Web Services Monitoring, Analysis for Future Usage and Failure Prediction

Syed Kashif Ali, Sarmad Sadik
National University of Science & Technology, Islamabad Pakistan
syedkashif5.12@gmail.com
sarmad.sadik@mcs.edu.pk

Abstract
Wide use of web services has dominated the software industry. Providing web services to its consumers according to Service Level Agreement (SLA) is a complex and difficult task. Failure to provide web services against agreed quality of service (QoS) parameters i.e., unavailability of web services and slow response time will cause increase in penalties. This may lead to unsatisfied consumers that can be devastating for business goals and revenue of service providers. In order to ensure the satisfaction of consumers and avoid any violations of SLA, monitoring is required on service provider side. However, monitoring against SLA is not enough - service providers must be able to analyze the past and current usage in order to predict future challenges. User’s behavior and usage analysis is used in many businesses for forecasting and decision making in different departments such as Marketing, Sales & Distribution, and Inventory Management. The monitoring data of web services can provide vital information to the service providers. On the basis of usage analysis the service provider can assess current and predict future challenges and can take certain risk measures to avoid violations of SLA. This research aims to provide a monitoring framework which empowers the service providers to monitor web services usage and failures. And analyze the monitoring data to predict future usage and failure patterns.

Keywords: Web, Service, Prediction, SOA, QoS.

I. Introduction
Service Oriented Architecture (SOA) is an emerging business-centric approach for many business organizations. Many business organizations are shifting towards Software-as-a-Service model (Philipp, 2010). Different organizations are offering many types of web services on internet. Some of these web services are very important or business critical for their consumers. Web service failures, unavailability, or delayed response can cause a huge failure or economic loss to consumer’s business. In above mentioned scenarios, the service provider has to compensate service consumer with penalty. These services failures when occurring iteratively will increase penalty costs and may lead to the loss of service consumers which is huge business loss for the service provider. Before a service provider start providing web services to a consumer, they must
agree on a contract called Service Level Agreement (SLA). A SLA defines Quality of Service (QoS) attributes for a service, to be provided to its consumer. It also defines the conditions under the service will be provided to its consumers. Besides that SLA also defines the penalty cost which is paid or compensated by the service provider in case of SLA violation. A service provider has to minimize SLA violation to increase its profits and decrease penalty costs. In order to ensure the SLA enforcement, an efficient monitoring mechanism is required at the service provider’s end. Different researchers have proposed many architectures and approaches for SLA monitoring. Most of them are used to validate SLA at runtime or find the reason of violation ex-post when the violation has occurred(Philipp , 2010). But only solving emerging service faults at deployment time or runtime is not enough (Shang, 2012). One must have to analyze, identify and predict the risks which can cause the SLA violation. Many business organizations, for forecasting purposes perform analysis of their historical sales data. The forecasting data can be helpful for many management decisions i.e. Sales revenue forecasting, inventory planning, operation planning and marketing (Gilmore ,2006). The domain of risk management has been used in different disciplines including software engineering. The goal of risk management in software engineering is to help to manage software projects in a specific time and budget boundaries but it is not limited to time and budget boundaries (Institute, 1992). Risk management can be applied throughout the system development life cycle. To make good business and technical decisions risk management can provide requisite data (Kokash, 2007).

Maintenance issues like service failures or crashes, unavailability of services or slow response time can be coped with proper risk management. In context of risk management, the historical data of web services usage like hits per web service, failure or unavailability of a web service between a particular time span can provide information about highly used web services. This information can determine current and future patterns of a web service usage and failures i.e. increase or decrease in web service usage growth and web service failure growth. This research paper aims to provide a web service monitoring and analyzing framework with the notion of future prediction for the service providers. The framework will help the service providers to predict the future increase or decrease in web service usage and failures. It will also help the service providers to take future business decisions and reduce risks and their impacts which can maximize their profits and minimize their penalty costs.

The rest of paper is organized as follows. In section 2; we present the literature review for SOA monitoring frameworks and their comparison with respect to risk management. We also provide a brief overview of usage analysis and future prediction in I.T and business organizations. Section 3 presents our proposed conceptual framework. In the end, section 4 concludes the paper with final remarks and highlights the conclusion & future work.

II. Literature Review

A. Web Service Monitoring:

In order to ensure satisfaction of the SLAs monitoring is required at every service provider and at the service consumer end (Farhana et al, 2008). Basically, there are three main types of web service monitoring: Provider side monitoring (centralized or distributed), customer or end user side moni-
Monitoring and third party monitoring. The drawback of provider-side and consumer-side monitoring is that in the case of problems neither side will trust the others (Balfagih, 2010). The third party monitoring has bottleneck performance issues when the messaging between consumers and providers is increased.

Authors in (Philipp, 2010) propose an event-based monitoring framework which predicts the SLA violation using machine learning techniques and runtime triggering of adaption actions for violation prevention.

A framework has been proposed (Vincent et al., 2012) a framework for application level monitoring in cloud. The proposed architecture detects violation of SLA at application level and with the help of tools resource allocation and scheduling of tasks are done.

In another research (Shang, 2012) authors has proposed a risk driven service composition approach. With the help of this approach fault source can be identified and tracked when a fault occurs and risk components (web services) can be removed earlier. Researchers in their work (Balfagih, 2010) provided an automated monitoring framework on the basis of a quality model to ensure the enforcement of SLA using agent technology. The quality model used in framework will point the related quality attributes of SLA and metrics from perspective of different stakeholders.

Authors of (Yinsheng, 2009) analyzed the limitation of web services monitoring at lower layer rather than at application level layer TCP/IP stack. They proposed a system model and indicator which analyses user’s behavior by browser information.

All of the mentioned monitoring frameworks provide a little or no risk management aspect and they provide no support for web service usage analysis. Table 1 provides the comparison of these frameworks with risk management perspective.

<table>
<thead>
<tr>
<th>Monitoring Type</th>
<th>Monitoring Purpose</th>
<th>Risk Management</th>
<th>Usage Support</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Philipp, 2010)</td>
<td>Provider Side - Centralized</td>
<td>Prediction and prevention of SLA violation</td>
<td>Run time action adaption</td>
<td>No support</td>
</tr>
<tr>
<td>(Vincent et al, 2012)</td>
<td>Provider Side - Distributed</td>
<td>SLA violation Detection in Clouds</td>
<td>Resource allocation and scheduling</td>
<td>Partial support (Resource based)</td>
</tr>
<tr>
<td>(Shang, 2012)</td>
<td>Provider Side - Centralized</td>
<td>Fault tracking and risky component removing</td>
<td>Risky component removal</td>
<td>No support</td>
</tr>
<tr>
<td>(Balfagih, 2010)</td>
<td>Provider &amp; Consumer Side - Agent based</td>
<td>Enforcement of SLA</td>
<td>NA</td>
<td>No Support</td>
</tr>
<tr>
<td>(Yinsheng, 2009)</td>
<td>Consumer Side</td>
<td>Browser based user’s behavior information gathering</td>
<td>NA</td>
<td>Partial Support (User’s Page Access)</td>
</tr>
</tbody>
</table>
**B. Usage Analysis & Decision Making**

With the rapid increase in internet users, it makes internet a perfect way for business organizations to interact with online consumers regardless of their geographical locations. In order to increase revenues more observations and importance must be given to online consumer’s behavior and their usage patterns. A study conducted (N. P et al, 2009) in Taiwan and Indonesia on online shopping shows that in Taiwan 70.1 percent of people are internet users and by 2014 the expected growth in the number of internet users in Indonesia will be 150 million. With this enormous growing trend Taiwan’s government as a part of their future strategy is planning to achieve e-commerce revenue of US$33.333 billion by the end of 2015. Understanding the user’s behavior can play a vital role to predict the required changes and cope with upcoming challenges. Similarly according to the research two third of the population of the internet users participate and visits the social networking websites and blogs (Report,2009). User’s behavior or usage analysis is also useful to understand the usage trends, improve advertisement placement polices, viral marketing and better workload management (Benevenutoy,2009).

**III. The Proposed Framework**

From the literature review, it is analyzed that there is a major drawback in existing monitoring frameworks from risk management point of view. Most of the frameworks do not or partially give the usage analysis and risk management support to providers. This is in fact very important for future decision making, prioritization of services from revenue aspect, allocation of resources for better availability and response time and adaption of new services and to track those services which are increasing penalty costs.

In order to overcome this drawback, a framework is proposed which will provide usage monitoring for analysis to service providers for decision making and risk management.

Figure 1 describes the conceptual architecture of our framework. The detailed description of components is given below.
- **Web Service Monitoring and Binding Layer:** This component/layer first parses all the requests of users. It saves the user’s information and requested service information. Secondly, it selects the requested service from the service repository and binds the requested service to the user and saves the response information.

- **Web Service Pool:** It contains actual services (software and Meta information) and registry and communication interfaces for users.

- **Usage Repository:** All the information of web service usage, i.e. (request and response) and its user’s information are saved in the usage repository. All of the information is saved with parallel process.

- **Web Service SLA Repository:** In this repository Meta information of web services is stored. This repository also holds the information of each SLA with every user. The information consists of quality of service parameters and the penalty costs in case of any type of SLA violation.

- **Analyzer & Report Generator:** It compiles the information from all the repositories on the basis of statistical forecasting models for analysis and presents it in different types of graphs, simulations and in numerical data, i.e. Current & past usage trends, average usage, expected growth, penalty trends to service provider.

The framework is divided into two parts. 1) Web Service Usage monitoring. 2) Usage Analysis for Risk Management.

First part is responsible for logging user’s request into usage repository and binding the requested service from the service repository to the consumer. When a user requests for a particular web service, monitoring layer will save information of user and web service that is being requested in usage repository. After saving information monitoring layer shall select the web service from the service pool and binds it the requested user and then save the response information i.e. time, status. Figure 2 illustrates the complete working sequence of first part of our framework.
The second part of our framework is back bone of our proposed framework which is responsible for analyzing usage repository and SLA repository for report generation. It can use following quantitative models for forecasting.

- Moving Average
- Regression
- Exponential Smoothing

Service provider will provide report generation parameters i.e. specific time span to analyzer and report generator. Analyzer & report generator will use the usage repository and web service SLA repository to generate results such as usage graphs (past & current usage pattern, and forecast expected usage pattern). Similarly analyzer & report generator will generate report for current SLA violations and penalties such as web service unavailability and forecast expected violations & penalties. Figure 3 describes the complete working sequence of second part of our framework.
The forecasting information generated by the proposed framework shall help the web service providers to point out those web services which are causing SLA violations and the root cause of these SLA violations can be identified and taken care off. Similarly the web services that usage is expected to grow will be identified and allocated with more resources in order to not compromising on their performance and avoiding any future anomalies.

IV. Conclusion

Web service usage monitoring data can be very useful for their service providers. This data can highlight revenue generating and highly used web services. Furthermore, analysis of this data with respect to their SLA parameters will help the service providers for risk management and to take future decisions in order to reduce penalty costs. The proposed monitoring framework which will help the service providers to monitor and analyze their web services usage according to SLA for risk management. At present, prototype of proposed framework is being implemented. In future, the framework will be extended for multiple and distributed service provider level monitoring and furthermore proposed framework will be integrated with existing monitoring frameworks to enhance the capabilities.

References


