Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 02, February -2018

Providing User Security Guarantee in Public Infrastructure clouds

HATTARKI POOJA[1], PREETI [2]

[1]Dep. of Computer Science, Godutai Engineering College for Women Gulbarga, Karnataka,India
[2]Dep. of Computer Science, Appa Institute Of Engineering and Technology Gulbarga, Karnataka,India

Abstract-*The infrastructure cloud (IaaS) service model offers improved resource flexibility and availability, where tenants – insulated from the minutiae of hardware maintenance – rent computing resources to deploy and operate complex systems. Large-scale services running on IaaS platforms demonstrate the viability of this model; nevertheless, many organizations operating on sensitive data avoid migrating operations to IaaS platforms due to security concerns. In this paper, 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. We continue with an extensive theoretical analysis with proofs about protocol resistance against attacks in the defined threat model. 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.*

I. Introduction

Cloud computing has progressed from a bold vision to massive deployments in various application domains. However, the complexity of technology underlying cloud computing introduces novel security risks and challenges.
Threats and mitigation techniques for the IaaS model have been under intensive scrutiny in recent years while the industry has invested in enhanced security solution and issued best practice recommendations. From an end-user point of view the security of cloud infrastructure implies unquestionable trust in the cloud provider, in some cases corroborated by reports of external auditors. While providers may offer security enhancements such as protection of data at rest, end-users have limited or no control over such mechanisms. There is a clear need for usable and cost-effective cloud platform security mechanisms suitable for organizations that rely on cloud infrastructure.

II. Existing System

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

III. Proposed System

Presented an IaaS storage protection scheme addressing access control. The authors analyses access rights management of shared versioned encrypted data on cloud infrastructure for a restricted group and propose a scalable and flexible key management scheme. Access rights are represented as a graph, making a distinction between data encryption keys and encrypted updates on the keys and enabling flexible join/leave client operations, similar to properties presented by the protocols in this paper. Despite its advantages, the requirement for client-side encryption limits the applicability of the scheme in and introduces important functional limitations on indexing and search. In our model, all cryptographic operations are performed on trusted IaaS compute hosts, which are able to allocate more computational resources than client devices. Abundant works have been proposed under different threat models to achieve various search functionality,

IV. Methodology

A software requirements specification (SRS) is a description of a software system to be developed. It lays out functional and non-functional requirements, and may include a set of use cases that describe user interactions that the software must provide. Software requirements specification establishes the basis for an agreement between customers and contractors or suppliers (in market-driven projects, these roles may be played by the marketing and development divisions) on what the software product is to do as well as what it is not expected to do. Software requirements specification permits a rigorous assessment of requirements before design can begin and reduces later redesign. It should also provide a realistic basis for

estimating product costs, risks, and schedules. The software requirements specification document enlists enough and necessary requirements that are required for the project development. To derive the requirements we need to have clear and thorough understanding of the products to be developed or being developed. This is achieved and refined with detailed and continuous communications with the project team and customer till the completion of the software Providing User Security Guarantee In Public Infrastructure clouds

V. Software Engineering Model

Spiral model was defined by Barry Boehm in his 1988 article, "A spiral Model of Software Development and Enhancement. This model was not the first model to discuss iterative development, but it was the first model to explain why the iteration models. As originally envisioned, the iterations were typically 6 months to 2 years long. Each phase starts with a design goal and ends with a client reviewing the progress thus far. Analysis and engineering efforts are applied at each phase of the project, with an eye toward the end goal of the project. The steps for Spiral Model can be generalized as follows:

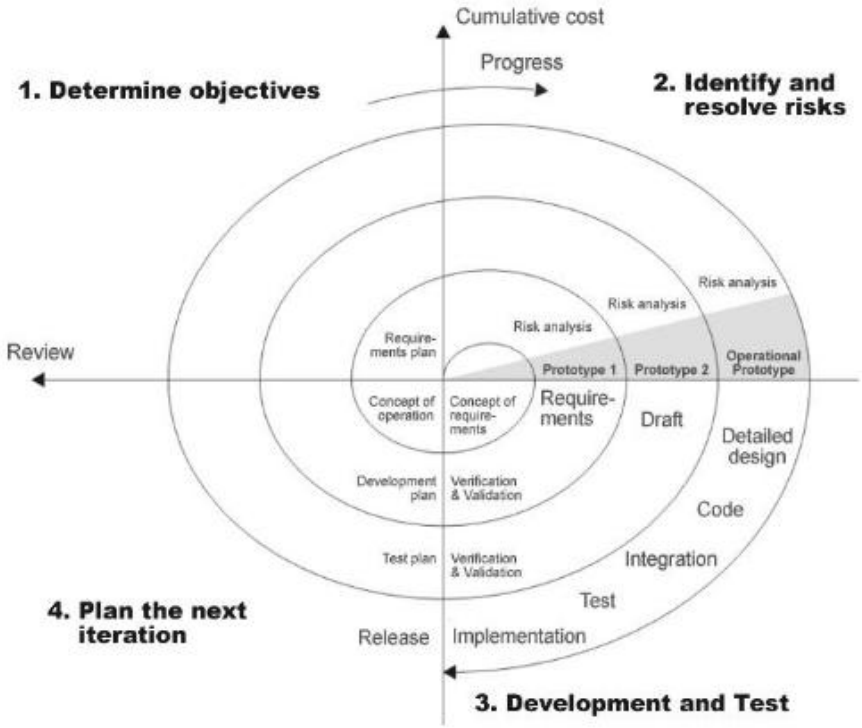

Fig: Spiral Model

Stages in SDLC:
1.Requirement Gathering
2. Analysis
3.Designing
4.Coding
5.Testing
6.Maintenance

VI. Conclusion

The cloud security model does not yet hold against the thread model develop for 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 trusted infrastructure cloud deployment with 2 Points

1. VM deployment on trusted compute hosts
2. Domain based protection of stored data

VII. Future Enhancement

We introduced a series of attacks and proved that the protocols hold in the specified threat model. To obtain further confidence in the semantic security properties of the protocols, we have modeled and verified them with Pro Verification. Finally, our performance tests have shown that the protocols introduce a insignificant performance overhead. This work has covered only a fraction of the IaaS attack landscape. Important topics for future work are strengthening the trust model in cloud network communications, data geolocation , and applying searchable encryption schemes to create secure cloud storage mechanisms. Our results show that it is possible and practical to provide strong platform software integrity guarantees for tenants and efficiently isolate their data using established cryptographic tools. With reasonable engineering effort the framework can be integrated into production environments to strengthen their security properties. In future we can develop the mobile application for Providing User security guarantee In public Infrastructure cloud

REFERENCES

1. Y. Kwak "International standards for building electronic health record (ehr)" Proc.Enterprise Netw. Comput. Healthcare Ind. pp. 18-23 Jun. 2005.

2. M. Eichelberg T. Aden J. Riesmeier A. Dogac Laleci "A survey and analysis of electronic healthcare record standards" ACM Comput. Surv. vol. 37 no. 4 pp. 277-315 2005.

3. T. Benson Principles of Health Interoperability HL7 and SNOMED 2009 Spinger.

4. J. Lähteenmäki J. Leppänen H. Kaijanranta "Interoperability of personal health records" Proc. IEEE 31st Annu. Int. Conf. Eng. Med. Biol. Soc. pp. 1726-1729 2009.

5. R. H. Dolin L. Alschuler C. Beebe "The HL7 Clinical Document Architecture" J.Am. Med. Inform. Assoc. vol. 8 pp. 552-569 2001.

6. R. H. Dolin L. Alschuler S. Boyer "The HL7 Clinical Document Architecture" J.Am. Med. Inform. Assoc. vol. 13 no. 1 pp. 30-39 2006.

7. M. L. Müller F. Ückert T. Bürkle "Cross-institutional data exchange using the clinical document architecture (CDA)" Int. J. Med. Inform. vol. 74 pp. 245-256 2005.

8. H. Yong G. Jinqiu Y. Ohta "A prototype model using clinical document architecture (cda) with a japanese local standard: designing and implementing a referral letter system" Acta Med Okayama vol. 62 pp. 15-20 2008.

