ISSN:2249-5789
Akhil Sharma et al, International Journal of Computer Science & Communication Networks,Vol 3(2), 69-72

Securing resource location with the help of phoenix coordinate system and host authentication in cloud environment

Akhil Sharma
Research scholar
LPU
akhilsharma90@outlook.com

Anu Kumari
Research scholar
LPU
anukumari90@outlook.com

Krishan Bansal
Lecturer
LPU
krishan.16348@lpu.co.in

Abstract

Cloud computing may be defined as a set of IT services that are provided to a client over a network with the ability to scale up or down their service requirements. Usually cloud services are delivered by a service provider who owns the infrastructure and provide services on pay and use basis. In this paper we will represent an approach to increase accuracy of virtual coordinate for secure allocation of resources in cloud environment. Also in this paper we have proposed a system through which we can overcome coordinate pollution attacks so to make resource locality easy and effective.

Keywords -Cloud computing, Phoenix, coordinate systems, IaaS, PaaS, SaaS

1. Introduction

Cloud computing may be defined as the delivery of computing services like hardware and software over the web. Cloud services allow businesses and individuals to use software and hardware that are managed by third parties at remote locations. Some of the examples of cloud services include data storage, networking sites, e-mail, and business online applications. With the help of cloud computing model we can get access to information and computer resources from anywhere where there is a network connection. Cloud service provider provides resources to user which are shared by all users. It including storage space, computer processing power, networks, and specialized corporate and user applications.

On the economic front, the main advantage of cloud computing is that customers only use what they need, and pay only for what they actually use. Resources are available to be accessible from the cloud, at any time and from anywhere via the Internet. And there is no need to care about where and how things are kept behind the scenes - you just buy the computer service you need as you would any other utility. For this reason, cloud computing has also been referred as utility computing, or "on-demand computing." This new generation of Web-based computing using remote servers housed in highly secure data centers for data storage and management, so organizations no longer need to buy and take care of their solutions internally.

The characteristics of cloud computing include the demand for self-service, spacious network access, resource sharing, rapid pliability and measured service. A self-request can made if we want to manage our own resources. Pooling of resources means that customers tap into a pool of computing resources, usually in remote data centers and these resources are basically shared. To determine location of data is due to the part security policies of different legislative domains where virtual resources can be placed and also the (often subjective) trust level of different countries. For example American companies don't want to place and process their critical data outside of America, whereas companies from European countries does want to move their critical data to the US because of patriot act [1]. Present approaches for geolocation can be divided into measurement based and semantic based geo location approaches, both often used as basis of public databases [2], [3]. However, both approaches do not work if the target relays the packets to the desired destination. In this particular case the cloud provider can move the resource to different data center in this both geolocating techniques are not able to detect the new placement of the virtual resource. To solve this problem we

propose the geolocating techniques based on virtual network coordinate systems (VCS) which uses *round trip time* (RTT) measurements to estimate geographical location.

2. Related work

2.1 Security policy assessment in cloud computing

In cloud computing it is sometime required to find in which jurisdiction the data is processed or stored because of several regulations, e.g., the European data protection law [4]. On the other hand there are regulations that enable governmental institutions in different countries to access data stored in a cloud, e.g., the USA Patriot Act [1]. In the above case we may not want to place the data in this jurisdiction. The importance of data locality is also stated in [5] and [6]. In [6] the authors propose to relocate the location of a cloud service by a third party. However, this gives only a situational view. Basescu et al. [7] propose a security management framework for cloud computing but this approach does not include the assessment whether the policies are correctly implemented or not. Iskander et al. represented in [8] a mechanism for the enforcement of authentication policies. Vimercati et al presented Policy enforcement by selective resource sharing based on selective encryption is proposed [9].

2.2 Geo locating Internet nodes

Since the Internet exists, people have been keen in finding out the geographic location behind a service provider, which is identified by an IP address. However, this mapping with a certain accuracy is not trivial. Several approaches have been developed, which can be divided into two groups: measurement based geolocation and semantic based geolocation. Latter uses sources as *whois* or DNS queries for finding a location, using *ping* or *traceroute*. Based on these techniques, several dedicated databases are available publicly. These databases are accurate and efficient on country-level, but consistency and accuracy issue remains [10]. With coming of IPv6 addresses these databases may be difficult to maintain. Padmanabhan et al.[11] proposed automated geolocating using latency delays. Youn et al. propose a more precise statistical geolocation scheme based on kernel density estimation. However, none of these systems was tested in complex network environment. Thus Vivaldi and phoenix coordinate systems are used to find location with precession and accuracy. But both of the system does not take into consideration coordinate attacks.

3. Background

Thomas et al.[12] in his paper showed how network coordinate system can be used to verify location of virtual cloud resources and to detect node movement and thus preventing policy violation. In this they evaluated three virtual network coordinate systems in regard to their performance of associating virtual cloud to geographical locations. The proposed solution highlights that VCS-based geolocation is possible even through location concealing relay nodes without the requirement of large scale measurements. Within the three selected coordination systems i.e. Vivaldi, Pharos and phoenix, Phoenix performs best, providing an accuracy of 52%.

But like other coordinate systems this system also face certain vulnerabilities which were not considered in the frame of the work. These, as such as byzantine attacks or coordinate inflation, deflation and oscillation attacks. So in this paper in the next section we will propose an approach to secure location of resources using Phoenix coordinate system and using host authentication mechanism so that resource allocation can be done in an efficient and better way and also to restrict resource allocation based upon locality.

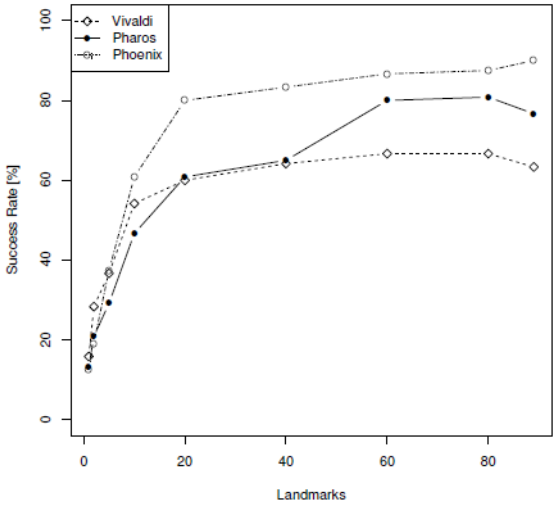

Figure 1. Phoenix success rate as compared to Vivaldi and pharos

4. Proposed System

In this section we will present the approach which can be used to set up resource location more accurately and then restricting them on the basis of locality. For this we are using Phoenix coordinate system with host authentication. For this approach there is a need of creating landmarks which will help in calculating coordinates more accurately. For this purpose we can use available locations like

universities or schools to act as landmarks to increase our accuracy.

So in this system when a new host had to be setup, firstly it will be provided with some random initial values using boot strap coordinates. Then new host will communicate with neighboring hosts around him so that he can find his own coordinates and communicate with agent host. When he will be communicate with neighbor host they will redirect its request to agent. Moreover the agent host will be broadcasting message continuously so that new host can easily trace the agent. During this process of agent finding, it will generate reference host list and finally it will be redirected to agent host. This agent will then authenticate new host by sending him a registration packet with its checksum and a secret key, which will uniquely identify our new host using MD5 one way cryptographic function. Moreover it will provide new host with reference list of authenticated hosts. And also multicast information about new host to remaining authenticated hosts. Using this mechanism of multicasting the message, the malicious node will node receive the secret key of the new host as we are sending the tagg only to registered hosts.

Now all these nodes can communicate with each other by authenticating each other with the help of secret key allocated to them which has already been shared, and new node can start NC calculation process. So in this way we can secure increase accuracy of virtual coordinates of the hosts as compared to standard phoenix coordinate system. Rest, phoenix algorithm can reduce its reference host list based upon the weight factor and we can calculate more precise coordinates of the hosts. Once the coordinates have been calculated we can create the dataset of these location and hence help in efficient resource allocation. And moreover this approach can be used to restrict resource allocation in other countries by using agents as a jurisdiction.

5. Conclusion and future work

In this paper we proposed a scheme for secure calculation of virtual coordinates using phoenix coordinate system and by authenticating hosts concept. If the reference host is not validated then we will not use it for coordinate's calculation and thus can be used for overcoming various problems such as coordinate attacks. Our future work will comprise of implementing it on a simulator and find out the efficiency of the proposed system. And moreover we will be trying to restrict resource allocation based upon the locality using the authentication mechanism.

6. References

[1] D. Fraser, "The canadian response to the USA Patriot Act," *Security Privacy, IEEE*, vol. 5, no. 5, pp. 66 –68, sept.-oct. 2007.

[2] "IP Addess Location," August 2011. [Online]. Available: http: //www.ipaddresslocation.org/

[3] "IP Addess Geolocation to Identify Website Visitor's Geographic Location," August 2011. [Online]. Available: http://www.ip2location.com/

[4] "Directive 2002/58/EC of the European Parliament and of the Council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications)," in Official Journal of the European Union, no. L201, 2002, pp. 0037–0047.

[5] ENISA, "Cloud computing security risk assessment," European Network and Information Security Agency (ENISA), Tech. Rep., 2009.

[6] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing," Gartner, Tech. Rep., 2008.

[7] C. Basescu, A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, "Managing data access on clouds: A generic framework for enforcing security policies," in *AINA*. IEEE Computer Society, 2011, pp. 459–466.

[8] M. K. Iskander, D. W. Wilkinson, A. J. Lee, and P. K. Chrysanthis, "Enforcing policy and data consistency of cloud transactions," in Proceedings of the Second International Workshop on Security and Privacy in Cloud Computing, ser. ICDCS-SPCC 2011. Washington, DC, USA: IEEE Computer Society, 2011.

[9] S. D. C. d. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, and P. Samarati, "Encryption-based policy enforcement for cloud storage," in *Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, ser. ICDCSW '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 42–51. [Online]. Available: http://dx.doi.org/10.1109/ICDCSW.2010.35

[10] I. Youn, B. L. Mark, and D. Richards, "Statistical geolocation of internet hosts," *Computer Communications and Networks, International Conference on*, vol. 0, pp. 1–6, 2009.

[11] V. N. Padmanabhan and L. Subramanian, "An investigation of geographic mapping techniques for internet hosts," in Proceedings
of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, ser. SIGCOMM '01. New York, NY, USA: ACM, 2001, pp. 173–185. [Online]. Available: http://doi.acm.org/10.1145/383059.383073

[12] E. Thomas, R. Thorsten, F. Volker, "Verification of Data Location in Cloud Networking" in 2011 Fourth IEEE International Conference on Utility and Cloud Computing

[13] D. Wu, P. Dhungel, X. Hei, *et al*., "Understanding peer exchange in Bittorrent systems," in *Proc. 2010 IEEE P2P*.

[14] T. S. E. Ng and H. Zhang, "A network positioning system for the Internet," in *Proc. 2004* USENIX *ATC*.

[15] Y. Mao, L. Saul, and J. M. Smith, "IDES: an Internet distance estimation service for large network," *IEEE J. Sel. Areas Commun.*, 200