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 4, April 2018

A Survey on 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, Palwal, Haryana, India[1]

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

ABSTRACT: Cloud computing is the lengthy dreamed vision of computing as a utility, in which users can remotely access their information into the cloud with a purpose to experience the on-call for excessive quality programs and services from a shared pool of configurable computing resources, by way of facts outsourcing, users can be relieved from the weight of neighborhood records storage and maintenance, as a result, allowing public audit-ability for cloud records storage safety is of vital importance in order that customers transactions can audited to test the integrity of outsourced facts whilst wanted. To soundly introduce a powerful augmented security vide Protecting Virtualized Infrastructures (PVI), the subsequent essential necessities need to be met with the certain criteria i.e. PVI has to be capable of successfully audit the cloud records transactions without annoying the nearby security and resource venerability of termed as facts and figures or records and to introduce no extra online burden to the cloud sourcing, especially to data repositories and archives. However, under this scheme, the motivation is to provide the amplified security technique using XOR/BITWISE based hashing algorithm for public auditing of information and cloud security in cloud computing and offer a privateers retaining security protocol, i.e., our scheme helps an external users or non trusted resources or parties not access the vital and venerable information over the shared cloud resource and infrastructure. Consequently, this scheme ensures that in the intra cloud if two parties or resources communicate or perform any transactions the PVI is responsible to provide the digital signature copy to be associated for auditing purpose and to ensure no as such mal-communication or mal-transactions is occurring.

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

I. INTRODUCTION

With evolution of computers the life of people became more and more easily. They were able to keep their data on their devices, and started finding ways to make them accessible to others, for example say by using floppy, writable disks, which was followed by portable hard-disk, all these where expensive in their own way during their time. The data was very much private on personal devices like PC, laptops, mobile phones etc, therefore sharing data with others was considered to be expensive. As the world of computing got more advanced the ways for sharing data started becoming cheaper and cheaper. In recent years a new term has evolved called as Cloud which is provided by different provides, and which is nothing but facility or service of different resources or components like hardware, platform, storage's, software etc, and it is gaining importance because it frees the user from maintenance perspective on a investment of some money for the use of these services provided by cloud service providers. Now to provide such service to the client, naturally the provider's must have and rather can have access to resources which are used by the people/clients. Among the reasons these access are greatly required are for maintenance perspective. And definitely since billions of clients will be thinking about using such service, the infrastructure ought to be capable enough to support them, and these resources ought to be shared between billions of client's. Service availability, data

DOI: 10.15680/IJIRCCE.2018.0604056

synchronization between different devices, availability of data via any devices which includes browser facility make cloud more attractive. Now since the info gets shared or stored in providers area, the client gets worried about privacy of its data, although there are certain agreements and SLA which are agreed by cloud provider and client. Now although client have a platform to generally share the info, the expense of securing his/her data or in a nutshell making its data private gets costlier. The cloud term is of interest not just to the patient clients but to organizations as well. With organization as a consumer the concern of data security becomes multi-fold. Consider a typical example of small scale business that has different departments like HR, Finance, etc. We will focus on finance department since finance details of any business/company/organization are considered to be very sensitive and must be confidential.

Therefore if the little scale company thinks of using the cloud services like storage. Storing all account/finance related information in cloud stored makes it prone to leakage of sensitive information tell un-authorized users. Therefore securing this finance data is vital before it gets uploaded to the storage cloud, and just in case the data stored in cloud storage gets tampered there should be a method to verify the integrity of the data, moving further specific band of people should have access to this data which may be folks from finance department of client company or special auditors. Simply speaking the client must have the ability to store the data securely, verify the integrity of the data, share the data securely with specific band of people.

The clients concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You can find multiple means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes more tedious for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised. The aforementioned approaches burdens the client by which makes it additionally accountable for securing it data before storing it to the cloud storage.

Cloud computing is a method in which computing power, memory, infrastructure can be delivered as a service. A Cloud computing is a set of network enabled services, guaranteed QOS, inexpensive computing infrastructures on demand with an easy and simple access. Cloud security is an evolving sub-domain of computer security, network and information security [8]. Security in cloud can be implemented remotely by client where the data centres and protocols in the security objectives of the service provider are: confidentiality for securing the data access and transfer ii) audit ability for checking whether the security aspect of applications has been tampered or not. Dimensions of cloud security have been aggregated into three areas like security and privacy, compliance and legal issues.

A. Cloud software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The application is accessible from various client devices through web browser.

B. Cloud platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired application created using programming languages and tools supported by the provider.

C. Cloud infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, network and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating system and application.

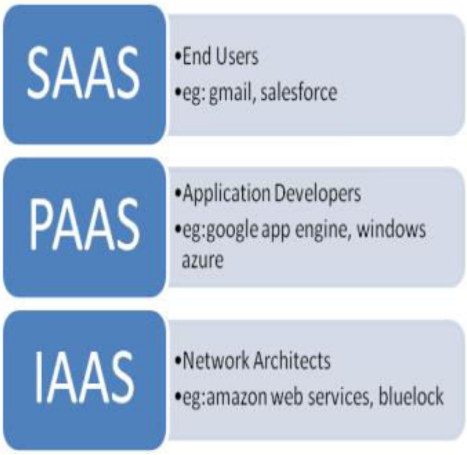

Figure 1.1: Various Cloud Services

Securing Virtual Machines on Private Cloud The new generation of processors can safeguard the hypervisor layer but not the VM layer. If the security in the VM layer is enhanced and is regulated by series of steps then it can be possible that both of these layers such as the hypervisor and the VMs can be secured by many attacks in the future. This section will describe an approach that can be adapted to secure most crucial and critical applications running on the most new generation of processors and hardware.
These applications can be categorized as:

1. Highly sensitive data
2. Security functions and administrative applications
3. Mission critical applications
4. Applications that are under regulatory controls

II. Literature Review

Especially, those researches have assessed such issues in a bottom-up approach to security where we are operating on little issues in the cloud computing arrangement that we hope will resolve the bigger issues and complexities of cloud security (Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010)[3]. Initially, they have shown that "how can we protect data, information and documents that can be published by a third party organization. After that, they have shown that how to protect co-processors and how they can be utilized to improve security. This research lastly discussed how XACML could be established in the Hadoop atmosphere and in protected federated query processing through SPARQL, Hadoop and MapReduce. Furthermore, there are many other security issues comprising security areas and features of Virtualization. Additionally, it is assumed that because of the issues and complexity of the cloud, it will be hard to attain an end-to-end security.

Though, the problems this research outlined and solution proposed are able to make sure additional protected operations yet a number of parts of the cloud fail. For a lot of systems and applications, we don't simply require data and information assurance however as well attainment of objectives. Thus, even if a rival has come into the system, the intention is to prevent the challenger so that the corporation has time to perform the desired tasks (Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010).

Moreover, (Chandran S. and Angepat M) state that cloud computing is probable to have the similar impact on software that founders have had on the hardware manufacturing. They move on to advocate that technology developers would be intelligent to plan and develop their next and advanced generation of systems to be established into cloud

DOI: 10.15680/IJIRCCE.2018.0604056

computing. Seeing that many of the forecasts can be clouded advertise, it is assessed that the recent IT procurement model presented by cloud computing is here to stay. In addition, the acceptance of cloud computing has turned out to be common and deep thus a number of forecasts will rely mainly on overcoming doubts of the cloud (Chandran S. and Angepat M).

III. PROPOSED METHODOLOGY

The below 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.

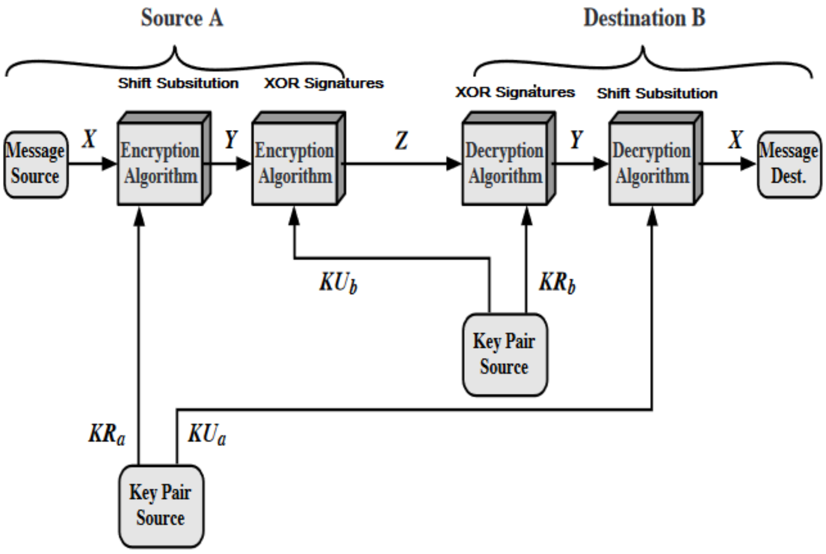

Figure 2: Proposed Scheme for Protecting Virtualized Infrastructures in Cloud Computing.

Substituted numbers	Hexadecimal	Take integer part
0<= t <= 19	K_t = 5A827999	[2^{30} x $2^{½}$]
20<= t <= 39	K_t = 6ED9EBA1	[2^{30} x $3^{½}$]
40<= t <= 59	K_t = 8F1BBCDC	[2^{30} x $5^{½}$]
60<= t <= 79	K_t = CA62C1D6	[2^{30} x $10^{½}$]

Table 1: substitution transformation using integer parts for hex decimal composition incorporating XOR encryption.

IV. CONCLUSION

This scheme proposes a brand new Amplified Shift Substitution modeling XOR/BITWISE rule to enhance the security performance of PVI under the cloud computing. For these PVI certificates will be originated based on environment performance and will decided by 2 primary factors: the amount of shift created and XOR/BITWISE operations with sandbox behavior. Consequently, this scheme proposes planning rule that is ready to expeditiously utilize Virtual Machine resources and therefore achieves far better security measures and infrastructure performance with the normal computing, however an exceedingly performance analysis on some wide glorious range of platform used in cloud, therefore, we tend to show that the amplified security by which the performance obtained by our planned rule led to considerably outperforms along with normal rule employed in numerous eventualities and cloud virtualized infrastructure.

REFERENCES

1. Babar, M. A., & Chauhan, M. A. (2011). A tale of migration to cloud computing for sharing experiences and observations. SECLOUD '11 Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing (pp. 50-56). New York: ACM.
2. 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.
3. 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
4. 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.
5. M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Computer Systems, vol. 20, no. 4,pp. 398-461,2002
6. 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.
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.