International Journal of Engineering Research and General Science Volume 2, Issue 5, August-September, 2014
ISSN 2091-2730

Survey on Web Image Mining

Kumari Priyanka Sinha [1], Praveen Kumar[1]

[1] Indian Institute of Information Technology

E-mail- Priyankasinha2008@gmail.com

Abstract— In this paper a literature survey on web image mining is presented. Web image mining is a technique of searching ,retrieving and accessing the data from an image, There are two type of web image mining techniques i.e. Text based web image mining and image based web image mining. The objective of this paper is to present tools and technique which are used in past and current evaluation. We are also going to showa chart for comparison between all past available techniques and we will show a summarize report for overall development in web image mining.

Keywords: Web image mining,Accountability, image retrieval, data mining,Web image ,Cloud Computing and mining.

INTRODUCTION

In the field of information technology (IT), there has emerged a new buzzword called Cloud Computing. It is de-scribed as the future and that everyone should move into the so called Cloud. Cloud computing has generated significant interest in both fields i.e. academic and industry, but it is still an evolving paradigm. Essentially, its aim to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pool of computers, networks, and storage resources. Confusion exists in IT communities about how a cloud differs from existing models and how these differences affect its adoption. Some see a cloud as a novel technical revolution, while others consider it a natural evolution of technology, economy, and culture [1]. Nevertheless, cloud computing is an important paradigm, with the potential to significantly reduce costs through optimization and increased operating and economic efficiencies [1], [2]. Furthermore, cloud computing could significantly enhance collaboration, agility, and scale, thus enabling a truly global computing model over the Internet infrastructure. However, without appropriate security and privacy solutions designed for clouds, this potentially revolutionizing computing paradigm could become a huge failure. Several surveys of potential cloud adopters indicate that security and privacy is the primary concern for itadoption.

TAXONOMY OF CLOUD COMPUTING

Cloud is Xaas offerings where X is software, hardware, platform, infrastructure, data, business etc. [3].The taxonomy is more than defining the fundamentals that provides a framework for understanding current cloud computing offerings and suggests what's to come. In Cloud Computing system we have to address fundamentals like virtualization,scalability, interoperability, quality of service, fail over mechanism and the cloud delivery models within the context of taxonomy. Our main idea behind this taxonomy is to find about fundamental of cloud computing.

CLOUD SERVICES MODELS

Software as a service (SaaS): In SaaS, the cloud providers enable and provide application software as on-demand services. Because clients acquire and use software components from different providers, crucial issues include securely composing them and ensuring that information handled by these composed services is well protected.

Platform as a service (PaaS):PaaS enables programming environments to access and utilize additional application building blocks. Such programming environments have a visible impact on the application architecture, such as constraints on which services the application can request from an OS. For example, a PaaS environment might limit access to well-defined parts of the file system, thus requiring a fi-negrained authorization service.

Infrastructure as a service (IaaS): In this service, the cloud provider supplies a set of virtualized infrastructural components such as virtual machines (VMs) and storage on which customers can build and run applications. The application will eventually reside on the VM and the virtual operating system. Issues such as trusting the VM image, hardening hosts, and securing inter-host communication are critical areas in IaaS.

Hardware as a service (Haas): According to Nicholas Carr the idea of buying IT hardware or even an entire data center as a pay as you go subscription service that scales up or down to meet your needs. But as a result of rapid advances in hardware virtualization,

IT automation and usage metering and pricing, It is the concept of Hardware as a service. This model is advantageous to the enterprise users, since, it don't need to invest in building and managing data centers.

CLOUD DEPLOYMENT MODELS

Public**:**The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling Cloud services [4].Public clouds are external or publicly available cloud environment that are accessible to multiple tenants.

Private**:**The Cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off premises [3].Private clouds are typically tailored environments with dedicated virtualized resources for particular organizations.

Community: The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and exist on-premises or off premises [4].Community clouds are tailored for particular groups of customers.

Hybrid:The Cloud infrastructure is a composition of two or more Clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load-balancing between Clouds)[5].It is Combination of any two cloud deployment model.

IV.VIRTUALIZATION MANAGEMENT

It is the technology that abstracts the coupling between the hardware and operating system. It used for providing abstraction of logical resource from their underlying physical resource in order to improve agility, flexibility, reduce costs.There are also types of virtualization[6] such as Server virtual-ization, storage virtualization and network virtualization. In a virtualized environment, computing resource can be dynamically created, expanded, shrunk or moved as per demandvaries. Therefore, it is well suited for dynamic cloud infra-structure which provides sharing, manageability and isolation.

V.FAULT TOLERANCE

Whenever there is a backup instance of application which is ready to take over without disruption in case of failure is called failover[7]. Fault tolerance is the feature of distributed computing in which system provides its intended service in case of failure of some of its component. Unlike isolated instances that are de-played in a silo structure multi-tenancy is a large community which is hosted by the provider. This could only be practical when the applications are stable, reliable, customizable, se-cure, and upgradeable which the provider usually handles. It can be viewed in two different perspectives, the client and the provider.

The clients could use a public Cloud service or actually be part of the organization that is hosting the Cloud, but would still be part of the infrastructure. The provider view is that multi-tenancy will allow for providers to enable economies of scale, availability, operational efficiency and use of applications to multiple users.

Service Level Agreement: A Service Level Agreement (SLA)[8] is in general a legal binding agreement about a service a client is buying from a Service Provider (SP). The agreement is a part of a much bigger contract between two partners that define the purchased service. The levels included are a frame of how the service should be delivered and failure to follow this agreement is usually followed by penalty, which should also be defined in the agreement. The three principles are the main concerns when dealing with information security and each principle requires different security mechanisms to be able to be enforced. For Cloud Computing to be considered to be secure, these principles are what it has to live up to.To enforce these principles there are different mechanisms that can be applied. The mechanisms are retrieved from a blog called Continuity Disaster.

VI. RISK

Isolations Failure:-The failure of hardware separates storage, memory, routing and even reputation between different tenants[9].

Compliance Risk: Investment in achieving certification may be put at risk by moving to the Cloud.

Management Interface Compromise: Customers man-agreement interfaces of Public Cloud providers are accessible through the Internet and mediate access to larger sets of resources, which pose an increased risk.

Data Protection: The ability of the customer to check the data handling practices of the Cloud provider and to ensure that the data is treated in a lawful manner.

Insecure or incomplete data deletion: Customer requesting that their data is deleted and it is not completely removed or deleted due to duplication.

Abuse and Nefarious Use of Cloud Computing: Easy access and lack of control of who is using Cloud Computing can provide entrance for malicious people.

Insecure Interfaces and APIs: Authentication and reusable aces tokens/passwordshave to be properly managed or security issues will rise.

Malicious Insider: Lack of insight at the Cloud provider's employees can trigger risks if employees have malicious intent and access to information he/she should not have.

Shared Technology Issues: With scalability come shared technology issues since the provider is using their own re-sources to provide more for the clients during peaks.

With sharing technology the risk of hypervisors appear since hypervisors work in between different clients.

Data Loss and Leakage: Improper deletion or backup of data records can lead to unwanted duplication of data that becomes available when it should not exist.

Account or Service Hijacking: Phishing for credentials to get access to sensitive data.

Unknown Risk Profile: No insight in what the provider do to keep your data safe or doing updates, patches etc.

VII.SECURITY AND PRIVACY

Cloud Computing is a new computing model, regardless of the system's architecture or service's deployment is different from the traditional computing model. Therefore traditional security policies are not able to respond to the emergence of new cloud computing security issues. We review the Security and Privacy implication and challenges of cloud computing[10].

computing, SLAs are necessary to control the use of computing resources. (Mainly used in utility based or on demand services).

VIII. SECURITY AND PRIVACY CHALLENGES

Since, Cloud computing environments are multi-domain environments in which each domain can use different security, privacy, and trust requirements and employ various mechanisms, interfaces, and semantics. Such domains could represent individually enabled services or other infrastructural or application components. It is important to leverage existing research on multi-domain policy integration and the secure-service composition to build a comprehensive policy-based management framework in cloud computing environments.

CONCLUSION

The core objective of this research was to explore the Taxonomy of cloud computing with security and privacy challenges. There are many open issues regarding the cloud computing but security and privacy risks are enormous. Enterprise looking into cloud computing technology as way to cut down on cost and increase profitability should seriously analyze the security and privacy risk of cloud computing. A taxonomy of cloud computing provide ideas of researcher and developer on the current cloud systems, hype and challenges. It also gives the information to evaluate and improve the existing and new cloud system. We see the Security and privacy implication with the existing challenges. The strength of cloud computing is the ability to manage risk more effectively from centralized point of view. Security updates and new patches can be applied more effectively. The weakness include list of issues such as security and privacy of business data which is being hosted in 3rd party data centers, being lock-in to a platform reliability/performance concerns, and the fears of making the wrong decision before the industry begins to mature. Enterprise should verify and understand the cloud security, its benefits with future scope, carefully analyze the security issues involved and plan for ways to resolve it before implementing the technology. Some pilot tools should be setup and good governance should be put in place to effectively deal with security issues and concerns. It should be planned and it should be gradual over a period of time. It has been identified that especially the areas of standardization and interoperability need to evolve. Virtualization and Hypervisors is so nascent. We should do much more experiment with them in order to provide services such as Iaas (Infrastructure as a Service). It means virtualization is next key issues for cloud computing.

The security addressed by the taxonomy only considers security measures between the client and the cloud. An important addition to the taxonomy will be to also consider the security mechanisms used within the cloud.

REFERENCES:

I. CLOUD SECURITY ALLIANCE, *SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V2.1*

II. D. CATTEDDU AND G. HOGBEN, *CLOUD COMPUTING: BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY, ENISA* 2009.

III. http://en.wikipedia.org/wiki/Cloud_computing

IV. Brandl D. *Don't cloud your compliance data.*2010.

V. Gathering Clouds of Xaas! http://www.ibm.com/developer

VI. BHASKAR PRASAD RIMAL AND IAN LUMB,*A TAXONOMY AND SURVEY OF CLOUD COMPUTING SYSTEMS, 2009*.

VII. National Institute of Standards and Technology (NIST http://csrc.**nist**.gov/publications/**nist**pubs/800-145/SP800-145.pdf)

VIII. . CSA (2009 December) Security guidance for critical areas of focus in Cloud Computing v2.1, Cloud Security Alliance.

IX. http://cloudtaxonomy.opencrowd.com

X. B. D. JAMES AND HASSAN TAKABI *SECURITY AND PRIVACY CHALLENGES IN CLOUD COMPUTING ENVIRONMENT*, 2010