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 5, May 2018

Protecting Virtualized Infrastructure in Cloud using Amplified Security Techniques

Priyanka[1], Deepika Goyal [2]

M. Tech. Student, Department of Computer Science & Engineering, Advance Institute of Technology and Management at Palwal, Haryana, India[1]

Assistant Professor, Department of Computer Science & Engineering, Advance Institute of Technology and Management at Palwal, Haryana, India[2]

ABSTRACT: Cloud computing has risen as maybe the most sizzling advancement in data innovation. Regardless of the greater part of the consideration that it has gathered, existing investigations centre solely around the issues that encompass information protection without investigating distributed computing design and arrangement suggestions. This plan offers an underlying exploratory investigation toward that path to guaranteeing the Protecting Virtualized Infrastructures (PVI). Along these lines the design ramifications of distributed computing for get to systems administration (concentrating on transmission capacity, dependability, nature of administration, and omnipresence) and server farm interconnectivity (concentrating on data transfer capacity, unwavering quality, security and protection, control over steering approaches, institutionalization, and metering and instalment). PVI must be guarantee the cloud records exchanges without irritating the adjacent security and asset respectability of named as raw numbers or records and to acquaint no additional online weight with the cloud sourcing, particularly to information vaults and documents. Nonetheless, under this plan, the inspiration is to give the intensified security strategy utilizing XOR/BITWISE based hashing calculation for open reviewing of data and cloud security in distributed computing and offer a privateers holding security convention, i.e., our plan helps an outer clients or non trusted assets or gatherings not get to the crucial and admired data over the mutual cloud asset and foundation. Subsequently, this plan guarantees that in the intra cloud if two gatherings or assets convey or play out any exchanges the PVI is mindful to give the computerized signature duplicate to be related for inspecting reason and to guarantee no thusly mal-correspondence or mal-exchanges is happening.

KEYWORDS: Cloud Computing, Cloud Security, Cryptography, Protecting Virtualized Infrastructures (PVI).

I. INTRODUCTION

Cloud computing is a well-known technology nowadays. Companies like Amazon, Google and Microsoft are enhancing the services provided for their users. Security issue is a barrier for users to adapt into cloud systems. Cloud service providers have been concerned of the non-adequate security measures and aspects like data integrity, control, audit, confidentiality, availability should be added. Privacy acts which are in use are out of date and are not protecting the private information of user in the cloud environment since they are not applicable to three parties like cloud service user, cloud service provider, cloud provider. Privacy issue becomes worse when applications are in multiple locations. Cloud computing offers storage of data with scalable power of processing that elevated IT to newer limits with low capital expenditure. If one runs the application in public domain or beyond firewall then there arises security consciousness and concerns. In cloud computing the consumers can access resources online at any time through Internet without managing the original resources issues like physical and technical management. Cloud computing resources are scalable and dynamic. The significant difference in cloud security is enterprise control loss opposed to particular technical challenge. In cloud based application access control is important. The application of security, infrastructure and platform is under provider's control.

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 5, May 2018

Vulnerability in virtualization: Virtualization is one of the main components of a cloud. But this poses major security risks. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization which is not met completely in today's scenario. The other issue is the control of administrator on host and guest operating systems. Current Virtual Machine Monitor (VMMs) do not offer perfect isolation. Many bugs have been found in all popular VMMs that allow escaping from VM. Virtual machine monitor should be 'root secure', meaning that no privilege within the virtualized guest environment permits interference with the host system. Some vulnerability has been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges. For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege. Another example would be the vulnerability in Xen caused due to an input validation error in tools/pygrub/src/GrubConf.py. This can be exploited by 'root' users of a guest domain to execute arbitrary commands in domain 0 via specially crafted entries in grub.conf when the guest system is booted. A perfection of properties like isolation, inspection and interposition is yet to be completely achieved in VMMs.

Security and Trust: Knowing that there are possibilities for security and trust issues on both sides of the cloud customer-provider relationship allows us to separate what each side should do to build a secure system. This is a paradigm shift from a traditional model where software and computing resources were both provided in-house. While in the internal model, system and network security was mostly handled by the system and network engineers, so even an insecure piece of software would only be accessible to people within the company and particularly offensive software could be removed with ease. In the cloud model, the network engineers are not concerned with these problems and it is up to the cloud customer to protect their data.

Layers and obligations for cloud security: Layers and obligations for cloud security : The broadness of cloud computing and the ramifications of security in the cloud make this a difficult problem to discuss with generalizations because each service provider-customer pair may have different contractual obligations

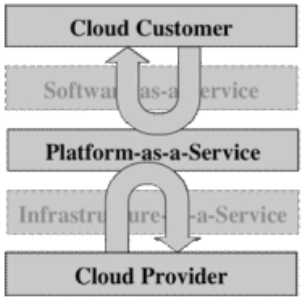

Fig 1. Example of the separation of security concerns between a PaaS customer and provider. Note that there is some overlap where the two meet

Authentication, access control and authorization: Unlike traditional client-based software development using tools such as Microsoft Visual Studio, PaaS offers a shared development environment, so authentication, access control, and authorization mechanisms must combine to ensure that customers are kept completely separate from each other. A strong and effective authentication framework is essential to ensure that individual users can be correctly identified without the authentication system succumbing to the numerous possible attacks. Attack vectors on cloud-based environments are similar to those encountered in noncloud environments and include: Impersonation Phishing and social engineering attacks Brute force (dictionary) attacks Password reset attacks Two-factor authentication such as smartcards or biometric mechanisms can provide increased protection from these attacks but at the expense of greater complexity and longer provisioning cycles. In most cases, PaaS vendors still rely on user name and passwords for authentication and then implement a mechanism that provides access control to data and application-level authorization based on verification of these credentials. They might use some technique for enhancing the security 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. 6, Issue 5, May 2018

authentication process, such as only requesting three characters from the password or answering a "secret question" or identifying a pre-agreed upon image. A major difference between PaaS cloud solutions and on-premise solutions is that the authentication mechanism may be externalized and use a claim-based identities from one or more identity provider. When considering a PaaS vendor, the operational standards that they implement should be looked upon. What are their password complexity requirements and how do they protect credentials? Do they enforce changing passwords on a reasonable timescale? What do they do to prevent password compromise? If users are proposing moving to a cloud-based environment, users should require that the cloud vendor's security policies and procedures is at least as stringent as the users. Although users may be meticulous at choosing complex passwords for their cloud-based accounts, if the vendor does not enforce this requirement, then other customers may not be so rigorous at enforcement, which could degrade the vendor's overall security posture as a result of a successful attack on another customer's environment. Regardless of the authentication mechanism used, it is essential that end-to-end encryption applies to the logon sequence. Ideally, this authentication would be carried out by using a cryptographic hashing mechanism so that the password itself never exposed. Combined with cryptographic security is the requirement for rapid and effective provisioning and de-provisioning of accounts. Authorization permissions apply at the application level and provide confirmation that a user, computer, device or assembly has the required permission to carry out an operation. Usually, authorization is carried out through a roles-based framework, with user accounts assigned to roles. Role-based assignment ensures greater flexibility, as users can dynamically assign user accounts to different roles, so as users move around the organization, they automatically receive the rights they need to carry out their roles. With PaaS, users should establish the control that they will have over authorization permissions and the level of access that their service provider has. As users are being provided with an application platform rather than installing their own applications (as with IaaS), they will require a greater level of trust in their cloud provider to secure both the infrastructure and platform layers.

II. LITERATURE REVIEW

Virtualization and multi tenancy Virtualization and multi tenancy are two of the core technologies that enables CC to be used as we know it today. A traditional way of hosting applications and data storage involves running one operating system (OS) on one physical server. This traditional hosting method can also be used to create a functioning but inefficient cloud. This is achieved by linking multiple servers using a Virtual LAN (VLAN). This is secure but inefficient in the long term as a large part of the physical hardware available end up being unused. Virtualization was created in order to solve this efficiency problem. By using a Virtual Machine Monitor (VMM) a single physical server can host multiple instances of an OS. This means that a single server can utilise the available hardware power in a more efficient manner (Srinivasan, Sarukesi, Rodrigues, Manoj, & Revathy, 2012). The figure below is a basic illustration of a VMM running multiple instances of an OS using a virtualization layer. The virtualization layer is often known as hypervisor. There are two main ways of utilising this hypervisor to run virtual machines (VM). These are known as full virtualization and paravirtualization. The difference between them lies in how much of the OS needs to be emulated. A VM deployed using full virtualization has to emulate the BIOS and drives of the OS, in addition to the other functions. A VM using paravirtualization runs a version of the OS that has been modified to work without needing a BIOS or similar components (Mishra et al., 2013). 8 There are also two major architectures used to deploy virtual machines, hosted architecture and hypervisor architecture. The difference here stems from the way the hypervisor is handled by the server. In a hosted architecture the hypervisor is a platform that the host OS runs as a normal application. The application is then charged with the upkeep of the virtual machines. On the other hand a hypervisor architecture skips the OS and is instead run directly on the hardware. Depending on which deployment method and architecture used different security aspects apply (Mishra, Mathur, Jain & Singh, 2013). Multi tenancy is closely tied to virtualization. In short, multi tenancy allows several users to share computing resources with logical separation of the different users, a user in this case is a tenant of the system (Mishra et al., 2013). In the context of cloud computing, each VM can be considered a tenant. However multi tenancy is not limited to multiple VMs running on the same hardware. Applications can also be utilised in a way that allows multiple tenants to use them, while at the same time separating the different users from each other (Mishra et al., 2013). While virtualization and multi tenancy are core technologies needed for cloud computing to remain efficient and viable they introduce new security risks.

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 5, May 2018

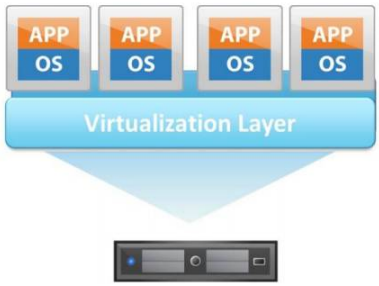

Fig.2. Descriptive image of Virtualization based on physical Operating System with CPU/Memory/Network Segregated Environment and Ecosystem thus forming the Infrastructure for Cloud Computing .

Security risks : While virtualization and multi tenancy are two staple technologies of CC they are still part of many security issues. As discussed in 2.4 the different types and different architectures for virtualization affect the security concerns related to these areas. However the difference between the different types of virtualization is less important than the overall cloud service type. It is also important to note that an emulated OS is still at risk from attacks that targets the traditional version of the OS. For instance a virtual machine running Windows is still at risk from attacks that target normal Windows machines. It is also important to note that hypervisors are additive to the overall security risk (Mishra et al., 2013) As was just stated, normal security risks associated with operative systems still apply to virtual instances, however securing multiple virtual machines is more difficult. This stems from the fact that if one VM gets infected it can infect other VM since there is no need to bypass things such as network protocols, the infected VM is already inside the network. The infected VM can then perform VM to VM attacks or attacks against the hypervisor software (Mishra et al., 2013). Running an antivirus software on the hosted VMs is all well and good but ensuring they are all up to date simultaneously is not so easy. If just one instance of the antivirus software is forgotten all VMs hosted on that platform are at risk. One solution to this is to run an antivirus software on the underlying platform hosting the VMs. This antivirus would not be used to secure the platform itself, rather it would be used to monitor and secure all the data processed by the VMs. This means you only need to update one central antivirus in order to secure all the tenants on that physical server. Aside from this it also means that a virus attacking a VM will have a harder time affecting the overall antivirus system, since it resides outside the infected VM (Tari, 2014). Another issue that might have a very severe negative impact on the organisation using a cloud computing solution is data leakage. Data leakage occurs due to the shared resources used by the VMs. These can have the form of cache based attacks or RAM based attacks (Tari, 2014). These attacks occurs since both the shared cache and RAM does not automatically flush upon completion of a computing task. This means a infected VM can recreate data based on the information left in the shared resources. In order to combat this the hosting platform can inject ‘noise’ into the cache in order to flush if from any remaining information left behind by a VM (Tari, 2014). To combat the RAM based attacks it is necessary to restrict a VMs ability to lock the memory bus. Both of these solution requires no expensive hardware modifications but can simply be introduced by adding software. The risks associated with multi tenancy described above have slightly different implications depending on which service model is being used. While the above mentioned solution with flushing the cache and preventing RAM bus locking works on all service models it is often better to prevent the issue from occurring in the first place. This is done by isolating the tenants from each other. In an IaaS environment this would mean isolating the data storage and processing resources. In a PaaS environment the isolation focus should be on isolating API calls as well as running services. In a SaaS environment the focus should instead be on isolating the transactions carried out on the same instance by different tenants. (Behl & Behl, 2012) 15 Regardless of the isolation degree chosen a user should never be fully aware of the exact server location for their data. While general information such as the country or region level is fine preventing the user from knowing the exact location decreases the risk of other malicious users learning the location. This means that multi tenancy attacks that rely on gaining access to a VM on the same physical server as the target will be much harder to achieve (Bouayad, Blilat, El Houda Mejhed, & El Ghazi, 2012). For instance, a cache based attack cannot be used if the target VM is in another geographical location. While isolation is a good solution it is important to note that it might mean less efficient resource sharing, this increases the cost and reduces the flexibility of cloud computing. An organisation must therefore carefully consider the cost and

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 5, May 2018

benefit of increased isolation. While some data might be considered sensitive enough to warrant full isolation that is not necessarily the case for all the data used by the organisation.

III. PROPOSED METHODOLOGY

The proposed Protecting Virtualized Infrastructure in Cloud using Amplified Security Techniques under the scheme will ensure confidentiality, integrity, authentication and non-repudiation. Data encryption/decryption is made using the generated key of asymmetric key algorithm. Due to his high speed characteristic, the advances encryption standard is used. Under the proposed scheme secret key transmission is encrypted using the algorithm which will protect virtual infrastructure in cloud using amplified security technique because the practice has proved that this technique successfully faces all the threats. The respective public key is used for the encryption activity and the reception advanced private key is used to decrypt the advanced encryption secret key will depict the assurance of authentication and non-repudiation will be the usage of digital signature with hash function based on bitwise notion.

Steps to complete the full process of proposed scheme encryption/decryption technique are defined as follows:

Encryption process

i. Get the data to be encrypted
ii. Generator advanced encryption standard based asymmetric key
iii. Encrypt data using respective asymmetric key
iv. Encrypt private key using public key (A)
v. Create signature using hash function and inculcate the private key (B)
vi. Sign advance virtual infrastructure using Private Key (B) and generate the digital certificate.

Decryption process

i. Verify signature using public key(B) and hash function of advanced encryption standard key encrypted notion.
ii. If signature verified, virtual infrastructure using Private Key (B) key using private key (A)
iii. If asymmetric key decrypted use it to decrypt data
iv. Get the data encrypted
v. Decrypt data using asymmetric Key
vi. Get Data decrypted

Pseudo Code

Step 1. Choose an arbitrary sequence of at least 64 bit and call it large Numbers. Let the length of Numbers in bits.

Step 2 Compute U = [SEED mod Long [(SEED+ 1) mod 2 n].

Step 3. Form q from U by setting the most significant bit (the 2159 bit) and the least significant bit to 1. In terms of Boolean operations, q = U OR 2159 OR 1. Note that 2159 < q < 2160.

Step 4. Compute d, 1 < d < denominator (n) such that: key ≡ 1 (mod denominator (n))

Step 5. Vk (virtual key) = XOR[(Key + offset + k) mod 2g].

Step 6. Form Encryption and Decryption on Vk (virtual key) and via asymmetric key manual originated using xor hashes

The above mentioned scheme will work with 64 bit based XOR and Shift Substitution encryption to form and establish the secure communication among the transaction components and resources.

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 5, May 2018

IV. SIMULATION AND RESULTS

Below is the simulation wherein the proposed algorithm and research work is been inculcated in Mobile app which will communicate with Azure based cloud with security measures defined and amplified security come in exist-stance ensuring secured data communication over client and server in bidirectional manner

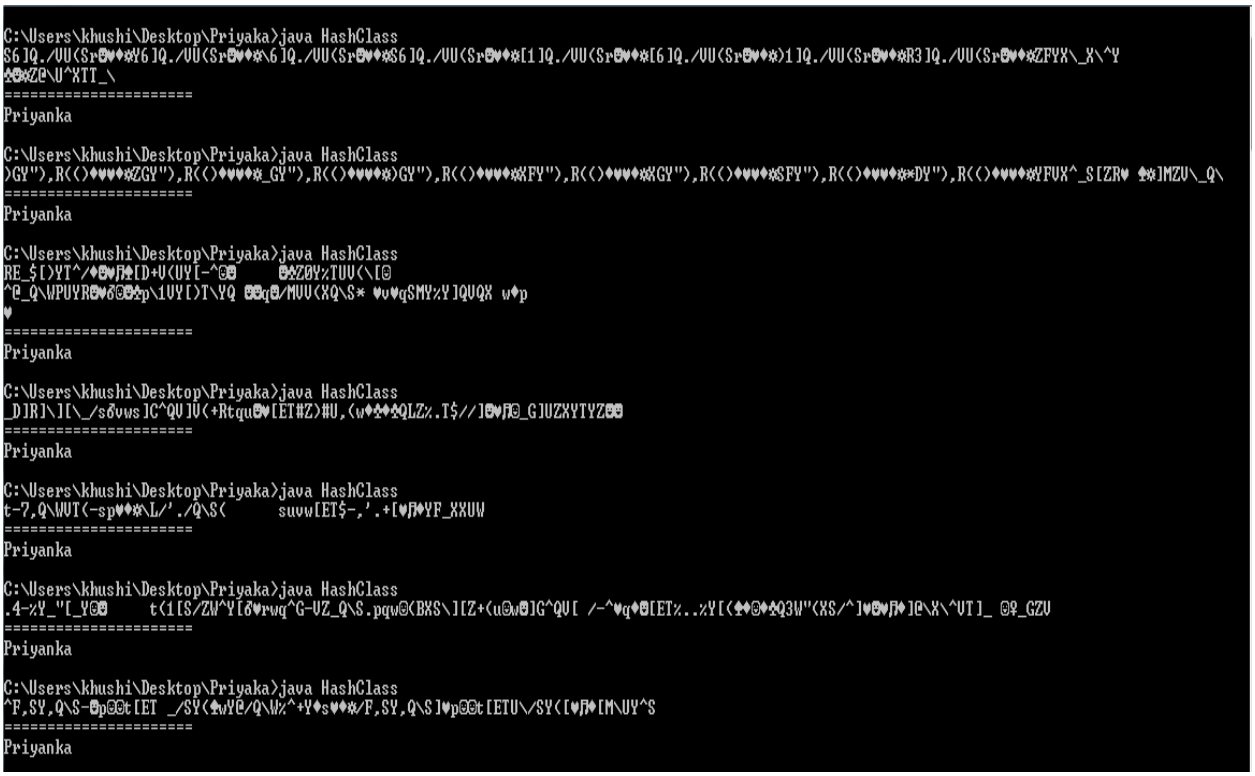

Fig.3 Indiscriminate 256 bit based signatures created using Protected Virtual Infrastructure Amplified Security Techniques based algorithm and forming Digital Certificate forming and Establishing the Secured and Trusted Communication Between Cloud Resources.

V. CONCLUSION AND FUTURE SCOPE

A strong cryptosystem together with a secure key encryption management system can ensure all security goals mentioned in conceptual framework of cloud computing will be covered. The protecting virtualized Infrastructure in cloud computing encryption technique enhances data security because the secret key used for data encryption and inverse for decryption itself is encrypted. For key security, asymmetric key is used to secure under the proposed secret key of data. To cover external party communication, proposed technique has considered authentication and non-repudiation using digital signature plus hash function along with public key. The result of the proposed encryption technique shows that data security requirement, processing time and key management are key elements to build secured cloud based cryptosystem. The main objective has been verified by building a Protecting Virtualized Infrastructure in Cloud using Amplified Security Techniques thus achieved.

For future scope The proposed scheme can be integrated as firm ware on cloud resources and the Virtual clusters can even communicate securely using 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. 6, Issue 5, May 2018

REFERENCES

1. Al-Anzi, F. S., Salman, A. A., Jacob, N. K., & Soni, J. (2014). Towards robust, scalable and secure network storage in Cloud Computing. In 2014 Fourth International Conference on Digital Information and Communication Technology and it's Applications (DICTAP) (pp. 51–55). http://doi.org/10.1109/DICTAP.2014.6821656 2
2. Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). Cloud computing: Security model comprising governance, risk management and compliance. In 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC) (pp. 1–6). http://doi.org/10.1109/ICDMIC.2014.6954232
3. Behl, A., & Behl, K. (2012). An analysis of cloud computing security issues. In 2012 World Congress on Information and Communication Technologies (WICT) (pp. 109–114). http://doi.org/10.1109/WICT.2012.6409059
4. Gregg, M. (2010). 10 Security Concerns for Cloud Computing. Retrieved February 28, 2012, from http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, Volume 4 Issue 2 , 39-51.
5. Boampong, P. A., & Wahsheh, L. A. (2012). Different Facets of Security in the Cloud. In Proceedings of the 15th Communications and Networking Simulation Symposium (pp. 5:1– 5:7). San Diego, CA, USA: Society for Computer Simulation International. Retrieved from http://dl.acm.org/citation.cfm?id=2331762.2331767
6. Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. International Journal of Information Security and Privacy, 4(2), 36-48. DOI: 10.4018/jisp.2010040103
7. Bouayad, A., Blilat, A., El Houda Mejhed, N., & El Ghazi, M. (2012). Cloud computing: Security challenges. In Information Science and Technology (CIST), 2012 Colloquium in (pp. 26–31). http://doi.org/10.1109/CIST.2012.6388058 Burkley, R. Virtualization Explained on a "Napkin." (2015). Retrieved June 9, 2015
8. Burkley, Chavan, P., Patil, P., Kulkarni, G., Sutar, R., & Belsare, S. (2013). IaaS Cloud Security. In 2013 International Conference on Machine Intelligence and Research Advancement (ICMIRA) (pp. 549–553). http://doi.org/10.1109/ICMIRA.2013.115
9. Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. In 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE) (Vol. 1, pp. 647–651). http://doi.org/10.1109/ICCSEE.2012.193 Cloud Security Alliance. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Retrieved 14 May, 2015, from https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
10. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. IEEE Security Privacy, 9(2), 50–57. http://doi.org/10.1109/MSP.2010.115 32 ISO/IEC TR 13335-1:2004 (2004) Information technology security techniques management of information and communications technology security part 1: concepts and models for information and communications technology security management. ISO/IEC, JTC 1, SC27, WG 1. Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066
11. Khalil, I. M., Khreishah, A., Bouktif, S., & Ahmad, A. (2013). Security Concerns in Cloud Computing. In 2013 Tenth International Conference on Information Technology: New Generations (ITNG) (pp. 411–416). http://doi.org/10.1109/ITNG.2013.127 Li, J., Li, J., Xie, D., & Cai, Z. (2015). Secure Auditing and Deduplicating Data in Cloud IEEE Transactions on Computers, PP(99), 1–1. http://doi.org/10.1109/TC.2015.2389960
12. Liu, M., Dou, W., Yu, S., & Zhang, Z. (2015). A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization. IEEE Transactions on Parallel and Distributed Systems, 26(3), 621–631. http://doi.org/10.1109/TPDS.2014.2314672
13. Mell, P., Grance, T. (2011). The NIST definition of Cloud Computing. (Artikelnr 800-145). National Institute of Standards and Technology. Retrieved 10 february, 2015, from http://www.nist.gov/itl/cloud/ M.E. Whitman, H.J. Mattord. (2009) Principles of information security (3rd ed.)Thompson Course Technology
14. Bowers K.D, Juels A, and Oprea A, "Hail: A high-availability and integrity layer for cloud storage," in Proc. of CCS'09. Chicago, IL, USA: ACM, 2009, pp. 187–198.
15. M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Computer Systems, vol. 20, no. 4,pp. 398-461,2002
16. Chang E.C, and Xu J, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.
17. 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.
18. 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
19. Dalia Attas and Omar Batrafi " Efficient integrity checking technique for securing client data in cloud computing", October 2011
20. Jaison Vimalraj.T,M.Manoj"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", March2012
21. Kayalvizhi S,Jagadeeswari "Data Dynamics for Storage Security and Public Auditability in Cloud Computing", February 10, 2012
22. 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.
23. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012
24. D. Srinivas "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011
25. 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.
26. 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
27. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-Security-risks-853
28. Cachin, C., Keidar, I., and Shraer , A. Trusti ng the cloud. ACM SIGACT News, 20:4 (2009), pp. 81- 86.