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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Maintaining User Security in Public Shared Clouds

Kiran S. Sawant[1], Nilesh D. Prajapati[2], Shrikant D. Chobhe[3], Prof.Ashutosh Choudhary[4]

B.E. Student, Raisoni College of Engineering & Management Chas, Ahmednagar, Maharashtra, India[1,2,3]

Asst. Professor, Raisoni College of Engineering & Management Chas, Ahmednagar, Maharashtra, India[4]

ABSTRACT:In this paper, we describe a framework for data and operation security in IaaS, consisting of protocols for trusted launch of virtual machines and domain-based storage protection. The protocols allow trust to be established by remotely attesting host platform configuration prior to launching guest virtual machines and ensure confidentiality of data in remote storage, with encryption keys maintained outside of the IaaS domain. The protocols allow trust to be established by remotely attesting host platform configuration prior to launching guest virtual machines and ensure confidentiality of data in remote storage, with encryption keys maintained outside of the IaaS domain. Presented experimental results demonstrate the validity and efficiency of the proposed protocols. The framework prototype was implemented on a test bed operating a public electronic health record system, showing that the proposed protocols can be integrated into existing cloud environments.

KEYWORDS:Security, Cloud Computing, Storage Protection, Trusted Computing.

I. INTRODUCTION

Cloud computing has progressed from a bold vision to massive deployments in various application domains. Howeverthe complexity of technology underlying cloud computing introduces novel security risks and challenges. A core enabling technology of IaaS is system virtualization [8], which enables hardware multiplexing and redefinition of supported hardware architectures into software abstractions. This redefinition is performed by the hypervisor, a software componentthat abstracts the hardware resources of the platform and presents a virtualized software platform where guest virtual machine (VM) instances can be deployed. In addition, the hypervisor also manages the I/O communication between VM instances and external components, including storage devices allocated to the VM instance. This is one of thevulnerable areas of IaaS environments since, as demonstrated in [6], improper allocationof block storage can lead to a breach of data confidentiality. There is a clear need for usable and cost-effective cloud platform security mechanisms suitablefor organizations that rely on cloud infrastructure. One such mechanism is platform integrity verificationfor compute hosts that support the virtualized cloud infrastructures everal large cloud vendors have signalled practicalimplementations of this mechanism, primarily to protect the cloud infrastructure from insider threats and advancedpersistent threats. We see two major improvement vectorsregarding these implementations. First, details of such proprietarysolutions are not disclosed and can thus not be implementedand improved by other cloud platforms. Second,to the best of our knowledge, none of the solutions providecloud tenants a proof regarding the integrity of computehosts supporting their slice of the cloud infrastructure.

In this project, we present DBSP (domain-based storage protection), a virtualdisk encryption mechanism where encryption of data is done directly on the compute host, while the key material necessary for re-generating encryption keys is stored in the volume metadata. This approach allows easy migration of encrypted data volumes and withdraws the control of the cloud provider over disk encryption keys. In addition, DBSP significantly reduces the risk of exposing encryption keys and keeps a low maintenance overhead for the tenant– in the same time providing additional control over the choice of the compute host based on its software stack.

The relevant security mechanism is encryption of virtual disk volumes, implemented and enforced at computehost level. While support data encryption at rest is offered by several cloud providers and can be configured by

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

tenantsin their VM instances, functionality and migration capabilities of such solutions are severely restricted. In most cases cloud providers maintain and manage the keys necessary for encryption and decryption of data at rest. This further convolutes the already complex data migration procedure between different cloud providers, disadvantaging tenants through a new variation of vendor lock-in. Tenants can choose to encrypt data on the operating system (OS) level within their VM environments and manage the encryption keys themselves.

II. RELATED WORK

2.1. Towards trusted cloud computing

The design of atrusted cloud computing platform (TCCP). TCCP enables Infrastructure as a Service (IaaS) providers such as Amazon EC2 to provide a closed box execution environment that guarantees confidential execution of guestvirtual machines. Moreover, it allows users to attest to the IaaS provider and determine whether or not the service is secure before they launch their virtual machines [1].

2.2 Seeding Clouds with Trust Anchors

In this paper, we identify three main challenges that cloud providers face when generating proofs that can placate a user's concerns:

1) That cloud vendors provide a proof of data security protection of their hosts and customer processing; 2) That such proofs have a clear meaning to cloud customers; and

3) That such proofs can be generated effectively and efficiently in a cloud computing environment [2].

2.3 **Domain Based Storage Protection with Secure Access Control for the Cloud**

Despite the variety of available open source cloud management platforms (e.g. Open Stack, Eucalyptus, Open Nebula), allocation of read-write permissions for shared data betweencollaborating tenants still remains an open problem. In thispaper we address the outlined gap. We improve and extendprevious work by adding capabilities to both grant access to data to other IaaS cloud clients and assign access permissions [3].

2.4 Security aspects of e-health systems migration to the cloud

In this paper, we will present current state of the art research in this field. We focused of several shortcomings of current healthcare solutions and standards, particularly for platform security, privacy aspect and requirements which is a crucial aspect for the overall security of healthcare IT systems. [5]

III. PROPOSED SYSTEM

In this proposed system a "Trusted Cloud Compute Platform"(TCCP) to ensure VMs are running on a trusted hardware and software stack on a remote and initially un-trusted host. To enable this, a trusted coordinator stores the list of attested hosts that run a "trusted virtual machine monitor" which can securely run the client's VM. Trusted hosts maintain in memory an individual trusted key use for identification each time a client launches a VM. The paper presents a good initial set of ideas for trusted VM launch and migration, in particular the use of a trusted coordinator. A limitation of this solution is that the trustedcoordinator maintains information about all hosts deployed onwhile support data encryption at rest is offered by several cloud providers and can be configured by tenants in their VM instances, functionality and migration capabilities of such solutions are severely restricted. In most cases cloud providers maintain and manage the keys necessary for encryption and decryption of data at rest. This further convolutes the already complex data migration procedure between different cloud providers, disadvantaging tenants through a new variation of vendor lock-in. Tenants can choose to encrypt data on the operating system (OS) level within their VM environments and manage the encryption keys themselves. However, this approach suffers from several drawbacks: first, the underlying compute host will still have access encryption keys whenever the VM performs cryptographic operations; second, this shifts towards the tenant the burden of maintaining the encryption software in all their VM instances and increases the attack surface; third, this requires injecting, migrating and later securely withdrawing encryption keys to each of the VM instances with access to the encrypted data, increasing the probability than an attacker eventually obtains the keys.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

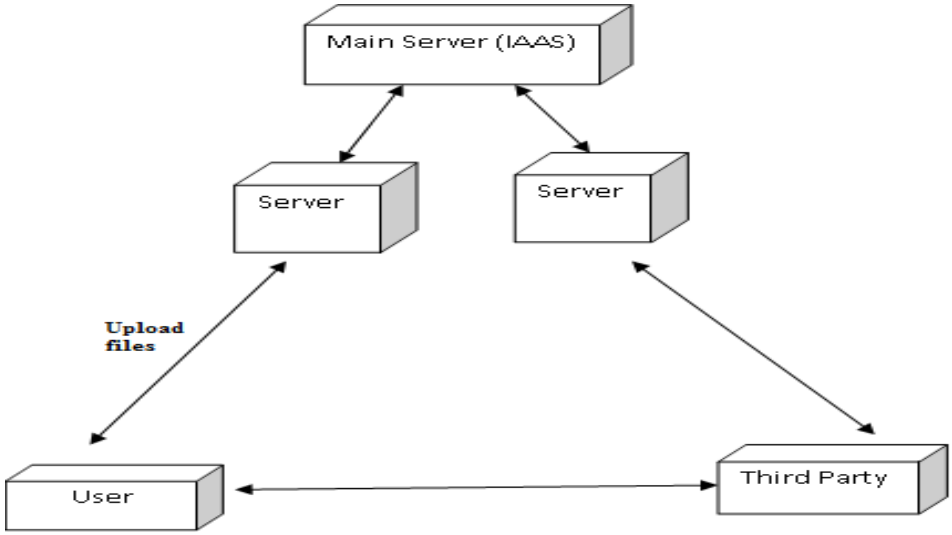

Fig1. System Architecture

3.1 Proposed AES algorithm

1. KeyExpansions—round keys are derived from the cipher key using key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. InitialRound
    1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey.

IV. SYSTEM FLOW

In the flow of proposed system, system user first needs to get login to the system. After that he needs to provide the token to validate the user. This token is get send on his mail id. If token match then only user will get access to the system. He considered as authorized user. After authentication user can send file request. If he having permission to perform the particular file operation then only he can access or perform that file operation.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

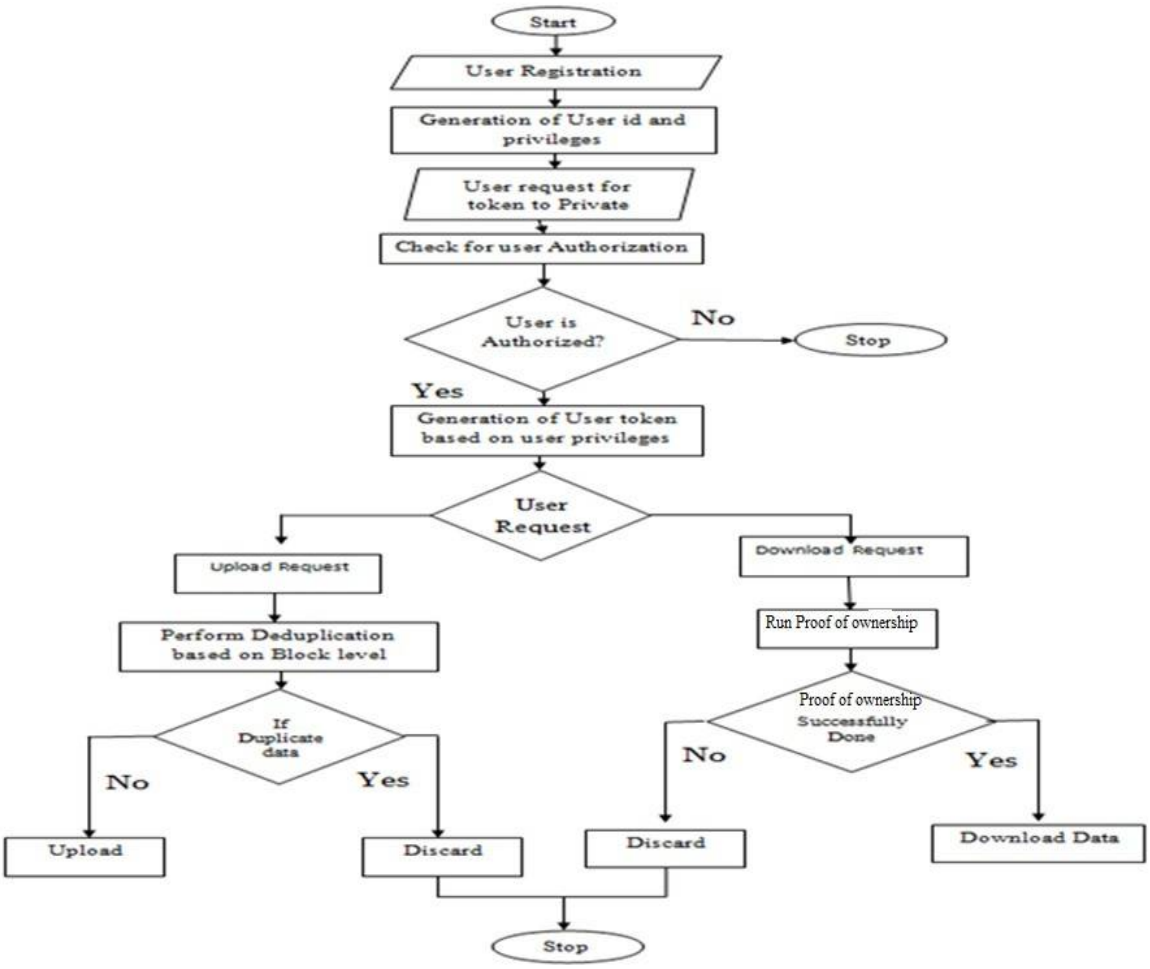

Fig. 2 System Flow

As per the above flow diagram total system get execute. User can only access the files if he have specific proof of ownership.

V. REQUIREMENT ANALYSIS

5.1.1 **HARDWARE REQUIRMENTS**
System: Pentium IV 2.4 GHz.
Hard Disk: 40 GB.
Monitor: 15 VGA Colour.
Mouse:Standard
Ram: 1GB.
5.1.2 **SOFTWARE REQUIRMENTS**
Operating System: Windows 7 and above.
Coding Language: java 1.7
IDE: Netbeans 7.4

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Database: MYSQL. 5.5

.

VI. EXPERIMENTAL RESULTS

Fig.3 PHR Registration

Owner can register his details in PHR.

Fig.4 PHR File Update

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Owner login in to PHR for upload the data.

Fig.5 Upload Data

To share the data in PHR owner can upload history.

Fig.6 File Upload By PHR owner

Owner can upload file to the cloud.

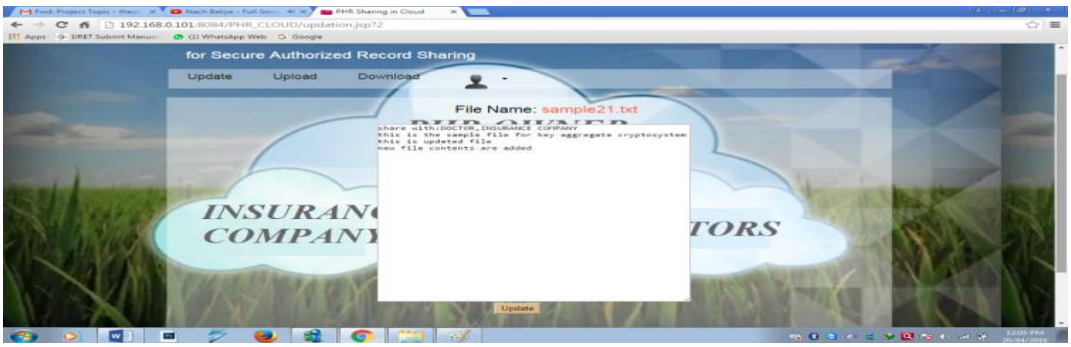

Fig.7 File Update by Doctor

Doctor or PHR owner can update the file present on the cloud.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

VII. CONCLUSION

The cloud security model does not yet hold against threat models developed for the traditional model where the hosts are operated and used bythe same organization. However, there is a steady progress towards strengthening the IaaS security model. In thiswork we presented a framework for trusted infrastructure cloud deployment, with two focus points: VM deploymenton trusted compute hosts and domain-based protection ofstored data. We described in detail the design, implementation and security evaluation of protocols for trusted VM launch and domain-based storage protection. The solutionsare based on requirements elicited by a public healthcareauthority, have been implemented in a popular open-sourceIaaS platform and tested on a prototype deployment of adistributed EHR system. In the security analysis, we introduceda series of attacks and proved that the protocols holdin the specified threat model.This work has covered only a fraction of the IaaS attack landscape. The additional concept is also implementing attribute based file sharing system.

REFERENCES

[1] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trustedcloud computing," in Proceedings of the 2009 Conference on HotTopics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA),USENIX Association, 2009.
[2] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel,"Seeding Clouds With Trust Anchors," in Proceedings of the 2010ACM Workshop on Cloud Computing Security, CCSW '10, (NewYork, NY, USA), pp. 43–46, ACM, 2010.
[3] N. Paladi, A. Michalas, and C. Gehrmann, "Domain based storage protection with secure access control for the cloud," in Proceedingsof the 2014 International Workshop on Security in Cloud Computing,ASIACCS '14, (New York, NY, USA), ACM, 2014.
[4] M. Jordon, "Cleaning up dirty disks in the cloud," Network Security,vol. 2012, no. 10, pp. 12–15, 2012.
[5] Cloud Security Alliance, "The notorious nine cloud computing topthreats 2013," February 2013.
[6] A. Michalas, N. Paladi, and C. Gehrmann, "Security aspects ofe-health systems migration to the cloud," in the 16th InternationalConference on E-health Networking, Application & Services (Healthcom'14), pp. 228–232, IEEE, Oct 2014.
[7] B. Bertholon, S. Varrette, and P. Bouvry, "Certicloud: a novel tpm based approach to ensure cloud IaaS security," in Cloud Computing, 2011 IEEE International Conference on, pp. 121–130, IEEE, 2011.
[8] M. Aslam, C. Gehrmann, L. Rasmussen, and M. Bj ¨orkman, "Securely launching virtual machines on trustworthy platforms in apublic cloud - an enterprise's perspective.," in CLOSER, pp. 511–521, SciTePress, 2012.
[9] A. Cooper and A. Martin, "Towards a secure, tamper-proof gridplatform," in Cluster Computing and the Grid, 2006. CCGRID 06.Sixth IEEE International Symposium on, vol. 1, pp. 8–pp, IEEE, 2006.
[10] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficientaccess to outsourced data," in Proceedings of the 2009 ACM workshopon Cloud computing security, pp. 55–66, ACM, 2009.
[11] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protectionfor the masses," IEEE Computer, vol. 45, no. 1, pp. 39–45, 2012.