A SURVEY ON SECURE DOMAIN BASED STORAGE PROTECTION USING MULTI CLOUD IN PUBLIC INFRASTRUCTURE

[1]Mrs. D. KAVITHA, [2]V.AMUTHA, [3]M.MAGESHWARI, [4]S.JAMUNA VAANI SRI

[1]Assistant Professor, [2,3,4]Student
Department of Computer Science and Engineering,
Valliammai Engineering College SRM Nagar, Kattankulathur-603203, Tamilnadu, India.

***ABSTRACT-* The infrastructure cloud (IaaS) service model offers improved resource flexibility where tenants rent computing resources to operate complex systems. Many organizations operating on sensitive data avoid migrating operations to IaaS platforms due to security concerns. Here a framework is proposed for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection. Thus once the user is authenticated they will be launched in virtual machines where they initiate the upload process into the cloud. The encryption keys are also maintained outside of the IaaS domain. Virtual machines and key management are used to secure the data. Authentication and session management includes all aspects of handling user authentication and managing active sessions.**

***Keywords* –Virtual machine, Domain-Based Storage Protection, Authentication, Session Management, Active sessions.**

1. INTRODUCTION

Cloud computing technology has become an integral trend in the market of information technology. The current market of IT witnessed a considerable change due to the presence of cloud computing which had become an integral part of most of the business. Today, most of the businesses, fromsingle to large enterprises, migrated to cloud computing in order to obtain a high level of productivity by entrusting their IT issues to an expert one. Cloud computing systems used to provide services of computing, that are not perfectly reliable and they could suffer from outages of services due to failures. To overcome this, an adaptive framework with dynamic method of fault tolerance is proposed [1]. Cloud storage contains large amount of data. It is important to providesecurity to Peta Bytes of data in cloud. CloudComputing Adaptation Framework (CCAF) isdeveloped for securing the cloud data. [11].Incloud computing the storage of data and information allows data owners to move data from their local computing systems to the cloud. Virtual machine migration plays a major role in service migration. Virtual machine mobility is used to move a service form one physical server to another server for getting closer to its customer. So this benefits the service providers by attracting more customers [12].

Because of convenience and efficiency, the popularity of cloud storage has increased rapidly. Remote Data Audit (RDA) protocol is used which can efficiently, securely and exactly validate the data [2]. While outsourcing its business -critical data and computation to the cloud, an enterprise loses control over them. The organization should decide what security measures to apply toCSPs. Resources are available on reservation basis, as well as on demand basis. Reservation is to be done for a fixed contract period with a fixed price. This paper focuseson the optimizing strategies aimed at reducing the total cost of cloud deployment [6].Computing resources such as software,hardware, networking, and storage can be accessed On-Demand. Storing sensitive data on un-trusted servers becomes an important issue. To guarantee the confidentiality classical encryption techniques are used. Attribute-Based Encryption (ABE) is one of the encryption technique are used in the cloud [13].

2. ADAPTIVE FRAMEWORK FOR RELIABLE CLOUD COMPUTING

An adaptive framework is presented to cope proactively and reactively with the problem of fault tolerance in cloud computing environment. To be proactive, the framework depends on customer requirements and the available information about virtual machine at the scheduling time. The framework employs both replication and checkpoint methods and it dynamically selects the suitable method according to the current condition of the cloud.

2.1 TECHNIQUES USED

2.1.1 SFT Algorithm

Selecting Fault Tolerance (SFT) is used with the objective select the appropriate method for tolerating faults in the cloud computingsystem. The algorithm is implemented in the SFTM (Selecting Fault Tolerance Manager) component of the Scheduler module. In order to achieve its objective, the algorithm depends on using customer's requirements and the available information about virtual machines. The algorithm prepares a list of virtual machines that can carry out the customer's request and satisfies the customer's requirements.

2.1.2 Replication Algorithm:

Replication is applied when there are multiple and available virtual machines in the cloud that can carry out the customer's request. However, it is a central challenge to define the optimal number of replicas. In addition, it is not an economical approach to perform replication for all virtual machines [7]. So, we only need to replicate requests executed on the most valuable virtual machines that will have a great impact on the performance of the cloud if they fail.

2.1.3 Checkpoint Algorithm:

Distributed systems, such as grid computing systems, have widely used checkpointing as a reactive fault tolerance method to alleviate the impact of failures when occurred. Moreover, most cloud computing systems implement replication techniques. However, from the perspective of the cloud service provider, replication results in profit loss due to allocating extra components to execute the replicas of a request, particularly these components may be useful for other requests. Replication leads to time loss due to waiting for components that execute replicas to be free from executing other requests. So, the main advantage of using check pointing over replication is to preserve the computing resources of the cloud to other customers' requests and to reduce the profit loss because of using replication.

ADVANTAGES

- Adaptive framework copes with the problem of fault tolerance in cloud computing environment.
- Improves the performance of the cloud in terms of throughput, overheads, monetary cost and availability.
- Replication and Checkpointing algorithm determines the mostappropriate fault tolerance method for each selected virtual machine.

DISADVANTAGES:

- The proposed framework only replicates the most valuable virtual machines and not all virtual machines as the static algorithm.
- This will decrease the number of virtual machines consumed in the replication

LIMITATIONS

- Investigations about applying the framework and the well-established fault detection and reliable control methods for complex industrial processes in the cloud computing environment.
- Providing more consideration to the migration of data centers and tasks between them.

3. CLOUD COMPUTING ADOPTATION FRAMEWORK:

Providing real-time data security for peta bytes of data is important for cloud computing. Cloud Computing Adaptation Framework (CCAF) is developed for securing the cloud data. Data Center has peta bytes of data; there is a big task to provide real-time protection. Business Process Modeling Notation (BPMN) is used to represent the status of data. It checks whether the data at rest or in use or in motion. BPMN is used to evaluate the security performance. The time to take control of security breach is between 50 to 125 hours. So we need additional security to ensure more data to be protected within 50 to 125 hours [11].

3.1CCAF Data Security:

It deals with data in transaction, data in modification and privacy of user data.

3.1.1 Security schema by XML

In this XACML (Extensible Access Control Markup Language) is used to defineset of rules and permissions to ensure the data security.

3.1.2 CCAF multilayered security

The features in CCAF multi-layered include access control, intrusion detection system (IDS) and intrusion prevention system (IPS).

3.1.2.1 THREE LAYERS OF SECURITY

1. Access control and firewall

It allows only restricted members to access the system.

2. IDS and IPS

Its aim is to detect attacks, intrusion and it also provides up-to-date technologies to prevent the attacks.

3. Convergent encryption

This layer includes the encryption of hash of plaintext using encryption key.

3.2. BUSINESS PROCESS MODELING NOTATION

It is a tool independent graphical process definition language to study performance of the system.

3.3. PENETRATION TESTING FOR ETHICAL HACKING:

Ethical Hacking is the way to test the system performance.The Ethical Hacking environment contains one 100 of virtual Machines were setup and each virtual machine with CCAF multilayered security turn ON.

ADVANTAGES

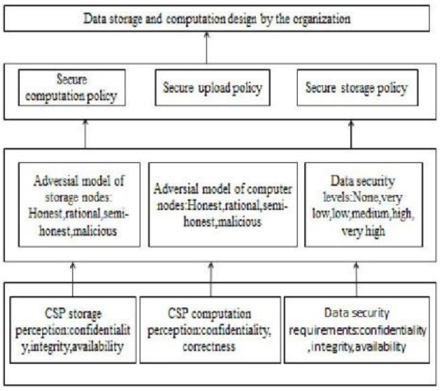
- CCAF multilayered security offers multiple protections and improvement of the 10PB data in the Data centers.
- CCAF multilayered security is better than the single layered security.
- Using BPMN with CCAF is more secure.

DISADVANTAGES

- In the Data Centers, daily 100 TB of data increases. So it is difficult for an organization to respond immediately, thus the data security network traffic increases.
- While the increase of the data, there is a possibility of data from external sources such as attack of viruses or from internal sources of users or clients accumulate hundreds of terabytes of data per day.

4. POLICY-BASED SECURITY FRAMEWORK

A decentralized dynamic and evolving policy-based security framework (Figure 1) for enterprise data and computation outsourcing to the cloud such that it allows the organization to retain the control over its data and computation. It is achieved by taking into account the perception of employee roles who constantly deals with certain types of data. This framework allows the organization to retain the control over the data and computation. In this multi-cloud is used for secure storage and computation [10] that is, trusted cloud that performs encryption and decryption. Untrusted commodity cloud which performs critical operations on encrypted data. It provides a set of policies for security such as Storage security policy, Upload security policy, Computation security policy. It is based on risk minimization while optimizing efficiency and flexibility. System architecture is proposed, allowing organization wide integration of untrusted public storage cloud [8].


Data storage and computation design by the organization
Secure computation policy
Secure upload policy
Secure storage policy
Adversial model of storage nodes: Honest,rational,semi-honest,malicious
Adversial model of computer nodes:Honest,rational,semi-honest,malicious
Data security levels:None,very low,low,medium,high, very high
CSP storage perception:confidentiality,integrity,availability
CSP computation perception:confidentiality, correctness
Data security requirements:confidentiality ,integrity,availability

(Figure1 .Policy-Based Security Framework)

4.1 TECHNIQUES USED

4.1.1 IDA Algorithm

It uses Information Dispersal Algorithm (IDA) to ensure availability, and by combining symmetric encryption with IDA, achieves high confidentiality

4.1.2 AES-CMAC Operation

AES-CMAC operation mode for encryption which produces a MAC for each data fragment and enables replacement in case of any integrity violation.

ADVANTAG ES

- It helps in secure outsourcing of cloud.
- It guarantees confidentiality, integrity and availability.
- It allows the organization to retain the control over the data.

DISADVANTAGES

- It does not deal with data movement and maintenance.

LIMITATIONS

- Analyzing in detail its efficiency vs security tradeoffs with respect to a pessimistic and optimistic view about CSP's trustworthiness.
- Instead of using several storage nodes or computation nodes in the same CSP multiple CSP's can be used which increases the reliability of the whole system.

5. ANALYSIS OF CLASSICAL ENCRYPTION TECHNIQUES

Cloud computing is the plays a major role in IT Industry. Computing resources such as software, hardware, networking, and storage can be accessed On- Demand. Storing sensitive data on third party servers becomes a major issue. A range of different techniques or security algorithms are used to maintain the security and privacy of the cloud. To guarantee the confidentiality classical encryption techniques are used [13].

5.1 Attribute-Based Encryption (ABE)

It is a public key cryptographic technique that works in a one to-many fashion and is also called fuzzy encryption. ABE uses attributes as identities for both encryption and decryption of data. The cipher text and a user's secret key depend on attributes. If the attributes of a user key match those of the cipher text, then decryption is allowed. In the cloud, data security is important to protect against inside attack, denial of service attack, and collision attack. Different access control policies are used to protect data which are stored locally and remotely. The approaches are,

5.1.1. Discretionary Access Control (DAC)

In this users are given complete control over resources on the basis of user identity.

5.1.2. Mandatory Access Control (MAC)

MAC is based on lattices and on the MAC decision on network configuration.

5.1.3 Role-Based Access Control (RBAC)

In this access is based on particular roles depending on the user.

5.1.4. Attribute-Based Access Control (ABC)

Attributes based on user requests,including names and value pairs, and are associated with actions, users, subjects, objects, contexts and policies.

SCHEMES

1. Key Policy ABE (KP-ABE)
2. Expressive Key Policy ABE (EKP-ABE)
3. Cipher text Policy Attribute-Set-Based Encryption (CP-ASBE)
4. Hierarchical Identity-Based Encryption (HIBE)
5. Hierarchical Attribute-Based Encryption (HABE)
6. Hierarchical Attribute-Set-Based Encryption(HASBE)
7. Cipher text Policy Weighted Attribute-Based Encryption (CP-WABE)
8. Key Policy Weighted Attribute-Based Encryption (KP-WABE)
9. Multi-Authority-based weighted Attributed-Based Encryption (MA-WABE)

ADVANTAGES

- Public key encryption methods store encrypted data on third party servers, while distributing decryption keys to only authorized users.

DISADVANTAGES

- It is difficult to efficiently manage the distribution of secret keys to authorized users.
- Data owners must be online wheneverencrypting or re-encrypting data, or distributing the secret keys.

6. PROTOCOL WITH BIDIRECTIONAL VERIFICATION FOR STORAGE SECURITY IN CLOUD

- An auditing framework is designed for cloud storage systems which propose an efficient and privacy preserving auditing protocol. Then, we extend our auditing protocol to support dynamic data operations, which is efficient and has been proven to be secure in the random oracle model. We extended our auditing protocol further to support bidirectional authentication and statistical analysis. In addition, we use a better load distribution strategy, which greatly reduces the computational overhead of the client.

6.1 TECHNIQUES USED

6.1.1 Keygen Algorithm

The client generates one pair of keys using some of the parameters. And this pair of keys will be used for the signature and decryption of the file. Through the encryption/decryption operation and some other measures, the server can tell which users/TPA's (Third Party Auditor) are real users/TPAs (i.e., the ones that have the right to receive service).Then the client generates a second pair of keys. This pair of keys is used to generate thefile block identifier. Depending on the identity, the verification party can determine whether thefile has been changed.

6.1.2 SigTagGen Algorithm

When the tags of each file block have been calculated, the user sends them and the file blocks to the CSP and then deletes the local backup (blockless verification). Now, the setting process is over. At the beginning of the validation phase, the parties must ensure that they are qualified. In order to obtain the appropriate permissions, the verification party (the TPA or user) should register her or his own identity. Simultaneously, in this program, we use a trusted public platform toprocess the registration information, and we think this platform is absolutely reliable.

6.1.3 Register Algorithm

The public platform verifies the identity of the third party and gives the *spk* to the third party. *Spk* is a key point in the intercommunication between TPA and CSP. The TPA must interact with the CSP to prove its identity before presenting verification requirements. After that, the TPA should generate the validation sequence and send it to the server.

ADVANTAGES

- It greatly reduces the computational overhead.
- It has a high probability of detecting any misbehavior of the server.

DISADVANTAGES

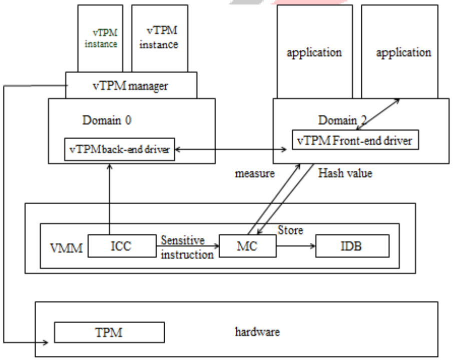
- Verification times are unlimited.
- Usage of space is increased by about 15% because of sentinel and error correcting code.

LIMITATIONS

- To explore more effective verification schemes. To improve the efficiency of dynamic operation.

7. MULTLIWAY DYNAMIC TRUST CHAIN MODEL (MDTCM) ON VIRTUAL MACHINE

A cloud system-based MDTCM (Figure 2) is built to show the feasibility of the virtual machine. MDTCM can better reflect the dynamic characteristics of the virtual machine, thereby providing a good basis for studies on the security of virtual machines. Communication among virtual machines can be completed by MDTCM only. No direct interactive communication takes place. The interaction between machine and the underlying VMM is also completed by MDTCM. It is transparent to the upper-layer virtual machine.

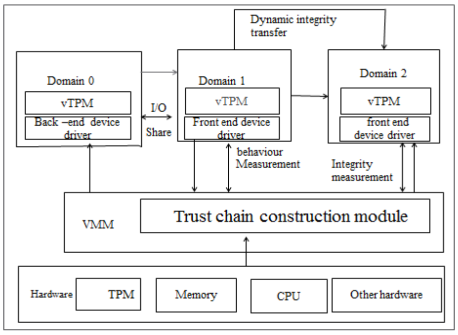


(Figure 2. Sketch map of MDTCM)

7.1. TECHNIQUES USED

7.1.1 Integrity Measurement

Integrity measurement mechanism (Figure 3) focuses on each component of the interactive machine. MC (Measurement Component) analyzes the behavior to initiate the measurement process. In the installation of the user application, MC is also responsible for measuring the application code. All the SHA-1 values consist of the VM's static data, and recorded by IDB. This measurement is carried out with the help of physical TPM. When sensitive instruction is transferred, MC sends a metric instruction to the Virtualized TPM of an interactive VM.



(Figure 3. Integrity Measurement Mechanism)

7.1.2 Behavior Measurement

According to the definition given by TCG [9], whether the computing platform can be trusted directly depends on its behavior, which should be consistent with the expectedstrategy. From the point of view of system security, two types of operations are selected as monitoring points.

1. The operation to make a change to the boundary, such as the creation and destruction of the VM and the expansion or reduction of the VM boundary.
2. The cross-border instruction that is the access and modification operation initiated by the other VM.

ADVANTAGES

- It guarantees the real-time credibility and communication security of a virtual machine.

DISADVANTAGES

- The simple vertical trust chain cannot guarantee credibility I real time while the virtual machine is running.
- Communication among virtual machine can be completed by MDTCM only. No direct interactive communication takes place.

LIMITATIONS

- It should consider strengthening the defense of information databases, which have a high confidentiality requirement and may be subjected to concentrated attacks.

8. MOBILITY-ORIENTED SCHEMEFOR VIRTUAL MACHINE MIGRATION

In cloud computing, the virtual machines should be able to migrate from one location to another location to meet the requirements of the cloud users. If virtual machine migrates across IP subnets, then the mobility is an important problem. Mobility oriented cloud data center network architecture is developed and is based on the identity/locator decoupling method of the mobility-driven networks. In proposed architecture, a virtual machine could implement live migration between IP subnets without interruption.

8.1. Mobility Oriented Cloud data center network architecture

In wireless network the mobile terminals moves from one location to another location where the location changes but identity remains unchanged. And this essence also works for the virtual machine mobility in cloud data center network. Thus the mobility management techniques can be introduced into cloud data center to support the virtual machine migration across IP subnets. A location management system is adopted to map the Entity-identity to Location-identifier and support dynamical Location-identifier update whenever virtual machine migrates [12].

8.1.1Decoupling of Entity-Identity and Location-Identifier

Decoupling of Entity-identity and Location-identifier is adopted to split the identity and the location of the virtual machine by defining separated name spaces.

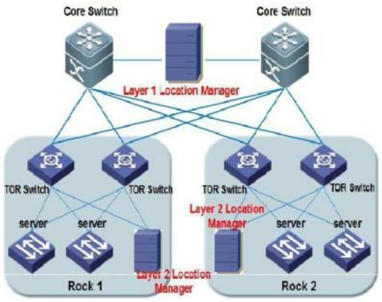
8.1.2 Packet Encapsulation and Communication Procedure

Physical server is responsible for encapsulation of packets. When the packet is intercepted by the hypervisor of the physical server, locators of both source anddestination are inserted into the packet as an additional header.

8.2 Mobility Management for Mobility-Oriented Cloud Data Center Network

8.2.1 Location Management

Location management for mobility-oriented cloud data center network can also be also divided into two parts, i.e. location query and location update, and it is responsible for keeping the current location of a virtual machine and updating it whenever it moves.



8.2.2. Migration Management

Migration management is used to trigger and handle the VM migration. There are 2 functions,

1. Migration decision

This function provides when to start virtual machine migration.

2. Migration execution

This function starts after migration decision function.

8.3 Live Virtual Machine Migration

It provides continuous service provisioning to hosted applications. It has 2 phases

8.3.1 Phase 1: VM image migration

VM image migration transfers the file system.

• Pre copy method

A pre-copy VM migration transfers entire memory image before resuming VM at the target server.

• Post copy method

Post -copy VM migration approach captures and transfers the VM's minimum system state to the target server before the Virtual Machine resume phase.

8.3.2 Phase 2: VM reconnection

It rebuilds the connection between new VM.

ADVANTAGES

- Virtual machine mobility is used tomove a service form one physical server to another server for getting closer to its customer. So this benefits the service providers by attracting more customers.

- Virtual machine mobility can be used to reschedule the computing resource in the cloud data center for the purpose of power saving or meeting user requirements. So the cost of operator is reduced and enhances the profit and also satisfies the user.

DISADVANTAGES

- The mobility is an important issue when a virtual machine migrates across IP subnets.
- Inefficient resource management policies poorly exploit system resources within Cloud Data Centers.

CONCLUSION

From a tenant point of view, the cloud security model does not yet hold against threat models developed for the traditional model where the hosts are operated and used by the same organization. However, there is a steady progress towards strengthening the IaaS security model. In this work we presented a framework for trusted infrastructure cloud deployment, with two focus points: VM deployment on trusted compute hosts and domain-based protection of stored data.

REFERENCES

[1] Mohammed Amoon,"Adaptive Framework for Reliable Cloud Computing Environment", IEEE Access, Vol.4, pp. 9469-9478, 2016.

[2] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, Tie Qiu, "An Efficient Protocol With Bidirectional Verification For Storage Security In Cloud Computing", IEEE Access, Vol.4, pp. 7899-7911,2016 .

[3] Sourya Joyee De, Asim K.Pal,"A Policy-Based Security Framework For Storage and Computation on Enterprise Data in the Cloud", 47th Hawaii International Conference on System Sciences, pp.4986-4997, 2014.

[4] Shungan Zhou, Ruiying Du, Jing Chen, Hua Deng, Jian Shen, Huanguo Zhang, "SSEM: Secure, Scalable and Efficient Multi-owner Data Sharing in the Cloud", China Communications, Vol.13, pp 231-243, 2016.

[5] Jie Zhu, Guoyuan Lin, Fucheng You, Huaqun Liu, Chunru Zhou, "Multiway dynamic trust chain model on virtual machine for cloud computing", China Communications, Vol.13, pp.83-91,2016.
[6] Sunirmal Khatua, Preetam Kumar Sur, Rajib Kumar Das, Nandini Mukherjee, "Heuristic-Based Resource Reservation Strategies for Public Cloud", IEEE Transactions on Cloud Computing,Vol.4,pp. 392-401,2016.
[7] E. Bauer and R. Adams. "Realiability and availability of Cloud Computing", Hoboken, NJ, USA: Wiley, 2012.
[8] Ronny Seiger, Stephan Groβ, Alexander Schill, "SecCSIE: A Secure Cloud Storage Integrator for Enterprises", IEEE 13thConference on Commerce and Enterprise Computing, pp.252-25, 2011.
[9] Sadeghi Ahmad-Reza, Selhorst Marcel, Stuble Christian, Winandy Marcel, "TCG Inside? :A note on TPM specifications compliance [C]". Proceedings of the 1st ACM workshop on Scalable trusted computing,ACM ,pp.47-56, 2006.
[10] S.Bugiel, S.Nurnberger, A. Sadeghi, and T.Schneider, "Twin Clouds: An Architecture for Secure Cloud Computing", Workshop on Cryptography and Security in Clouds, 2011.
[11] Victor Chang and Muthu Ramachandran,"Towards achieving data security with the cloud computing adoption framework", IEEE Transactions on services computing, vol.9, no.1, 2016.
Bo hu[1], (member, IEEE), Shanzhi chen[2], (senior member