Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

CloudNet Security: Cloud Assets by WAN using Reallocation of Virtual Machine

Nanda M, Prasanna Kumar M
Department of Computer Science and Engineering, EW Institute of Technology, Bangalore, Karnataka, India

Abstract— In Virtualization innovation and the simplicity with which virtual machines (VMs) can be moved inside of the LAN have changed the extent of asset administration from assigning assets on a solitary server to controlling pools of assets inside of a server farm. We expect WAN movement of virtual machines to in like manner change the extent of provisioning assets from a solitary server farm to various server farms spread the nation over or around the globe. In this paper, we introduce the CloudNet security engineering comprising of distributed computing stages connected with a virtual private system (VPN)- based system foundation to give consistent and secure network in the middle of big business and cloud server farm destinations. To understand our vision of effectively pooling topographically appropriated server farm assets, CloudNet gives enhanced backing to live WAN movement of virtual machines. In particular, we display an arrangement of advancements that minimize the expense of exchanging stockpiling and virtual machine memory amid movements over low transmission capacity and high-dormancy Internet joins. We assess our framework on an operational cloud stage circulated over the cloud and client framework.

Keywords— Cloud computing, virtualization, Cloud network, wide area network (WAN) migration.

I. INTRODUCTION

Today's endeavors run their server applications in information focuses, which furnish them with computational and capacity assets. Distributed computing stages, both open and private, give another street to both little and vast ventures to have their applications by leasing assets on interest and paying taking into account real use. In this way, an ordinary venture's IT administrations will be spread over the company's server farms and additionally progressively apportioned assets in cloud server farms.

From an IT point of view, it would be perfect if both in-house server farms and private and open mists could be considered as an adaptable pool of figuring and capacity assets that are consistently associated with defeat their land partition. The administration of such a pool of assets requires the capacity to adaptably outline to various locales and in addition the capacity to move applications and their information crosswise over and inside of pools. The spryness with which such choices can be made and actualized decides the responsiveness with which venture IT can meet changing business needs. Virtualization is a key technology that has enabled such agility within a data center. Hardware virtualization provides a logical separation between applications and the underlying physical server resources, thereby enabling a flexible mapping of virtual machines (VMs) to servers in a data center. Furthermore, virtual machine platforms support resizing of VIM containers to accommodate changing workloads as well as the ability to live-migrate virtual machines from one server to another without incurring application downtimes. This same flexibility is also desirable across geographically distributed data centers. Such cross-data-center management requires efficient migration of both memory and disk state between data centers, overcoming constraints imposed by the WAN connectivity between them [9]. In this paper, we propose a platform called CloudNet security to achieve the vision of seamlessly connected resource pools that permit flexible placement and live migration of applications and their data across sites.

CloudNet makes the following Contributions:1)The design and implementation of a cloud computing platform that seamlessly connects resources at multiple data center and enterprise sites.2)A centralized virtual private network (VPN) Controller architecture that automates reconfiguration of VPN endpoints; 3)A holistic view of WAN VM migration that handles persistent storage, network connections, and memory state with minimal downtime; 4)Optimizations that minimize total migration time, application downtime, and volume of data transferred. 5) A coordination system that synchronizes the migration of multitier applications.

II. RELATED WORK

CloudNet security provides a networking infrastructure for linking data centers to clouds and an optimized form of live VM migration. These two features are valuable for a variety of situations such as cloud bursting, enterprise IT consolidation, and "follow-the-sun" workloads. We have previously presented our vision for these use cases [1]; in this paper, we focus on the infrastructure required to meet these goals.

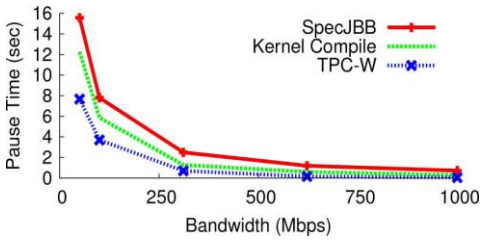

Fig. 1. Low-bandwidth links can significantly increase the downtime experienced during migration.

Fig.1 shows the downtime of VMs running several different applications, as the available bandwidth is varied (assumes shared storage and a constant 10-ms round-trip latency). This nearly 200 increase is unacceptable for most applications and illustrates the importance of optimizing VM migration algorithms to better handle low-bandwidth connections. CloudNet security coordinates the hypervisor's memory migration with a disk replication system so that the entire VM state can be transferred if needed. Current LAN-based live migration techniques must be optimized for WAN environments, and cloud computing network infrastructure must be enhanced to support dynamic relocation of resources between cloud and enterprise sites; these challenges are the primary focus of this paper.

A straightforward implementation of VM migration between IP networks results in significant network management and configuration complexity [5]. As a result, virtualizing network connectivity is key in CloudNet for achieving the task of WAN migration seamlessly relative to applications. However, reconfiguring the VPNs that CloudNet uses to provide this abstraction has typically taken a long time because of manual (or nearly manual) provisioning and configuration. CloudNet explicitly recognizes the need to set up new VPN endpoints quickly and exploits the capability of BGP route servers [6] to achieve this.

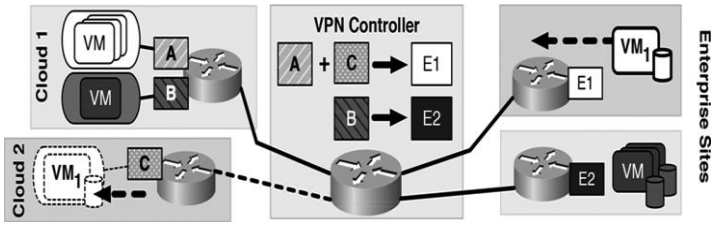

Fig. 2. VPN Controller remaps the route targets (A, B, C) advertised by each cloud datacentre to match the proper enterprise VPN (E1 or E2). To migrate VM1 to Cloud Site 2, the VPN controller redefines E1's VPN to include route target A and C, then performs the disk and memory migration.

Fig. 2 illustrates an example where is to be migrated from enterprise site E1 to Cloud Site 2. The VPN Controller must extend E1's VPLS to include route targets and, while Enterprise 2's VPLS only includes route target. Once the change is made by the VPN Controller, it is propagated to the other endpoints via BGP. This ensures that each customer's resources are isolated within their own private network, providing CloudNet's virtual cloud pool abstraction.

III. IMPLEMENTATION

Enterprise site or cloud server is a service provider it stores the user data. Cloud server got data from the client site where it holds data in cloud. Cloud site or user upload data to cloud through the WAN where it sent the data to store it in cloud. Our implementation only supports removing memory redundancy during migrations. TPA will be initiated to verify over the cloud server work by taking the message or data from the cloud server. By considering message from cloud it compared along with message that the data owner compute it in his part. After finishing the verification, the TPA will inform the user if the CS was trusted or not. After uploading file to the cloud by the data owner, Now receiver wants the data from the cloud then he needs to login by entering access information to cloud. Access information contains file name and security key. If he/she knows the correct information then only he can access the data from cloud otherwise user will be blocked by the cloud server.

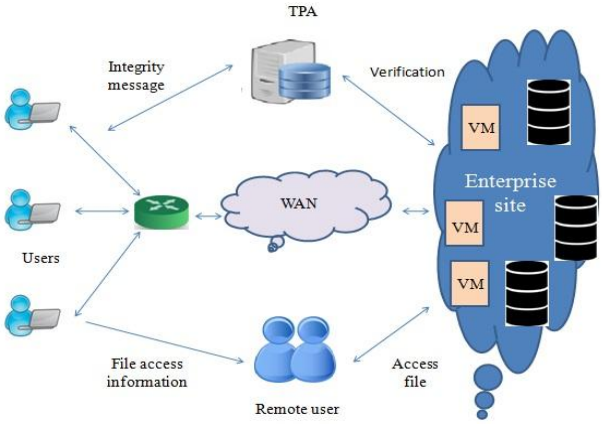

Fig. 3. CloudNet security architecture

IV. EXPERIMENTAL RESULTS

Figures shows (a) the cloud cluster consists of fire walls and peers. The cloud server is responsible for data storage and file authorization for an end user. (b) Data owner uploads their data file into the cloud server and the cloud server will connect to fire wall, the data file is stored in a normal peer and the backup file will be stored in Bootstrap peer. (c) The normal peer software consists of five components: schema mapping, data loader, data indexer, access control, and query executor. The data file will stored in normal peer with their tags such as file name, secret key, digital sign, and owner name. (d)The data consumer is nothing but the end user who will request and gets file contents response from the corresponding cloud servers and fire walls. End user should register before downloading any files from the cloud server. After registration he should login. If the file name and secret key is correct then the end user is getting the file response from the cloud or else he will be considered as an attacker and also he will be blocked in corresponding cloud and fire wall. If he wants to access the file after blocking he wants to UN block from the cloud. (e) If user is entered a wrong secrete key, then considered as an attacker. Attacker is one who is integrating the cloud file by adding malicious data to the corresponding cloud. (f) The bootstrap peer is the entry point of the whole network.

It has several responsibilities. First, the bootstrap peer serves for various administration purposes; including monitoring and managing normal peers and also scheduling various network management events. Second, the bootstrap peer acts as a central repository for metadata of corporate network applications, including shared global schema, participant normal peer list, and role definitions.

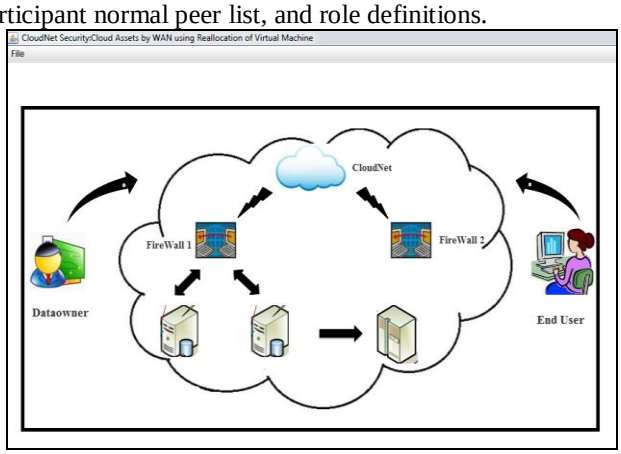

Fig. (a). CloudNet Security architecture

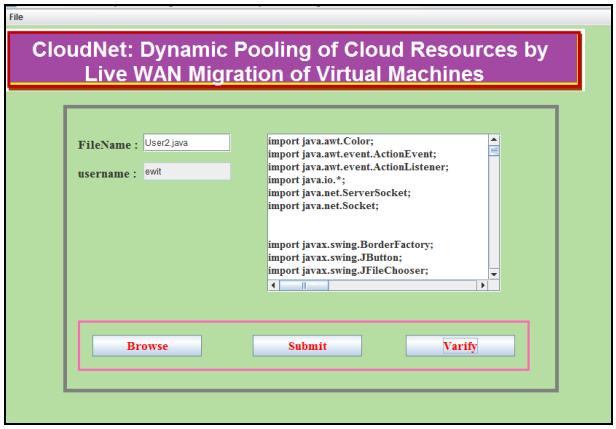

Fig. (b). Integrity check mechanism by TPA

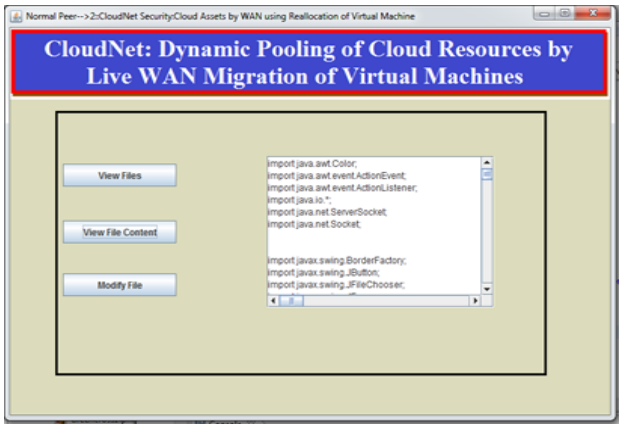

Fig. (c). Data Migration in cloud

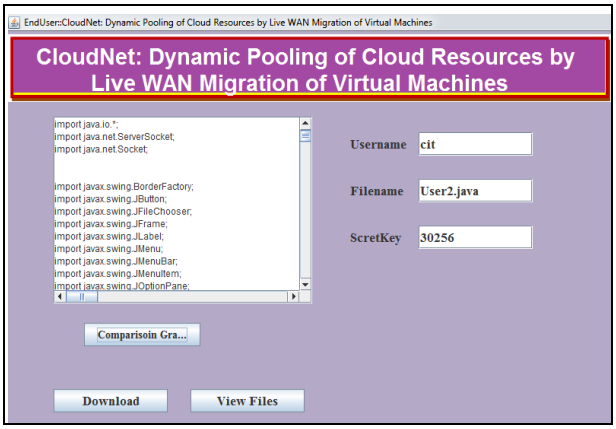

Fig. (d). Registered consumer's activity

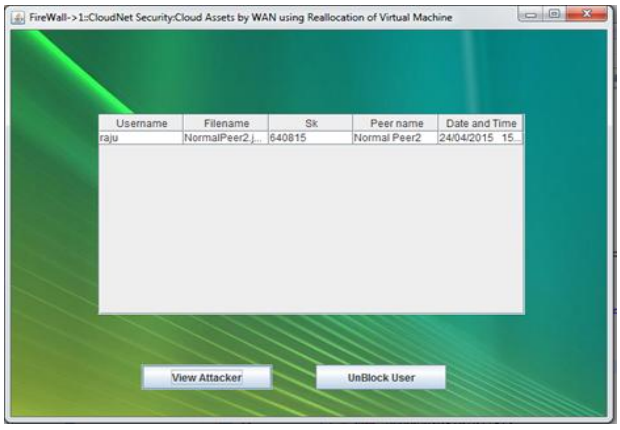

Fig. (e). Attacker detection at firewall

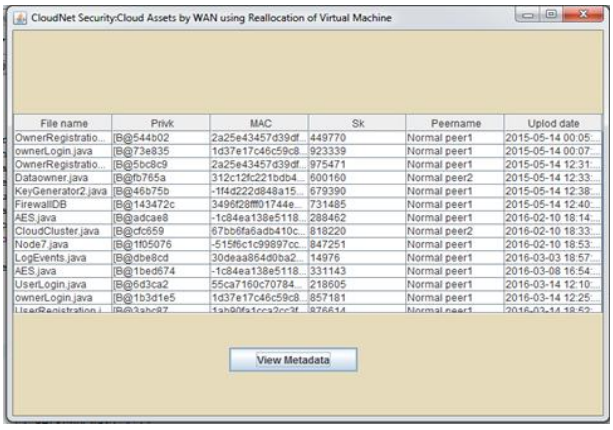

Fig. (f). Metadata information at Bootstrap peer.

V. CONCLUSION AND FUTURE SCOPE

CloudNet underpins a comprehensive perspective of WAN movement that handles persevering capacity, system associations, and memory state with negligible downtime even in low-transfer speed, high-dormancy settings. Brings down both aggregate relocation time and application-experienced downtime. Diminishing this downtime is basic for avoiding application disturbances amid WAN relocations. CloudNet security utilization of both offbeat and synchronous plate replication further minimizes the effect of WAN dormancy on application execution amid relocations. The future work includes the implementation of the algorithm that includes data integrity check mechanism between the bestpeer and the cloud service provider. This algorithm will further help in detecting the leakage of data or intrusions done by the cloud service provider itself.

ACKNOWLEDGMENT

I would like to thank to my parents, friends, Proof Readers and thanks to my respected guide for their support in every step. He always guided and motivated me to complete this research paper.

REFERENCES

[1] T. Wood, K. K. Ramakrishnan, P. Shenoy, and J. Van der Merwe, "*Enterprise-ready virtual cloud pools: Vision, opportunities, and challenges*," Oxford Comput. J., vol. 55, no. 8, pp. 995–1004, Jun. 2012.

[2] A. Anand, V. Sekar, and A. Akella, "*SmartRE: An architecture for coordinated network-wide redundancy elimination,"* Comput. Commun. Rev., vol. 39, no. 4, pp. 87–98, 2009.

[3] S. Barker, T.Wood, P. Shenoy, and R. Sitaraman, "*An empirical study of memory sharing in virtual machines,*" in Proc. USENIX Annu. Tech. Conf., Jun. 2012, p. 25.

[4] R. Bradford, E. Kotsovinos, A. Feldmann, and H. Schiöberg, "*Live wide-area migration of virtual machines including local persistent."*

[5] M. Hajjat et al., *"Cloudward bound: Planning for beneficial migration of enterprise applications to the cloud*," in Proc. SIGCOMM, 2010, pp. 243–254.

[6] Van der Merwe et al., *"Dynamic connectivity management with an intelligent route service control point*," in Proc. SIGCOMM Workshop Internet Netw. Manage., 2006, pp. 29–34.J.

[7] C. Clark et al., "*Live migration of virtual machines*," in Proc. NSDI, May 2005, pp. 273–286

[8] Cisco, San Jose, CA, USA, "*Virtual machine mobility with VMware VMotion and Cisco data center interconnect technologies,"* Sep. 2009

[9] T. Wood, A. Gerber, K. Ramakrishnan, J. Van der Merwe, and P. Shenoy, "*The case for enterprise ready virtual private clouds,"* in Proc. USENIX Hot Cloud, San Diego, CA, USA, Jun. 2009, Art. no. 4.

[10] T. Wood, K. K. Ramakrishnan, P. Shenoy, and J. Van der Merwe, "*CloudNet: Dynamic pooling of cloud resources by live WAN migration of virtual machines*," in Proc. VEE, Mar. 2011, p. 121132

[11] B. Aggarwal et al., *"EndRE: An end-system redundancy elimination service for enterprises*," in Proc. NSDI, 2010, p. 28.

[12] H. Liu, H. Jin, C.-Z. Xu, and X. Liao, "*Performance and energy modeling for live migration of virtual machines*," Cluster Comput., vol.16, no. 2, pp. 249–264, Jun. 2013.

[13] A. I. Sundararaj and P. A. Dinda, "*Towards virtual networks for virtual machine grid computing*," in Proc. 3rd VM, 2004, p. 14.

[14] A. Murphy, "*Enabling long distance live migration with F5 a VMware VMotion,"* Tech. rep., f5 Tech. Brief, 2011.

[15] R. N. Mysore et al., "*PortLand: A scalable fault-tolerant layer 2 data center network fabric*," in Proc. ACM SIGCOMM, New York, NY, USA, 2009, pp. 39–50.

[16] M. Nelson, B.-H. Lim, and G. Hutchins, "*Fast transparent migration for virtual machines*," in Proc. USENIX ATEC, 2005, p. 25.

[17] P. Riteau, C. Morin, and T. Priol, "*Shrinker: Improving live migration of virtual clusters over WANs with distributed data deduplication and content-based addressing,*" in Proc. 17th Euro-Par, 2011, vol. Part I, pp. 431–442.

[18] P. Ruth, J. Rhee, D. Xu, R. Kennell, and S. Goasguen, "*Autonomic live adaptation of virtual computational environments in a multi-domain infrastructure,"* in Proc. ICAC, 2006, pp. 5–14.

