Data Coloring in Trusted and Ambiguous Cloud Computing using Sheltered Possessions Machine Learning Technique

[1]Ellappan Venugopal, [2]Dr Rajesh Thumma, [3] Dr. R. Sreeparimala, [4]Dr.Anusha K,[5] Dr. T. Thulasimani

[1]Assistant Professor, Department of Electronics and Communication Engineering, Image and Signal processing (SIG), School of Electrical Engineering and Computing ,Adama Science and technology University, Adama, Ethiopia.

[2]Associate Professor, Department of Electronics and Communication Engineering, Anurag Group of Institutions, Venkatapur (v), Hyderabad, Telangana-500088.

[3]Associate Professor, Department of Mathematics, Sri Eshwar College of Engineering, Coimbatore, Tamilnadu – 641202.

[4]Associate Professor, School of Computer Science and Engineering, VIT Chennai, Vellore Institute of Technology, Chennai, Tamilnadu – 600 127.

[5]Assistant Professor, Department of Mathematics, Bannari Amman Institute of Technology, Sathyamangalam-638401, Erode District, Tamilnadu, India.

Abstract - Confidence and security prevent businesses from fully embracing cloud platforms. To protect the clouds, providers must first secure virtualized data-center resources, uphold user privacy, and protect data integrity. The authors suggest that the trust overlay network be used through multiple data centers to implement a reputation system to build trust between service providers and data owners. Data coloring and software watermarking methods protect shared data objects and highly distributed software modules. These strategies protect multi-path authentication, enable a single sign-on in the cloud, and tighten access control for sensitive data in the public and private clouds. Protection against tampering is tamper proofing, so unauthorized changes to the software (for example, removing a watermark) can lead to passive code. We will briefly examine the technology available for each type of protection. P2P technology opens our work to low cost copyrighted content delivery. The advantages are mainly delivery cost, high content availability and copyright compliance in exploring P2P network resources.

Key Terms: Cloud Service, Data Coloring, Watermarking, Machine Learning, Shelter Possios

1. Introduction

Cloud computing allows a new business model that supports on-demand, spot payment and economy-of-scale IT services over the Internet. The Internet cloud acts as a service factory built into virtualized data centers. The idea is to turn desktop computing into a service-oriented platform using virtual server clusters in data centers. However, the lack of trust between cloud users and providers has hampered the universal acceptance of clouds as outsourced computing services. The main source of illegal file sharing is associates who ignore copyright laws and associate with pirates [1].

To resolve this peer-to-peer issue, we recommend a copyright-compliant system for legalized P2P content delivery. Our goal is to prevent mass piracy within the boundaries of the P2P content delivery network. In particular, our scheme appeals to protect large-scale corrupted content from deteriorating over time. The recent rise in interest in mobile agent systems has led researchers to focus on fundamentally different perspectives on security. A malicious host attack is usually a property ownership violation. The client code may contain trade secrets or copyrighted material, which, if infringed on the client's integrity, may cause financial loss to the client owner [2].

We will look at malicious-host attack situations next. Cloud users are increasingly concerned about whether data center owners could abuse the system by randomly using private datasets or releasing sensitive data to unauthorized third parties. How to increase trust between these service providers and data owners is related to cloud security. To address these issues, we propose a reputation-based trust-management scheme developed using data coloring and software watermarking. Information on relevant trust models is available elsewhere [3].

2. Problem Statement

A. Cyber-trust requirements in cloud services

Cloud Security Alliance 5 identifies some critical issues for reliable cloud computing and discusses many recent issues related to cloud security and privacy.1,6,7 Public and private clouds require different levels of security management. We can identify different service-level agreements (SLAs) using variable degrees of shared responsibility between cloud providers and customers. Serious security issues include data integrity, consumer privacy and trust between providers, individual users and user groups. The three most popular cloud service models have different security requirements [4][5].

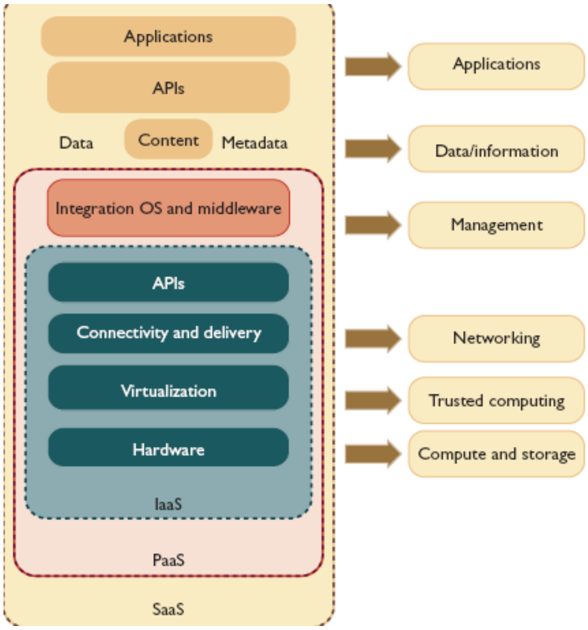

Figure 1. API Cloud Service Model

The Infrastructure-in-a-Service (IAS) model is based on an internal implementation layer that extends to create a platform-a-service (PASS) layer with OS and middleware support. PaaS extends across the Software-a-Service (SaaS) model and creates applications on data, content and metadata using specialized APIs. This indicates that SaaS requires all security measures at all levels. On the other hand, IAS protection is required primarily at the networking, trusted computing, and computer / storage levels, while PASS provides additional protection at the IAS support and resource management level [6] [7].

3. Secure infrastructure as a service

The IAS model allows users to lease computer, storage, network and other resources in a virtualized environment. The user does not control or regulate basic cloud infrastructure, but has control over the OS, storage, executed applications, and certain network components. The best example of IaaS is Amazon's Elastic Compute Cloud (EC2). At the cloud infrastructure level, CSPs can enable network security using intrusion-detection systems (IDS), firewalls, antivirus programs, and distributed denial-service (DDOS) protection.

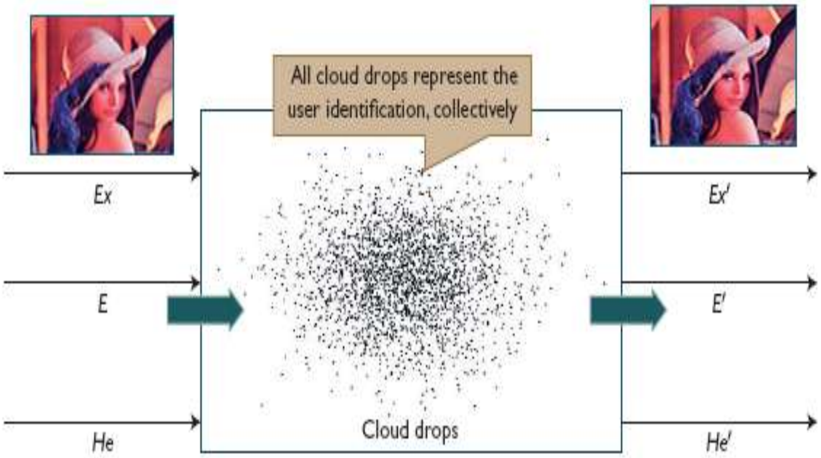
All cloud drops represent the user identification, collectively
Ex
E
He
Cloud drops
Ex'
E'
He'

Figure 2. Forward and Backward data coloring processes by adding or removing unique cloud drops (colors) in data objects.

A. Securing the platform as a service

Cloud platforms are built on top of IaaS with system integration and virtualization middleware support. Such platforms allow users to integrate user-built software applications into cloud infrastructure using provider-supported programming languages and software tools (such as Java, Python, or .NET). Basic cloud infrastructure is not controlled by the user. Popular pass platforms include Google Play Engine (GAE) or Microsoft Windows Azure. This requires assigning VMs to enable security, security enforcement, potential risk management and confidence building across all cloud customers and providers.

B. Existing system

Internet clouds act as service factories built around web-level datacenters. Elastic cloud sources and large processed datasets are subject to security breaches, privacy breaches and copyright infringement. Provided cloud resources are vulnerable to cyber attacks. Cloud platforms built by Google, IBM and Amazon reveal these vulnerabilities. We propose a new approach to integrating trusted data accessed by virtual clusters, secure datacenters, and popular systems [7]. Specifies a range of P2P reputation systems to protect clouds and datacenters at the site level and data objects at the file-access level. Image management in cloud environments is a challenging issue. If we store these images, these images can be accessed by unauthorized persons and viruses. The current system does not have complete security for images. It only has text security [8].

C. Specific approach

The authors suggest that the trust overlay network be used through multiple data centers to implement a reputation system to build trust between service providers and data owners. Data coloring and software watermarking methods protect shared data objects and highly distributed software modules. Using water marking and data coloring techniques, we are going to create a dummy image when a guest or unauthorized person accesses the original image.

4. Watermarking and Data Coloring Techniques

Watermarking is a technology that allows you to create duplicate images of images in a cloud environment. When an unauthorized person or virus accesses that image, it can only access duplicate images. After obtaining permission only from the owner, the new person can access the image. But he cannot modify the image and settings.

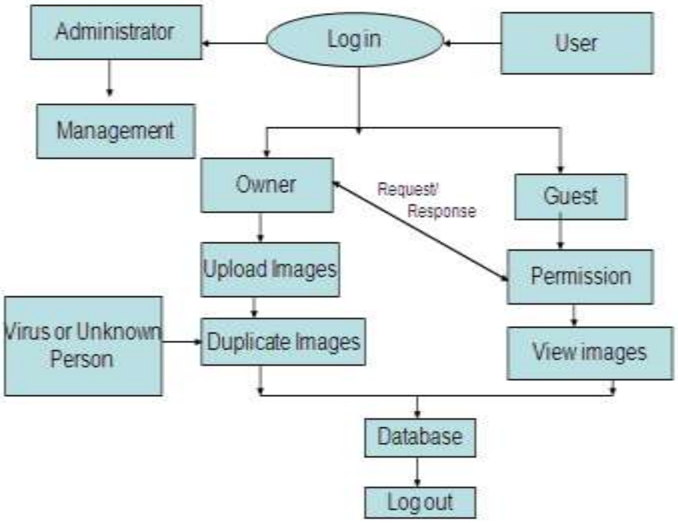

Figure 3. Data Coloring and Watermarking Representation in Cloud Space

By using shared files and datasets in cloud computing, privacy, security and copyright can be compromised in an hostile cloud computing environment. We want to work in a trusted software environment that provides useful tools for creating cloud applications on protected datasets. In the past, watermarking was primarily used for digital copyright management. Christian Kolberg and Clark Thompson suggested using watermarking to protect software modules. 12 Second Order Trust Model Die Lee & Co. to Protect Data Owners. Indicated, which provides a dim membership functionality. Colors to protect large datasets in the cloud. We consider cloud security as a community asset. To protect this, we combine the benefits of secure cloud storage and software watermarking through data coloring and trust negotiations. Figure 4 illustrates the data-coloring concept. The image of the woman is a protected data object.

A. Cyber-trust requirements in cloud services

Cloud Security Alliance 5 identifies some critical issues for trusted cloud computing and several recent works discuss common issues related to cloud security and privacy. Public and private clouds require different levels of security. We can identify different service-level agreements (SLAs) using variable degrees of shared responsibility between cloud providers and customers.

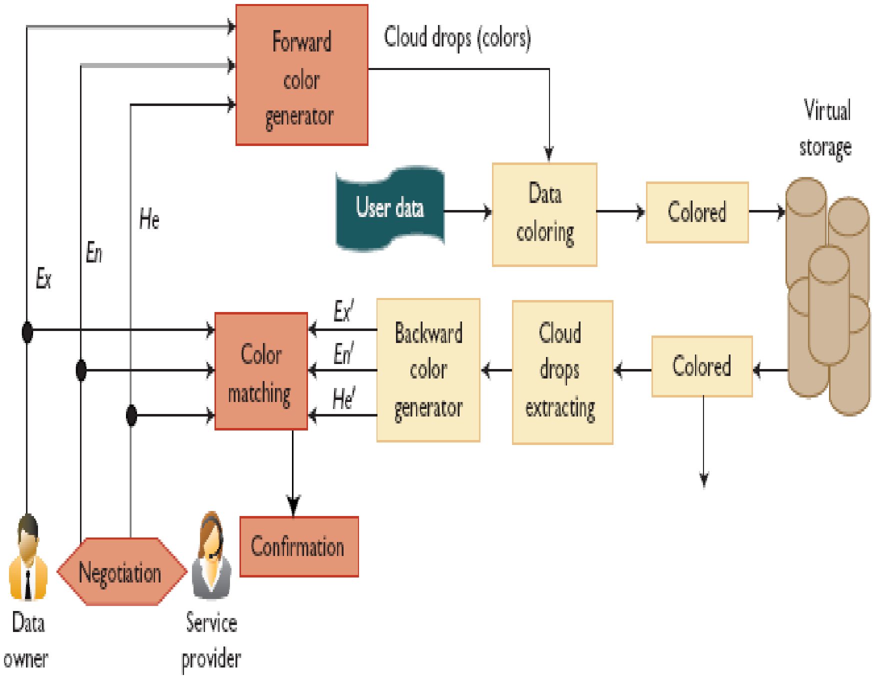

Figure 4. Data Coloring and User Identification Color Matching through Sheltered Possessions Machine Learning Technique

The Infrastructure-in-a-Service (IAS) model is based on an internal implementation layer that extends to create a platform-a-service (PASS) layer with OS and middleware support. PaaS extends across the Software-a-Service (SaaS) model and creates applications on data, content and metadata using specialized APIs.

B. Reliable cloud computing in data centers

Malware-based attacks such as worms, viruses and DoS exploit system vulnerability and allow intruders to gain access to critical information. Dangerous cloud platforms can cost businesses billions of dollars and disrupt public services. This structure helps prevent network attacks by setting up reliable work areas for various cloud applications. Security compliance requires CSPs to protect all data-center servers and storage areas. Our architecture protects VM monitors (or hypervisors) from software-based attacks and data and information from theft, corruption and natural disasters. We can build reputation systems using peer-to-peer (P2P) technology or a series of reputation systems between virtualized data centers and distributed file systems (see Figure 3). In such systems, we may protect active copyright by using active content to prevent piracy.

C. Data integrity and privacy protection

Cloud resources that they can access through security protocols such as HTTPS or Secure Sockets Layer (SSL), Security Auditing and Compliance Verification. Excellent access control to protect data integrity, repel intruders and hackers and make a single sign-on or sign-off. Shared datasets from malicious modification, deletion or copyright infringement. A way to prevent ISPs or CSPs from invading user privacy. CSPs battling spyware and web bugs; And VPN channels for personal firewalls, shared datasets, resource sites and cloud clients protected from Java, JavaScript and ActiveX applications.

D. Impression-guided data-center protection

In the past, most reputation systems were designed for P2P social networking or online shopping services. We can modify such systems to protect cloud platform resources or user applications within the cloud. A centralized assessment system is easier to implement, but requires more powerful and reliable server resources. Distribution reputation systems are more measurable and reliable to deal with failures. The reputation system we recommend for providers helps us create content-conscious trust zones using the VMware Whistle and RSA DLP package for data tracking monitoring. Reputation refers to the collective evaluation of consumers and resource owners. Researchers have previously suggested several reputation systems for P2P, multi-agent or e-commerce systems. To support trusted cloud services, we propose to build a trust overlay network to model trust relationships between data-center modules. Ranfang Shou and Kai Hwang first introduced the idea of a trust overlay for e-commerce.

5. Conclusion and future improvements

It can initiate various trust-management events, including authentication and recognition. Virtual storage supports color generation, embedding and extraction. By combining secure data storage and data coloring, data objects can be prevented from being damaged, stolen, altered or deleted. Therefore, legal users only have access to the data objects they want. The computational complexity of the three data features is much lower than that done on traditional encryption and decryption calculations on PKI services. The watermark based scheme offers very little overhead in color and fading processes. N and Hi functions work 'Ensures data owner privacy. These features can uniquely identify different data objects. Providers can implement our specific reproduction and data-coloring system to protect data-center access at the coarse-grain level and to securely secure data access at the best data level. In the future, we expect that *security as a service* (SECaaS) and *data protection as a service* (DPaaS) 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, 2019.
2. Nandhini. R, Pavithra. P, Abinaya. P and S.Manikandan, "Information Technology Architectures for Grid Computing and Applications ", International Journal of Advanced Research Computer Engineering and Technology, ISSN:2278-1323, Vol.3, No.06, pp:2239-2242,June'2014
3. Haripriya S, Indumathi , S.Manikandan, "Virtual Network Connection Using Mobile Phones", COMPUSOFT, An International Journal of Advanced Computer Technology, ISSN:2320-0790, Vol.03, Issue: 06, pp-980-984, June-2014.
4. S. Song et al., "Trusted P2P Transactions with Fuzzy Reputation Aggregation," *IEEE Internet Computing*, vol. 9, no. 6, 2015, pp. 24–34.
5. Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, Apr. 2019; 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, 2019.
7. J. Rittinghouse and J. Ransome, *Cloud Computing: Implementation, Management and Security,* CRC Publisher, 2018.
8. X. Lou and K. Hwang, "Collusive Piracy Prevention in P2P Content Delivery Networks," *IEEE Trans. Computers,* July 2017, pp. 970–983.
9. Bornea M.A , Vassalos V, Kotidis Y, and Deligiannakis A, (2009) "Double Index NEsted-loops Reactive join for Result Rate Optimization," Proc. IEEE Int'l Conf. Data Eng. (ICDE).

10. Negri M. and Pelagatti G. (2010) “Join During Merge: An Improved Sort Based Algorithm,” Information Processing Letters vol. 21, no. 1, pp. 11-16.
11. S. Manikandan and K. Manikanda Kumaran, "Identifying Semantic Identifying Semantic Relations Between Disease And Treatment Using Machine Learning Approach", International Journal of Engineering Research & Technology(IJERT), essn:2278-0181,Vol.2,June - 2013.