DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5041

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

OVERCOMING ISSUES OF THE CLOUD STORAGE SECURITY USING VIRTUALIZING RAM AND SERVER SIDE FLASH MEMORY

Vijyendra Karpatne
Dept. of Computer Science
Karpagam Academy of Higher Education
Coimbatore, India

Dr. E.J.Thomson Fredrik
Dept. of Computer Science
Karpagam Academy of Higher Education
Coimbatore, India

Abstract: Despite many advances made to the cloud environment, Data storage in Cloud Computing continuously faces information security issues. These challenges, though few and concentrated, impact the growth of cloud computing in the business industry as many strive to hold onto their data in house for as long as possible. The security issues in storage are marked as one of the biggest challenge because movement of data without any loss or attack is never simple in cloud. This paper analyses various challenges in Cloud storage security. Virtualizing RAM technique and server side flash memory is proposed to overcome the challenges of cloud storage security. The proposed Virtualizing RAM technique will help in several manners as using a very large amount of memory to improve, performance, utilization of Cloud storage data. The results of implementing Virtualizing RAM technique and server side flash memory shows that data security of cloud storage is enhanced and cloud storage memory is used efficiently.

Keywords: Cloud Environment; Cloud Services; Cloud-based Service Provider

1. INTRODUCTION

Each year, as cloud computing continues to grow within the business industry, IT security departments are asked what is the number one security issue facing top companies using cloud computing and data security, what can be done to resolve the issue. It is essential for a company's success to ensure the safeguarding of their customer's data, internal documentation, trade secrets, and company processes. Because of the many benefits of cloud computing, including its flexibility, accessibility, and capacity to retain data storage, this technology has become a mainstay for many technology dependent companies today moving away from traditional online competing. However, cloud computing is not without its own set of data security vulnerabilities buildings, similar to traditional storage data sharing capabilities over the years. As cloud computing continues to grow moment turn over the business industry, security risks grow and data security experts are necessary to produce security solutions. It is essential for companies to protect their most valuable digital assets despite the security issues in today's digital world. Security experts are entrusted to provide these data security solutions and services to the business industry [1].

2.LITERATURE REVIEW

In [2], Ouedraogo *et al*, 2015 revealed that although initiatives such as SLA and virtual machines monitoring, and recent development in encryption mechanisms, have contributed to addressing some of the salient issues of security and privacy in the cloud, larger initiatives, other than standards, aiming at enabling security transparency and a mutual auditability in the cloud remain to be seen. Given the current reluctance of some major businesses to embrace the trend, owing mainly to the devolution of some of the security aspects to a third party, the authors argue that undertaking some initiatives in that direction is a key to sustaining the current momentum of the cloud.

In [3], the authors provided related solutions by discussing a number of desiderata for establishing a better security transparency between a Cloud Service Provider (CSP) and a Cloud Service Consumer (CSC). M2 Press wire, a news communication outlet based in the UK, published an article explaining how nearly 100 percent of business cloud applications lack enterprise grade security and compliance features. The news outlet shared how there is a lack of effective or comprehensive security solutions to provide granular visibility and control over cloud apps and to meet new cloud security regulations to qualify as enterprise-grade services for businesses in the EU. This gap in provider service is causing organizations from doing business in the cloud until cloud application security and compliance standards are applied.

In [4], Pragaladan and Sathappan,2016 provided insight and suggestions on how cloud-based service providers can act to ensure high confidentiality and security in cloud business data storage transactions. The authors completed a research study in how the cloud-based transactional services presently cause the major problem on the confidentiality and integrity regulations as cloud software components are not developed for a different form of transactional process. This process concerns businesses as it does not support the confidentiality ideas of many k-anonymity real world applications.

In [5], PR Newswire, a news communication outlet based in California, published an article detailing the 'Treacherous Twelve' cloud computing top threats in 2016 released by the Cloud Security Alliance. This article covers the Cloud Security Alliance (CSA) Top Threats Working Group's new research report, developed to serve as an up-to-date guide to help cloud users and providers make informed decisions about risk mitigation within a cloud strategy. In creating "The Treacherous 12: Cloud Computing Top Threats in 2016," the CSA Top Threats Working Group conducted research in two primary stages: 1) the group presented 20 concerns via a series of consultations, asking working group members to indicate the importance of each concern to their organization, and 2) after considering all the survey results, the working group identified and ranked the top 12 most salient cloud security concerns from among the previously short-listed group of concerns. Per the report, 270 respondents participated in the survey process and identified the following security issues in cloud computing.

In [6], the MENA Report, a trade journal published by Intel Corp based in London, released an article directed towards the United States as a new global report from The State of Cloud Adoption revealed a critical need for improved trust to advance cloud adoption by world governments, businesses, and consumers. Per the report, with a majority (77 percent) of participants noting that their organizations trust cloud computing more than a year ago, only 13 percent completely trust public cloud providers to secure sensitive data.

3.CHALLENGES OF CLOUD STORAGE SECURITY

To handle the storage and usage of memory efficiently

How the large amount of data will be processed and handled? How the performance can be increased and how the applications can be used to take advantage of a very large amount of memory to improve.

To reduce security risks in cloud-service adoption.

Each technical layer, including applications, systems, and data, has a different threshold requirement for security. Depending on the type of data, for example web information, social releases, regulatory documentation, or mission-critical applications, the necessary security concern and measures will likely differ. It is essential for companies to determine whether or not the data in question is suitable for a cloud environment.

Issues from cloud-based service provider

It is important for the company to investigate the potential service provider before entering into any new service agreements internally and with the provider. With the rise of popularity regarding the cloud computing industry, many new cloud-based service providers have entered the source pool but may not have enough experience or knowledge to accommodate many companies they market their services to.

Cloud Data Protection

Cloud computing has existed since the Internet was created. Companies have used computers, email, websites, and remote virtual private networks within the last decade. Connection between a company and their partners and customers to exchange data is a form of cloud computing. The difference today is the use of cloud-based service providers who now allow more remote access to users and devices than in recent history. Due to this new advancement, technology network complexity has expanded, requiring stronger levels of security measures and controls in place than before. The traditional measures of security, designed to protect single facilities and internal equipment with defined security parameters and minimal entry points to access company data, do not cross the company's threshold to protect the data stored within the cloud environment.

Lack of Knowledge in Cloud Security Environment

Cloud computing has become a general term and idea, where employees with basic information technology knowledge can relate the terminology to specific company data structures such as Amazon, Apple's iTunes, or Google Drive. This generalized understanding assists employees in processing the basic concepts; however, this basic theory is not enough to ensure a company's success. A company must understand what the cloud environment encompasses, what security measures are lacking, and how to determine the best approach for their data storage and remote connectivity.

Mistrust of companies regarding cloud security

Companies thrive by the safety, confidentiality, availability, and integrity of the data they store to serve their customers. Often times, the larger the company, the greater is the concern to secure the data. As covered by the media, large companies including Target, Wells Fargo, Sony, and others have lost profits, reputation, and favor among their customer base as data intrusion occurs and private information is stolen. Many companies who have less knowledge of IT security are likely to blame the cloud environment if they do not have the sole control over security protection measures.

4.PROPOSED SOLUTION

To overcome the security issues in cloud storage, the virtualizing RAM & server-side flash memory can be used. This technique will help in improving the performance of the system and will help to accomplish the smooth transition of application/organization to cloud. This technique can be so effective for storage in cloud as the host machine dumps its entire memory into a file. This helps to increase memory usage efficiency and it also helps to enable new use cases. Nodes on the server side are getting connected to the memory pool to contribute memory. They also store and retrieve data. The memory pool can be accessed at application level and operating system level. The API is an agent through which the pool is accessed to create a shared memory cache at an application level. At operating system level, a page cache can utilize a pool as a very large memory resource.

In-order-to implement the idea on virtualizing RAM, we may need to make sure that the hardware is capable of supporting virtualization. The idea is to provide software based virtualization solution which will allow a system to function as multiple virtual system. In independent partition, multiple apps & operating system can be run.

After installing the host operating system, the virtual machines can be added. Addition of virtual machines can be accomplished using server manager tool. The action list and the virtual machine’s list appears for the host machine and each virtual machine. Actions like connect, save, shut down, turn off, settings will be available for users.

Selection of a manager is an important factor for implementing the virtualizing technique. Reliable server manager tool with server virtualization software which are easily available in the market, can be used.

Once the server manager tool is installed, the wizard can be launched by selecting File option and the virtual machine can be created. The amount of RAM will be recommended by virtual machine. Once the process has been completed, the virtual machine will appear in your console. Virtualization of RAM will be achieved. More virtual machine can be created but the most important factor to keep in mind is amount of RAM.

The implementation of server side flash is easy because it is used as a high speed cache and it can be confined to the server it's installed. Upon installation of flashing software, it starts interacting with input and output at various levels e.g. OS level, File level. The server side flash technique increases compatibility of PCIe. It means at the lower cost the possibility of innovation is more.

Security risks about the data flowing in cloud environment are the concerns and while migration the app/org to the cloud, this problem can be addressed and solved easily. The data which are migrated to cloud are definitely considered very critical and the securing those data and delivering to cloud without any damage is really a big challenge. But the flashing technique will be helping to resolve this problem to some extent. The server side flash memory can allow the proper file permission to the specific files where the data are stored. Before we do that, we need to have policy in place. Once we have policy in place, the secure network can be ensured while data migration into cloud. The administrators can provide the necessary permissions to the for transferring the large amount of data. Moreover, the encryption can be implemented on data which are getting transferred in cloud. This will give more comfort to the provider to handle the data being migrated to the cloud.

As we all know great economic benefits are offered by the cloud service providers but they may end up in position to significant potential risk in keeping safe the organization data. So its very important to understand and make decisions about where and when to use cloud solutions. To gain confidence, the issues can be forecasted and outlined before the cloud service provide is opted or any kind of agreement is signed for apps/org migration in cloud. Every organization should have the understanding about the provider and respond and evaluate every question or requirement to ensure its valid for their needs. To have the perfect understanding between the organization and the service provider it is required to consider all the point about security risk. Few of the areas which are very important to consider related to data security.

Service provider should be able to ensure that they are good to enforce administrative delegation if needed. The organizations should be accountable for their data and should agree to go for audit when their data are live in public cloud. Organizations are required to know about the data center where the service provider will have the storage. In-fact the public cloud works under shared environment so its very important to ensure segregation of data. Enterprise must have agreement with providers and ensure that provider has ability for data recovery. Business continuity should also be main concern which can be agreed upon.

While moving the apps/org in cloud the RAM virtualization helps in lots of ways to protect the data in cloud. Organizations can believe the service provider who uses this RAM virtualization to handle the data during migration. But it is a responsibility of an organization to make sure that the data which they are handing over to the cloud service provider, will be safe and protected by all means. The points which are generally overlooked and ignored by service providers and organization are to be covered properly. When RAM Virtualization takes place, it should be made sure that the sensitive data are not available within the Virtual memory.

Some of the VMs are not used for a longer time and becomes dormant. Organizations need to take necessary agree mental decisions to protect themselves. There are more risks which should be considered which can cause during RAM Virtualization or after the process ends. All factors should be considered well.

When the organization/application are moved or migrated to cloud, the virtual network is being used. While writing the agreement, org must ensure that the service providers have the complete visibility on the virtual networks too in order to protect their data in cloud. The cloud service provider's API is something organization must know about. There should not be any risk on the org data due the API being used by the cloud service provider.

The great restrictions are the delimitation of threshold. The organization must understand that to what extent the service provider can provide the service based on the agreement signed. It is very important to understand the level of security needed on organization data versus the level of security signed on the agreement. While moving the apps or organization to cloud the protection of data are most important as these will ensure the continuity of business. Nowadays it is common for cloud service provider to offer the remote connectivity to their clients. It can be added as a benchmark to the service and can attract number of clients. But the organizations or clients must ensure that the same amount of security measures are applied on the data when it is being moved to cloud or exchanged.

Risk calculation and expansion of responsive measures can work in succession to prevent or moderate data security breaches. Rather than waiting for a crack to happen, organizations can identify weak spots in their existing systems, and develop preventive measures. Most significantly, organizations and cloud service provider both should establish comprehensive data-detailed security policies, and create a security-conscious labor force, through training and periodic reminders. Companies may also invest in new data security technologies to stay ahead of ever-evolving security threats.

Although memory flash technique and RAM Virtualization are extremely useful and secure while transferring data in cloud, they do come with security risks. Organizations & cloud providers using this technique while migrating the data into the corporate network is a security concern for organization approval. But with all the news about malware and data breaches, surely organization realize that memory flash device can be infected and will be careful before plugging them into the corporate network.

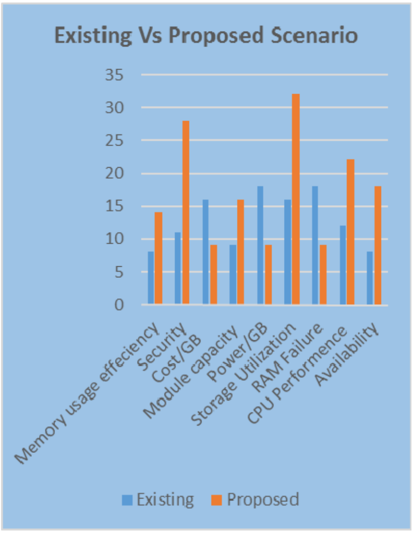
Organizations should ensure that provider's system using memory flash are checked for malware before they are connected to the cloud or corporate network. This can be accomplished by deploying a malware scanning kiosk or station where devices are thoroughly scanned for any malware before they can be connected to the corporate network.

In addition to malware scanning, limits can be set on allowed memory flash devices and file types based on the user’s role at the organization. For instance, if an organization has no need to use executable files, these types of files should be blocked. To avoid file types being hoaxed and getting past filters, it is also important to perform file type verification. In addition, since data in cloud network are commonly used as attack paths, it is advisable to sanitize files or data and remove any possible embedded scripts. In this way unknown threats, such as zero-day threats and targeted threats, can be prevented.

In order to avoid implementing memory flash directly to the cloud network, the security system can securely transfer the allowed files from the drive to a corporate portal from where the user can download the files. This removes the need to have memory flash drives connected directly to the network, eliminating the risk of booby-trapped. Metadefender product can be used to scan devices quickly and reliably by utilizing multiple, built-in anti-malware engines (up to 30 engines) that work simultaneously to detect malicious code. Metadefender can further bolster memory security by applying user-based file policies, verifying file types and sanitizing files. In addition, secure file transfer can be used to transfer allowed files and avoid the need for additional drives to be plugged into the corporate network. Cloud service provider must ensure and give confidence to the organizations about the data security threat while implementing the memory flash.

5. RESULTS AND DISCUSSION

We observed that it was more difficult for potential cloud users as lack of resources/expertise and security took the places for the challenges in cloud. RAM virtualization and flashing memory technique help to drive to use the memory efficiently and to make the data more secure. The cost which is considered as evergreen challenge is getting reduced, when we implement the virtualization and flashing technique on a large scale. During implementation, we observed that the capacity of each module increases drastically, even though the large amount of data is handled when virtualization is implemented. The below two graphs clearly show that the raise or downfall in terms of point value between the existing situation and the situation which we observed after simulating the virtualization and flashing memory.



The usage of power can be lowered down by implementing the virtualization and flashing technique. The above graphs comparison shows the huge downfall in usage in power. This helps organization to save more money. The storage capacity drastically increases when virtualization is implemented. There is no doubt about it and it has been proven that storage capacity and security increases for about 50%. There have been circumstances where we have experienced the problems in cloud because of RAM failure. In these scenario there has be no protection on data while moving the application or org to cloud. Virtualization helps to decrease the possibility of RAM failure and ensures the data protection. While migration of apps or organization in cloud, we must have an availability of storage which can be used while migration. The virtualization helps to increase the availability drastically and ensures the smoother migration.

6. CONCLUSION

Companies desire a technology that is flexible, adaptable, and evolving with an exit door available should a better technology solution be developed. The cloud is not a one type of functionality that has to be decommissioned if requirement changes are needed. Though the cloud has been existed as a piece of the IT scope over the last 15 years, the use of cloud storage and cloud-based service providers by the business industry is still new. Since the creation of computers, we have seen external forces find new ways to crack systems and exploit data which puts off many smaller businesses from taking the leap into the cloud environment. The fears are rooted in the mystery of the cloud environment, how it functions, processes, and enforces security measures. Companies, who have an IT staff which understands the cloud environment, where the benefits outweigh the risks, are more likely to embrace the technology, finding it practical and cost-effective. The usage of virtualizing RAM technique and server side flash memory in cloud computing storage is enhancing that data security of cloud storage and improves the efficient usage of cloud storage memory.

REFERENCES

1. Lord N (2017) 27 Data Security Experts Reveal The #1 Information Security Issue Most Companies Face With Cloud Computing & Storage. Accessed 1st June, 2017 from https://digitalguardian.com/blog/27-data-security-experts-reveal-1-information-security-issue-most-companies-face-cloud
2. Ouedraogo M, Mignon S, Cholez H, Furnell S, Dubois, E (2015) Security transparency: The next frontier for security research in the cloud. J Cloud Computing 4(1): 1-14
3. M2 Presswire (2016) Nearly 100 percent of business cloud applications lack enterprise grade security and compliance features, according to blue coat elastica shadow data threat report. Coventry
4. Pragaladan R, Sathappan S (2016) A Survival Study on Confidentiality and Security in Cloud Business Data Storage Transaction. IJ Comp Sci Info Sec 14(10):34–39, Pittsburg
5. PR Newswire (2016) Cloud Security Alliance Releases 'The Treacherous Twelve' Cloud Computing Top Threats in 2016. PR Newswire US.
6. MENA Report (2016) United States : New report reveals critical need for improved trust to advance cloud adoption. London.