Analyzing of Protocol in Cloud Computing using Shared authority based Privacy-Preserving Authentication

Priti
M.Tech(CSE), Shri Baba Mast Nath Engineering College , Rohtak, India.

Sunita
Department of Computer Science and Engineering, Shri Baba Mast Nath Engineering College, Rohtak, India.

Rajiv Sharma
Department of Computer Science and Engineering, Shri Baba Mast Nath Engineering College, Rohtak, India.

Arvind
Department of Computer Science and Engineering, Shri Baba Mast Nath Engineering College, Rohtak, India.

Abstract – Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized datacenter resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. In this paper, we investigate the problem of data security in cloud data storage, which is essentially a distributed storage system. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

1. INTRODUCTION

Cloud computing enables a new business model that supports on demand, pay-for-use, and economies-of-scale IT services over the Internet. The Internet cloud works as a service factory built around virtualized data centers. Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. The idea is to migrate desktop computing to a service oriented platform using virtual server clusters at data centers. However, a lack of trust between cloud users and providers has hindered the universal acceptance of clouds as outsourced computing services. To promote multitenancy, we must design the cloud ecosystem to be secure, trustworthy, and dependable. 2 In reality, trust is a social problem, not a purely technical issue. However, we believe that technology can enhance trust, justice, reputation, credibility, and assurance in Internet applications. To increase the adoption of Web and cloud services, cloud service providers (CSPs) must first establish trust and security to alleviate the worries of a large number of users. A healthy cloud ecosystem should be free from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations. Both public and private clouds demand "trusted zones" for data, virtual machines (VMs), and user identity, as VMware and EMC 3 originally introduced. Data integrity issues in the cloud differ from those in traditional database systems. Cloud users are most concerned about whether data-center owners will abuse the system by randomly using private datasets or releasing sensitive data to a third party without authorization. Cloud security hinges on how to establish trust between these service providers and data owners. To address these issues, we propose a reputation-based trust-management scheme augmented with data coloring and software watermarking. Information about related trust models is available elsewhere.

2. EXITNG MODEL AND SECURITY

Securing Infrastructure as a Service: the IaaS model lets users lease compute storage, network, and other resources in a virtualized environment. The user doesn't manage or control the underlying cloud infrastructure but has control over the OS, storage, deployed applications, and possibly certain networking components. Amazon's Elastic Compute Cloud (EC2) is a good example of IaaS. At the cloud infrastructure level, CSPs can enforce network security with intrusion-detection systems (IDSs), firewalls, antivirus programs, distributed denial-of-service (DDoS) defenses, and so on.

Securing Platform as a Service: Cloud platforms are built on top of IaaS with system integration and virtualization

middleware support, such platforms let users deploy user-built software applications onto the cloud infrastructure using provider-supported programming languages and software tools (such as Java, Python, or .NET). The user doesn't manage the underlying cloud infrastructure. Popular PaaS platforms include the Google App Engine (GAE) or Microsoft Windows Azure. This level requires securing the provisioned VMs, enforcing security compliance, managing potential risk, and establishing trust among all cloud users and providers.

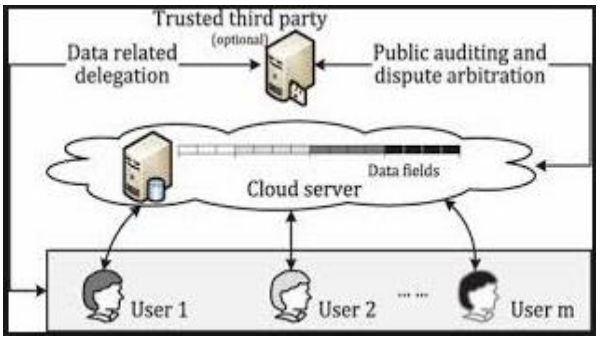

Fig: Trusted Third Party Cloud Security

Securing Software as a Service: SaaS employs browser-initiated application software to serve thousands of cloud customers, who make no upfront investment in servers or software licensing, from the provider's perspective, costs are rather low compared with conventional application hosting. SaaS — as heavily pushed by Google, Microsoft, Salesforce.com, and so on — requires that data be protected from loss, distortion, or theft. Transactional security and copyright compliance are designed to protect all intellectual property rights at this level. Data encryption and coloring offer options for upholding data integrity and user privacy.

A trusty different certificate authority (CAs) resolves

Worm containment and DDoS defense: Internet worm containment and distributed defense against DDoS attacks are necessary to insulate infrastructure from malware, trojans, and cyber criminals. This demands that we secure federated identities in public clouds.

Reputation systems for data centers: We can build reputation systems using peer-to-peer (P2P) technology or a hierarchy of reputation systems among virtualized data centers and distributed file systems. In such systems, we can protect intellectual copyright using proactive content poisoning to prevent piracy. We discuss using reputation systems in more detail shortly.

Data coloring: Our architecture can uses data coloring at the software file or data object level. This lets us segregate user access and insulate sensitive information from provider access..

Defense of Virtualized Resources Virtualization enhances cloud security. First, VMs add an additional layer of software that could become a single point of failure. That is, virtualization lets us divide or partition a single physical machine into multiple VMs (as with server consolidation), giving each VM better security isolation and protecting each partition from DDoS attacks by other partitions. Security attacks in one VM are isolated and contained — VM failures don't propagate to other VMs. A hypervisor provides the same visibility as the guest OS but with complete guest isolation. This fault containment and failure isolation VMs provide allows for a more secure and robust environment. Furthermore, a sandbox provides a trusted zone for running programs. It can provide a tightly controlled set of resources for guest OSs, which lets us define a security test bed on which to run untested code and programs from untrusted third-party vendors. With virtualization, the VM is decoupled from the physical hardware; we can represent it as a software component and regard it as binary or digital data. This implies that we can save, clone, encrypt, move, or restore the VM with ease. VMs also enable higher availability and faster disaster recovery. Live Migration and Open Virtual Format.

3. PORPOSED MODELLING

We address the aforementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. The main contributions are as follows:

1)Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.

2)Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.

3)Apply cipher text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users .We are using CloudSim Simulator for cloud based storage service.

4. CONCLUSION

In this work, we have to identify a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is

enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation.

It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

REFERENCES

[1] Rich Maggiani, 2009 Cloud Computing Is Changing How We Communicate", In IEEE 978-1-4244-4358-1/09.
[2] The Notorious Nine, Cloud Security Alliance, February 2013[Online]Available: http://www.cloudsecurityalliance.org/topthreats
[3] Ted Samson, Nine Top Threats to Cloud Computing Security, Info World, February 25, 2013 [Online] Available: http://www.infoworld.com
[4] Jianfeng Yang and Zhibin Chen, 2010 Cloud Computing Research and Security Issues", In IEEE 978-1-4244-5392-4/10.
[5] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian and Aoying Zhou,2010 Security and Privacy in Cloud Computing: A Survey, In Sixth International Conference on Semantics, Knowledge and Grids.
[6] Krešimir Popović and Željko Hocenski 2010 Cloud computing security issues and challenges, In MIPRO.
[7] Farhan Bashir Shaikh and Sajjad Haider,2011, Security Threats in Cloud Computing, In 6th International Conference on Internet Technology and Secured Transactions.
[8] Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Dr. Atanu Rakshit, 2009 Cloud Security Issues, In IEEE International Conference on Services Computing.
[9] Midya Azad Ismail, Klinsega Jeberson,"Secure Data Sharing Through Cloud Computing", In International Journal of Computer Engineering & Technology(IJCET), 2014,vol. 5, pp. 41-47
[10] Hong Lui, Huansheng Ning, Qingxu Xiong, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transaction, vol. pp no. 99, 2014.
[11] Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta, Sagar Bhavsar, Vibha Mittal, "Enhanced Security for Cloud Storage using File Encryption" Available: http://arxiv.org/ftp/arxiv/papers/1303/1303.7075.pdf

.

Authors

Ms. Priti
Department of Computer Science and Engineering, Shri Baba Mast Nath Engineering College, Rohtak, M.tech – 4th sem