Privacy-preserving security in hybrid cloud

Kamini Shukla
Computer Application Department
Kavikulguru Institute of Science And Technology, Ramtek
Dist. : Nagpur, India
kamini_shukla@yahoo.co.in

***Abstract*— Any businesses planning to deploy hybrid clouds should understand the different security needs and follow the industry best practices to mitigate any risks. Once secure, a hybrid cloud environment can help businesses transition more applications into public clouds, providing additional cost savings. We should focus not only on enhancing the cloud but also on building tools, technologies and processes that will make it easier for developers and architects to plug in applications to the cloud securely and easily.**

***Index Terms*— Batch Authentication, KeyGen, SigGen.**

I. INTRODUCTION

In its simplistic definition [1], a hybrid cloud is a combination of both public and private clouds. It could be a combination of a private cloud inside an organization with one or more public cloud providers or a private cloud hosted on third-party premises with one or more public cloud providers. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Organizations use the Cloud in a variety of different service models and deployment models (Private, Public, and Hybrid).

There are number of security issues/concerns associated with cloud computing but these issues fall into two broad categories:

Security issues faced by cloud providers and security issues faced by their customers[1] In most cases, the provider must ensure that their infrastructure is secure and that their clients data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. Users rely on the cloud providers for cloud data storage and maintenance. They may also dynamically interact with the cloud provider to access and update their stored data for various application purposes. For ensuring the storage security of their outsourced data, hoping to keep their data private. Cloud security is the set of security protocols and technologies that protect the cloud [2] resources and the integrity of data stored in a cloud-computing environment. Cloud security [3] differs from traditional computer security in that it is not focused on preventing access to specific machines. As Infrastructure as a Service (IaaS) grows, many IT organizations see valuable opportunities to move workloads to third-party clouds on a temporary basis. But this agility can come at a cost; the simple Internet connectivity typically used for this migration places significant limitations on security and performance. To avoid these compromises, enterprises need to make sure their hybrid cloud connectivity strategy addresses the following key elements:

- End-to-end security
- On-demand provisioning
- Deep app visibility
- Optimized app delivery

Cloud Bridge enables enterprises to meet all four of these requirements through a single solution. Extending the security and performance of datacenter networks to any public cloud, Cloud Bridge unlocks the full agility of IaaS— without compromises.

II.CLOUD COMPUTING MODELS

- Storage-as-a-service
- Database-as-a-service
- Information-as-a-service
- Business-Process-as-a-Service
- Application-as-a-service
- Platform-as-a-service
- Integration-as-a-service
- Security-as-a-service
- Management-as-a-service
- Testing-as-a-service
- Infrastructure-as-a-service

III.CLOUD COMPUTING BENEFITS

- Expand scalability
- Lower infrastructure costs
- Increase utilization
- Improve end-user productivity
- Improve reliability
- Increase security
- Saving Effort for IT Tasks
- Gain access to more sophisticated applications
- Save energy

IV.CLOUD PROVIDER SERVICE PRACTICES

- Isolation of networks
- Isolation of management networks
- Isolation of customer data networks
- Secure customer access to cloud-based resources
- Secure, consistent backups and restoration of cloud-based resources
- Strong authentication, authorization and auditing mechanisms

- A library of secure and up-to-date templates of base OS and applications

V. CUSTOMER SECURITY BEST PRACTICES

- Follow standard best practices for securing operating systems
- Encrypt critical data

VI.SECURITY CONSIDERATIONS

As organizations use hybrid clouds for their business needs, they must understand the new security requirements of a hybrid cloud environment. While hybrid clouds offer the security advantages of private clouds, there are some unique security challenges that arise as the perimeter extends beyond the organization's boundaries. Along with the typical security considerations associated with private clouds, one should consider some additional factors in a hybrid environment.

1) Perimeter extension: As a hybrid cloud extends the IT perimeter outside the organizational boundaries, it opens up a larger surface area for attacks with a section of the hybrid cloud infrastructure under the control of the service provider.

2) Identity and access management: An easier approach to solving the identity needs of hybrid clouds is to extend the existing enterprise identity and access management to the public clouds. This opens up concerns about how this approach will affect the enterprise identity and its impact on the organization's security.

3) Management tools: When organizations manage complex hybrid cloud environments using a management tool, either as a part of the cloud platform or as a third-party tool, organizations should consider the security implications of using such a tool. For example, the management tool should be able to handle the identity and enforce security uniformly across hybrid cloud environments.

4) Data migration: A hybrid cloud makes the data flow from a private environment to a public cloud much easier. There are privacy and integrity concerns associated with such data movement because the privacy controls in the public cloud environment vary significantly from the private cloud's.

5) Security policies: There are risks associated with the security policies spanning the hybrid cloud environment such as issues with how encryption keys are managed in a public cloud compared to a pure private cloud environment.

6) Privacy: Finally, providers ensure that all critical data (credit card numbers, for example) are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

7) Protect credentials: Two types of security credentials: access keys and X.509 certificates. Access key has two parts [3]: your *access key ID* and your *secret access key*. Secret key calculate signature to include request for authentication. To prevent in-flight tampering, all requests should be sent over HTTPS.

- VII. PRIVATE CLOUD SECURITY

A private cloud implementation aims to avoid many of the objections regarding cloud-computing security. Because a private cloud setup is implemented safely within the corporate firewall, a private cloud provides more control over the company's data, and it ensures security, with greater potential risk for data loss due to natural disaster. Physical security is typically handled by your service provider (Security Whitepaper), which is an additional benefit of using the cloud. In this section, some specific tools, features are recommended to implement basic security and then implement additional security best practices using standard methods as appropriate or as they see fit. The organization implementing the private cloud is responsible for network and application-level security, running and managing IT resources instead of passing that responsibility on to a third-party Companies initiate private cloud projects to enable their IT infrastructure to become more capable of quickly adapting to continually evolving needs and requirements.

VIII.PROBLEM STATEMENT

A. Threat Model

We consider a cloud service involving three different entities, the cloud user, cloud server, which is managed by cloud service provider, the third party auditor , who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud security service on behalf of the user upon request. Users rely on the cloud server for cloud data storage and maintenance. They may also dynamically interact with the cloud server to access and update their stored data for various application purposes. The users may resort to third party for ensuring the storage security of their outsourced data, while hoping to keep their data private While providing the cloud data storage based services, for their own benefits the cloud server might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the cloud server may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the third party, is reliable and independent, and thus has no incentive to collude with either the cloud server or the users. However, any possible leakage of user's outsourced data should be prohibited.

B. Design Goals of hybrid cloud

To enable privacy-preserving[4]. under the aforementioned model, our protocol design should achieve the following security and performance guarantee: 1) Confidentiality 2) Integrity 3) Availability 4) Lightweight: to allow with minimum communication and computation overhead.5) Secure and efficient capability.

C. Notation and Preliminaries

F outsourced data, denoted as a sequence of n blocks m1 . . . mn ∈ Zp for some large prime p.fkey( ) – pseudorandom function defined as: $\{0, 1\}* \times key \rightarrow Zp$.

key( ) – pseudorandom permutation

MACkey() – message authentication code function, defined as: $\{0, 1\}* \times key \rightarrow \{0, 1\}l$.

H(), h ( ) hash functions, defined as: $\{0, 1\}* \rightarrow G$, where G is some group, And some necessary cryptographic background for our proposed scheme.

IX.THE PROPOSED SCHEMES

To achieve privacy-preserving uniquely integrate the authenticator with random mask technique, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random

function. With random mask, the third party no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user's data content, no matter how many linear combinations of the same set of file blocks can be collected. Specifically, our contribution in this work can be summarized as the following three aspects:

1) To motivate the public key authentication system security in cloud-computing. [5].and provide a privacy-preserving authentication protocol, i.e., our scheme supports an external authentication to authenticate user's outsourced data in the cloud without learning knowledge on the data content.

2) To the best of our knowledge, our scheme is to support scalable and efficient public authentication in the cloud computing. In particular, our scheme achieves batch authentication where multiple delegated authenticating tasks from different users can be performed simultaneously

.3) We prove the security and justify the performance, SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once. Kerberos based. Initial sign-on prompts the user for credentials, and gets a Kerberos ticket-granting ticket (TGT).

Additional software applications requiring authentication, such as email clients etc., use the ticket-granting ticket to acquire service tickets, proving the user's identity to the mailserver / wiki server / etc. without prompting the user to re-enter credentials.

We use public key-based authentication.

X .SCHEME DETAILS

Encryption and decryption are done using the commutative ring R=<Z_n, +, X>with two arithmetic operation addition and multiplication. In RSA, the ring is public because the modulus n is public. Anyone can send data using this ring to do encryption. Key Generation Group RSA uses multiplicative groups G of prime order p.

H( ) is a secure hash function: {0, 1}∗ → G, which maps strings uniformly to G.

Another hash function h( ) : G → Zp maps group element of G uniformly to Zp.

The proposed scheme is as follows:

A. Setup Phase:

The cloud user runs RSA KeyGen to generate the system's public and secret parameters. The secret parameter is private_key= (d) and the public parameters are public_key = (e, n). Given data file F = (m1, . . . ,mn), the user runs RSA SigGen to compute signature _i for each block mi: _i ← (H(i) umi)x ∈ G (i = 1, . . . , n). Denote the set of signatures by _ = {_i}1≤i≤n. The user then sends {F, _} to the server and deletes them from its local storage. The cloud user runs RSAKeyGen to generate the system's public and secret parameter.

B. Authentication Phase:

Support for Batch Authentication With the establishment of privacy-preserving public authentication in Cloud Computing, Third party authenticator may concurrently handle multiple authentication delegations upon different users' requests. The individual authentication of these tasks for Third party authenticator can be tedious and very inefficient. Given K authenticating delegations on K distinct data files from K different users, it is more advantageous for Third party authenticator to batch these multiple tasks together and authenticated at one time. Keeping this natural demand in mind, we propose to explore the technique of aggregate signature, which supports the aggregation of multiple signatures by distinct signers on distinct messages into a single signature and thus provides efficient verification for the authenticity of all messages. Using this signature aggregation technique, we can now aggregate K verification equations into a single one, so that the simultaneous authentication of multiple tasks can be achieved. As analyzed at the beginning of this section, this approach ensures the privacy of user content during the authentication process.

XI. CONCLUSION

The economic benefits offered by public clouds are attractive enough for many organizations to push some of their non-critical workloads to such services while also using private clouds for their mission-critical needs. Such hybrid cloud deployments have proven to be advantageous not just in terms of better economics but also in terms of business agility. Advantages of infrastructures under cloud in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.

REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

[2] Jinesh Varia Amazon Web Services - Architecting for The Cloud: Best Practices January 2010 jvaria@amazon.com

[3] S. Swidler, How to keep your AWS credentials on an EC2 instance-securely, http://clouddevelopertips.blogspot.com/2009/08/how-to-keep-your-aws-credentials-on-ec2.html, 2009-08-31

[4] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.

[5] Cloud Security Alliance, "Security guidance for critical areas of-focus-in-cloud-computing," 2009,http://www.cloudsecurity alliances.org.