ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Providing User Security Guarantees in Public Infrastructure Clouds

Ramya[1], Sandhya[2], Supriya[3] , Karpagam[4]

B.E. Scholar, Department of CSE, T.J.S Engineering College, Chennai, India[1][2] [3]

Asst. Professor, Department of CSE, T.J.S Engineering College, Chennai, India[4]

ABSTRACT: The infrastructure cloud (IaaS) service model offers improved resource flexibility where tenants rent computing resources to operate complex systems. In our project, we describe a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection.Thus once the user is authenticated, they will be launched in virtual machines where they initiate the upload process into the cloud. The cloud user files are uploaded and stored in domain based. To provide resistance against cloud based web application attacks (focusing on session hijacking and broken authentication). Authentication is a critical aspect of this process, but even solid authentication mechanisms can be undermined by flawed credential management functions, including password change, forgot my password; remember my password, account update, and other related functions. For session management, we have implemented cookie management and idle timeout.

I. INTRODUCTION TO IAAS

There is a steady progress towards strengthening the IaaS security model. In this work we presented a frame work for trusted infrastructure cloud deployment, with two focus points: VM deployment on trusted compute hosts and domain-based protection of stored data. We present DBSP (Domain-Based Storage Protection), a virtual disk encryption mechanism where encryption of data is done directly on the compute host. These protocols are successively applied to deploy a cloud infrastructure providing additional user guarantees of cloud host integrity and storage security. For protocol purposes, each domain manager, secure component and trusted third party has a public/private key pair (pk=sk).

II. EXISTING SYSTEM

The existing system 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.

Disadvantages:

1. The underlying compute host will still have access encryption keys whenever the VM performs cryptographic operations;
2. This shifts towards the tenant the burden of maintaining the encryption software in all their VM instances and increases the attack surface;
3. This requires injecting, migrating and later securely withdrawing encryption keys to each of the VM instances with access to the encrypted data.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

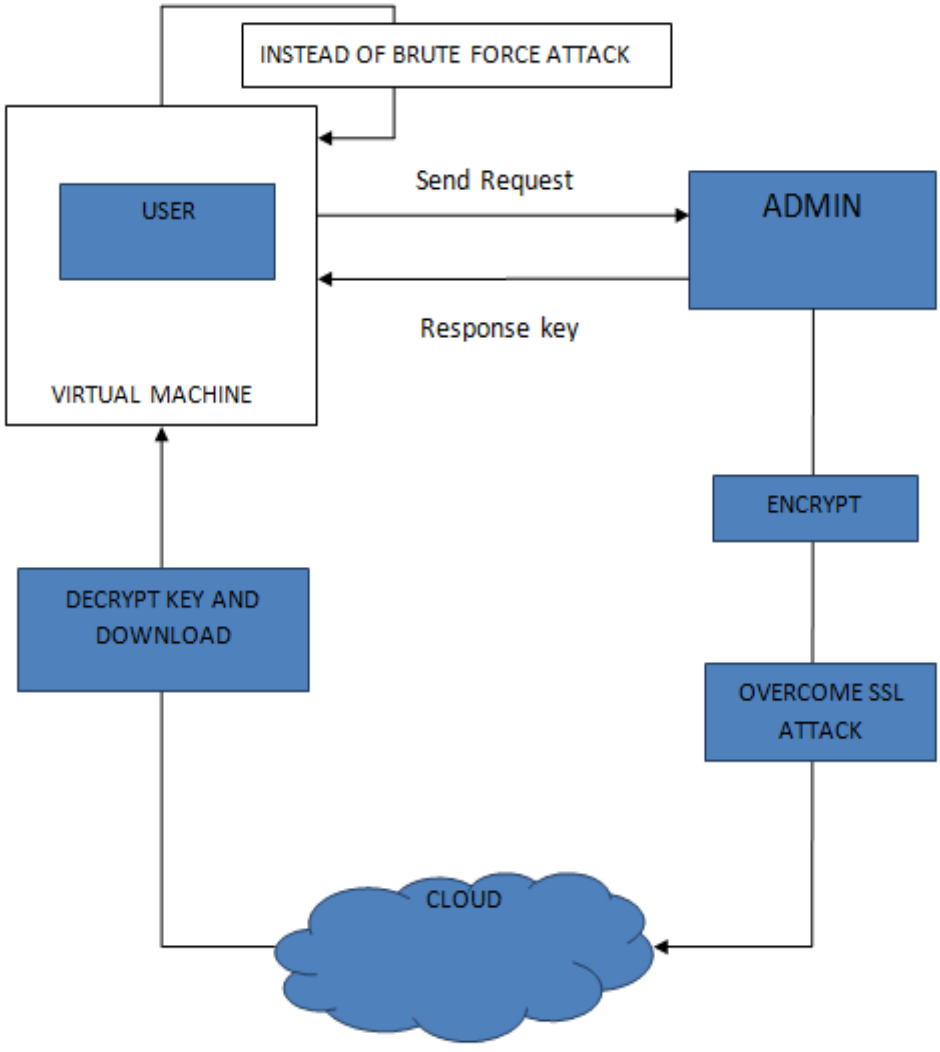
III. PROPOSED SYSTEM

In our proposed system encryption keys are maintained outside of the IaaS domain. For key encryption we proposed **RSA algorithm**. For data owner file encryption, we use **camellia algorithm**. Finally the files are stored in public cloud named **CloudMe**.In either case, if the session tokens are not properly protected, an attacker can hijack an active session and assume the identity of a user. Creating a scheme to create strong session tokens and protect them throughout their lifecycle has proven elusive for many developers. Also to invoke user data security by encrypting the user files using **camellia algorithm** and storing in public cloud named **CloudMe**.

Advantages:

1 .We propose a set of protocols for trusted launch of virtual machines in IaaS.
2. DBSP significantly reduces the risk of exposing encryption keys and keeps a low maintenance overhead for the tenant.
3. High security for user data implementing secure cloud storage.

Architecture Diagram:



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Modules:

- Identity Management
- Key Generation &maintenance scheme
- Virtual Machine
- Broken authentication and session management
- Infrastructure as a service (IAAS)
- Encryption Algorithm (RSA for key and camellia for data)
- Secure Cloud Storage

Encryption Algorithm (RSA for key and Camellia for data):

RSA:

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

Camellia Algorithm:

Camellia was jointly developed by Nippon Telegraph and Telephone Corporation and Mitsubishi Electric Corporation in 2000 [CamelliaSpec]. Camellia specifies the 128-bit block size and 128-, Encryption Standard (AES). Camellia is characterized by its suitability for both software and hardware implementations as well as its high level of security. From a practical viewpoint, it is designed to enable flexibility in software and hardware implementations on 32-bit processors widely used over the Internet and many applications, 8-bit processors used in smart cards, cryptographic hardware, embedded systems, and so on [CamelliaTech]. In particular, Camellia was selected as a recommended cryptographic primitive by the EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) project [NESSIE] and also included in the list of cryptographic techniques for Japanese e-Government systems which were selected by the Japan **Cryptography Research and Evaluation Committees(CRYPTREC)**.Camellia can be divided into "key scheduling part" and "data randomizing part".

Key Scheduling Part:

In the key schedule part of Camellia, the 128-bit variables of KL and KR are defined as follows. For 128-bit keys, the 128-bit key K is used as KL and KR is 0. For 192-bit keys, the leftmost 128-bits of key K are used as KL and the concatenation of the rightmost 64-bits of K and the complement of the rightmost 64-bits of K are used as KR. For 256-bit keys, the leftmost 128-bits of key K are used as KL and the rightmost 128-bits of K are used as KR.

Data Randomizing Part:

Encryption for 128-bit keys
128-bit plaintext M is divided into the left 64-bit D1 and the right 64-bit D2.
D1 = M >> 64;
D2 = M & MASK64;
Encryption for 192- and 256-bit keys
128-bit plaintext M is divided into the left 64-bit D1 and the right 64-bit D2.
D1 = M >> 64;
D2 = M & MASK64;

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Hardware Requirements:

Processor	: Pentium –I Core
Ram	: 2 GB
Hard Disk	: 1.28GB

Software Requirements:

Operating System	: Windows2007/2008/2010
Front End	: Java
Script	: JavaScript
Front End Tool	: Net Beans 8.0.1
Application Server	: Tomcat 5.0/6.X
Back End	: MySql
Back End Tool	: SQLYog

IV. CONCLUSION

From a tenant point of view, the cloud security model does not yet hold against threat models developed for the traditional model where the hosts are operated and used by the same organization. However, there is a steady progress towards strengthening the IaaS security model. In this work we presented a framework for trusted infrastructure cloud deployment, with two focus points: VM deployment on trusted compute hosts and domain-based protection of stored data.

REFERENCES

[1] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the 2009 Conference on Hot Topics 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 2010 ACM Workshop on Cloud Computing Security, CCSW '10, (New York, 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 Proceedings of 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 top threats 2013," February 2013.
[6] B. Bertholon, S. Varrette, and P. Bouvry, "Certicloud: a novel tpm- based approach to ensure cloud IaaS security," in Cloud Computing.