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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A Review on Hybrid Techniques of Security In Cloud Computing

Saurin Khedia[1], Nishant Khatri[2]

M.E. Scholar, Department of Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India[1]

Assistant Professor, Department of Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India[2]

ABSTRACT: Security and privacy in cloud computing is one of the most challenging ongoing research areas because data owner stores their sensitive data to remote servers and users also access required data from remote cloud servers which is not controlled and managed by data owners. Since cloud computing is rest on internet, various security issues like privacy, data integrity, confidentiality, authentication and trust encounter. In this paper, we will comprehensively survey the various existing hybrid security techniques of cloud computing. We will compare these combinations of security techniques with their key features and drawbacks of each.

KEYWORDS: cloud computing, security, privacy, authentication, confidentiality, data integrity

I. INTRODUCTION

Cloud computing simply means internet computing. Cloud is a computing model that refers to both the applications derived as services over the Internet, the hardware and system software in the datacenters that provide those services. Cloud Computing is a kind of computing technique where IT services are provided by massive low-cost computing units connected by IP networks [1]. This concept also explains the applications that are broaden to be accessible through the Internet. Cloud applications use large datacenters and effective servers that host web applications and services. According to NIST, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]".

II. SERVICE MODELS OF CLOUD COMPUTING

Cloud computing is composed of three service models:

- *Software as a Service (SaaS)*

Cloud consumers release their applications on a hosting environment, which can be accessed through networks from various clients (e.g. web browser, PDA, etc.) by application users. Cloud consumers do not have control over the Cloud infrastructure that often employs a multi-tenancy system architecture, namely, different Cloud consumer's applications are organized in a single logical environment on the SaaS Cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery, and maintenance. Examples of SaaS includes Salesforce.com, Google Mail, Google Docs and so forth [3].

- *Platform as a Service (PaaS)*

PaaS is a development platform supporting the full "Software Life Cycle" which allows Cloud consumers to develop Cloud services and applications (e.g. SaaS) directly on the PaaS Cloud. Hence the difference between SaaS and PaaS is that SaaS only hosts completed Cloud applications whereas PaaS offers a development platform that hosts both completed and in-progress Cloud applications. This requires PaaS, in addition to supporting application hosting environment, to possess development infrastructure including programming environment, tools, configuration management, and so forth. An example of PaaS is Google App Engine [3].

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

- *Infrastructure as a Service (IaaS)*

Cloud consumers directly use IT infrastructures (processing, storage, networks, and other fundamental computing resources) provided in the IaaS Cloud. Virtualization is extensively used in IaaS Cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from Cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VM's. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple Cloud consumers) can run on a single application (i.e. the same logic machine). An example of IaaS is Amazon's EC2 [3].

III. DEPLOYMENT MODELS OF CLOUD COMPUTING

In Cloud computing, the available deployment models are:

- *Public Cloud*

A Public Cloud is a model which allows users access to the Cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for Cloud optimization. This helps Cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure. Public Clouds are less secure than the other Cloud models because it places an additional burden of ensuring all applications and data accessed on the Public Cloud are not subjected to malicious attacks. Therefore trust and privacy concerns are rife when dealing with Public Clouds [4].

- *Private Cloud*

A Private Cloud is set up within an organization's internal enterprise datacenter. It is easier to align with security, compliance and regulatory requirements, and provides more enterprise control over deployment and use. In the Private Cloud, scalable resources and virtual applications provided by the Cloud vendor are pooled together and available for Cloud users to share and use. It differs in the Public Cloud in that all the Cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the Private Cloud can be much more secure than that of the Public Cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private Cloud [4].

- *Hybrid Cloud*

A Hybrid Cloud is a Private Cloud linked to one or more external Cloud Services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both Public and Private Clouds. Hybrid Clouds provide more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems [4].

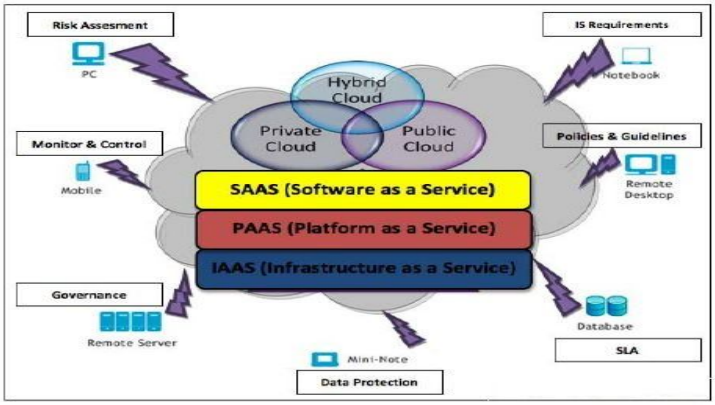

Fig: Cloud Computing Models [4]

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

IV. PROBLEM STATEMENT

Security in the Cloud is now the main challenge in Cloud Computing. Due to lack of understanding and proper application, there have been lot of speculations for many organizations to use services of Cloud computing as data is stored at any physical location outside their own control. This facility has raised various security questions like privacy, confidentiality, integrity etc. and demanded a trusted environment where data confidentiality can be maintained. Thus, we need to determine the perfect blend of security using different techniques to provide the most efficient authentication, confidentiality and integrity of data over network.

Name of Attacks	Description
Tampering	An attacker may alter information either stored in local files, database or is sent over public network.
Eavesdropping Information Disclosure	This type of attack occurs when attacker gains access in the data path and gains access to monitor and read the messages.
Repudiation	Sender tries to repudiate, or refuse the validity of a statement or contract which is sent by him/her.
Elevation of Privileges	An attacker may access unauthorized to information and resources.
Man-in-the-Middle Attack	This type of attack occurs when an attack infiltrates the communication channel in order to monitor the communication and modify the messages for malicious purposes.
Replay Attack	A replay attack is defined as when an attacker or originator sends a valid data with intention to use it maliciously or fraudulently.
Identity Spoofing	Identity spoofing occurs when an attacker impersonates the users as the originator of the message in order to gain access on a network.
Differential Analysis Threat	When new versions are released, a differential analysis of the new and old version would indicate where differences in the code exist.
Viruses and Worms	Viruses and worms are very common and well known attacks. These are piece of code that decrease the performance of hardware and application even these malicious codes corrupts files on local file system.

Table: Types of Attacks [5]

V. RELATED WORK

In this section, we will review some hybrid security techniques as below:

- Satish Kumar and Anita Ganpati [6] proposes a scheme in which authentication process is carried out in two levels or two tiers. First tier uses simple username and password on a standard cloud user's interface. Second tier is use of any personal device like mobile which have a unique id and in possession of the authenticated user only. The advantage of this scheme is that it enhances the strength of authentication as if cloud server has to authenticate the standard user password and id as well as the associated device's id and password simultaneously with each other. Problem with this method is that it involves additional hardware which is costly.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

- V. Sulochana and R. Parimelazhagan [7] presents a puzzle based authentication scheme in which cloud user registers and solves the puzzle, puzzle solving time and sequence of image block is stored and validated by local server and the cloud user get authenticated and start accessing the cloud services. A major drawback of this method is that if attacker once identifies the stored pattern, he could easily break the security.

- Prashant Rewagad and Yogita Pawar [8] proposed to make use of digital signature and Diffie Hellman key exchange blended with Advanced Encryption Standard (AES) encryption algorithm to protect confidentiality of data stored in cloud. They proposed a three way mechanism architecture which makes it tough for hackers to crack the security system, thereby protecting data stored in cloud. But this method requires many parameters which makes it heavy enough and also requires a proper key management.

- Sarbjeet Singh and Maninder Singh [9] proposed a multi-authentication scheme for cloud security in which authentication process is carried out in two tiers. First tier uses general username and password. Second tier is pre-determined series of steps. The advantage of this scheme is that it does not require any additional hardware and software. So this can be used and accessed from anywhere across the globe. They concluded that the strength of any authentication technique depends upon the probability of breaking that technique.

- H.A. Dinesha and V.K. Agrawal [10] presents a technique which authenticates the cloud access in multiple levels. It generates the password and concatenates the generated password at multiple levels. At each level the user has to input password to gain access. Advantage of this technique is that it uses multi-tier approach. It is quite difficult to break multilevel security as compared to single level. Disadvantage of this technique is that it uses passwords at every level but password remembrance is very hectic task for users.

- Neha Tirthani and R Ganeshan [11] contemplated a design for cloud architecture which ensures secured movement of data at client and server end. It uses the non breakability of Elliptic Curve Cryptography for data encryption and Diffie Hellman key exchange mechanism for connection establishment. Problem is that it uses a traditional one tier authentication which is vulnerable to security attacks.

- Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby [12] propose a new data security model based on studying of cloud computing architecture. A software is implemented to select the suitable and the highest security encryption algorithm. The proposed model solves cloud user security problems, help cloud provider to select the most suitable encryption algorithm to its cloud. However, this model proves to be costly as it requires additional software.

- Uma Somani, Kanika Lakhani and Manish Mundra [13] proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique include both digital signature scheme and public key cryptography to enhance the security of cloud computing and solves the dual problem of authentication and security. The strength of their work is the framework proposed to address security and privacy issue.

VI. CONCLUSION

This paper presented various hybrid security techniques for cloud computing. With wide variety of applications of cloud computing, security solutions are mainly privacy aware and data owner centric. We discussed some of the diverse schemes in our survey which have been proposed in literature. From our observations, we conclude that the reviewed hybrid security techniques lack resistance to some or the other attacks. However none of the technique fulfils all the criteria of the evaluation. So using this work one can get encouragement to develop a new security technique that may satisfy all the criteria of the evaluation.

REFERENCES

[1] Ling Qian, Zhiguo Luo, Yujian Du and Leitao Guo, “Cloud Computing: An Overview”, Springer-Verlag Berlin Heidelberg CloudCom, LNCS 5931, pp. 626-631, 2009.

[2] Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing”, National Institute of Standards and Technology Special Publication 800-145, 2011.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

[3] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 27-33, 2010.
[4] S. Ramgovind, MM. Eloff and E. Smith, "The Management of Security in Cloud Computing," IEEE Information Security for South Africa (ISSA), pp. 1-7, 2010.
[5] Sherif el-etriby, Eman M. Mohamed and Hatem S. Abdelkader, "Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing," 3rd International Conference on Communications and Information Technology (ICCIT), pp. 800-805, 2012.
[6] Satish Kumar and Anita Ganpati, "Multi-Authentication for Cloud Security: A Framework," International Journal of Computer Science & Engineering Technology (IJCSET),Vol. 5, Issue 4, pp. 295-303, Apr. 2014.
[7] V. Sulochana and R. Parimelazhagan, "A Puzzle Based Authentication Scheme for Cloud Computing," International Journal of Computer Trends and Technology (IJCTT), Vol. 6, Issue 4, pp. 210-213, Dec. 2013.
[8] Prashant Rewagad and Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," IEEE International Conference on Communication Systems and Network Technologies (CSNT), pp. 437-439, 2013.
[9] Sarbjeet Singh and Maninder Singh, "Design and Implementation of Multi-tier Authentication Scheme in Cloud," International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 5, pp. 181-187, Sep. 2012.
[10] H.A. Dinesha and V.K. Agrawal, "Multi-level Authentication Technique for Accessing Cloud Services," IEEE International Conference on Computing, Communication and Applications (ICCCA), pp. 1-4, 2012.
[11] Neha Tirthani and R. Ganeshan, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research (IACR), ePrint archive, 2014.
[12] Eman M. Mohamed, Hatem S. Abdelkader and Sherif el-etriby, "Enhanced Data Security Model for Cloud Computing," IEEE 8th International Conference on Informatics and Systems (INFOS2012), pp. CC12-CC17 , 2012.
[13] Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC2010), pp. 211-216, 2010.

BIOGRAPHY

Saurin Khedia is pursuing his M.E. degree in Computer Engineering from Sigma Institute of Engineering, Gujarat Technological University, Gujarat, India. He received his B.E. degree in Information Technology from PIET, Gujarat University, Gujarat, India in 2012. His research interests include Distributed Systems, Cloud Computing, Security and Privacy related issues in Cloud.

Nishant Khatri received his M.Tech degree in Comp. Science & Engineering from Amity University, Rajasthan, India in 2013. He received his B.E. degree in Computer Engineering from R.K. College of Engineering, Saurashtra University, Gujarat, India in 2011. Currently he is working as Assistant Professor in Computer Engineering Department at Sigma Institute of Engineering, Vadodara, India. His research interests include Data Mining, Cloud Computing and Security issues in Cloud.