IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 6, June 2024

Impact Factor: 5.731

Multi-Tenant IaaS Cloud Security Evaluation Model

Jasmine Sharon S[1] and S. Nagasundaram[2]

MCA Student, Department of Computer Applications[1]

Professor, Department of Computer Applications[2]

Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

jassharon26@gmail.com and snagasundaram.scs@velsuniv.ac.in

Abstract: *Tenants that rent computer resources to run sophisticated systems might benefit from increased resource flexibility provided by the infrastructure cloud (IaaS) service model. The user will thus be launched into virtual computers after completing the authentication procedure, where they will start the upload process to the cloud.Secure data access is offered by suggested system's implementation of virtual machines and key management.Session management and failed authentication are other key components of suggested solution. All facets of managing active sessions and handling user authentication fall under the purview of authentication and session management. The act of updating an account, changing a password, remembering a password, and other similar operations are examples of credential management functions that can compromise even the most robust authentication schemes.*

Keywords: Security, IaaS, Data Security, Encryption, Multi-Cloud Storage

I. INTRODUCTION

The infrastructure cloud (IaaS) service model provides increased resource flexibility by renting computer resources to run complicated applications. Many organizations operating on sensitive data avoids migrating operations to IaaS platforms due to security concerns. In this project, this paperdescribes a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection. After authentication, users will launch virtual computers to begin uploading to the cloud. This suggested solution maintains encryption keys outside the IaaS domain.For key encryption This paper proposed RSA algorithm. In proposed system, implementing virtual machines and key management secure data access has been provided.

TheObjective of project is to create beneficial system for end users. Since technology is getting upgraded every day, this paperproposes to create a virtual environment where infrastructure can be rendered as a service to the end users. By setting up virtual machines, file access has been made secure and unauthorized access is been prohibited. Also, objective is to provide secure encryption and multiple cloud storage environment. For each user private key is been rendered from the admin side for accessing the downloaded file. For security two encryption algorithms are used. For file encryption This paperhas proposed RSA & data encryption.This paper proposed camellia algorithm.

The rapid adoption of cloud computing, particularly Infrastructure as a Service (IaaS), has revolutionized how organizations access and manage IT resources. However, handing over critical data and infrastructure to a third-party provider necessitates a high degree of trust. This project aims to address this need by developing a comprehensive security assessment model specifically for IaaS cloud environments. This project seeks to develop a standardized security assessment model for IaaS cloud environments. This model will provide organizations with a clear framework for evaluating the security posture of potential cloud providers. It will go beyond the Cloud Trust Protocol (CTP) by incorporating additional security considerations critical for IaaS deployments.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

II. LITERATURE REVIEW

1. Duan, Y., Xiao, Y., & Tian, H (2012), A Trust-Oriented Security Model for Cloud Computing

The study emphasizes the necessity of trust-based security models in cloud computing settings, which address issues such as data confidentiality, integrity, and availability. It also offers topics for future study to improve trustworthiness and resilience, emphasizing the importance of trust-based techniques in strengthening cloud computing infrastructures.

2. Partha Sen, Pritam Sen, Sunirmal Khatua,(2015), A distributed approach towards trusted cloud computing platform

The paper discusses the Distributed Trusted Cloud Computing Platform (DTCCP) as a solution to barriers to enterprise cloud adoption, including privacy, security, data sensitivity, and computation integrity. It serves as an oracle, ensuring cloud users' trustworthiness and enabling private execution environments for guest Virtual Machines. Its distributed governance model ensures smooth operation and scalability. The paper also suggests implementing a fully functional prototype to explore its performance in real-world scenarios.

3. Benoît Bertholon, SebastienVarrette, Pascal Bouvry (2011), CERTICLOUD: a Novel TPM-based Approach to Ensure Cloud IaaS Security

This paper focuses on ensuring the integrity of user-deployed Virtual Machines (VMs). It uses Trusted Platform Module (TPM) hardware and Trusted Computing Group (TCG) concepts, with key protocols like TCRR and Verify MyVM for robust cryptographic attack validation. It leverages Trusted Platform Module (TPM) technology to enhance the integrity, confidentiality, and overall security of cloud-based infrastructure. The approach offers benefits like improved trust, compliance, and data protection.

4. Bhargava, B., Ranchal, R., & Hassan, M. M. (2018), Trust-based Security in the Internet of Things with Fog Computing

The paper proposes a fog computing-based framework for trust management in IoT devices, focusing on resource-limited devices. The framework provides processing power and storage closer to data sources, enhancing trust management within the fog layer of an IoT environment. The paper suggests its practical applicability in real-world IoT scenarios, aiming for a more resilient, secure, and trustworthy future.

5. Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee (2011),TrustCloud: A Framework for Accountability and Trust in Cloud Computing

The study emphasizes the need for research on cloud accountability and the risks of not achieving it. It proposes detective approaches to increase accountability, complementing preventive ones. The shift from system health to data integrity requires a file-centric perspective. Real-time and post-mortem approaches are identified for cloud computing at different levels. The paper suggests developing solutions for each layer, such as a logging mechanism for the system layer.

6. Tsai, W.-T., Kuo, C.-T., & Yan, K.-Q. (2020), Trust-based Access Control Model for Cloud Computing

The paper highlights the importance of trust-based access control models in improving security and access control in cloud computing. It highlights the limitations of traditional mechanisms and highlights the effectiveness of trust relationships between users, resources, and service providers. Future research directions may include scalability enhancement, performance concerns, and integrating emerging technologies like blockchain or machine learning.

7. Ishugupta, ashutoshkumarsingh,chung-nan lee,rajkumarbuyya (2022), Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments

The article presents a comprehensive analysis of techniques for data protection in cloud computing and information security. It highlights research gaps and future directions, comparing techniques and analyzing their relevance. It argues that no technique alone is effective in ensuring data security. A robust solution can be developed by integrating techniques for complete security in the sharing environment. The analysis serves as a milestone for researchers and emerging applications in secure data storage and sharing.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

8. Zhenguo Chen, Liqin Tian and Chuang Lin(2018), Trust evaluation model of cloud user based on behavior data

The article introduces a novel trust evaluation model that uses behavior data, interaction data, and historical data to detect user states based on trust. This model has a higher abnormal detection rate and is light weight. Simulation results show it can better monitor user status and detect anomalies, making the cloud platform more secure. The model is designed to be dynamically updated.

9. Zhanjiang Tan; Zhuo Tang; Renfa Li; Ahmed Sallam; Liu Yang (2011), Research on trust-based access control model in cloud computing

The trust-based access control model in cloud computing is crucial in mitigating security risks and enhancing access control mechanisms. It integrates trust relationships between users, resources, and service providers, enabling adaptive, context-aware decisions. The model's practical implications include real-world applications and regulatory compliance. Future research should explore scalability enhancements, performance optimizations, and emerging technologies like blockchain or machine learning.

10. wenjuan Li, Jiyi Wu, Jian Cao, Nan Chen, Qifei Zhang & Rajkumar Buyya (2021), Blockchain-based trust management in cloud computing systems

This article presents a taxonomy and review of blockchain-based trust management approaches in cloud computing systems. It categorizes approaches into basic trust framework, enhanced trust interaction framework, and data management. A novel hybrid trust management framework and double-blockchain-based cloud transaction model are proposed to improve efficiency and adaptiveness. The paper highlights the benefits of using blockchain technology for decentralized trust management, including eliminating single points of failure, tracing and interpreting trust behavior, and preventing malicious data use.

III. PROPOSED METHODOLOGY

This research presents DBSP (domain-based storage protection), a virtual disc encryption system that enables seamless data transfer without cloud provider authority. The system uses volume metadata for key material generation and data encryption on the compute host. The user's secret key is encrypted using the RSA algorithm. The architecture involves multi-cloud storage, with user data split into four parts and encrypted using the camellia algorithm. Cloud-Trust, a cloud security assessment initiative, focuses on assessing IaaS cloud security against sophisticated attacks, including Advanced Persistent Threats (APTs).

It emphasizes a tiered defense-in-depth strategy, including checklists for generic security controls and essential components for each tier, such as network security tools, granular access restrictions, and virtual machine image security. Cloud-Trust also provides a methodology for calculating a company's cloud security posture, allowing organizations to rate or score their security, making informed decisions for enhancement. This approach is beneficial for businesses seeking an impartial evaluation of their IaaS cloud security.

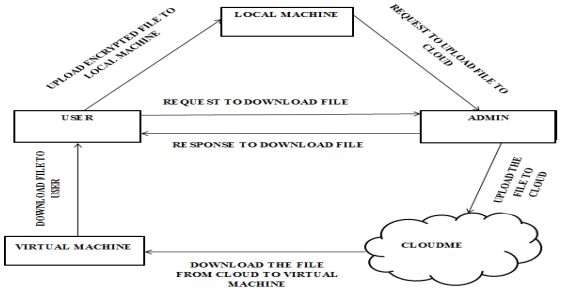

Figure 1 System Architecture

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

IV. RESULTS & DISCUSSIONS

Even with cloud computing's many benefits, security issues continue to be a major barrier, particularly for businesses that handle sensitive data. A security assessment paradigm called Cloud-Trust is developed expressly to solve these issues in Infrastructure as a Service (IaaS) clouds.

This model concentrates on how vulnerable IaaS clouds are to advanced threats, namely Advanced Persistent Threats (APTs). APTs are persistent, targeted cyberattacks with the goal of stealing or interfering with vital data. IaaS settings become extremely vulnerable when insufficient security protections are relied upon, as shown by Cloud-Trust. It highlights how crucial it is to have a "defense-in-depth" strategy, constructing several security layers to incrementally increase the difficulty of an attacker's penetration of the system.

Using network security tools, granular access restrictions, and virtual machine image security are essential components of this defense plan. By protecting virtual machine images, one may prevent vulnerabilities that can allow access to the data of other users. By limiting the likelihood of unauthorized access or privilege escalation, granular access controls make guarantee that only authorized users have access to certain resources. Lastly, to keep the cloud network safe from hackers, robust network security techniques like segmentation and intrusion detection/prevention systems are important.

Cloud-Trust enables enterprises to measure their cloud security posture and make wise decisions by providing a framework to evaluate IaaS security based on these best practices. This reduces the danger of assaults and increases user confidence in cloud settings, which opens the door for broader use.

Figure 2 Encrypt the data

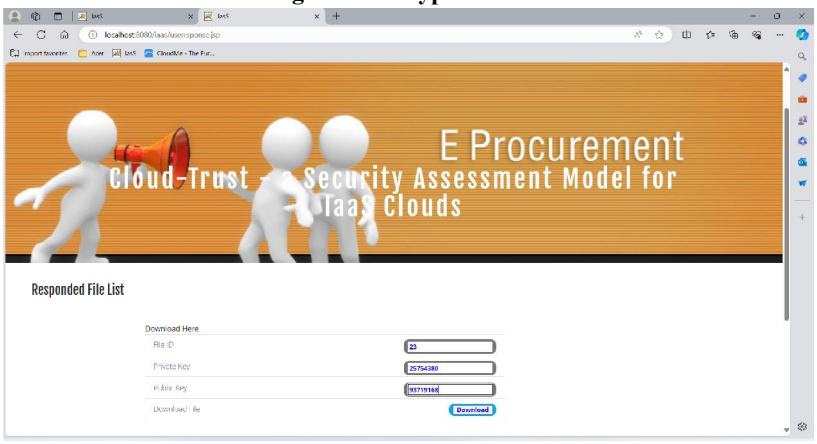

Figure 3 Download the file using private and public key

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

V. 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,the IaaS security model is getting stronger over time. This work 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.

This paper described in detail the design, implementation and security evaluation of protocols for trusted VM launch and domain-based storage protection. The solutions are based on requirements elicited by a public healthcare authority, have been implemented in a popular open-source IaaS platform and tested on a prototype deployment of a distributed EHR system. In the security analysis, this paper 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, this paperhas modelled and verified them. Finally, the performance tests have shown that the protocols introduce an 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 and applying searchable encryption schemes to create secure cloud storage mechanisms.The 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.

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.

[7]. M. Aslam, C. Gehrmann, L. Rasmusson, and M. Bjorkman, “Securely launching virtual machines on trustworthy platforms in a public cloud - an enterprise’s perspective.,” in CLOSER, pp. 511– 521, SciTePress, 2012.

[8]. Cooper and A. Martin, “Towards a secure, tamper-proof grid platform,” in Cluster Computing and the Grid, 2006. CCGRID 06. Sixth IEEE International Symposium on, vol. 1, pp. 8–pp, IEEE, 2006.

[9]. W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and efficient access to outsourced data,” in Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 55–66, ACM, 2009.

[10]. D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud data protection for the masses,” IEEE Computer, vol. 45, no. 1, pp. 39–45, 2012.