Augment secrecy in Cloud computing using Biometric encryption

Rajashekar M.B
Asst Prof in Dept of CS&E
CIT Engg college
Ponnampet, India.

Sangana Kottireddy
Asst Prof in Dept of IS&E
CIT Engg college
Ponnampet,India.

Vindhya K.V
Student of IS&E
CIT Engg college.
Ponnampet,India.

Rashmi R
Student of IS&E
CIT Engg college.
Ponnampet,India.

***Abstract*-The core technologies used in cloud computing is Virtualization. It has also been used to present dynamic resource allocation and service provisioning, particularly in IaaS Cloud environment. Consequently virtualization makes it possible for cloud computing to offer both hardware and software services to the users on demand. In fact, there are several reasons for the companies to migrate towards cloud computing such as processor capabilities, bus speed, storage size, memory and managed to reduce the cost of committed servers. Nevertheless, virtualization and cloud computing contain many security issues that make a difference to the biometric information privacy in the cloud computing. The different security issues are virtual machine ware escape, mobility, diversity monitoring and many more. In addition to this the secrecy of a particular user is an issue in biometric data. Therefore, in this paper we propose biometric encryption to improve the privacy in cloud computing for biometric data. Also, we discuss about the virtualization for cloud computing. Without a doubt, in this paper we overview the security issues of cloud computing.**

Keywords-Biometric Encryption, Virtualization, Cloud computing.

I. INTRODUCTION

Cloud computing is definitely not a new technology; instead it is one of a new way of delivering computing resources and services. The Cloud computing development has introduced new changes and opportunities to the evolving IT industry. Dynamically allocating scalable resources to multiple users is the general purpose of Cloud computing. Users of the cloud can obtain on-demand basis cloud services and acquire it globally. It also gives measured services , that is customers pay for only that they use [1]. In addition, it also offers an effective way of reducing IT expenses, Capital Expenditures (CapEx), and Operational Expenditure (OpEx), [1, 2], hence it provides economic benefits to both customers and organizations. It uses many other technologies that build the cloud environment today. Amongst these technologies which Cloud computing makes use of, Virtualization. It can be defined as a technology of abstraction or execution environment which ignores the complexity of hardware layer and without the need of real hardware multiple operating systems can be run [3, 4]. Virtualization offers dynamic resource allocation along with service provisioning, mainly in IaaS Cloud environment [1]. Nevertheless it plays a major role in building environment for Cloud computing. Cloud computing environment exclusively depends on virtualization technology to carry its business services SaaS, PaaS, and IaaS. Virtualization technology must be very well understood at all the levels and not only focus on CPU, Memory, fairly it now also involves application system storage as well as networking.

II. VIRTUALIZATION IN CLOUD COMPUTING

The core technologies used in cloud computing is Virtualization. In the 1960s when applications were multiplexed on very high cost mainframes there was a need for a technology that allow for as much as possible of resource utilization, and hence virtualization technology emerged. It utilizes virtual machine monitor VMM in hardware resource multiplexing, server consolidation and supports simultaneous execution of multiple instances of OSs [3, 5], thus, it can take be in charge over the executing flow of the guest OS. It is a thin layer software layer which usually runs on a machine's hardware. It also might run on top of a host OS on the host system. It is accountable of supervising the VMs and it does not allow direct interaction with the host hardware. Guest OSs running on VMs interacts with the host systems resources only via the VMMs. The VMM typically runs in the most privileged level and considered trusted component while the guest OS is considered not trusted and hence runs on user mode. In a while, as technology advanced which causes advancing in the capabilities of processor, bus speed, size of storage, memory and managed to reduce the cost of dedicated servers, there was almost no need to utilize such a technology as virtualization [4].Despite all above mentioned aspects of new technology, new challenges arose. This new superior inexpensive technology led to increase of underutilized machines that brought upon it a significant space and management overhead. Therefore, organizations realized the necessity of using VM [4], as they could not pay for care track of every server's application versions, patches. Along with this, securing becomes a burden for

ISSN: 2278 – 7798

the organizations . As a result, to beat these roblems organizations moved back to VMs, fused those VMs onto few physical servers and efficiently managed those VMs via VM monitor VMM; sometime it is refered to as the hypervisor.

III. VIRTUALIZATION TYPES

Virtualization environments can be deployed in two ways, VMM is deployed. Type I is known as Full virtualization where VMM is interfaced directly with the system hardware. And this type of architecture is also called as native architecture, Figure 1. In the case of Type II it is not interfaced directly with the hardware of the system, but it runs as an application beside the host OS. Type II is called Para-virtualization Figure 2. We now dicuss about the two types of virtualization and how the two architectures have an impact over the security of virtualization environment.

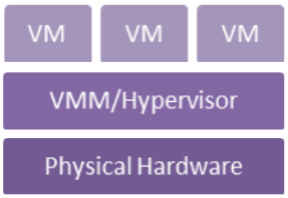

Fig.1. Full Virtualization Architecture

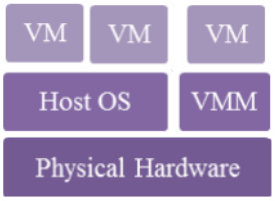

Fig.2. ParaVirtualization Architecture

A- Fullvirtualization

This is considered when the hypervisor is implemented directly on top of the physical hardware or when embedded in the host OS kernel. It is also called hardware virtualization because shared resources such as device drivers and hardware layer resources are virtualized by the VMM for guest OS. Xen hypervisor and KVM hypervisor is an examples of this type.

B- Para virtualization

Para virtualization is commonly deployed on those machines that don't support Full virtualization such as Intel "x86" architecture. It runs as software and it is enabled by the host OS which provides I\O drivers and bootstrapping code[4, 7, 8]. This type is known to be less secure because no matter how secure the VMM is, it is effected by the security of the host OS itself. An example of this virtualization architecture is the implementation of virtual environments using VMware, Sun VirtualBox, and Microsoft Virtual PC. In both the above architectures, VMM's main goal is to support three key attributes in virtual environment [4, 9]:

- Isolation
- Interposition
- Inspection

Isolation

VMM or the hypervisor provides isolation through virtual memory abstraction and will not let the VMs to share physical memory. Thus, It lets the VMs to think that each of them is possesses its own address space and has full control over it.

Interposition

This key wants that VMM has the capability to manage all privileged operations on a physical hardware. This means that VMM is always interfacing with the physical hardware and mediate all the requests from the guest OS to the underlying hardware. This gives some level of security. It ensures that no direct interaction with lower hardware layer.

Inspection

Inspection refers to VMM have full access to all VMs states. This contains CPU, memory, and device states. However, Virtualization has now primarily contributed as solution for security, reliability, and administration in that along with its associated techniques help to solve number of security issues. According to IBM researcher in , a single system could implement a multiple-level secure system by dividing it into multiple single- level virtual systems and securely separating them.

IV. VIRTUALIZATION ADVANTAGES

a) Resource Pool

This characteristic provides a uniform abstraction of resources [4]. This means that a physical machine is not viewed as limited entity with particular fixed capabilities, in fact, this feature shows how virtualization consolidates a collection of VMs onto a single machine. Thus, it lowers resource costs and space requirements.

b) Flexibility

This feature allows the user to run multiple instances of an operating system one a single computer. VMs can be migrated easily to another physical machine. It is also possible to change the specifications of virtual computers while they are running; Adding RAM, HDD .

c) Availability

It ensures that VM image can be incessantly run in the need of shutting down the physical node . This means if an upgrade or maintenance is to be done to that physical machine; it can be done with no touching the availability of the VM instance. As a result a VM hosted in the particular physical machine needs to be migrated to another physical machine and can be restored back after maintenance is complete.

d) Scalability

Strong involvement in creation of the cloud. It is considered as one of the basic features of virtualization. It assures the process of adding or removing VM instances when the demand for capacity or new VMs increases over time .

e) Cost

Virtualization offers efficient cost-reducing due to resource utilization. This can be achieved by consolidating

ISSN: 2278 – 7798

Number of servers into one physical server, hence reducing the capital expenditure .

a) Security

Though many argue that virtualization is facing security challenges, it offers isolation between the VM instances. Isolation provides encapsulation, i.e. no VM is allowed to communicate directly with the other. However, isolation, if not deployed properly, it pauses threat by itself. This emphasizes that virtualization offers some level of security. For example, a web server VM hosted in a machine alongside with database VM and email VM and If the attacker compromised that web server VM the other VM instances are unaffected.

V. BIOMETRICS ENCRYPTION

Authentication is a mechanism used to identify people and to provide the authorization for them. Authentication and identification have been used in many fields to provide proper security mechanisms. Authentication and identification are used in access control, verification, security audit, etc. Moreover, identification can be achieved by using the behavior features or physiological features. Apart from this, the science of using these features is called biometric identification.

Biometric identification includes iris, voice, fingerprint, face reorganization and etc. Biometric identification is more flexible authentication method than the secret key, because it is extremely difficult to be forgotten or even lost. However, the secret key is considered more secure approach, because some Biometric identification has been hacked using fake Biometric information attack, such as fake fingerprints attacks. In public security and banks, biometric identification has been applied as a strong security mechanism and strong solution .

Biometric encryption (BE): it is a solution that has been used to protect biometric identification. Indeed, cryptography was the solution to overcome the threats on biometric identification. Therefore, encryption was proposed as a patent by Bodo. After that, the first version of biometric encryption was completely proposed by other researchers . Biometric encryption also was proposed for face reorganization to enhance the privacy. Also, biometric encryption has been used in Tele- healthcare systems. Furthermore, biometric encryption was implemented in a standalone system using fingerprint fuzzy fault schema . In addition, a new framework of biometric encryption was proposed with filter-bank based fingerprint feature. Besides, the security of Mobile-ad hoc network was enhanced through unimodal biometric encryption key.Moreover, a cell phone was developed with biometric encryption based on user's behavior to authenticate the cell phone user. Actually, biometric technology uses three models: key release, key binding and key generation. Recently, the feasibility of deploying biometric encryption has been conducted for mobile Cloud computing .

Biometric encryption differs from normal password encryption, because it merges the biometric image with random generated key using BE binding algorithm to generate Biometrically-encrypted key. In the decryption process, the Biometrically-encrypted key is merged with the biometric image using BE retrieval algorithm to get the key retrieved .

Cloud Computing Security Issues and BE Effects

Despite all those charming features and strong support that virtualization technology provides to the computing environment that utilizes it. It has a huge impact on the development of these relying environments. Although, as mentioned before, virtualization is not new technology as Cloud, it has several security issues. These security issues have migrated into Cloud computing environment. Most of these security issues are based on the virtualization level.

However, Biometric encryption provides extra level security for privacy against these security issues. It is important to mention that BE does not solve the security issues in Cloud computing. But, it secures Biometric data against most of these security issues. BE provides extra level of security for the attacker in the Cloud which is the encryption mechanism.

A. VM Hopping

This kind of threat is directly affecting the customers/users of the Cloud. It is always due to resource sharing, a feature which virtualization offers. Resource sharing allows the physical machine and its resources such as CPU, memory networking and storage to be shared among the users reside in that particular physical machine, these users/tenants are called residents and thus the machine is going to provide co-residency/multi-tenancy. Although multi-tenancy is one of the most crucial goals of virtualization, it is considered as the weakest point in a chain. It exposes virtualized environments to huge risk and hence, it is huge threat to Cloud computing. However, this attack cannot directly occur from outside. This means an attacker needs to be placed in that particular physical machine as where his target resides. Although, the attacker should follow some steps vary from allocating his victim to execute arbitrary commands, this should allow the attacker to be able to break the isolation control and attack his victim.

BE effects: when VM hopping occurs, the attacker can get access to neighbor's VM ware; however, the biometric data is encrypted and it is not readable for the attacker. However, if the attacker could control the whole VM ware and get access to the biometric device, the biometric information will be readable for the attacker.

B. VM Mobility

VM mobility addresses a crucial security issue. VM mobility offers some flexibility in migrating VM instance from storage to another over the network. This security issue is usually due to weak configuration of the cloud network environment. Although this flexibility provides robust support to physical security to protect against stealing the storage, yet it leads to other security issues such as, it allows the attacker to get a copy of the VM which is transmitted from a machine to another. This

ISSN: 2278 – 7798

type of breach violates the confidentiality and integrity of users' data and thus shows that users' data is at risk when it is stored in the cloud. However, extenuating the risk caused by VM Mobility is not a duty of the users . Cloud providers also share some responsibilities in reducing such risk. Therefore, security management of users data stored in the cloud should be written in a Service Level Agreements (SLA) that clearly states the obligations of both Cloud providers and Cloud users.

BE effects: even though the attacker can get a copy of the VM, the attacker gets encrypted biometrics data.

C. VM Diversity

Virtualization technology offers an ease of use in which it allows the users to competently make many VMs. This freedom shows that securing and managing these VMs is a huge burden due to various OSs that can be deployed in seconds . This kind of diversity makes VM security management a challenge. However, a proper SLA could help address this issue. Looking at Cloud computing release service models, we can say that VM security management in this context is not the responsibility of the cloud service provider (CSP) alone, in fact, it is also the responsibility of the cloud user. For example, in IaaS, the CSP must ensure security and sturdiness of the underlying infrastructure such as the hypervisor, whereas the user must properly ensure that his VM and offered service is configured correctly and secured, and this includes keeping the guest OS patched and up-to-date. However, this is not limited to IaaS. PaaS service model also requires some security and maintenance but PaaS is somewhat robust against VM diversity.

BE effects: different VMs may contain different types of operating systems. These operating systems contain different weaknesses, so it is the duty of the VMs owners to keep their VMs updated as well as BE. This approach can protect their data in case of intrusion to their VMs.

D. Denial of service

Denial of service is stopping an available service; it is blocking the performance and the functionality of the source. Virtualization environment is a shared resources environment where VMs share the same CPU, memory, bandwidth and disk. Furthermore, the provider always has limited capacity of those resources. Apart from this, one VM can exhaust these shared physical resources which will cause denial of services. Moreover, if the VMs in the same physical machine which use the shared resources at the same time, denial of service will occur. The supplier should be aware of the utmost usage of its resources which the VMs can use. Also the provider should configure its resources in a appropriate manner to prevent denial of services. Denial of service is a grave matter that should be treated with well configuration and monitoring

BE effects: when the service is down, there are no effects for biometrics encryption. Biometric encryption targets the confidentiality of biometric information only and it is not targeting the availability of the data.

E. VM Escape

VMM is intended to allow VMs to share system resources in controlled approach. Therefore, VMM must enforce isolation between VMs and system resources by preventing any direct interaction with the lower hardware layer. Exploiting a compromised VM in a way that allows an attacker to take control over the hypervisor is known as VM escape. VM escape, the program running in a virtual machine is able to completely bypass the virtual layer (hypervisor layer), and get access to the host machine. Thereby, it escalates to root privileges, basically escape from the virtual machine privileges. This vulnerability will allow the attacker to likely have control over all guest Oss resulting in a complete collapse of the security framework of the environment. VM escape is the worst case when the isolation between the VMs and host is compromised.

BE effects: when VM escape occurs, the attacker will control the main host machine and get the root privileges. Therefore, the attacker can have access to all the resource as well as biometric devices, so the attacker can read the biometric information. When VM escape occurs BE does not help to protect biometric information.

E. VM Monitoring

The primary attribute in virtualization technology is isolation VMs from each other inside a single host. Apart from this, without a proper configuration for the host machine, one VM can get an access and monitor other VMs. This means the provider lost the confidentiality of the system. One VM can lunch a cross-VM side channel attack to extract the memory information about the victim. Moreover, ARP poisoning can be lunched to turn the traffic from the victim VM to the attacker VM, which allows the attacker to monitor all the traffic of the victim VM. Monitoring VMs is a critical issue which the provider must prevent to keep the confidentiality of its system .

BE effects: if the attacker could sniff the data of another VMs, the data of BE will be encrypted which will provide other security layer and extra challenges for the attacker.

F. Virtual machinescommunications

A clipboard in virtual machine technology allows the interaction between the hosts VMs; this is very relevant method to do the communication between hosts. However, in the same time, malicious can be given easily as well. Another example, some of the providers do not apply full isolation for the VMs by allowing the VMs to access the host virtual machine and use a familiar application. This action is very difficult and proper isolation should be used. In virtual machine environment, encryption is a good live out to keep the transferred data protected and confidential.

BE effects: malicious codes can transmit the wanted data to the attacker or allow the attacker to apply a successful intrusion to other VMs. BE keeps the biometric data encrypted and not readable for the attacker.

ISSN: 2278 – 7798

G. Host Control VM

The host is the regulator of all the virtual machines; the host is the director, the examiner and the defender of the virtual machines on it. So the host can observe all the traffic of those virtual machines, and control them as well. Different studies on the virtualization technology showed that the host can affect the VMs . So the host security is very essential to secure the virtual machines, also a proper configuration should be applied and access control constraint to the host to keep all the virtual machines secured as well.

BE effects: it is a good carry out to keep the data of the VMs, encrypted in the host; therefore, even if the host is controlled by an attacker, the attacker cannot read the encrypted biometrics data. However, if the attacker could gain the root rights, biometric information will be readable to the attacker.

VI CONCLUSION

Virtualization has some safety issues. These safety issues migrated to the cloud environments which affect the privacy of biometric data. Biometric encryption is a resolution which is anticipated in this paper. Actually, Biometric encryption provides privacy to the biometrics data in the cloud. Therefore, Biometric encryption is hugely recommended to be implemented in the Cloud computing. Indeed, this approach gives extra safety level to the Cloud computing.

Moreover, it overcomes many safety weaknesses in Cloud computing related to biometric data confidentiality. Indeed, confidentiality is enhanced in Cloud computing by using biometric encryption for biometric data. However, Biometric encryption will not tell the safety issues in Cloud computing, but it secures Biometric data against most of those security issues. Until this moment, there is no related research studied Biometric encryption in Cloud computing. However, biometric encryption in Cloud computing will be implemented in the future. Therefore, biometric encryption for biometric data in Cloud computing will be deployed and evaluated as well.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers whose comments have helped improve the presentation of this paper .

REFERENCES

[1] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," Communications Surveys & Tutorials, IEEE, vol. 15, pp. 843-859, 2013.

[2] M. A. Bamiah and S. N. Brohi, "Seven deadly threats and vulnerabilities in cloud computing," International Journal of Advanced Engineering Sciences and Technologies, Vol,(9), 2011.

[3] T. Brooks, C. Caicedo, and J. Park, "Security challenges and countermeasures for trusted virtualized computing environments," in Internet Security (WorldCIS), 2012 World Congress on, 2012, pp. 117-122.

[4] M. Price, N. Wilkins-Diehr, D. Gannon, G. Klimeck, S. Oster, and S. Pamidighantam, "The Paradox of Security in Virtual Environments."

[5] Y. Dai, X. Wang, Y. Shi, J. Ren, and Y. Qi, "Isolate secure executing environment for a safe cloud," in Communications in China (ICCC), 2012 1st IEEE International Conference on, 2012, pp. 79-84.

[6] Y. Wen, J. Zhao, G. Zhao, H. Chen, and D. Wang, "A Survey of Virtualization Technologies Focusing on Untrusted Code Execution," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, 2012, pp. 378-383.

[7] C. Li, A. Raghunathan, and N. K. Jha, "A trusted virtual machine in an untrusted management environment," Services Computing, IEEE Transactions on, vol. 5, pp. 472-483, 2012.

[8] F. Sabahi, "Virtualization-level security in cloud computing," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 250-254.

.

ISSN: 2278 – 7798