An Integrated Approach for Cloud based Web Secure Web Services

[1]Sakshi Bhatia, [2]Dr.Vikram Singh, [3]Aastha
[1,3]Technological Institute of Textile and sciences, Haryana, India.
[2]Chaudhary Devi Lal Unversity,Haryana, India.

Abstract
Cloud computing is the provision of dynamically scalable and often virtualized resources as a service over the Internet on a utility basis. Cloud computing services often provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. The term cloud is used as a metaphor for the Internet, based on how the Internet is depicted in computer network diagrams and is an abstraction of the underlying infrastructure it conceals. We are providing a location independent way of database access without contacting the data at one place. The databases are presents in different locations in the form of clouds. Whenever user will send a request it will itself resolve the query and present it to the user. We want to present it as database services that will provide the computing capability over the web. It is described as" a computing capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Keywords
cloud, web service, computing, security

I. Introduction

Cloud computing provides cheap and pay-as-you-go computing resources are rapidly gaining momentum as an alternative to traditional IT Infrastructure. As more and more consumers delegate their tasks to cloud providers, Service Level Agreements (SLA) between consumers and providers emerge as a key aspect. Due to the dynamic nature of the cloud, continuous monitoring on Quality of Service (QoS) attributes is necessary to enforce SLAs. Also numerous other factors such as trust (on the cloud provider) come into consideration, particularly for enterprise customers that may outsource its critical data. With the advancement of the modern human society, basic essential services are commonly provided such that everyone can easily obtain access to them.

This vision of the computing utility based on the service provisioning model anticipates the massive transformation of the entire computing industry in the 21st century whereby computing services will be readily available on demand, like other utility services available in today's society. Similarly, computing service users (consumers) need to pay providers only when they access computing services. In addition, consumers no longer need to invest heavily or encounter difficulties in building and maintaining complex IT infrastructure.

Cloud is defined as both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.

Software practitioners are facing numerous new challenges toward creating software for millions of consumers to use as a service rather than to run on their individual computers. Over the years, new computing paradigms have been proposed and adopted, with the emergence of technological advances such as multicore processors and networked computing environments, to edge closer toward achieving this grand vision. As shown in Fig. 1, these new computing paradigms include cluster computing, Grid computing, P2P computing, service computing, market- oriented computing, and

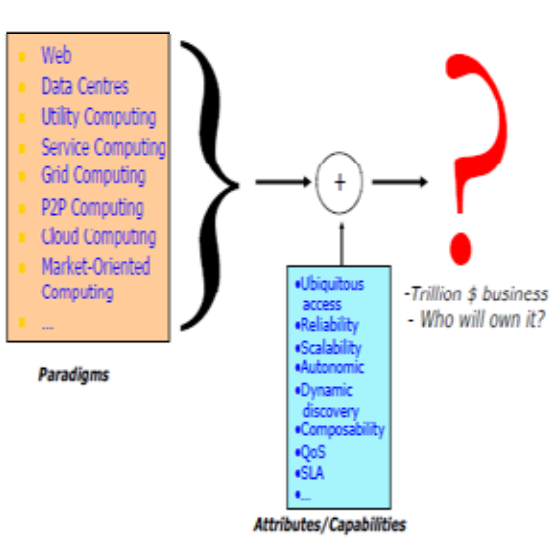

Fig. 1: Various paradigms promising to deliver IT as a service.

most recently Cloud computing. All these paradigms promise to provide certain attributes or capabilities in order to realize the possibly 1 trillion dollars worth of the utility/pervasive computing industry as quoted by Sun Microsystems co-founder Bill Joy. Computing services need to be highly reliable, scalable, and autonomic to support ubiquitous access, dynamic discovery and composability. In particular, consumers can determine the required service level through Quality of Service (QoS) parameters and Service Level Agreements (SLAs). Of all these computing paradigms, the two most promising ones appear to be Grid computing and Cloud computing.

II. Technical security issues in cloud computing

The new concept of Cloud Computing offers dynamically scalable resources provisioned as a service over the Internet and therefore promises a lot of economic benefits to be distributed among its adopters. Depending on the type of resources provided by the Cloud, distinct layers can be defined (see Fig. 2).The bottom-most layer provides basic infrastructure components such as CPUs, memory, and storage, and is henceforth often denoted as Infrastructure-as a-Service (IaaS).

Amazon's Elastic Compute Cloud (EC2) is a prominent example for an IaaS offer. On top of IaaS, more platform-oriented services allow the usage of hosting environments tailored to a specific need. Google App Engine is an example for a Web platform as as service (PaaS) which enables to deploy and dynamically

scale Python and Java based Web applications. Finally, the top-most layer provides it users with ready to use applications also known as Software as-a Service (SaaS). To access these Cloud services, two main technologies can be currently identified. Web Services are commonly used to provide access to IaaS services and Web browsers are used to access SaaS applications. In PaaS environments both approaches can be found.

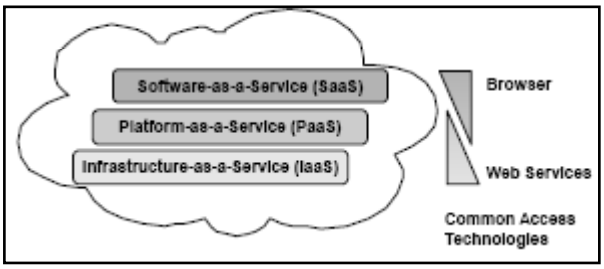

Fig. 2: Cloud layers and access technologies

All of these layers come with the promise to reduce first of all capital expenditures (CapEx). This includes reduced hardware costs in the IaaS layer and reduced license costs in all layers. Especially in the IaaS layer it is not required anymore to engineer the own data center for peak performance cases, which occur in general very seldom and which usually result in a poor utilization of the available resources. Additionally, reductions of the operational expenditures (OpEx) in terms of reduced hardware, license and patch management are promised as well.

On the other hand, along with these benefits, Cloud Computing also raises severe concerns especially regarding the security level provided by such a concept. Completely relying the own data and execution tasks to an external company, eventually residing in another Country with a different regulatory environment may cause companies not to consider Cloud Computing but to stick to the conventional local data center approach. Although there is a clear demand for in-depth discussion of security issues in Cloud Computing, the current surveys on Cloud security issues focus primarily on data confidentiality, data safety and data privacy and discuss mostly organizational means to overcome these issues.

We provide an overview on technical security issues of Cloud Computing environments. Starting with real-world examples of attacks performed on Cloud computing systems (here the Amazon EC2 service), we give an overview of existing and upcoming threats to Cloud Computing security.

III. Web data integration using cloud

As businesses continue to deploy cloud-based systems, many are ignoring the fact that there needs to be some mechanism to synchronize data to and from your cloud and the core enterprise systems. Data integration is the extraction, transformation and loading of data from disparate systems into a data warehouse or data mart for the purposes of manipulation and reporting. Data integration has traditionally focused on manipulating and analyzing historical data, either to detect trends or to support "what-if" queries by adjusting some of the values.

A data-integration strategy needs to be within the foundation of your cloud computing plan. This includes cloud-to-enterprise and cloud-to-cloud. This integration needs to be innate to the architecture. Cloud data integration includes:

1. Back office synchronization

As more front office applications (e.g., sales force automation, customer service, and human resources) are deployed in the cloud, your organization needs to synchronize the data within them with back office applications (e.g., general ledger, accounts payable, payroll). This synchronization is critical to ensuring timely, relevant, and trustworthy information is delivered throughout your enterprise.

2. Customer master synchronization

Beyond the data that now resides in the cloud, your organization may still have financial data locked in Oracle applications and their customer master data in SAP. To break down these data silos and improve business processes, you need a single view of customer data. A cloud data integration solution can help create that single view, which can have positively impact on both customer satisfaction and your bottom line.

3. CRM integration

Your sales organization wants a single view the customer—orders in line with Account and Opportunity information .With more organizations adopting Sales force CRM, the demand for self-service cloud-based data integration that can be managed by non technical business users is also growing.

4. Data migration

As your organization modernizes its IT infrastructure by moving off legacy applications on premise to new cloud-based applications, you need to have confidence that you can easily migrate data to and from the cloud. Similarly, if your company or department has merged with another, or you've acquired a new entity, you need to migrate and merge data quickly to start recognizing return on your investment.

5. Data replication

Many companies are required to keep an on-premise copy of all cloud-based data for compliance, disaster recovery, or business intelligence reporting purposes.

6. Business / IT alignment

Line of business is administering the SaaS applications and IT wants to avoid data silos and untrustworthy point solutions. The right approach to cloud data integration can play a key role in aligning business users with IT.

7. Data Archiving

For regulatory compliance, organizations are required to retain data for a longer period, sometimes up to 10 years. Inactive data from enterprise applications, such as Oracle E-Business Suite, PeopleSoft, Siebel, SAP, and other custom applications and databases can be archived to on-premise or cloud storage.

8. Legacy application retirement

Many companies spend significant amount of their IT budget maintaining legacy applications which have depreciated in business value. The data in these legacy applications can be retired to on-premise or cloud storage, and yet remain easily accessible for reporting or compliance audit purposes.

IV. Web security

Web security has evolved along with the Web itself, and the varying threats and attacks that need to be controlled at any one time. Initially, the biggest threat to people using the Web was one

of accidentally viewing inappropriate content.

The actual malware threat only shifted to the Web in the last several years, initially with the bad guys bringing up their own Web sites that were then listed by the URL filtering lists. Today, the reality is very different. Over 84% of all malware -infected Web sites are legitimate. Web sites deemed to be safe by URL filtering lists. Organizations of all shapes and sizes need to be considering a secure Web gateway solution to provide effective security for Web usage.

V. Cloud-based web security types

Cloud-based Web security can be divided into two primary architectural categories. Pure cloud Web security solutions run as software completely within Infrastructure-as-a-Service (IaaS) facilities, without any on-premises equipment or software.

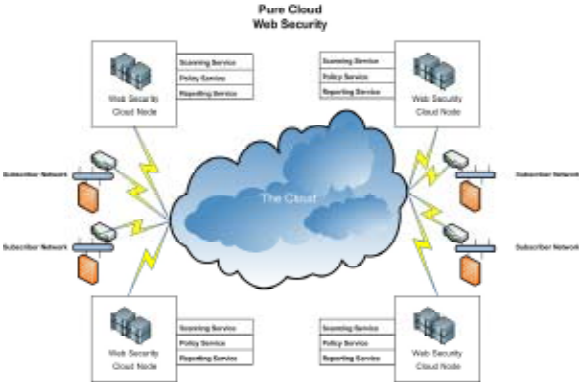

Fig. 3: Pure cloud web security

Pure cloud Web security is managed through browser-based tools and causes all subscriber HTTP/HTTPS traffic to route through the cloud node to deliver services like URL filtering, malware blocking, and content filtering.

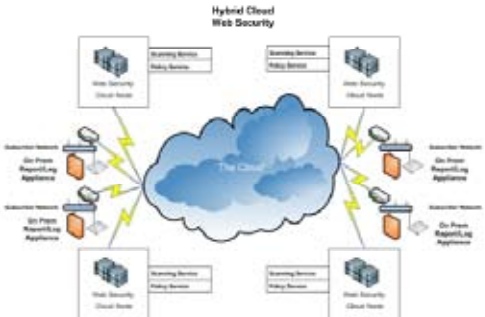

Fig. 4: Hybrid cloud web security

Hybrid cloud Web security solutions run a combination of on-premises hardware/software and cloud-based software. The hybrid approach is often designed to meet specific requirements of existing on-premises appliance installations, such as adding support for mobile users or meeting requirements for logging and reporting data storage.

VI. Literature survey

As previously mentioned, Cloud Computing is an abstraction for a complex on-demand scalable computation grid, that is accessible to users through web-enabled devices. Although the specifics of this paradigm are still being defined and revised, Cloud Computing typically consists of some basic components (e.g. CPUs, storage mediums, network interconnects, etc.) upon which any number of applications can be deployed.

A Cloud Computing platform will incorporate some or all of these components, and each component has its own security concerns and issues. In recent months the interest in Cloud Computing has sharply increased, with many of the mainstay computer companies investing money and personal into research and development of both hardware and software systems. For instance, Microsoft recently announced its intention to release a Windows type operating system to run on a Cloud system. [1] Other forerunners of computing and Internet technology such as IBM [2], Goggle [3] and Amazon [4] are actively pursuing Cloud Computing systems. As this technology becomes more widespread and accessible, the need for proper security becomes ever more evident.

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public [1].

The Web Service Level Agreement (WSLA) framework is targeted at defining and monitoring SLAs for Web Services[2].
The assertions of the service provider are based on a detailed definition of the service parameters including how basic metrics are to be measured in systems and how they are aggregated into composite metrics [3] What's occurring is that data is being relocated into cloud services, either through database-as-a-services or applications-as-a-service[4].Cloud data storage security, which has always been an important aspect of quality of service[5].

It provides dynamically scalable geographic information technology, spatial data, and spatial applications as a web service [6]. In order to keep your enterprise secure, it is important to understand exactly how the cloud computing infrastructure works[7]. Cloud security issues focus primarily on data confidentiality, data safety and data privacy and discuss mostly organizational means to overcome these issues [8].

In Phishing attack, the attacker lures the victim to a fake Web page (either using spoofed emails or attacks on the DNS), where the victim enters username and password(s)[9].Naive use of XML Signature may result in signed documents remaining vulnerable to undetected modification by an adversary [10].In [11] a method – called inline approach – was introduced to protect some key properties of the message structure and thereby hinder wrapping attacks, but shortly later in [12] it was shown how to perform a wrapping attack anyhow. Web security has evolved along with the Web itself, and the varying threats and attacks that need to be controlled at any one time [13].The rapid adoption of these cloud solutions has resulted in more fragmented data and the need to integrate data "in the cloud" with data in on-premise applications and databases [14].

VII. Proposed architecture

The first phase of this project will consist of a more thorough review of what security applications exist or are being currently developed for Cloud Computing Systems. Also, we will analyze what is being done at the academic research level. We must identify the strengths and weaknesses of existing applications and

concepts. As we previously stated, we will discover the specific weaknesses that compose the general weaknesses. Additionally, we must have a solid understanding of the hardware infrastructure of a Cloud Computing system, specifically, how communication is handled and where potential security weaknesses may exists. Once these weaknesses are clearly recognized, we will be better equipped to set specific objectives for the SCC application. At the end of this phase, we will have created a step by step design plan that will define the application architecture and set specific milestones for development. This phase is currently in progress, and will take 3 months to complete.

The second phase will be to develop a software prototype of our application. Using the Information we ascertained in the first phase, we will create a prototype of our security application. We will rigorously test our application to ensure it provides the maximum amount of protection. As we do so, we will be able to improve the quality of our application. At first, this application may be limited to the platform on which it is developed (most likely the EC2), so we will continue to work to make it suitable on many different platforms. We will then carry on with development until our application is stable and mature. At the end of this phase, we will have an application that is deployable in the real world and usable on actual Cloud Computing systems.

We are approaching the concept of open cloud to integrate different web services under one unit. The basic principle of model many clouds will continue to be deferent in a number of important ways, providing unique value for organizations. It is not our intention to define standards for every capability in the cloud and creates a single homogeneous cloud environment. Rather, as cloud computing matures, there are several key principles that must be followed to ensure the cloud is open and delivers the choice, flexibility and agility organizations demand:

1. Cloud providers must work together to ensure that the challenges to cloud adoption (security, integration, portability, interoperability, governance/management, metering/monitoring) are addressed through open collaboration and the appropriate use of standards.

2. Cloud providers must not use their market position to lock customers into their particular platforms and limit their choice of providers.

3. Cloud providers must use and adopt existing standards wherever appropriate. The IT industry has invested heavily in existing standards and standards organizations; there is no need to duplicate or reinvent them.

4. When new standards (or adjustments to existing standards) are needed.

VIII. Conclusion

While some features of Cloud Computing are more secure, some are more vulnerable to exploitation and attack, these aspects can be categorized into two groups: general security weaknesses and specific security weaknesses. A typical Cloud Computing platform has various layers and we wish to address the issues in the platform and applications layers. We aim to develop a lightweight easily deployable security application that addresses most if not all of the aforementioned concerns.

References

[1] Armbrust, M., Fox, A., Gri_th, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M., "Above the clouds: A berkeley view of cloud computing". Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley (Feb 2009)

[2] Keller, A., Ludwig, H., "The wsla framework: Specifying and monitoring service level agreements for web services". J. Netw. Syst. Manage. 11(1) (2003) pp. 57-81.

[3] Ludwig, H., Keller, A., Dan, A., King, R., Franck, R., "Web service level agreement (WSLA) language specification". IBM Corporation (2003)

[4] "The importance of data integration in the era of cloud compuing", [Online] Available : http://www.ebizq.net/blogs/linthicum/2009/01/the_importance_of_data_integra.php

[5] Tribhuwan, M.R. ; Bhuyar, V.A. ; Pirzade, S., Ensuring Data Storage Security in Cloud Computing service. In: 2010 IEEE International Conference on Advances in recent tech in comm. and computing.

[6] Xiaolin Lu, "Service and cloud computing oriented web GIS for labor and social security applications", 20102nd international conference on information science and engg.

[7] SearchCloudSecurity.com, [Online] Available : http://searchcloudsecurity.techtarget.com/tip/Cloud-computing-security-model-overview-Network-infrastructure-issues

[8] J. Heiser, M. Nicolett, "Assessing the security risks of cloud computing", Gartner Report, 2009. [Online]. Available: http://www.gartner.com/DisplayDocument? id=685308.

[9] R. Dhamija, J. D. Tygar, M. A. Hearst, "Why phishing works," in Proceedings of the 2006 Conference on Human Factors in Computing Systems (CHI), Montr´eal, Qu´ebec, Canada. ACM, 2006, pp. 581–590.

[10] M. McIntosh, P. Austel, "XML signature element wrapping attacks and countermeasures", in SWS '05: Proceedings of the 2005 workshop on Secure web services. ACM Press, 2005, pp. 20–27.

[11] S. Gajek, L. Liao, J. Schwenk, "Breaking and fixing the inline approach", in SWS '07: Proceedings of the 2007 ACM workshop on Secure web services. New York, NY, USA: ACM, 2007, pp. 37–43.

[12] N. Gruschka, L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited", in ICWS '09: Proceedings of the IEEE International Conference on Web Services. Los Angeles, USA: IEEE, 2009.

[13] M86 White paper, [Online] Available : http://www.m86security.com/documents/pdfs/white_papers/business/WP_Hybrid_Web_Security.pdf

[14] Informatica, data integration company, [Online] Available: http://www.informatica.com/solutions/on_demand/Pages/index.aspx

Ms Sakshi Bhatia received her B.E. degree in Computer Science & Engineering from Kurukshetra University in 2004 and M.Tech. degree in Computer Science & Engineering from CDLU Sirsa in 2011(likely to be completed). She was Lecturer in the Department of Computer Science & Engineering in Jind Institute of Engineering & Technology,Jind,Haryana in 2005- 06. She has been Lecturer/Assistnat Professor in the Department of Computer Science& Engineering in Technological Institute of Textiles & Sciences, Bhiwani, Haryana since 2006. Her research interests include Wireless communication, software engineering and cloud computing.

Dr. Vikram Singh is working as a Professor of Computer Science at Chaudhary Devi Lal University, Sirsa, since December 2008. He joined Chaudhary Devi Lal University, Sirsa in August 2004 as a Reader in the Department of Computer Science & Engineering. Before that he has worked as a Lecturer in the Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, from August 1998 to July 2004. Earlier, he has worked as a System Programmer in a World Bank Project for about four and half years; and also as a Project Associate at National Institute of Technical Teachers' Training & Research, Chandigarh, for about nine months.

Dr. Vikram Singh has earned his Masters in Physics and Computer Applications; and Doctorate in Computer Science from Kurukshetra University, Kurukshetra. He is a member of Haryana State Counseling Society, Panchkula and also a member of its Board of Governors. He has also served as outside member on Expert Committees/Board of Studies of UGC, IGNOU, KU Kurukshetra, MDU Rohtak, HPU Shimla and other universities/ institutes of the region

Dr. Vikram Singh has published three books on related subjects and contributed chapters in four edited books. He has published as many as thirty five research papers/articles in International/ National journals apart from paper presentation/publication in conference proceedings. He has also delivered about a dozen invited talks at refresher courses in the colleges/universities of the region. He has also delivered fifteen resource person/invited talks at various national/international seminars/conferences. He has chaired twelve technical sessions at conferences/seminars. He has further been a part of organisation of ten workshops/ conferences. Presently, he is supervising eight research scholars for their Doctorate work. Areas of his research interest include operating systems, simulation and modeling, and data mining.

Aastha received her B. Tech degree in Computer science & Engineering from Kurukshetra University, Kurukshetra, India, in 2006 and the M.Tech degree in Computer Science & Engineering from Guru Jambeshwar University of Science & Technology, Hisar, India in 2009. She was a lecturer with department of IT , MMEC, Mullana in 2007. She is an Assistant Professor, Department of Computer Science, The Technological Institute of Textile & Sciences, Bhiwani, Maharishi Dayanand University, Rohtak from 2010 till now.