ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 13, March 2018

PROVIDING USER SECURITY GUARANTEES IN PUBLIC INFRASTRUCTURE CLOUDS

E.ARPUTHARAJ SOLOMON
Department of Computer Science and Engineering
Kamaraj College of Engineering and Technology
Near Virudhunagar, Madurai, Tamil Nadu, India

S.SANTHOSH KUMAR
Department of Computer Science and Engineering
Kamaraj College of Engineering and Technology
Near Virudhunagar, Madurai, Tamil Nadu, India

M.RAJASEKARAN M.E., (A/P CSE)
Department of Computer Science and Engineering
Kamaraj College of Engineering and Technology
Near Virudhunagar, Madurai, Tamil Nadu, 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.

IndexTerms–viability, migratingoperations
Encryption keys

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 solutions and issued best practice recommendations While providers may offer security enhancements such as protection of data at rest s and to maximise the company's earning potential.

. 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

One such mechanism is platform integrity verification for compute hosts that support the virtualized cloud infrastructure. Several large cloud vendors have signaled practical implementations of this mechanism, primarily to protect the cloud infrastructure from insider threats and advanced persistent threats

While 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

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 13, March 2018

within their VM environments and manage the encryption keys themselves

II. LITERATURE SURVEY

N. Paladi and A. Michalas [1] says that It addresses the lack of reliable for data placement control in cloud storage systems. We analyse the currently available solutions and identify their shortcoming. This mechanism aims to provide granular control over the capabilities of tenants to access data placed on geographically dispersed storage units comprising the cloud storage. Physical location of data in cloud storage is an increasingly urgent problem. In ashort time it has evolved from the concern of a few regulated businesses to an important consideration for many cloud storage users

The another author S. Kamara and C.Papamanthou [2] says that the present a new method for constructing sub-linear SSE schemes. Our approach is highly parallelizable and dynamic. Our scheme also achieves the following of the important properties it enjoys a strong notion of security attacks and compared to existing sub-linear dynamic SSE schemes. It retain the ability to perform keyword searches without revealing information about the contents of the documents and queries.

A.Michalas, N. Paladi, and C. Gehrmann says that a adoption of health solutions advances, new computing paradigms such as cloud computing bring the potential to improve efficiency in managing medical health records and help the reduce costs.It has security risk and multiple data cannot be stored at a time.

.

N. Paladi, A. Michalas, and C. Gehrmann says that the reliable data sharing mechanisms, by providing an XML-based language framework which enables of clients of IaaS clouds to securely share data and clearly define access rights granted to peers.The prototyped as acode of extension for popular cloud platform In many businesses and individuals continue to view cloud computing as a technology that risks exposing their data to unauthorized users.

.

N. Paladi, C. Gehrmann, and F. Morenius says that Domain-Based Storage Protection (DBSP) a dataConfidentiality and integrity protection mechanism for IaaS environments, which relies on trusted computing principles to provide for transparent storage isolation between IaaS clients. VM instance which does not possess the client-provided ASfor a certain domain would not complete a trusted launch procedure and would not obtain the session domain key for the respective administrative domain.

III.INVENTORY AND INVOICE SYSTEM

A. SYSTEM REQUIREMENTS

1.ASP.NET with C#
2.MYSQL

1.ASP.NET WITH C#:

ASP.NET is an open source web framework for building modern web apps and services with .NET.It creates websites based on HTML5,CSS and Javascript that are simple,fast and can scale to millions of users.

FEATURES OF ASP.NET :

- Building and Minification Feature
- Strongly typed data controls
- Model Binding
- Enhanced support for asynchronous

2. MYSQL:

MySQL is Associate in Nursing ASCII text file on-line database management system(RDBMS). MySQL may be a main element of the LAMP. Many high-profile,large-scale websites,including Google , Facebook,Twitter, Flickr,and YouTube uses MySql.

FEATURES OF MYSQL:

- Secure
- Client/ Server Architecture
- Scalable

B. SYSTEM DESIGN

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 13, March 2018

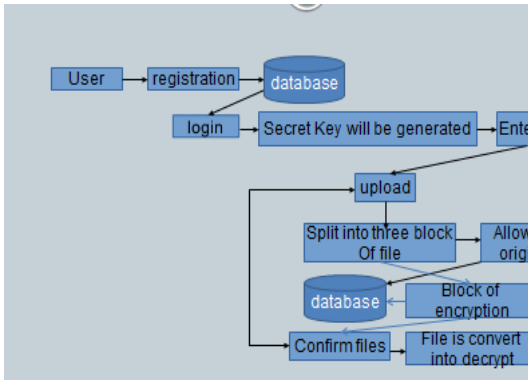


Figure 1 : System design

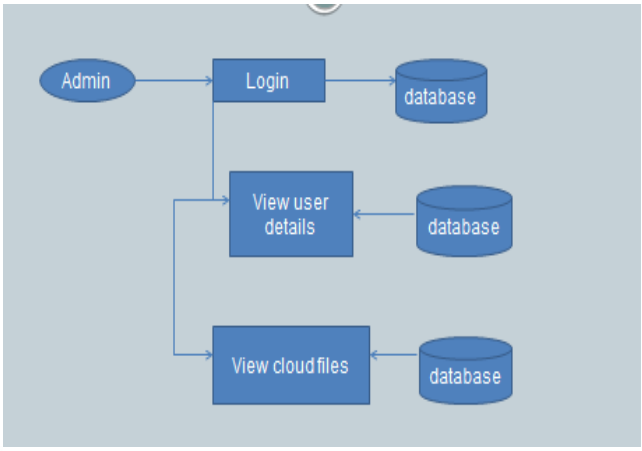


Figure 2 : Admin Level

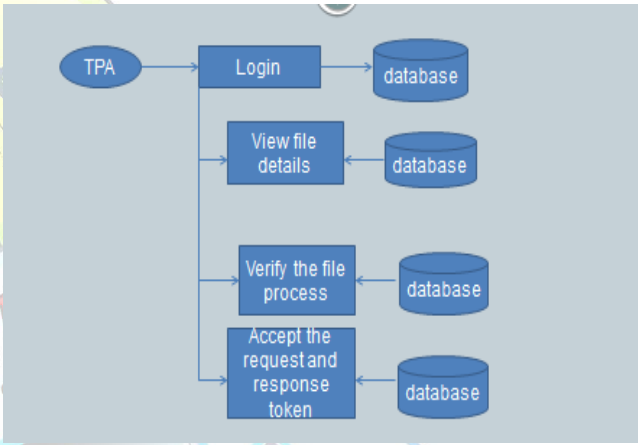


Figure 3 : TPA Level

The proposed system contains three modules.presented an IaaS storage protection scheme addressing access control. The authors analyse 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.

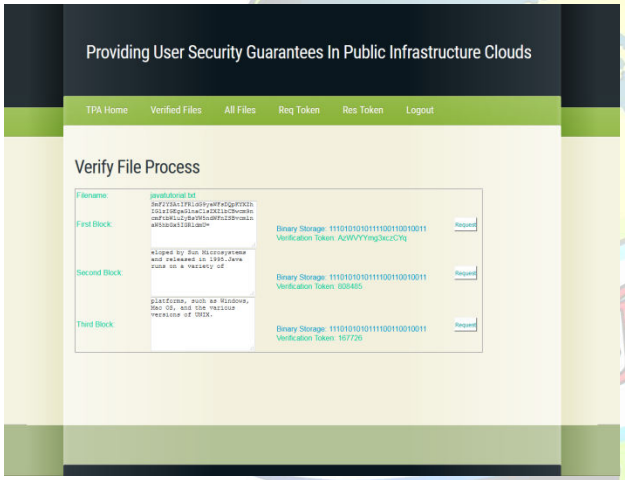
Despite its advantages, the requirement for client-side encryption limits the applicability of the scheme in and introduces important functional limitations on indexing and search. In our model, all cryptographic operations are performed on trusted IaaS compute hosts, which are able to allocate more computational resources than client devices.Abundant works have been proposed under different threat models to achieve various search functionality,

C. FLOW DIAGRAM

IV.SNAPSHOT.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 13, March 2018



V.CONCLUSION

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.

VI.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

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 13, March 2018

International Workshop on Security in Cloud Computing, ASIACCS '14, (New York, NY, USA), ACM, 2014

[4] cloud security alliance"The notorious nine cloud computing top threats 2013," February 2013

[5] M.Jordon "cleaning up dirty disks in the cloud Network Security, vol. 2012, no. 10, pp. 12–15, 2012