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. 7, Issue 5, May 2019

Shielding Virtualized Resource in Cloud Computing

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

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

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

ABSTRACT: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. A key component of Cloud computing is virtualization. While Cloud computing is not equivalent to virtualization, virtualization technology is heavily used to operate a cloud environment. In a virtual environment, one host that previously ran a single Operating System now has the ability to run multiple guest operating systems as virtual machines. Virtual machines can be created quickly and easily in a cloud environment. The infrastructure is invisible or abstracted from the consumer. The hypervisor is the software that manages communications between the physical server's memory, CPU or processing capability and the virtual machines that are running. The hypervisor allows virtual machines to be quickly provisioned or decommissioned. The down side to this virtual world is an increased opportunity for hackers to exploit vulnerabilities. The attack surface has increased because vulnerabilities may not only exist in the physical equipment but vulnerabilities may exist in the virtualized environment. Consequently, we proposed the scheme to ensure the secured shielded virtual resource in cloud computing using digital signatures by using hashing algorithm.

KEYWORDS: Shielding Virtualized Resource, Cloud Computing, Cloud Security, Cryptography, Security, Intrusion Detection System, Denial of Service, Distributed Denial of Service, Remote to Local

I. INTRODUCTION

Data placed in the Cloud will be accessed through Application Programming Interfaces (APIs) and other interfaces. Malfunctions and errors in the interface software, and also the software used to run the Cloud, can lead to the unwanted exposure of users data and impugn upon the data's integrity. For example a (fixed) flaw in Apache, a popular HTTP server, allowed an attacker to gain complete control over the web server. Data exposure can also occur when a software malfunction affects the access policies governing users data. This has been seen in several Cloud based services in which a software malfunction resulted in which a users privacy settings were overwritten and the user data exposed to non-authorised entities]. Threats can also exist as a result of poorly designed or implemented security measures. If these measures can be bypassed, or are non-existent, the software can be easily abused by malicious entities. Regardless of the threat origin, APIs and other interfaces need to be made secure against accidental and malicious attempts to circumvent the APIs and their security measures.

Virtualization Issues: The underlying virtualization architecture allows IaaS service providers the ability to host several machine images on a single server. Therefore practical attacks on such services, concentrating on Amazon EC2. First, the authors showed that they could map the internal structure of the cloud, allowing them to determine if two virtual machines were co-resident with each other i.e. were running on the same physical machine.

Data Loss or Leakage: Demonstrated that they were able to, purposefully, add a virtual machine to the cloud so that it was co-resident with another machine. Finally, the authors were able to show that once a machine was co-resident, they would be able to launch several attacks that would allow them to learn information regarding CPU cache use, network traffic rates and keystroke timings.

Service Aggregation: Aggregated services offer services based upon the functionality offered by existing services. Often aggregated services offer the combined functionality of existing services allowing for rapid service construction.

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. 7, Issue 5, May 2019

However, service aggregation presents consumers with several interesting problems. Data is now being shared across multiple service providers whose privacy policies will also subject to change. Under whose privacy policy is the data governed by, how to combine the two policies? Furthermore, service aggregation can occur in an ad-hoc and rapid manner implying that less stringent controls could have been applied to the protection of data, increasing the likelihood of a problem.

Data Loss or Leakage: Although insecure APIs can lead to data loss or the unwanted exposure of information, consumers can also loose their information through other means.

Availability Issues: Availability issues are when user's data is made inaccessible to the consumer. The data has been made unavailable. Such a lack of availability can be a result of access privilege revocation, data deletion or restricting physical access to the data itself. Availability issues can be attributed to an attacker using flooding based attacks. For example, Denial of Services attacks, attempt to flood the service with requests in an attempt to overwhelm the service and cease all of the services intended operations.

II. RELATED WORK

A Patel, M Taghavi, K Bakhtiyari, JC Junior [1] 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.

P Jain [2] 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 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.

F Lombardi, R Di Pietro [3] 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 again st 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.

D Zissis, D Lekkas [4] depicts that, the recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of 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. 7, Issue 5, May 2019

effectiveness of traditional protection mechanisms. As a result the aim of this paper is twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

Comparison Of Various Security Algorithms:-

Algorithms / Parameters	DES	3DES	AES	Blowfish	RSA	Diffie-Hellman
Encryption technique	Asymmetric key	Asymmetric key	Asymmetric key	Asymmetric key	Symmetric key	Symmetric key
Keys used	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Different key used for encryption and decryption.	Key exchange.
Throughput	Lower than AES.	Lower than DES.	Lower than blowfish.	Very High	High	Low
Encryption ratio	High	Moderate	High	High	High	High
Key Lengths	56 bits.	112 to 168 bits.	128,192 or 256 bits.	32 bits to 448 bits.	>1024 bits	Key exchange management.
Rounds	16	48	10,12,14	16	1	56
Tunability	No	No	No	Yes	Yes	Yes
Security against	Brute force attack	Brute force, choosen-plain text, known plain text.	Chosen plain, known plain text.	Dictionary attacks	Timing attacks.	EavesDropping.
Flexibility support	No	Yes	Yes	Yes	Yes	No
Modification	No,DES does not support any modification	The key size is increased from 56 to 168 bits	128,192 or 256,Its structure was flexible to multiples of 64	Key length in blowfish should be multiples of 32	Key length in RSA algorithm can be 256 ,512,1024,2048, 4096 bits	No modification in key length.
Created by	IBM	IBM	Vincent Rijmen , Joan daeman	Bruce Schiener	Ron Rivest,Shamir & leonard Adleman	Whitfield diffie, Martin Hellman
Year	1970	1978	1978	1993	1978	2002
Structure of the Algorithm	Feistal structure	Feistal structure	Feistal structure	Feistal structure	Feistal structure	Tree based
Cloud Compatibility	Yes (Generally not used)	Yes	Yes	Yes	Yes	Yes
Algorithm used in Cloud	Not used in Cloud (it is prone to many attacks and easy to break)	Not used in Cloud (it is prone to many attacks and easy to break)	Google Drive, OneDrive, Dropbox	Mozy Backup, Foopchat, GigaTribe	Amazon web Services, RSAWeb	CurveCP

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. 7, Issue 5, May 2019

III. PROPOSED ALGORITHM

Under the proposed scheme we will originate the next dimension of Digital Certificates Patterns using Bitwise Random Patterns based on hashing model where two or more Shielding Virtualized Resource can communicate within itself (intra) or outside the resource (extra) using this digital certificates. A computerized authentications or advanced testaments plot is a scientific plan for showing the validity of an advanced message or archive. A substantial computerized endorsement gives a beneficiary or recipient motivation to trust that the message was made and sent by a known or confided in sender. Advanced certificates are generally utilized for programming conveyance, budgetary exchanges, electronic casting a ballot and in different circumstances where it is imperative to distinguish falsification or altering. Alongside verification, advanced certificates additionally have the property of uprightness, which guarantees that the got messages are not controlled or adjusted or changed amid the transmission of message from sender to recipient. Because of its significance and so as to utilize it in different sorts of utilizations, numerous kinds of computerized declarations plot have been proposed, for example, Dynamic Key Generation, bunch authentications, unquestionable endorsements and so on. In the Dynamic Key Generation conspire, there are three members, in particular, the requester, the underwriter and the verifier. In the first place, the requester blinds the message and sends the visually impaired message to the underwriter. Subsequent to accepting the visually impaired message, the endorser can utilize a private key to sign it and send the Dynamic Key Generation back to the requester. When the requester gets it, user un-visor the Dynamic Key Generation to acquire the endorsements and sends it to the verifier. After the verifier gets the declarations, he/she can utilize an open key to confirm the authenticity of the authentications. The principle contrasts between the computerized declarations and the Dynamic Key Generation are as per the following.

(1) In the Dynamic Signatures Generation scheme, the content of the message should be visually impaired to the signer.

(2) When the public knows the message-certificates pair, the signer should not be able to trace the Message-certificates pairs.

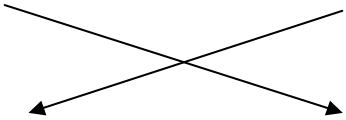
	Shielding Virtualized Resource 1..n	**Security Model**	**Shielding Virtualized Resource 2..n**
Obtain the Series of Numbers	$2^{\wedge 32}$		x^2-(32)=0
Generate Exponentials	k ^ m, *p* ^m	Exponentials	k = x, *p* =x
Picks the number from exponentials	t = 8	random number	t = 6
Each evaluate k^n exp *p*	6^8 exp 7 = 36		6^6 exp 17 = 35
Exchange the values from sandbox based on cipher values	C = 36 *D* = 35		*D* = 35 *C* = 36
Every at that point raises the esteem they got to the intensity of their mystery *n* Bit *p*.	B^n ^ *p* = BIT 36^8 xor 35 = x	Infuse sandbox composition	A^n ^ *p* =BIT 36^6 mod 37 = 1
The outcome is a common mystery key.	Cipher Value	Digital Certificate	Cipher Value

Table 1 : Pseudo Code Of Proposed Scheme

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. 7, Issue 5, May 2019

IV. SIMULATION AND RESULTS

Above Signatures Scheme is a sort of Digital Certificates that uses security endeavors to ensure the organized correspondence between two to more social events, resources, and frameworks using Shielded Virtual Resource in Cloud Computing. The guideline point of convergence of cutting edge confirmation or imprints is ensuring the steady quality and flexibility of data correspondence among resources and frameworks. This investigation was revolved around hash-based encryption systems, therefore, we have used sandbox based substitution with replacing the incorporating descriptor key inside in the encryption structure, which ensures the flexibility of mechanized stamps and better execution. Additional future work is to put our new proposed arrangement estimation into a veritable firmware and framework correspondence structures with security. Regardless of the way that we have separated how the proposed computation improves the whole execution of security systems, the data used in our examination is produced and may not be illustrative of this present reality circumstances. We mean to complete a strong storing structure and use diverse arranging computations in it to find how our booking figuring can improve this present system's presentation and proposed plan can be used in firmware as extended security using the automated underwriting or checks for assessing reason.

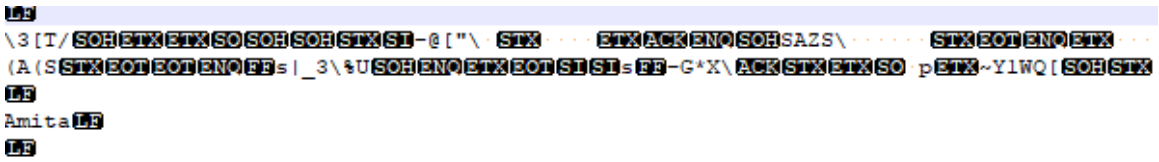


Figure1: Cipher Data as Digital Signatures Generated using Proposed Scheme

Comparison Analyses of Proposed Algorithm					
Characteristics	**Blow Fish**	**RSA**	**DES**	**AES**	**Proposed**
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Size	32-448 bits	1024 bits	56 bits	128,192,256 bits	256 bits
Initial Vector Size	64 bits	1024 bits	64 bits	128 bits	64 Bits
Security	Users and providers are secure	Only users are secure.	Users and providers are secure.	Users and providers are secure.	Users and providers are secure.
Memory Usage	Execute in lower than 5 kb	Highest memory usage algorithm	Higher than AES	Low RAM	High Memory
Scalability	Scalable	Not scalable	Scalable	Scalable	Scalable
Information Encryption Capacity	Lower than AES	Encryption of small data	Lower than AES	Encryption of huge amount of data	Encryption of huge amount of data
Execution Time	Lower than AES	Maximum time	Same as AES	Faster than DES/RSA	Faster than rest
Key Used	One key for encryption and decryption.	Private key for decryption. Public key for encryption	One key for encryption and decryption.	One key for encryption and decryption.	Two key for encryption and decryption.

Table 2: Comparative Analysis between various Security Algorithm and Proposed Scheme

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. 7, Issue 5, May 2019

To test the proposed scheme we have conducted experiments that apply both algorithms to evaluate the performance:-

Machine No.	CPU Speed	L2 Cache	Cores	RAM	Bit	CPU Description	Virtual Machine	Memory
1	2.0 GHZ	2.4 MB	4	4 GB	32	i3 Intel	YES	4 GB
2	2.4 GHZ	4.2 MB	4	8 GB	64	i3 Intel	YES	8 GB

Table 3: Infrastructure used for Measuring and evaluating the performance proposed Algorithm in above scheme.

Machine	CPU Time in Seconds
1	1.127
2	0.723

Table 4 : CPU Time in Seconds using under Different Virtual Resources

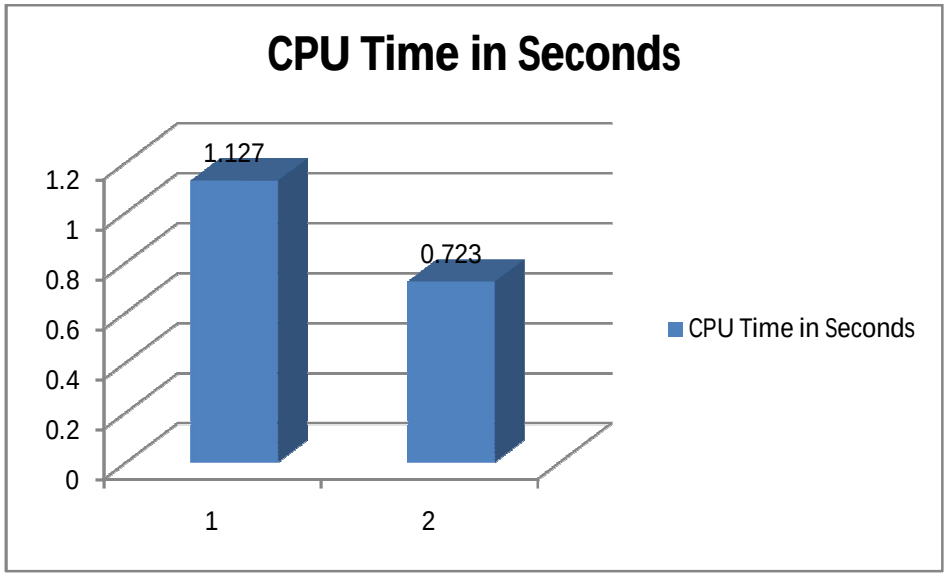


Chart 1: Bar Graph Depicting Time Utilized By Proposed Algorithm In Two Different Virtual Machines.

V. CONCLUSION AND FUTURE SCOPE

Distributed cloud computing offers another method for administrations by re-organizing different assets and giving them to clients dependent on their requests. It likewise assumes an essential job in the cutting edge versatile systems and administrations using Shielding Virtualized Resource in Cyber-Physical and Social Computing (CPSC). Putting away information in the cloud incredibly diminishes the capacity weight of clients and brings them to get to comfort, in this manner it has turned out to be a standout amongst the most critical cloud administrations. Be that as it may, cloud information security, protection and trust become a pivotal issue that impacts the achievement of distributed computing and may block the advancement of security risks. To begin with, putting away information at cloud expands the danger of information spillage and unapproved get to. Second, cloud server farms are turning into the objectives of assaults and interruptions, which challenge cloud information security. Third, information the board tasks, for example,

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. 7, Issue 5, May 2019

information stockpiling, reinforcement, relocation, cancellation, update, pursuit, question, .and access in the cloud may not be completely trusted by its proprietors. Information proprietors ought to ideally review the dependability of information management. Any wellsprings of interruptions and assaults ought to have the capacity to be identified and followed. The above necessities really present a major security challenge, particularly for enormous information stockpiling and the board. Fourth, information procedure and calculation in the cloud could unveil the security of information proprietors or related substances to unapproved equalities. Step by step instructions to approve cloud information process and secure information handling result is another fascinating and significant look into the subject. Cloud information security, protection, and trust are without a doubt getting to be key issues that sway the achievement of distributed computing. Cryptography is broadly connected to guarantee information security, protection, and trust in distributed computing. In any case, existing arrangements are as yet flawed and inefficient, in this manner unreasonable. Putting away encoded information in the cloud makes it difficult to perform evaluating the information the executives in spite of the fact that the danger of security spillage is incredibly diminished. Key administration for access control and disavowal presents extra calculation and correspondence costs. What's more, activities, for example, combination, total, and mining on scrambled information are as yet illogical to be sent because of high calculation multifaceted nature and indecency. Cryptography in distributed computing guarantees numerous novel arrangements and in the meantime, numerous difficulties are yet to be survived. This extraordinary issue expects to unite specialists and professionals to evolve about different parts of cryptography and information security in distributed computing, investigate key speculations, explore innovation empowering agents, create significant applications and advance new answers for conquering real difficulties in this energizing examination region and to define flexible secured standards using cryptography.

For future reference, the virtual machines can incorporate the proposed scheme as an integral part of the cloud ecosystem manufactured by the various esteemed organization so the better-secured communication can be established based on de-facto standards.

REFERENCES

1. A Patel, M Taghavi, K Bakhtiyari, JC JúNior, An intrusion detection and prevention system in cloud computing: A systematic review. IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012
2. P Jain , Security Issues and their solution in cloud computing, Journal of Computing & Business Research, 2012.
3. F Lombardi, R Di Pietro, Secure virtualization for cloud computing Journal of network and computer applications, 2011 - Elsevier
4. D Zissis, D Lekkas , Addressing cloud computing security issues - Future Generation computer systems, 2012
5. Robert H. Deng, School of Information Systems, Singapore Management University, 80 Stamford Road, Singapore 178902.
6. 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
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.