ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

A Review on Shielding Virtualized Resource in Cloud Computing using Augmented Protection Techniques

Amita Pathania [1], Dr. Dinesh Kumar [2]

M. Tech Student, Department of Computer Science & Engineering, SRCEM at Palwal , Haryana, India[1]

Head of Department, Department of Computer Science & Engineering, SRCEM at Palwal , Haryana, India[2]

ABSTRACT: An intermittently connected network (ICN) is defined as a mobile network that uses cooperation between nodes to facilitate communication. This cooperation consists of nodes carrying messages from other nodes to help deliver them to their destinations. An ICN does not require an infrastructure and routing information is not retained by the nodes. While this may be a useful environment for message dissemination, it creates routing challenges. In particular, providing satisfactory delivery performance is difficult with no network infrastructure or routing information. In this paper, context aware techniques are used to improve the delivery probability in an ICN. The examined context aware techniques are environmental, historical and personal against early and popular ICN routing protocols. It is shown via extensive simulation that context aware employment in ICN routing methods increase the delivery probability by 15%.

KEYWORDS: Shielding Virtualized Resource, Cloud Computing, Cloud Security, Cryptography.

I. INTRODUCTION

Now days the expression cloud computing is analogical to web. However, The terms distributed computing depends on cloud illustrations utilized in the scenario to converse with distributed systems with delineate Internet. Distributed computing is Internet based processing where virtual shared servers give programming, framework, stage, gadgets and different assets and facilitating to clients on a compensation as-you-utilize premise. All data that a digitized framework brings to the table is given as an administration in the distributed computing model. Clients can get to these administrations accessible on the "Web cloud" without having any past ability on dealing with the assets included. Along these lines, clients can focus more on their center business forms as opposed to investing energy and picking up information on assets expected to deal with their business forms.

Cloud computing clients don't claim the physical framework; rather they lease the use from a third-party supplier. This causes them to stay away from colossal capital speculations. They expend assets as an administration and pay just for assets that they utilize. Most distributed computing foundations comprise of administrations conveyed through shared assets. This builds proficiency as servers are not superfluously left inactive, which can decrease costs fundamentally while expanding the speed of utilization improvement. Cloud Architecture Cloud figuring engineering comprises of two segments "the front end" and "the back end". The front end of the distributed computing framework contains the customer's gadget (or it might be PC system) and a few applications are required for getting to the distributed computing framework. Back end alludes to the cloud itself which may incorporate different PC machines, information stockpiling frameworks and servers. Gathering of these mists make an entire distributed computing framework. The entire framework is managed by means of a focal server that is likewise utilized for checking client ís request and movement guaranteeing smooth working of the framework. A unique kind of programming called "Middleware" is utilized to permit PCs that are associated on the system to speak with one another. Distributed computing frameworks additionally should have a duplicate of all its clients information to re-establish the administration which may emerge

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

because of a gadget breakdown. Making duplicate of information is called repetition and distributed or cloud computing specialist co-ops give information excess therein.

Operation models in cloud computing:

1. **Public Cloud** : Public or Open cloud is customary distributed computing where assets are progressively provisioned on a fine-grained, self-benefit premise over the Internet or VPN or potentially from an utility that outsider supplier or provider who charges on a fine-grained premise or on the bases what is used based charges only or even free of costs example like iGoogle, Amazon web services (AWS) etc

2. **Community Cloud:** In the event that few associations have comparable prerequisites and try to share framework to understand the advantages of distributed computing, at that point a network cloud can be set up. This is a more costly alternative when contrasted with open cloud as the expenses are spread over less clients when contrasted with an open cloud. Be that as it may, this choice may offer a larger amount of protection, security as well as arrangement consistence.

3. **Hybrid Cloud:** Hybrid Cloud implies either two separate mists consolidated (open, private, inner or outer) or a mix of virtualized cloud server examples utilized together with genuine physical equipment. The most right meaning of the expression "Hybrid Cloud" is presumably the utilization of physical equipment and virtualized cloud server examples together to give a solitary regular administration. Two mists that have been consolidated are all the more effectively called a "joined or hybrid cloud".

4. **Private Cloud:** Private clouds describe offerings that deploy cloud computing on private networks. It consists of applications or virtual machines in a company's own set of hosts. They provide the benefits of utility computing -shared hardware costs, the ability to recover from failure, and the ability to scale up or down depending upon demand.

Vulnerabilities in Cloud Computing:

Endeavors need to shield known and unknown vulnerabilities in a broad range of critical applications and systems that are being targeted by cybercriminals.

1. **Un-patchable Systems**: Systems such as point-of-sale devices, kiosks and medical or other embedded devices are often considered unp-atchable. Often, low-bandwidth connections with remote locations make deploying large patches prohibitively time consuming or expensive. At other times, regulations or service level agreement uptime requirements may preclude systems from being patched.

2. **Legacy Web Applications:** The larger part of records that are ruptured are the consequence of SQL Injection assaults on web applications. Web applications are especially defenseless on the grounds that they're characteristically open and available to assailants. What's more, substance and usefulness is progressively intricate and developers are regularly untrained in secure programming advancement rehearses. Edge security won't shield these frameworks and it tends to be hard to find and dole out the custom advancement assets important to settle the code.

3. **Enterprise Applications**: Every year a huge number of basic programming defect vulnerabilities are accounted for in working frameworks, databases, servers, and different applications. Fixing these vulnerabilities can be troublesome and tedious, expecting frameworks to be rebooted and affecting administration level understandings. Notwithstanding when a fix is accessible, it can take weeks or even a long time before the fix can be completely sent.

4. **Unsupported Operating Systems and Applications:** Patches are never again created or issued for more seasoned working frameworks and applications that have achieved their finish of-life, for example, Oracle 10.1 and Solaris 8. Regularly, the time and cost required to relocate to a fresher form is essentially too high, and associations require a more prompt, financially savvy arrangement. At the point when bolster for

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Windows 2000 finished July 2010, virtual fixing turned into the main financially savvy approach to guarantee proceeded with assurance for these and other unsupported frameworks.

II. LITERATURE REVIEW

1. **J Li, Y Zhang, X Chen, Y Xiang** depicts Data sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a potential technique for realizing fine-grained data sharing, attribute-based encryption (ABE) has drawn wide attentions. However, most of the existing ABE solutions suffer from the disadvantages of high computation overhead and weak data security, which has severely impeded resource-constrained mobile devices to customize the service. The problem of simultaneously achieving fine-grainedness, high-efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. This paper addresses this challenging issue by proposing a new attribute-based data sharing scheme suitable for resource-limited mobile users in cloud computing. The proposed scheme eliminates a majority of the computation task by adding system public parameters besides moving partial encryption computation offline. In addition, a public ciphertext test phase is performed before the decryption phase, which eliminates most of computation overhead due to illegitimate ciphertexts. For the sake of data security, a Chameleon hash function is used to generate an immediate ciphertext, which will be blinded by the offline ciphertexts to obtain the final online ciphertexts. The proposed scheme is proven secure against adaptively chosen-ciphertext attacks, which is widely recognized as a standard security notion. Extensive performance analysis indicates that the proposed scheme is secure and efficient.

2. **M Qiu, K Gai, B Thuraisingham, L Tao** depicts that, As one of the most significant issues in the financial industry, customers' privacy information protection has been considered a challenging research over years. The constant emergence of the novel technologies often leads to dynamic threats from both internal and external service providers. We consider the implementations of mobile cloud-based financial services an important approach of service provisions, which also causes risks to privacy protections due to the data sharing with the unknown third parties. The data generated by mobility are usually associated with mobile users' personal privacy information. This paper addresses this issue and proposes an approach proactively protect financial customers' privacy information using Attributed-Based Access Control (ABAC) as well as data self-deterministic scheme. The proposed approach is called Proactive Dynamic Secure Data Scheme (P2DS), which aims to guarantee the unanticipated parties cannot reach the privacy data. There are two main algorithms supporting the proposed scheme, which are Attribute-based Semantic Access Control (A-SAC) Algorithm and Proactive Determinative Access (PDA) Algorithm. The main contributions of this paper have three aspects. First, we propose a semantic approach for constraining data accesses. Second, we propose a user-centric approach that proactively prevents users' data from unexpected operations on the cloud side. Finally, the proposed scheme has a higher-level secure sustainability since it can deal with dynamic threats, including the emerging and future hazards. We have examined that our proposed scheme had a quality performance matching our expected goal.

3. **A Patel, M Taghavi, K Bakhtiyari, JC JúNior** depicts that, the distributed and open structure of cloud computing and services becomes an attractive target for potential cyber-attacks by intruders. The traditional Intrusion Detection and Prevention Systems (IDPS) are largely inefficient to be deployed in cloud computing environments due to their openness and specific essence. This paper surveys, explores and informs researchers about the latest developed IDPSs and alarm management techniques by providing a comprehensive taxonomy and investigating possible solutions to detect and prevent intrusions in cloud computing systems. Considering the desired characteristics of IDPS and cloud computing systems, a list of germane requirements is identified and four concepts of autonomic computing self-management, ontology, risk management, and fuzzy theory are leveraged to satisfy these requirements.

4. **P Jain** depicts that, Cloud computing is model which uses combine concept of "software-as-a-service" and "utility computing", provide convenient and on-demand services to requested end users. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, thus infecting the entire cloud and affects many customers who are sharing the infected cloud. This paper firstly lists the parameters that affect the security of the cloud then it explores

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, and infected application and security issues. It also discuses some tips for tackling these issues and problems.

5. F Lombardi, R Di Pietro depicts that, Cloud computing adoption and diffusion are threatened by unresolved security issues that affect both the cloud provider and the cloud user. In this paper, we show how virtualization can increase the security of cloud computing, by protecting both the integrity of guest virtual machines and the cloud infrastructure components. In particular, we propose a novel architecture, Advanced Cloud Protection System (ACPS), aimed at guaranteeing increased security to cloud resources. ACPS can be deployed on several cloud solutions and can effectively monitor the integrity of guest and infrastructure components while remaining fully transparent to virtual machines and to cloud users. ACPS can locally react to security breaches as well as notify a further security management layer of such events. A prototype of our ACPS proposal is fully implemented on two current open source solutions: Eucalyptus and OpenECP. The prototype is tested against effectiveness and performance. In particular: (a) effectiveness is shown testing our prototype against attacks known in the literature; (b) performance evaluation of the ACPS prototype is carried out under different types of workload. Results show that our proposal is resilient against attacks and that the introduced overhead is small when compared to the provided features.

III. RESEARCH GAP

Security Issues in IaaS: with IaaS the developer has better control over the security as long as there is no security hole in the virtualization manager. Also, Attanasio and Gajek et al (2007) discuss that though in theory virtual machines might be able to address these issues but in practice there are plenty of security problems. The other factor is the reliability of the data that is stored within the provider's hardware. Due to the growing virtualization of 'everything' in information society, retaining the ultimate control over data to the owner of data regardless of its physical location will become a topic of utmost interest. Descher et al (2009) indicates that to achieve maximum trust and security on a cloud resource, several techniques would have to be applied. The security responsibilities of both the provider and the consumer greatly differ between cloud service models. Amazon's Elastic Compute Cloud (EC2) (Amazon 2010) infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. Adrian et al (2009) describes that the consumer, in turn, is responsible for the security controls that relate to the IT system including the OS, applications and data. To promote greater security as well as customer confidence in and adoption of Cloud Computing architectures and services, there are some recommendations by security analysts. They are the following. All management and control interactions between Cloud Providers and Cloud Customers must take place over secure channels that utilize standards-based protocols and support authentication, authorization, confidentiality, integrity and accountability. Without these basic protections, the provider and its customers are vulnerable to unwanted disclosure, impersonation, identity and/or service theft or misuse, and repudiation. These protections must exist for Customers when they access the services offered by the Cloud Provider for the purposes of signup, provisioning, payment, monitoring, and other management and control related functions. Providers should move to offer strong mutual authentication mechanisms for their Customers in order to provide greater protection for Customer accounts. Given that management and control interactions have very real financial impact, it is critical that these mechanisms be protected by more than just a simple password. If a Provider must use password authentication to grant Customer access to account, control and management functions, then the Provider should take steps to ensure that the passwords chosen are strong and passed only over encrypted channels. Today, very few Providers enforce strong password composition rules that are otherwise in effect throughout modern enterprises. Additional access monitoring to detect and prevent fraudulent access is also advised. By default, Resources allocated by the Provider shall not interact with any other Resource not owned by the same Customer. This includes (physical or virtual) compute, networking and storage resources, (virtual) applications and services, and other related objects. The Customer to which a Resource is assigned is called its "owner". This recommendation is necessary to ensure that objects that exist in the Cloud are not inadvertently exposed to unauthorized consumers. The Provider may offer a mechanism to allow Customers to manage access to the Resources that they own thereby allowing other Customers or Cloud Consumers to access their content and services. A default denies policy is recommended regardless of what other access configurations may be possible. If some aspect of a Resource is to be shared between multiple Customers, the Provider must implement security controls that ensure that the intended owner of the object is compartmentalized from the rest of the population. The

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Provider must enforce sufficient protections preventing unauthorized access, manipulation or destruction of objects under their care. That is, a Provider must be able to demonstrate that security protections are in place preventing Customer A from accessing, manipulating or destroying Resources associated with Customer B. Ideally, these controls will be validated using a trusted third party who will act as an auditor. The Provider should make available (sanitized) audit reports to Customers as requested. Providers must implement controls preventing the accidental or malicious access, use, modification or destruction of Resources under their care. As Providers have physical access to the underlying infrastructure, they can circumvent many common security protections. Consequently, it is imperative that Providers implement controls that restrict their own employees' access to Resources. Further, all authorized access must be audited and regularly reviewed in order to promote accountability and ensure that actions are taken in accordance with their stated security policy the same is described as under:-

1. **Impact of deployment mode:** IaaS is prone to various degrees of security issues based on the cloud deployment model through which it is being delivered. Public cloud poses the major risk whereas private cloud seems to have lesser impact. Physical security of infrastructure and disaster management if any damage is incurred to the infrastructure (either naturally or intentionally), is of utmost importance. Infrastructure not only pertains to the hardware where data is processed and stored but also the path where it is getting transmitted. As pointed out by Thomas Ristenpart et al (2009), in a typical cloud environment, data will be transmitted from source to destination through umpteen number of third party infrastructure devices.
2. **Security Policies**: It must be possible to resolve, define policies and enforce policies of security in support of access control, resource allocation and other decisions in a machine readable and consistent way. The policies defining method 15 should be robust that licenses and SLAs can be automatically enforced.
3. **Service Automation :** There must be an automated way to analyse and manage control flows of security and processes in support of security audits. This includes reporting any events that violate any policies of security or agreements of customer license.

IV. PROPOSED METHODOLOGY

To protect from the above mentioned vulnerabilities in cloud we proposed the hashing based digital certificated on as Shielding Virtualized Resource (SVR) under cloud using Augmented Protection Techniques (APT) enable to ensure that data theft or hacking should not happen and the resource should be protected from such deeds the proposed scheme is depicted in below diagram i.e. Figure 1.

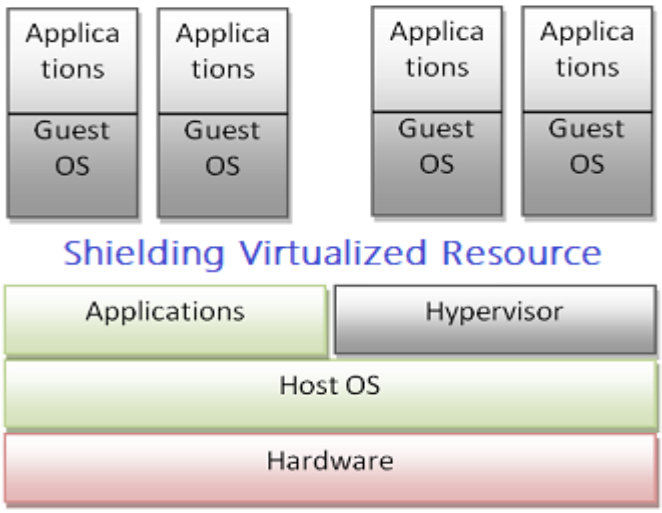

Figure 1. Shielding Virtualized Resource (SVR)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

REFERENCES

1. Secure attribute-based data sharing for resource-limited users in cloud computingJ Li, Y Zhang, X Chen, Y Xiang - Computers & Security, 2018
2. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry M Qiu, K Gai, B Thuraisingham, L Tao… - Future Generation - 2018.
3. An intrusion detection and prevention system in cloud computing: A systematic review A Patel, M Taghavi, K Bakhtiyari, JC JúNior.
4. Security Issues and their solution in cloud computing P Jain - … Journal of Computing & Business Research, 2012.
5. Secure virtualization for cloud computing F Lombardi, R Di Pietro - Journal of network and computer applications, 2011 - Elsevier
6. Addressing cloud computing security issues D Zissis, D Lekkas - Future Generation computer systems, 2012
7. Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing environments," in Proceedings of Natural Sciences and Engineering, Sweden, pp. 2-4, 2010.
8. Cong Wang,Qian Wang,Kui Ren Ninig Cao and Wenjing Lou"Towards Secure and Dependable storage services in cloud computing",IEEE Transaction on service computing,vol 5,no 2,june 2012
9. Dalia Attas and Omar Batrafi " Efficient integrity checking technique for securing client data in cloud computing", October 2011
10. Jaison Vimalraj.T,M.Manoj"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", March2012
11. Kayalvizhi S,Jagadeeswari "Data Dynamics for Storage Security and Public Auditability in Cloud Computing", February 10, 2012
12. Metri P. and Sarote G., "Privacy Issues and Challenges in Cloud computing," International Journal of Advanced Engineering Sciences and Technologies, vol. 5, no. 1, pp. 5-6, 2011.
13. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012
14. D. Srinivas "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011
15. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing tokeep online storage services honest," in Proc. Of HotOS'07., CA USA: USENIX Association, 2007, pp. 1–6.
16. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality ofService (IWQoS '09), pp. 1-9, July 2009
17. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-Security-risks-853
18. Cachin, C., Keidar, I., and Shraer , A. Trusti ng the cloud. ACM SIGACT News, 20:4 (2009), pp. 81- 86.