Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Coloring in Trusted Uncertain Cloud Computing with Protection Control

D. Parameswari[1], G. Micheal[2], Dr. K. P. Kaliyamurthie[3]
[2] Associate Professor, [3] Head of the Department
[1, 2, 3] Department of Computer Science and Engineering,
Bharath University, Chennai, India

Abstract - Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data-center 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. Data coloring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds. Defense against tampering is tamper-proofing, so that unauthorized modifications to software (for example, to remove a watermark) will result in nonfunctional code. We briefly survey the available technology for each type of defense. Our work opens up the low-cost P2P technology for copyrighted content delivery. The advantage lies mainly in minimum delivery cost, higher content availability, and copyright compliance in exploring P2P network resources.

Key Terms: Cloud Service, Data Coloring, Watermarking

I. 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.1 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. The main sources of illegal file sharing are peers who ignore copyright laws and collude with pirates.

To solve this peer collusion problem, we propose a copyright-compliant system for legalized P2P content delivery. Our goal is to stop collusive piracy within the boundary of a P2P content delivery network. In particular, our scheme appeals to protecting large-scale perishable contents that diminish in value as time elapses. A recent surge of interest in ªmobile agentº systems has caused researchers to focus attention on a fundamentally different view of security. A malicious host attack typically takes the form of intellectual property violations. The client code may contain trade secrets or copyrighted material that, should the integrity of the client be violated, will incur financial losses to the owner of the client.

We will next consider three malicious-host attack scenarios. 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.

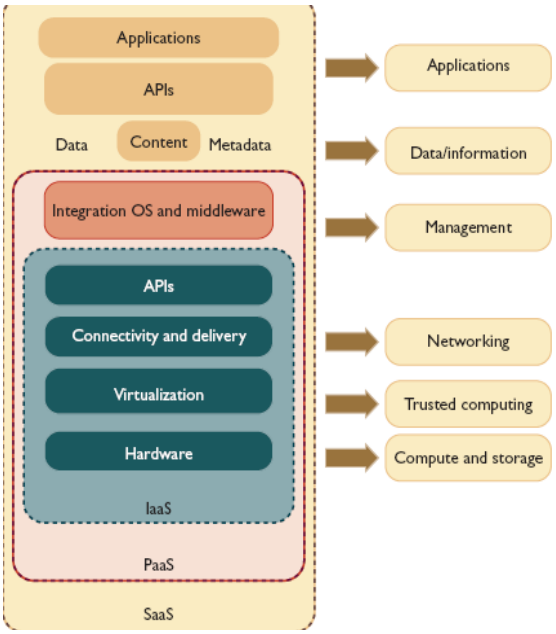
II. PROBLEM STATEMENT

2.1 Cyber-Trust Demands in Cloud Services

The Cloud Security Alliance5 has identified a few critical issues for trusted cloud computing, and several recent works discuss general issues on cloud security and privacy.1,6,7 Public and private clouds demand different levels of security enforcement. We can distinguish among different *service-level agreements* (SLAs) by their variable degree of shared responsibility between cloud providers and users. Critical security issues include data integrity, user confidentiality, and trust among providers, individual users, and user groups. The three most popular cloud service models have varying security demands.

The *infrastructure-as-a-service* (IaaS) model sits at the innermost implementation layer, which is extended to form the *platform-as-a-service* (PaaS) layer by adding OS and middleware support. PaaS further extends to the *software-as-a-service* (SaaS) model by creating applications on data, content, and metadata using special APIs. This implies that SaaS demands all protection functions at all levels. At the other extreme, IaaS demands protection mainly at the

networking, trusted computing, and compute/storage levels, whereas PaaS embodies the IaaS support plus additional protection at the resource-management level.



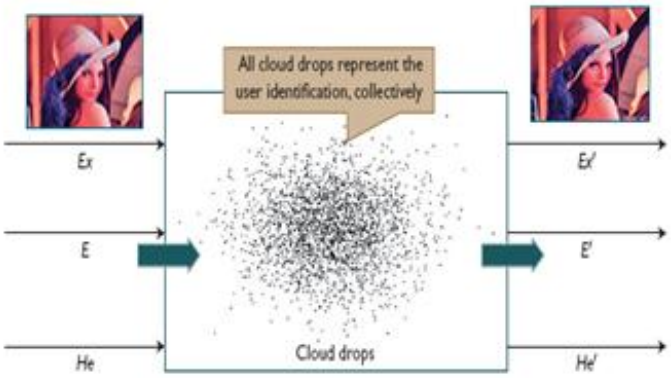
Cloud Service Model

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.

Forward and Backward data coloring processes by adding or removing unique cloud drops in data objects.
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.

2.2 Existing system

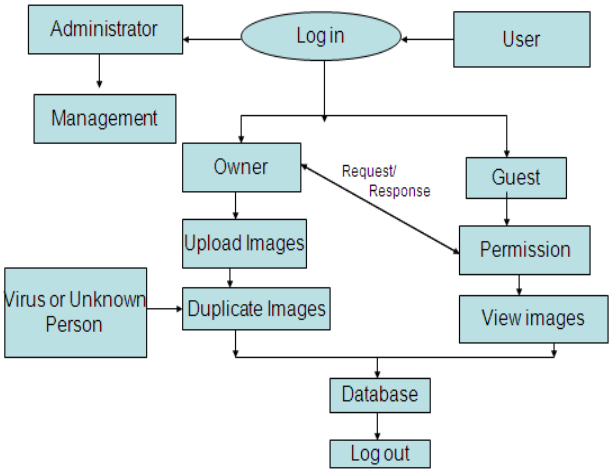
Internet clouds work as service factories built around web-scale datacenters. The elastic cloud resources and huge datasets processed are subject to security breaches, privacy abuses, and copyright violations. Provisioned cloud resources on-demand are especially vulnerable to cyber attacks. The cloud platforms built by Google, IBM, and Amazon all reveal this weaknesses. We propose a new approach to integrating virtual clusters, security-reinforced datacenters, and trusted data accesses guided by reputation systems. A hierarchy of P2P reputation systems is suggested to protect clouds and datacenters at the site level and to safeguard the data objects at the file-access level. Image management in Cloud environments is a challenging problem. If we are stored, these images may be accessed by the unauthorized persons and viruses. The Existing System does not have full security for the Images. It has security for Texts only.

2.3 Proposed system

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. Data coloring and software watermarking techniques protect shared data objects and massively distributed software modules. By using the Water Marking and Data Coloring Techniques, We are going to make the Duplicate image, When the Guest or the unauthorized person access the original Image.

III. WATERMARKING AND DATA COLORING TECHNIQUE

The Water Marking is a technique that provides the ability to make duplicate copies of Images in Cloud environment. When, the unauthorized persons or Viruses access that Image, it can only access the Duplicate Images. After getting the permission from the owner only, new person can access the image. But he can't modify the Image and settings.



Data Coloring and Watermarking

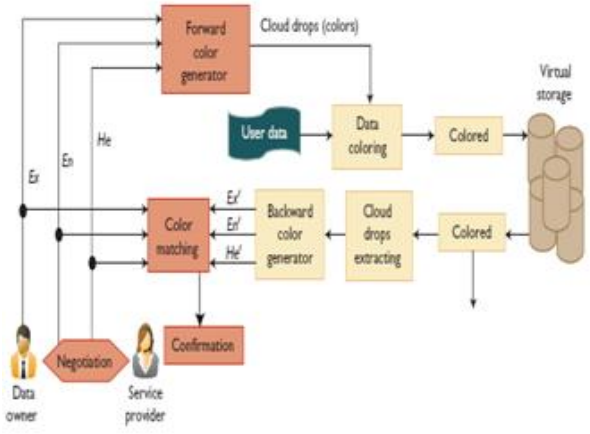
Given cloud computing's use of shared files and datasets, an adversary could compromise privacy, security, and copyright in a cloud computing environment. We want to work in a trusted software environment that provides useful tools for building cloud applications over protected datasets. In the past, watermarking was mainly used for digital copyright management. The trust model and his colleagues propose offers a second-order fuzzy membership function for protecting data owners.13 We extend this model to add unique data colors to protect large datasets in the cloud. We consider cloud security a community property. To guard it, we combine the advantages of secured cloud storage and software watermarking through data coloring and trust negotiation. Figure 4 illustrates the data-coloring concept. The woman's image is the data object being protected

3.1 Cyber-Trust Demands in Cloud Services

The Cloud Security Alliance5 has identified a few critical issues for trusted cloud computing, and several recent works discuss general issues on cloud security and privacy. Public and private clouds demand different levels of security enforcement. We can distinguish among different service-level agreements (SLAs) by their variable degree of shared responsibility between cloud providers and users.

Data Coloring and User Identification Color Matching through Trust Negotiation.

The infrastructure-as-a-service (IaaS) model sits at the innermost implementation layer, which is extended to form the *platform-as-a-service* (PaaS) layer by adding OS and middleware support. PaaS further extends to the software-as-a-service model by creating applications on data, content, and metadata using special APIs.



3.2 Trusted Cloud Computing over Data Centers

Malware-based attacks such as worms, viruses, and DoS exploit system vulnerabilities and give intruders unauthorized access to critical information. Risky cloud platforms can cause businesses to lose billions of dollars and might disrupt public services. This architecture helps insulate network attacks by establishing trusted operational zones for various cloud applications. Security compliance demands that CSPs protect all data-center servers and storage areas. Our architecture protects VM monitors (or *hypervisors*) from software-based attacks and safeguards data and information from theft, corruption, and natural disasters.

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 (see Figure 3). In such systems, we can protect intellectual copyright using proactive content poisoning to prevent piracy

3.3 Data Integrity and Privacy Protection

Cloud resources they can access with security protocols such as HTTPS or Secure Sockets Layer (SSL), as well as security auditing and compliance checking. Fine-grained access control to protect data integrity and deter intruders or hackers, as well as single sign-on or sign-off. Shared datasets that are protected from malicious alteration, deletion, or copyright violations. a method to prevent ISPs or CSPs from invading user privacy. CSPs that fight against spy ware and Web bugs; and personal firewalls and shared datasets protected from Java, JavaScript, and ActiveX Applets, as well as established VPN channels between resource sites and cloud clients.

3.4 Reputation-Guided Data-Center Protection

In the past, most reputation systems were designed for P2P social networking or online shopping services. We can convert such systems to protect cloud platform resources or user applications on the cloud. A centralized reputation system is easier to implement but demands more powerful and reliable server resources. Distributed reputation systems are more scalable and reliable for handling failures. The reputation system we propose can help providers build content-aware trusted zones using the VMware vShield and the RSA DLP package for data traversing monitoring.

Reputation represents a collective evaluation by users and resource owners. Researchers have proposed many reputation systems in the past for P2P, multi-agent, or e-commerce systems. To support trusted cloud services, we suggest building a *trust-overlay network* to model the trust relationships among data-center modules. Runfang Zhou and Kai Hwang first introduced the idea of a trust overlay for e-commerce.

IV. CONCLUSION AND FUTURE ENHANCEMENT

This can initiate various trust-management events, including authentication and authorization. Virtual storage supports color generation, embedding, and extraction. Combining secure data storage and data coloring, we can prevent data objects from being damaged, stolen, altered, or deleted. Thus, legitimate users have sole access to their desired data objects. The computational complexity of the three data characteristics is much lower than that performed in conventional encryption and decryption calculations in PKI services. The watermark-based scheme thus incurs a very low overhead in the coloring and discoloring processes. The *En* and *He* functions' randomness guarantees data owner privacy. These characteristics can uniquely distinguish different data objects.

Providers can implement our proposed reputation system and data-coloring mechanism to protect data-center access at a coarse-grained level and secure data access at a fine-grained file level. In the future, we expect that *security as a service* and *data protection as a service* will grow rapidly. These are crucial to the universal acceptance of Web-scale cloud computing in personal, business, finance, and digital government applications. Internet clouds demand that we globalize operating and security standards. The interoperability and mesh-up among different clouds are wide-open problems. Cloud security infrastructure and trust management will play an indispensable role in upgrading federated cloud services.

REFERENCES

[1] K. Hwang, G. Fox, and J. Dongarra, *Distributed Systems and Cloud Computing: Clusters, Grids/P2P, and Internet Clouds*, Morgan Kaufmann, to appear, 2010.

[2] K. Hwang, S. Kulkarni, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Management," *IEEE Int'l Conf. Dependable, Autonomic, and Secure Computing* (DASC 09), IEEE CS Press, 2009.

[3] J. Nick, "Journey to the Private Cloud: Security and Compliance," tech. presentation, EMC, Tsinghua Univ., 25 May 2010.

[4] S. Song et al., "Trusted P2P Transactions with Fuzzy Reputation Aggregation," *IEEE Internet Computing*, vol. 9, no. 6, 2005, pp. 24–34.

[5] "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, Apr. 2009; www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[6] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly Media, 2009.

[7] J. Rittinghouse and J. Ransome, *Cloud Computing: Implementation, Management and Security*, CRC Publisher, 2010.

[8] X. Lou and K. Hwang, "Collusive Piracy Prevention in P2P Content Delivery Networks," *IEEE Trans. Comput-ers*, July 2009, pp. 970–983.

