

Mathematical definition:

The goal is to divide secret S (e.g., a safe combination) into n pieces of data $D_1,\ldots\ldots,D_n$ in such a way that:

1. Knowledge of any k or more D_i pieces makes S easily computable.
2. Knowledge of any k-1 or fewer D_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called \left(k,n\right) threshold scheme. If k=n then all participants are required to reconstruct the secret.

Shamir's secret-sharing scheme:

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k\,\! points to define a polynomial of degree k-1.

Suppose we want to use a (k,n) threshold scheme to share our secret Swithout loss of generality assumed to be an element in a finite field F of size P where $0 < k \leq n < P$; S<P and P is a prime number.

Choose at random $k-1$ positive integers $a_1, \cdots, a_{k-1}$ with $a_i < P$,and let $a_0 = S$. Build the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-}$. Let us construct any n points out of it, for instance set $i = 1, \cdots, n$ to retrieve $(i, f(i))$. Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

One Time Password:

One Time Password (OTP) authentication is a method to reduce the potential for compromised user credentials. The concept behind OTP is that every session initiated by a user generates a unique user credential that is only valid for that session or for a very short period of time. Even if an attacker is capable of obtaining this user credential, it may either no longer be valid or be prohibited from additional use [12].

Security of one-time-password protocols:

The main security property that protocols employing one-time passwords should achieve is: strong mutualauthentication based on knowledge of one-time passwords. Our work will address one-time passwords in thecontext of PAKE protocols, which provide an additional property: secure key exchange.

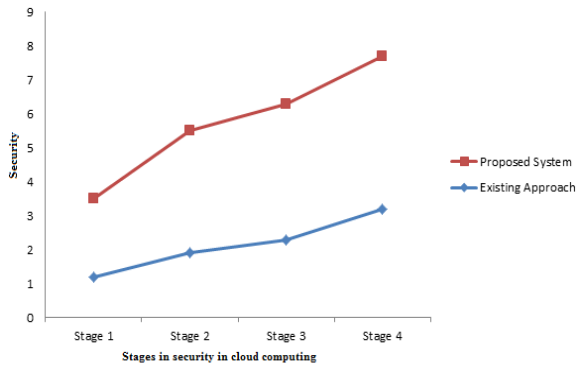
The motivation for using one-time passwords is that the compromise of one password should not affectthe security of sessions involving another password. The one-time password serves to mutually authenticatethe client and the server; there are no other long-term values like public keys or certificates. Authentication isbased on knowledge of the shared password. Informally, a protocol will provide secure mutual authenticationif no honest party A^ accepts a session as being with party B^ unless B^ participated in the protocol, and viceversa. We want a one-time-password protocol to give secure mutual authentication for the current sessioneven if other one-time passwords have been revealed [12].

In addition to mutually authenticating two parties to each other, we want a protocol that will also output asession key that can be used to encrypt and protect the integrity of future communications between those twoparties. This is a common feature required of many secure communication protocols.. Using SSL to establish an authentic channel requires that the user can obtain and properly use an authentic public key for the server. In other words, it requires a public key infrastructure, where as one-time-PAKE only needs shared passwords.

V. EXPERIMENTAL RESULTS

In our results we mainly show that there is vast difference in security provided by existing approach and proposed system.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org



Graph showing the difference between two approaches

From the above graph it can be observed that our proposed approach will be yield high security when compared with native approach. The different stages that will be occurring in cloud computing while considering the data from one system to other. It can also be observed that at each stage the proposed strategy obtain high security.

CONCLUSION

In this paper we conclude that in cloud computing the main important factor is security that will be the primary need of any user who are accessing in a particular network. The native approach which is trusted computing platform will be not giving maximum security to the users. The experimental study introduces Shamir's secret sharing algorithm which will be giving the maximum security. The experimental study reveals that the proposed approach yields the maximum security in the cloud computing.

VI. REFERENCES

[1]. Cloud Computing and the Lessons from the Past by Mikkilineni, Rao.

[2]. On Technical Security Issues in Cloud Computing by Jensen, M.

[3]. Cloud computing from Wikipedia.

[4]. Securing Virtual and Cloud Environments". In I. Ivanovo et al. Cloud Computing and Services Science, Service Science: by Mariana Carroll, Paula Kotzé, Alta van der Merwe.

[5]. Cloud Computing entry". By Net Lingo.

[6]. The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[7].Secure virtualization: benefits, risks and constraints, 1st International Conference on Cloud Computing and Services Science by M Carroll, P Kotzé, Alta van der Merwe (2011).

[8] "Addressing cloud computing security issues". Future Generation Computer Systems by Zissis, Dimitrios; Lekkas (2010).

[9]. Securing the Cloud: Cloud Computer Security Techniques and Tactics by Waltham.

[10]. Efficient Load Balancing in Cloud: A Practical Implementation by Anirban Kundu, Guanxiong Xu, Ruopeng Liu.

[11]. One Time Password Authentication for Open High Performance Computing Environments by Stephen Chan, Stephen Lau slau, Adrian Wong.

[12]. Towards Trusted Cloud Computing by Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues.

1. Shaik Fayaz, Asst,Professor, Dept. of CSE, ESWAR College of Engineering.