INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS
VOL. 2, ISSUE 2, FEB. 2013 ISSN NO: 2319-7463

Integrate Military with Distributed Cloud Computing and Secure Virtualization

J. MOUNIKA REDDY[1], J. MARY MONIKA[2]

[1,2]Department of Computer Science & Engineering, Velammal Institute of Technology

[1]selectmounika@gmail.com, [2]moniejoseph@gmail.com

ABSTRACT

Cloud computing is known as a novel information technology (IT) concept, which involves facilitated and rapid access to networks, servers, data saving media, applications and services via Internet with minimum hardware requirements. Use of information systems and technologies at the battlefield is not new. Information superiority is a force multiplier and is crucial to mission success. Distributed cloud computing in the Military systems is operational today. In the near future extensive use of military clouds at the battlefield is predicted. Integrating cloud computing logic to military applications will increase the flexibility, cost-effectiveness, efficiency and accessibility capabilities. In this paper, distributed cloud computing concepts are defined. Cloud computing supported battlefield applications are analyzed. The effects of cloud computing systems on the information domain in future warfare are discussed. Battlefield opportunities and novelties which might be introduced by distributed cloud computing systems are researched. The role of military clouds in future warfare is proposed in this paper. It was concluded that military clouds will be indispensible components of the future battlefield. Military clouds have the potential of increasing situational awareness at the battlefield and facilitating the settlement of information superiority.

KEYWORDS: cloud computing, virtualization, military, IT.

INTRODUCTION

Distributed computing in cloud Examples: Distributed computing is nothing more than utilizing many networked computers to partition (split it into many smaller pieces) a question or problem and allow the network to solve the issue piecemeal.

Distributed Cloud Computing is more secure - Because all data are not in the same place, it is really difficult, I would say nearly impossible to lose your Data. Even if you lose from time to time a small amount of Data, it won't be too damageable.

Distributed Cloud Computing needs less network capacity - If Internet was managed on a distributed cloud, the information will be spread everywhere and will be more likely to be close from where we are accessing it. The distributed cloud will take a look at where is the closest server which can provide us with the information. Then we won't have to access a server on the other side of the world.

Distributed Cloud Computing don't need Air Conditioning - Because there is only one or two computers in the same place, we don't have to cool them. Their impact on the ambient temperature is negligible.

Distributed Cloud Computing will require less electricity - Because the server will be closer from the access point, because we don't need air conditioning, because we use less replication, we already saved a lot of energy. But we can even go further. On a completely distributed Internet, we can imagine a smart grid. A grid which will take into account the electricity demand of where is located the server to decide if it should use it now or not. For example during the evening, when everyone is using the electricity, the servers won't be used, but early the morning, or during the day when the electricity is cheap and the demand is low, the servers will be used.

It seems to me that Distributed Cloud Computing is the solution to optimize the use of resources and therefore the impact of Internet and of the information technology on the environment. It is time to think differently and to innovate to create an environment-friendly internet[1]. Distributed computing on cloud is nothing but next generation framework to utilize the maximum value of resources over distributed architecture.

EXISTING SYSTEM

The Global Positioning System for Military Users: Current Modernization Plans and Alternatives

As the Department of Defense's (DoD's) Global Positioning System (GPS) satellites reach the end of their service lives, the department plans to replace them with ones that can counter deliberate interference by generating stronger signals. Analysis by the Congressional Budget Office (CBO) indicates that an alternative approach—namely, improving military receivers to retain the GPS signal even in the presence of such jamming—would be less expensive than DoD's plan for upgrading its constellation of GPS satellites. Furthermore, the alternative would yield benefits almost a decade earlier than DoD's plan. However, the improvements to military receivers could make them larger and heavier (and thereby less useful to personnel operating on foot) until they could incorporate the substantial gains that have been achieved in miniaturization in other applications.

DoD's Plan

The GPS uses a constellation of at least 24 satellites, each of which transmits precise data on the time and its location. Receivers—both military and civilian—use the data transmitted by the satellites to calculate their own position; information from a minimum of 4 satellites is required to determine a position accurately in three dimensions. Since 1995 (when GPS became fully operational), the U.S. military has come to rely on it to precisely locate both enemy and friendly forces. However, because the GPS signal from space is very weak by the time it reaches Earth (like the light from a 25-watt lightbulb shining 12,500 miles away), the system can easily be swamped by interference**.**

In 2000, DoD initiated plans to reduce the system's susceptibility to intentional interference. As a first step toward providing some protection against jamming, DoD decided that GPS satellites would transmit additional signals, available only to military users, each of which covered a wider range of frequencies than those already being transmitted. Those signals, called M-code signals, are more difficult for enemy jammers to overwhelm and can improve the ability of military receivers to operate in the presence of jammers. Ten satellites capable of transmitting M-code signals were already in orbit as of August 2011.

To maintain the constellation as existing and new satellites reach the end of their service lives, DoD plans to launch a total of 50 satellites through 2030 at an average rate of 2 to 3 satellites each year starting in 2012. The department has already purchased—but not yet launched—10 of those GPS satellites capable of transmitting M-code signals. DoD plans to acquire 40 more satellites—known as GPS III—that are capable of transmitting stronger M-code signals than existing satellites over the next 10 to 15 years.

DoD’s plans to develop and purchase the new satellites in three phases. In the first phase, DoD plans to acquire 8 GPS IIIA satellites capable of emitting M-code signals that are three times stronger than those transmitted by current GPS satellites. The first IIIA satellite is scheduled to be launched in 2014. In the second phase, DoD plans to acquire 16 GPS IIIB satellites with M-code signals that are five times stronger than those of current satellites. For the final phase, the department's plan calls for an initial purchase of 8 GPS IIIC satellites, which will be equipped with a special antenna capable of focusing the M-code signals in a "spotbeam"; however, CBO assumes that the department would need to purchase an additional 8 IIIC satellites in order to have enough IIIC satellites in orbit to take advantage of the IIIC's advanced capabilities. Those satellites will transmit signals with the same strength as IIIB satellites and will be able to use the spotbeam to illuminate an area with a diameter of 600 miles on the Earth's surface with signals 100 times stronger than those of current GPS satellites. In addition, IIIC satellites will be equipped with high-speed cross-links, which will allow continuous data updates. As a result, those satellites will be able to provide more accurate data to receivers, enabling a user's location to be determined within 6 inches, instead of 10 feet (using current satellites) or 3 feet (using IIIA and IIIB models). After the 16th IIIC satellite is launched in 2030, the entire constellation should be composed of GPS III satellites, 16 of which will be IIICs.

Over the next 15 years, DoD also plans to develop software to control the M-code signals and the new GPS III satellites and to develop and purchase receivers that are capable of processing the M-code signals. Although 10 satellites capable of transmitting the harder-to-jam M-code signals are currently in orbit (the first one since 2005), no users have been able to benefit from them because DoD does not have the ability to monitor or control the signals, nor has it fielded receivers to process the signals. DoD plans to have a new control system fully in place by the end of 2016. To make the entire planned system functional, however, additional control capabilities, such as being able to update satellite data transmissions continuously when IIIC satellites enter the constellation and to control their spotbeam antenna, will need to be developed. Moreover, to make the planned system useful, M-code-capable receivers will need to be fielded as well. DoD's current plan envisions fielding the first such receivers in 2017, but because the various armed services now field more than 400,000 GPS receivers, it may be 2030 before all units are fully equipped.

If the satellites and receivers perform as planned, the combination of all of the upgrades proposed by DoD would enable military receivers to operate in the presence of much stronger jamming signals than they can withstand today. For example, the effective range of a 10-watt jammer trying to cause a military receiver within the spotbeam of a GPS IIIC satellite to lose the GPS signal would be reduced by 96 percent, shrinking from 55 miles to about 2 miles.

Although the planned upgrades to GPS satellites will not increase the strength of civilian signals and will not improve the performance of civilian receivers in the presence of interference, other planned improvements will benefit both military and civilian users. In particular, GPS IIIA satellites will transmit signals that will enable both types of users to determine their position to within 3 feet, compared with the 10 feet that is possible with signals from current satellites. And once enough IIIC satellites enter the constellation, positioning within 6 inches will be possible for all users, according to DoD.

CBO estimates that it will cost DoD roughly $22 billion from 2012 to 2025 to modernize the GPS. That total would include the cost from 2012 onward to develop and purchase the 40 GPS III satellites (including $3.6 billion for the additional 8 IIIC satellites), to develop the software and capability needed to control those satellites and their transmissions, and to develop and purchase hundreds of thousands of military receivers capable of receiving and interpreting the M-code signals.

The Government Accountability Office and the Defense Science Board have reviewed DoD's plan to modernize the GPS and raised several concerns, particularly regarding the plan's focus on improving the satellites rather than the receivers and the plan's lack of coordination in terms of the timing for various capabilities. CBO has developed options by which it explores those concerns.[2][3][4][5]

DRAWBACKS

- The GPS signal from space is very weak by the time it reaches Earth the system can easily be swamped by interference.
- CBO estimates that it will cost DoD roughly $22 billion from 2012 to 2025 to modernize the GPS.

PROPOSED WORK

Can sensitive data for tactical military environments be protected in the cloud?

When storing, accessing, and disseminating military data in the cloud, top concerns include security, data reliability and redundancy, and data location. The good news is that these can be delivered when secure virtualization pairs with a distributed cloud computing scenario.

While the promise of cloud computing, with its lower costs and improved access through utility computing and storage, is very attractive, it is currently difficult to achieve for users with highly sensitive data.

A natural way to further this approach is through some form of non-public cloud. A cloud approach – whether private, community, or a hybrid – would provide a host of benefits, including significant cost savings and increased agility for military organizations. Yet there are multiple challenges to deploying these kinds of tactical solutions today using current cloud technologies. However, a distributed computing approach to secure virtualization provides a viable solution to concerns surrounding data's security, reliability, and location within a cloud computing environment for the military.

Security in the cloud

Security remains the greatest concern about using the cloud, even for private and community clouds. Questions being raised include:

- If all our key data is in the cloud, won't it be a more tempting, target-rich environment for hackers?
- With key data in the cloud, what happens if the cloud environment is impacted by a natural or manmade disaster?
- How can we take advantage of the cost savings of the cloud while still maintaining the separation needed between data classifications: unclassified, secret, and top secret?

The good news is that through a creative combination of highly secure virtualization and distributed computing, technologies are already available to address these concerns.

While all data may be "in the cloud," it doesn't mean it needs to be kept in one location, either physical or virtual. One way to lower the attack footprint of a private cloud is to use a distributed computing approach. With a distributed approach, multiple physical data centers make up the cloud and data is spread among the servers at various locations**.** Data isn't replicated on each server, but rather shards, or pieces of each database, are spread across the servers as designated by redundancy and location policies created by the administrator. Because the data is not all in one location, it's more difficult for an unauthorized person to acquire meaningful data. For example, a database of key targets might be sharded so that the ID of a target is on a server at site A, the location of the target is on a server at site B, and the people associated with a target are on a server at site C.

Because each shard of data is in multiple locations as defined by the redundancy policy, if a site experiences a catastrophic failure, no data will be lost and users will be able to access data from nodes at other sites. With a distributed data approach, even if a cloud data center is attacked and all data is lost at that location, the system knows where all the replicas of each shard of data are located and the system continues to operate without that data center. The system also recognizes that additional replicas of the shards that were stored at that data center must be created to adhere to the redundancy policy. As an example, the target data entered by the warfighter may have been stored in a nearby cloud server, or node. If that node was destroyed shortly thereafter, the target data would not be lost, as replicas were created and stored on multiple servers immediately after the data were entered.

While distributed computing improves security for cloud-based data, an extra- secure_virtualization technology is required to fully realize the cost savings of cloud computing and the ability to host multiple networks on a single system. Secure software virtualization was created to address the needs of tactical military systems that require information and applications operating at different security levels to securely coexist on a single hardware platform. This removes the need for the costly deployment of multiple computer systems to facilitate communications and information from different forces or different intelligence levels in the battlefield.

Virtualization has become a major enabling technology for moving to the cloud by allowing multiple applications to co-reside on a single server platform and efficiently serve different types of data and applications to clients that connect to it. Size, Weight, Power, and Cost (SWaP-C) are usually improved with virtualized systems, which can be critical in field deployments. However, in a typical virtualized system, much of the virtualization of memory and devices is held in the same hypervisor code; hence, any breach of that code gives access to all of the memory and devices on that physical system.[6]

CLOUD A PAPA
ViFiB

CONCLUSION

Virtualization and distributed cloud computing allow computer users access to powerful computers and software applications hosted by remote groups of servers, but security concerns related to data privacy are limiting public confidence -- and slowing adoption of the new technology. Now researchers from North Carolina State University have developed new techniques and software that may be the key to resolving those security concerns and boosting confidence in the sector.

Virtualization allows the pooling of the computational power and storage of multiple computers, which can then be shared by multiple users. For example, under the cloud computing paradigm, businesses can lease computer resources from a data center to operate Web sites and interact with customers -- without having to pay for the overhead of buying and maintaining their own IT infrastructures. The virtualization manager, commonly referred to as a "hypervisor," is a type of software that creates "virtual machines" that operate in isolation from one another on a common computer. In other words, the hypervisor allows different operating systems to run in isolation from one another -- even though each of these systems is using computing power and storage capability on the same computer. This is the technique that enables concepts like distributed cloud computing to function.

One of the major threats to virtualization -- and distributed cloud computing -- is malicious software that enables computer viruses or other malware that have compromised one customer's system to spread to the underlying hypervisor and, ultimately, to the systems of other customers. In short, a key concern is that one cloud computing customer could download a virus -- such as one that steals user data -- and then spread that virus to the systems of all the other customers.

"If this sort of attack is feasible, it undermines consumer confidence in cloud computing,", "since consumers couldn't trust that their information would remain confidential."

But Jiang and his Ph.D. student Zhi Wang have now developed a software called Hypersafe that leverages existing hardware features to secure hypervisors against such attacks. "We can guarantee the integrity of the underlying hypervisor by protecting it from being compromised by any malware downloaded by an individual user," Jiang says. "By doing so, we can ensure the hypervisor's isolation."

For malware to affect a hypervisor, it typically needs to run its own code in the hypervisor. HyperSafe utilizes two components to prevent that from happening. First, the HyperSafe program "has a technique called non-bypassable memory lockdown, which explicitly and reliably bars the introduction of new code by anyone other than the hypervisor administrator," Jiang says. "This also prevents attempts to modify existing hypervisor code by external users."

Second, HyperSafe uses a technique called restricted pointer indexing. This technique "initially characterizes a hypervisor's normal behavior, and then prevents any deviation from that profile," Jiang says. "Only the hypervisor administrators themselves can introduce changes to the hypervisor code."

The research was funded by the U.S. Army Research Office and the National Science Foundation. [7]

REFERENCES

[1]. www.freecloudalliance.org/news

[2]. Georg Zur Bonsen, Daniel Ammann, Michael Ammann, Etienne Favey, Pascal Flammant, "Continuous Navigation Combining GPS with Sensor-Based Dead Reckoning", GPS World, Archived from the original on Nov., 2006.

[3]. "NAVSTAR GPS User Equipment Introduction", United States Government. (http://www. navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf.Chapter7).

[4]."GPS Support Notes", 19 January 2007, archived from the original on 27 March 2009. (http://web.archive.org/web/20090327051208/http://www.navmanwireless.com/uploads/EK/C8/EKC8zb1ITsNwDqWcqLQxiQ/Support_Notes_GPS_OperatingParameters.pdf. Retrieved 10 November, 2008).

[5]. "XM982 Excalibur Precision Guided Extended Range Artillery Projectile". "GlobalSecurity.org". May, 2007. (http://www.globalsecurity.org/military/systems/munitions/m982-155.htm). Retrieved Sept., 2007.

[6]. http://meraki.com/press-releases/2010/05/26/meraki-expands-international-presence-by-partnering-with-uk-based-cloud-distribution.

[7]. www.sciencedaily.com/releases.