Innovative Science and Technology Publications

International Journal of Future Innovative Science and Technology
ISSN: 2454- 194X Volume - 2, Issue - 2

Manuscript Title

PRIVACY-PRESERVING PUBLIC AUDITING FOR MULTIPLE CLOUD SERVICE PROVIDERS

[1]G Porkodi, [2]V K Manavalasundhram,

P.G. Scholar, Associate Professor,

Department of Computer Science and Engineering,

[(1&2)]VELALER COLLEGE OF ENGINEERING ANG TECHNOLOGY, Thindal, Erode.

May – 2016

www.istpublications.com

International Journal of Future Innovative Science and Technology, ISSN: 2454- 194X

Volume-2, Issue-2, May - 2016 editor@istpublications.com

PRIVACY-PRESERVING PUBLIC AUDITING FOR MULTIPLE CLOUD SERVICE PROVIDERS

[1]G Porkodi, [2]V K Manavalasundhram,

P.G. Scholar, Associate Professor,
Department of Computer Science and Engineering,
[(1&2)]VELALER COLLEGE OF ENGINEERING ANG TECHNOLOGY, Thindal, Erode.

ABSTRACT

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free.To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. This project proposes a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. In addition, it articulates performance optimization mechanisms for this scheme, and in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers.

Keywords: Cloud Computing, Third Party Auditor, Optimization Mechanisms, Integrity;

1. INTRODUCTION

1.1 CLOUD COMPUTING

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

2.1 CLOUD SECURITY ISSUES

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection

sphere. An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This might be done once, multiple times, or continuously. An attacker that also has access to the processing logic of the cloud can also modify the functions and their input and output data.

Four architectural patterns are distinguished:

Replication of applications allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result.

Partition of application System into tiers allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.

Partition of application logic into fragments allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.

Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

2. RELATED WORKS

Exploring Information Leakage In Third-Party Compute Clouds

Third-party cloud computing represents the promise of outsourcing as applied to computation. Services, such as Microsoft's Azure and Amazon's EC2, allow users to instantiate virtual machines (VMs) on demand and thus purchase precisely the capacity they require when they require it. In turn, the use of virtualization allows third-party cloud providers to maximize the utilization of their sunk capital costs by multiplexing many customer VMs across a shared physical infrastructure. However, in this paper, the authors showed that this approach can also introduce new vulnerabilities. Using the Amazon EC2 service as a case study, they showed that it is possible to map the internal cloud infrastructure, identify where a particular target VM is likely to reside, and then instantiate new VMs until one is placed co-resident with the target. They explored how such placement can then be used to mount cross-VM side-channel attacks to extract information from a target VM on the same machine.It has become increasingly popular to talk of "cloud computing" as the next infrastructure for hosting data and deploying software and services. In addition to the plethora of technical approaches associated with the term, cloud computing is also used to refer to a new business model in which core computing and software capabilities are outsourced on demand to shared third-party infrastructure. While this model, exemplified by Amazon's Elastic Compute Cloud (EC2) Some of these risks are self-evident and relate to the new trust relationship between customer and cloud provider.In particular, to maximize efficiency multiple VMs may be simultaneously assigned to execute on the same physical server. Moreover, many cloud providers allow "multi-tenancy" — multiplexing the virtual machines of disjoint customers upon the same physical hardware. Thus it is conceivable that a customer's VM could be assigned to the same physical server as their adversary. This in turn, engenders a new threat that the adversary might penetrate the isolation between VMs (e.g., via a

vulnerability that allows an "escape" to the hypervisor or via side-channels between VMs) and violate customer confidentiality.This explores the practicality of mounting such cross-VM attacks in existing third-party compute clouds. The attacks they considered require two main steps: placement and extraction. Placement refers to the adversary arranging to place their malicious VM on the same physical machine as that of a target customer.Using Amazon's EC2 as a case study, they demonstrated that careful empirical "mapping "can reveal how to launch VMs in a way that maximizes the likelihood of an advantageous placement. They found that in some natural attack scenarios, just a few dollars invested in launching VMs can produce a 40% chance of placing a malicious VM on the same physical server as a target customer. Using the same platform they also demonstrated the existence of simple, low-overhead, "co-residence" checks to determine when such an advantageous placement has taken place.

Cross-Vm Side Channels And Their Use To Extract Private

The construction of an access-driven side-channel attack by which a malicious virtual machine (VM) extracts fine-grained information from a victim VM running on the same physical computer. This attack is the first such attack demonstrated on a symmetric multiprocessing system virtualized using a modern VMM (Xen). This paper addresses these challenges and demonstrates the attack in a lab setting by extracting an ElGamal decryption key from a victim using the most recent version of the libgcrypt cryptographic library.Modern virtualization technologies such as Xen, HyperV, and VMWare are rapidly becoming the cornerstone for the security of critical computing systems. This reliance stems from their seemingly strong isolation guarantees, meaning their ability to prevent guest virtual machines (VMs) running on the same system from interfering with each other's execution or, worse, exfiltrating confidential data across VM boundaries.

All Your Clouds Are Belonging To Us Security Analysis Of Cloud Management Interfaces

Cloud Computing resources are handled through control interfaces. It is through these interfaces that the new machine images can be added, existing ones can be modified, and instances can be started or ceased. Effectively, a successful attack on a Cloud control interface grants the attacker a complete power over the victim's account, with all the stored data included. In this paper, the authors provided a security analysis pertaining to the control interfaces of a large Public Cloud (Amazon) and widely used Private Cloud software (Eucalyptus). Their research results are alarming: in regards to the Amazon EC2 and S3 services, the control interfaces could be compromised via the novel signature wrapping and advanced XSS techniques. Similarly, the Eucalyptus control interfaces were vulnerable to classical signature wrapping attacks, and had nearly no protection against XSS. The cloud computing paradigm has been hailed for its promise of enormous cost-saving potential. In spite of this euphoria, the consequences regarding a migration to the cloud need to be thoroughly considered. They demonstrated that these control interfaces are highly vulnerable to several new and classical variants of signature wrapping. For these attacks, knowledge of a single signed SOAP message is sufficient to attain a complete compromization of the security within the customer's account. The reason for this easiness is that one can generate arbitrary SOAP messages accepted by this interface from only one valid

signature. To make things even worse, in one attack variant, knowledge of the (public) X.509 certificate alone enabled a successful execution of an arbitrary cloud control operation on behalf of the certificate owner.

Towards Ensuring Client-Side Computational Integrity

Privacy is considered one of the key challenges when moving services to the Cloud. Solution like access control is brittle, while fully homomorphic encryption that is hailed as the silver bullet for this problem is far from practical. At the same time it is a brittle model: data is stored in clear and vulnerable to corrupt insiders, phishing attacks on system administrators (as it was the case with the Google Aurora attacks), or a higher authority that can override the security policy.A second solution involves trusted hardware at the servers or the clients to ensure the correctness of processing as well as the confidentiality of the data. Often Trusted Computing Modules (TPM) present on most modern motherboards and even mobile hardware are relied upon, but these are not safe against adversaries with physical access to the module. Robust secure co-processors, such as the IBM4758 are expensive and slow compared with a modern computer and using those to perform all computations would deny most benefits of cloud computing. They decompose any computation to an equivalent logic circuit, and implement the basic gates in terms of the "plus" and "multiply" operations. The circuit results in a cipher text encoding the result of the computation that is sent back to the user for decryption. There are two key problems with this approach: first, no practical fully homomorphic encryption schemes exists yet [28]; second, as we will argue, even if fully homomorphic encryption was available at the cost of other cryptographic operations today, it would still be inefficient for most computations and could be replaced with a simpler architecture that is already realizable at a low cost today.

3. CONCLUSION

It is believed that almost all the system objectives that have been planned at the commencement of the software development have been net with and the implementation process of the paper is completed. A trial run of the system has been made and is giving good results the procedures for processing is simple and regular order. The process of preparing plans been missed out which might be considered for further modification of the application. The paper effectively stores and retrieves the records from the cloud space database server. The records are encrypted and decrypted whenever necessary so that they are secure.

4. FUTURE ENHANCEMENTS

The following enhancements are should be in future.

- The application if developed as web services, then many applications can make use of the records.
- The data integrity in cloud environment is not considered. The error situation can be recovered if there is any mismatch.
- The web site and database can be hosted in real cloud place during the implementation.

5.REFERENCES

[1]. Hubbard D. and Sutton M. (2010), 'Top Threats to Cloud Computing V1.0', Cloud SecurityAlliance,http://www.Cloudsecurityalliance. org/top threats.

[2]. Danezis G. and Livshits B. (2011), 'Towards Ensuring Client-Side Computational Integrity (Position Paper)', Proc. ACM Cloud Computing Security Workshop (CCSW'11), pp. 125-130.

[3]. Somorovsky J., Heiderich M., Jensen M., Schwenk J., Gruschka N., and Lo Iacono L (2011), 'All Your Clouds Are Belong to Us: Security Analysis Of Cloud Management Interfaces,' Proc. Third ACM Workshop Cloud Computing Security Workshop.

[4]. Burkhart M. and Strasser M. (2010), 'SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics', Proc.USENIX Security Symp,pp. 223-240

[5]. Mell P. and Grance T. (2011), The NIST Definition of Cloud Computing (Draft).Recommendations of the National Institute of Standards and Technology (NIST),Special Publication 800-145 (Draft).

[6].Groß S. and Schill A. (2011), 'Towards User Centric Data Governance and Control in the Cloud', Proc. IFIP WG 11.4 Int'l Conf. Open Problems in Network Security (iNetSeC), pp. 132-144.

[7]. Ristenpart T., Ristenpart E., Tromer H., Shacham S., and Savage S. (2009),'Exploring Information Leakage in Third-Party Compute Clouds', Proc.ACM Conf. Computer and Comm. Security (CCS '09), pp. 199-212.