2014

Trustworthiness of Web Services

Britto N. Arockiasamy
University of North Florida, n00637040@ospreys.unf.edu

TRUSTWORTHINESS OF WEB SERVICES

by

Britto N. Arockiasamy

A thesis submitted to the
School of Computing
in partial fulfillment of the requirements for the degree of

Master of Science in Computing and Information Sciences

UNIVERSITY OF NORTH FLORIDA
SCHOOL OF COMPUTING

December, 2014

The thesis "Trustworthiness of Web Services" submitted by Britto N. Arockiasamy in partial fulfillment of the requirements for the degree of Master of Science in Computing and Information Sciences has been

Approved by the thesis committee: Date

Dr. Karthikeyan Umapathy
Thesis Advisor and Committee Chairperson

Dr. Ching-Hua Chuan

Dr. Swapnoneel Roy

Accepted for the School of Computing:

Dr. Asai Asaithambi
Director of the School

Accepted for the College of Computing, Engineering, and Construction:

Dr. Mark Tumeo
Dean of the College

Accepted for the University:

Dr. John Kantner
Dean of the Graduate School

ACKNOWLEDGEMENT

I am grateful to my advisor, Dr. Karthikeyan Umapathy, for being my mentor. I would like to thank him for all of his assistance throughout my thesis. With his advice and assistance, I was able to complete my thesis in a systematic and organized manner. I would also like to thank Dr. Ching-Hua Chuan and Dr. Swapnoneel Roy for serving as committee members. Their suggestions and advice were tremendously helpful in improving the quality of my thesis.

Furthermore, I would like to thank Mr. Jim Littleton for reviewing my thesis document for compliance with the thesis requirements and Dr. Roger Eggen for steering me through the Graduate School process. I also want to give special thanks to all faculty and staff at the School of Computing for their support and encouragement.

Finally, I would like to express appreciation and thanks to my beloved wife, Prabha, for her personal support and great patience.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Workflow systems orchestrate various business tasks to attain an objective. Web services can be leveraged to handle individual tasks. Before anyone intends to leverage service components, it is imperative and essential to evaluate the trustworthiness of these services. Therefore, choosing a trustworthy service has become an important decision while designing a workflow system. Trustworthiness can be defined as the likelihood of a service functioning as it is intended.

Selection of a service that satisfies business goals involves collecting relevant information such as security mechanisms, reliability, performance and availability. It is important to arrive at total trustworthiness, which incorporates all of the above mentioned multi-facet values relevant to a service. These values can be gathered and analyzed to derive the total trustworthiness of a service. Measuring trustworthiness of a service involves arriving at a suitable value that would help an end-user make a decision for the given business settings.

The primary focus of this thesis is to gather relevant details and measure trustworthiness based on inputs provided by the user. A conceptual model was developed after extensive literature review to identify factors that influence trustworthiness of a service. A mechanism was created to gather concept values for a given service and utilize those values to calculate trustworthiness index value. A proof-of-concept prototype was also developed. The prototype is a web-based application that implements the mechanism to measure the trustworthiness of the service. The prototype was evaluated using a scenario-based

analysis method to demonstrate the utility of the trustworthiness mechanism using three different scenarios. Results of the evaluation shows that trustworthiness is a multidimensional concept, the relevant conceptual values can be collected, a trustworthiness index value can be calculated based on the gathered concepts, and a trustworthiness index can be interpreted to select the most relevant service for a given requirement.

Chapter 1

INTRODUCTION

In Service Oriented Architecture, all business functions are generally offered as services. The services are coordinated sequentially or in a parallel manner to create a comprehensive workflow to accomplish a business objective. Organizations from various domains such as travel, health and finance access web services via the Internet to achieve their business goals and business process needs (D. Zhang, 2004).

In a nutshell, a web service is a software program that provides a specific set of functionality that is accessible by a client program or other web service via the Internet. The web service can be written in common programming languages such as Java, VB.NET, and C#, and if it adheres to web service standards, clients can access the service and its functionality.

A typical web service might use Simple Object Access Protocol (SOAP) over Hypertext Transfer Protocol (HTTP) for the interaction between a client and the service. The information flows as an Extensible Markup Language (XML) document using SOAP. The clients can learn about capability and how to access a service from Web Services Description Language (WSDL) documents published by the service provider. The WSDL has the uniform resource identifier (URI) information for the client to access a web service, and ports and operations information for using its functionality.

Designing web services is one of the major components in enterprise systems integration because most organizations conduct business online using web services (Umapathy & Purao, 2010). Organizations that offer business functionalities as web services can change their algorithms as long as they adhere to the interfaces exposed to the client. The coupling between the client and a web service is generally intact, and clients do not need to worry about how the application is implemented. This is one of the major strengths of a web service, and due to this flexibility, the usage of web services has increased exponentially (Guinard et al., 2010). Web services are hosted on web servers, and the physical location of the service does not need to be exposed to clients as long as the URI takes them to the correct server. In other words, clients are ignorant of the physical location of the web service, changes to its location, and changes to its implementation – as long as the changes do not affect the existing functionality of the web service.

Organizations can choose a web service to perform certain activities within a business process. Due to the increasing number of readily available web services, organizations are choosing web services to execute their business activities; however, there are many factors that need to be considered before choosing a suitable web service (Sun et al., 2007). Some of the important factors are availability, reliability, performance, and security (Sun, et al., 2007). A review of the existing research indicates there are few tools available to gather and analyze these factors in order to arrive at a common value that would encourage an organization to choose a suitable web service for the relevant business activity or process. Conceptual analysis of the relevant factors is important when selecting a suitable web service, and among these relevant factors, trustworthiness could be one of the factor

considered during service selection. Trustworthiness can be defined as the level of confidence that a software component will function as intended (J. Zhang, 2005). Trustworthiness can be measured as the probability that having a catastrophic flaw will be acceptably low (Parnas et al., 1990). In order to measure trustworthiness as a probability, the software component must go through numerous tests – both formal and rigorous. In a web service, there are several factors that affect the trustworthiness of the service; therefore, conducting tests to measure trustworthiness is impractical.

We can define trustworthiness of a service as a likelihood of a service to perform as intended. Trustworthiness of a web service should be measured as an aggregation of relevant concepts. Total trustworthiness encompasses many factors and concepts that are based on the business domain and the requirements of a business process. This total trustworthiness is a comprehensive value where each concept attributes its share towards the total evaluation of the trustworthiness of a web service; however, this solely depends upon the requirement of an organization's business settings. For instance, for an organization in the healthcare domain, the process of choosing a web service is predominantly based from the point of view of security – a patient's information must be kept strictly confidential as required by the Health Insurance Portability and Accountability Act (HIPPA), which demands total protection of a patient's information regarding his or her health, and personal information.

A leading healthcare organization in Jacksonville, Florida was approached to learn about the process used for selecting web services from vendors. The process followed by the

organization was informative and adaptive to the present technology; however, the process concentrated only on a web service's security rather than evaluating all the relevant factors of trustworthiness of the service. Furthermore, the process lacked a comprehensive approach for measuring total trustworthiness of a web service due to its lack of a framework to calculate trustworthiness, as well as available tools. This thesis attempts to alleviate and address limitations on the lack of framework and tools to calculate trustworthiness of a web service.

The key focus of this thesis is to gather the pertinent details associated with the trustworthiness of a web service and to evaluate those details in order to arrive at a total trustworthiness value based on the set of business requirements provided by a user. This thesis identifies the conceptual factors that contribute to the trustworthiness of a web service and provides a web application to collect and analyze the various factors. A computing model has been developed to collect the relevant details of a web service and to calculate the total trustworthiness of a web service based on the set of business requirements provided by a user. This model addresses the end-user's issues in choosing a suitable web service and helps the user achieve the organization's business goals. The web application collects all relevant trustworthiness factors of a web service, evaluates the factors based on the user's business preference setting, and arrives at a total trustworthiness value of a web service. Using the total trustworthiness value, users can choose a suitable web service that best satisfies their business objectives.

Chapter 2

BACKGROUND AND LITERATURE REVIEW

2.1 Transactions and Web Services

Electronic business is built on transactions that are abundantly dependent on sharing information (Jin et al., 2011). Whether it is a making a transaction or sharing some information, there needs to be at least two entities communicating with each other. This sort of communication or sharing of information can be in many styles. The common style may be one of the following: Producer-User, Provider-Consumer, Server-Client, Sender-Receiver, or Publisher-Subscriber.

In early days, this communication between entities mainly occurred within a specific environment. Eventually, when the Internet came into the arena, the barriers based on environments, systems, domains, and other similar boundaries started withering out and data kept flooding across all these boundaries without any impediments or obstacles.

Web services have taken advantage of these developments to allow anyone to offer a service across the Internet, and allow everyone to consume that service within certain limitations. This idea has become the backbone of today's online business slowly and steadily. The concept of using and leveraging the services gave birth to service-oriented architecture (SOA). Web service is one of the major components for implementing

business applications using SOA (Alonso et al., 2004). Consuming services via Internet has been made relatively less cumbersome and more efficient in the recent past with the latest technological advancements than in the early days.

2.1.1 Evolution of XML

Evolution of XML, the pioneer technology, was also one of the reasons that brought web service technology to the Internet world. In the beginning, the HyperText Markup Language (HTML) tags had limited usage. There were only limited tags in HTML and the constraints were heavy for transferring data or information. XML provides capability to develop a platform independent user-defined markup document for exchanging data. XML needs to have tags along with the data to describe the message content. Thus, the volume of XML message becomes immensely huge and started having its own disadvantages due to larger payload.

When web service started using these XML messages for their inputs and outputs, W3C (World Wide Web Consortium) came out with some standardization. These XML messages, when sent to a web service, will be wrapped in another envelope called a SOAP envelope. SOAP is a protocol for exchanging messages among web services and service clients.

2.1.2 SOAP (Simple Object Access Protocol)

SOAP provides a simple format to transfer messages over the Internet. SOAP contains three main elements called envelope, header, and body (Gudgin et al., 2007). The envelope is the root element of SOAP. Body and header elements are contained within the envelope element. The XML message travels inside the body element, while the header element (optional) contains other related information about the message, such as schema, username, password, and namespace. The header element is also used for embedding information associated with other SOAP related specifications such as WS-Addressing and WS-Security.

SOAP specifications have two significant versions: SOAP version 1.1 (old) and SOAP version 1.2 (current). The initial acronym SOAP (Simple Object Access Protocol) was dropped in the second version of SOAP specification by W3C. Hence, the word SOAP stands as a simple word and not an acronym.

SOAP can be embedded within HTTP for transporting a message from a destination to another destination. The format type of the HTTP communication while carrying SOAP message should be 'text/xml'. The XML message content is generally named as payload. Typically, SOAP message travels over HTTP for the message transfer, but other protocols like MQ, SMTP can also be used. The following figure taken from the Microsoft MSDN site provides an idea of the whole life cycle of a SOAP message exchange (Microsoft-XMLWS, 2014).

Figure 1. Anatomy of an XML SOAP message exchange

From figure 1, it can be seen how a web service leverages SOAP protocol for the communication between the servers and clients to send and receive the business content that is intended for its business operation using SOAP message exchanges. The SOAP message is serialized during the transport along the network and then gets de-serialized by the receiver. The SOAP request sent by a client is received by a server and the server responds back by sending a SOAP response to the client. The XML content that travels inside the envelope element is the business content. It has the business request information to the server and the server response also is another XML that is nothing but the business content. All that is done is just adding the paraphernalia around the business content while communicating to the web service as it travels through the Internet to reach the service and get back the results to the client.

2.1.3 WSDL (Web service Descriptive Language)

In general, a web service is a service available on the Internet for others to use for their business process requirements as explained earlier. In this context, it becomes imperative that the web services make themselves known to the other business applications and processes so that these services can be accessed by the users. A web service exhibits a detailed XML document describing the functionalities offered by the service and where to access them. This detailed document is called Web service Descriptive Language (WSDL) that explains everything a client needs to know about the service (Christensen et al., 2001). Some of the basic elements in WSDL are Message, Service, Port, Binding, Operations, Port Types, End point, and Types. These basic elements in a web service are explained below.

Message: Message is a payload (information/data) that travels across a network between clients and servers. These Messages can be of different types but the typical types are request-only, request-response, and publish.

Service: The service is the collection of different functionalities where each function offered is based on a contract. Technically, a service defines the various ports that are supported by the service.

End Point: An end point is a network port where a server application listens for the client's request and communicates with the client. Hence a URI is an endpoint with the binding defined. The endpoint only receives the messages or receives the request message and

gives back a response message in relation to the input request message or just publishes some messages like a notification board.

Port Type: Port Types are contracts for the different functionalities offered by a service (equivalent to the interfaces in a program). In general, a program is considered as a service and the various operations inside a program would be the different Port Types. Hence, the Port Type is the basic interface to leverage the functions offered by the web service.

Binding: The binding stands for the protocol through which the offered port types are accessed for the respective services. For example, the SOAP/HTTP protocol can be a binding for a Port Type that can be accessed using this protocol. It is a style of communication the Port Type supports.

Apart from the above basic elements there is an element called proxy service that is employed in most of the web services. Proxy services offer mediation between a client and a web service. The SOAP address location would give the client the Uniform Resource Locator (URL) of the web service to be accessed. In current industrial standards, most of the web services will have a proxy in the DMZ (demilitarized zone) and hence, the client will get the URL to those proxy points rather than a real web service at the backend of the proxy. The proxies provide a security shield to a web service from the Internet attacks. The client accesses the proxy's URL and the proxy decides whether to allow the client to access the service or not.

2.2 Usage of Web Services

Web services are used in multiple scenarios from one end point to another end point communication, between a server and a client, between a server and a server, or among various servers (He et al., 2004). At the same time, a web service can be used in a publish mode, where a service will be published and many clients or servers can subscribe to that service. In a shared environment, business processes may contain various workflows to accomplish the business requirement. A workflow has to orchestrate various task components in an effective manner to attain the business process objective. In SOA, the individual tasks have to be offered as services especially as web services that are independent in nature, wherein the workflow can combine and orchestrate these independent services to achieve the ultimate business requirement.

The workflow will need to complete multiple individual tasks to get a desired result. These tasks have to be completed in a sequential or in a parallel mode as orchestrated by the workflow for a successful implementation. In a shared environment, each task might be an individual service and in the Internet environment these services can be offered as web services so that any process or any consumer can leverage readily available services. SOA model emphasizes this usage of web services as a backbone in a process implementation.

2.3 Choosing a Suitable Web Service and Related Issues

Many organizations have their own ways of deciding the choice of web services for any specific business need, but there seems to be a lack of methodology or process by which the trustworthiness of the service can be measured in a systematic manner (J. Zhang, 2005).

Today's businesses encompass various types of business domains based on the functionalities and process areas. The domain of healthcare is one of the prominent domains affected by the recent government's act and regulation known as ACA (Affordable Care Act). A healthcare domain organization's process of choosing a web service is mostly based on the security point of view as the patient's information is supposed to be kept strictly confidential. As mentioned in the introduction, a prominent Healthcare organization was approached to learn its process to select web services from outside vendors. It was learned that the organization has been using a process that is more informative and adaptive to the current technology. However, it was also learned that the process evaluates predominantly the security area of the web service usage rather than a comprehensive approach of measuring the total trustworthiness of the web service.

Total trustworthiness encompasses many factors and concepts that are based on business domains and the business requirement of an organization as well as the utilization of appropriate web service standards specifications. It is a comprehensive value where every concept attributes its share in the total evaluation of the trustworthiness of a service. Derivation of the trustworthiness value would depend upon the given business

requirements and standards utilized by a service. Therefore, the process followed to derive trustworthiness should be flexible to incorporate relevant concepts to get the desired results to fulfill the business requirement.

Consequently, the collection of the various concepts that are involved in choosing and deciding a service relevant to business processes is paramount. After collecting relevant concepts, those concepts need to be weighed based on the business requirements while evaluating the overall trustworthiness of the service. As such, there are not many tools available for collection of these relevant concepts and to evaluate these collected concepts to measure the trustworthiness of a web service.

2.4 Standards Relevant to Trustworthiness of Web Services

In the above subsections, we provided an overview of general concepts about web services, XML technology, and their respective usage in the industry. The following subsections provide an overview of various standards in connection with the web services trustworthiness.

2.4.1 Web Services Security

Web Services Security v1.1 (WS-Security) is the approved standard by OASIS (Organization for the Advancement of Structured Information Standards) for the implementation of security related concepts in building safe and secure web services. WS

Security specifications explain in detail the foundation and specification for implementing security while constructing a web service. This specification generally speaks about the following security features of the web service and some other security features as well (WS-Security, 2006):

- Web Services Security Kerberos Token Profile
- Web Services Security SAML Token Profile
- Web Services Security: SOAP Message Security
- Web Services Security Username Token Profile
- Web Services Security X.509 Certificate Token Profile

The specification concepts are highly relevant in assessing the trustworthiness of a web service as adherence to these specifications while implementing a service, embolden and increase the holistic trustworthiness of that service. While we analyze and evaluate the web service trustworthiness, data related to the above specified security features implemented by services will be gathered for the purpose of establishing web service trustworthiness.

2.4.2 Web Services Reliability

Web Services Reliability (WS-Reliability) specifies how a service can send reliable messages during SOAP message transfers (Iwasa et al., 2004). When the sender transfers a message to a receiver, the receiver needs to be assured that the message is delivered and exactly once. In other words, we can say that duplicate message delivery is not accepted.

Reliability is an essential property of web service functionality, as the communication between a client and a server needs to be fail-safe to execute a transaction. This is important especially when the transaction involves multiple agents comprising multiple tasks. It is paramount to ensure that a web service is built based on this specification so that the communication among services is not compromised. The more reliable a web service, the more trustworthy it will be.

Service reliability is one of the basic criteria based on which a customer wants to select a service. Thus, while evaluating the trustworthiness, the reliability level of a service becomes an indispensable component of the total trustworthiness measurement.

2.4.3 Web Services Security Policy

Web Services Security Policy (WS-SecurityPolicy) has specifications for the security assertions that work with the security framework in conjunction with the web service architecture (Lawrence et al., 2007). It describes how a SOAP message can be secured using assertions. In general, the components that are involved in a transaction need to communicate among each other by asserting themselves in the secured environment without compromising underlying security requirements. WS Policy assertions are applied to WS Security specifications. Some of the contents of this specification are: Security policy model, Policy considerations, Protection assertions, and Token assertions.

All of the required tokens essentially adhere to the specification standards. The level of cryptography algorithms need to be on par with the criteria according to the specification. In the case of web service security, the encryption of the message, the security strength of the tokens exchanged, the methodology of the token sharing protocol, the endpoint policy subject assertions, along with all other mentioned assertions, add to and strengthen the earlier security policy specification. Some of the token assertions are: Username token assertion, X509 token assertion, Kerberos token assertion, and Security Assertion Markup Language (SAML) token assertion.

While evaluating the total trustworthiness of a web service, the measurement of the adherence to WS-SecurityPolicy specification is important and highly relevant. In our analysis of the web service total trustworthiness, steps will be taken to make sure that proper weight will be applied to security policy implementations.

2.4.4 WS-Trust v1.4

WS-Security provides the base guidelines for building a secured web service while WS-Trust specification emphasizes the importance of the safe and secured way of distributing security tokens among the various domains and networks that are involved during the exchange of the messages.

When we think about the secured message exchange among various parties that are involved in a transaction, the parties should be assured that they are exchanging the

messages in a real secure way. In other words, they need to exchange the credentials among themselves and these credentials need to be verified by renowned, accepted third party trust domains.

Alternatively, we can say that this specification extends the criteria of the WS Security in providing detailed standards for the security tokens, the way to communicate to the other registries including the WSDL descriptions. This requirement also establishes the extensions specification needed in order to build a solid framework in instituting the security of a web service. The following are the core components of this standard: Issuing and requesting a security token, and Brokerage a trust relation.

It is imperative that in our analysis of the total trustworthiness of a web service to ensure the WS-Trust specifications are met and implemented in appropriate ways as given in the guidelines. This is because a well implemented web service on these guidelines will ultimately increase the overall trustworthiness of a service and the service provider.

2.5 Literature Review

The phenomenon of trustworthiness and in particular, measurement of trustworthiness, is well researched in the context of web sites. This thesis will take advantage of the lessons learned from previous research on measuring trustworthiness of web sites.

The work of Toma (2010) focused on how people accept and proceed with sites that offer social networking as a service. Toma analyzed the provisions given for an online dating social networking structure and how people have entrusted organizations that offer this facility (Toma, 2010). Toma argues that trust is fundamentally attributed to the extent of how much we can reduce risk in attaining a higher level of comfort when progressing through an online website. The level of trustworthiness can be increased on a variety of factors. This paper goes through various methodologies and algorithms in calculating the accuracy of trustworthiness established through a website. A similar approach is employed in this thesis by considering various factors related to trusting web services and developing a methodology and algorithm to calculate trustworthiness of web services.

Infonetica Inc (2006) argues trustworthiness is a subjective opinion since what one person sees as trustworthy may not be agreed upon by other people. The author argues that trustworthiness of a website can be based on a person's demographic interest or alternatively comparing it with an already trusted web site. The paper further argues that instead of measuring trustworthiness as binary (yes or no) , it should be measured based on "confidence threshold" (Infonetica, 2006). One could set up a rating system based on their "risk tolerance" and "what the website offers" and any website that has high enough rating could be deemed trustworthy. In this thesis, users will be provided the opportunity to adjust factors important for them and provide confidence values on trustworthiness value so that services can be compared.

Murley (2006) has developed guidelines for evaluating information provided in web sites. Murley argues that it is very important to evaluate information found in the Web before using it, since anyone can publish anything in the Web, "information that was reliable when it was first published can become unreliable if it is not kept up-to-date, if the computer or network where the information resides is accidentally corrupted, or if the website is intentionally damaged" (Murley, 2006). Murley provides criteria for evaluating information found in web sites: authority (basically the identity and credentials of the web site author), objectivity (does the information have hint of bias?), accuracy (is the information accurate and complete?, does it provide citations?), coverage (does the source contain only information to a certain date?, does it include all relevant information?), and timeliness (is the information updated regularly?). In this thesis, authority, objectivity, accuracy, coverage, and timeliness will be used as factors to determine trustworthiness of web services.

The research of Pasternak and Roth (2010) argues that simplistic algorithm that measures trustworthiness through one scale may declare web site a trustworthy based on factual information presented even though the person publishing the information may be untrustworthy. The authors propose that trustworthiness should not be assessed as "scalar but as three separate values: truthfulness, completeness, and bias" (Pasternack & Roth, 2010). By doing so, the authors claim that the user can meaningfully assess the "extent to which a document or information source can be relied upon" (Pasternack & Roth, 2010). In this thesis, truthfulness, completeness, and bias will be used as factors to determine trustworthiness of web services.

2.5.1 Prior Work on Web Service Trustworthiness

Zhao et al. (Zhao et al., 2010) propose a reputation-based approach that utilizes user feedback to assess trustworthiness of web services. The authors have developed a prototype system called as service-Xchange, which acts as a search engine and service repository. This approach relies on user feedback to assess quality of the service and its trustworthiness. Thus, if a service does not have any user feedback, then its trustworthiness could not be assessed. Also, authors use only one factor (user feedback) to assess trustworthiness which is contrary to the findings from other trustworthiness literature on web sites.

Xiong and Perros (2008) argue that Service Level Agreement (SLA) is highly important for organizations taking part in online business transactions. SLA describes a contract between the service provider and the client (Xiong & Perros, 2008). SLA defines the quality of service (security, performance, and availability) agreed upon by the service provider and the client. The authors have developed a trust-based resource provisioning optimization model to assess trustworthiness of service providers. This model includes a trust manager, that negotiates SLA with potential service provides on behalf of a client and assess service trustworthiness based on SLA metrics. The authors' model uses only SLA metrics to assess trustworthiness ignoring other potential factors that could affect trustworthiness of a service.

Mehdi et al. (Mehdi et al., 2012) argue that in the context of large-scale systems, agent-based web services are necessary to fulfill complex user requests and system goals. The authors consider the problem of selecting trustworthy web services as a machine learning problem. The authors propose that trustworthiness can be calculated using probabilistic models. In particular, they evaluate two models: Bayesian Networks and Mixture of Multinomial Dirichlet Distributions. The authors conducted a simulation study to assess these two models empirically. Their study indicates that the Mixture of Multinomial Dirichlet Distributions model has better accuracy in modeling trust. Their approach relies primarily on feedback related to prior experience to calculate trustworthiness, ignoring other potential factors. Also the authors have developed their approach specifically for agent-based composite services, whereas the approach adopted in this thesis can be applied in all contexts.

The research of Wang et al. (2009) proposes to measure trustworthiness of a service based on the fidelity of support services. Fidelity of a supporting service is the probability that the supporting service would provide valid information (Wang et al., 2009). Unlike other approaches, the authors consider fidelity of supporting service as an important factor for assessing trustworthiness of primary services. The authors have developed a probabilistic model to calculate fidelity of a support service. While the fidelity of supporting services is an important factor for assessing trustworthiness, it is not the only factor that should be used for assessing trustworthiness. The authors' approach of assessing trustworthiness cannot be used in the context of atomic services (i.e., individual or a single service), which is the focus of this thesis.

Zhang (2005) argues that current standards and prior research are closely related to either security or non-functional aspects of web services. The author suggests that a separate framework is needed that takes into account both functional and non-functional aspects of web services to assess its trustworthiness. The author provides four reasons for why a service can be declared untrustworthy: (1) unfulfilled requirements, (2) malicious acts and code changes, (3) erratic Internet behaviors or resource scarcity that results in unacceptable delays, and (4) the poor interoperation of selected services.

Furthermore, the author identifies following challenges that need to be addressed to evaluate a total trustworthiness of a web service: (1) testing a web service for a specific requirement, (2) testing a web service for a specific user environment, (3) testing functional requirements, (4) testing non-functional requirements, and (5) testing the dynamic nature of a web service. The author argues that current approaches do not take a holistic view of trustworthiness, and we need new approaches for effective and efficient assessment of trustworthiness.

To address the above gaps, the author proposes a new framework called WS-Trustworthy, which comprises standards such as WS-Security, WS-Policy, WS-Trust, WS-Privacy, WS-Federation, WS-Secure Conversation, and WS-Authorization. While the author's WS-Trustworthy provides a promising starting point for evaluating web service trustworthiness holistically, it falls short as the framework does not provide a meaningful way to calculate trustworthiness taking those factors into consideration. Certainly, issues and gaps

identified by the author establish a context and pave the way for this thesis. This thesis aims at addressing the challenges put forth by the Zhang (2003).

Chapter 3

CONCEPTUAL MODELING

From the literature review, it is clear that trustworthiness is a multi-dimensional concept as it is influenced by multiple factors. In this thesis a conceptual model has been developed in order to identify relevant factors that influence trustworthiness of a web service. The literature review provided the context for bringing together all the concepts related to web services and trustworthiness. After scrutinizing and analyzing numerous factors that are relevant to web service and trustworthiness contexts, factors that influence assessment of trustworthiness were gathered. A holistic conceptual model was developed using principles of generalization and specialization. This model consists of all the relevant factors that can potentially influence assessment of the total trustworthiness of a web service. The principle of generalization was applied to group factors that had common characteristics and principle of specialization was applied to separate factors based on differences. The entire process was performed iteratively until the review and analysis of literature did not reveal any new relevant factors. See figure 2 for the conceptual model.

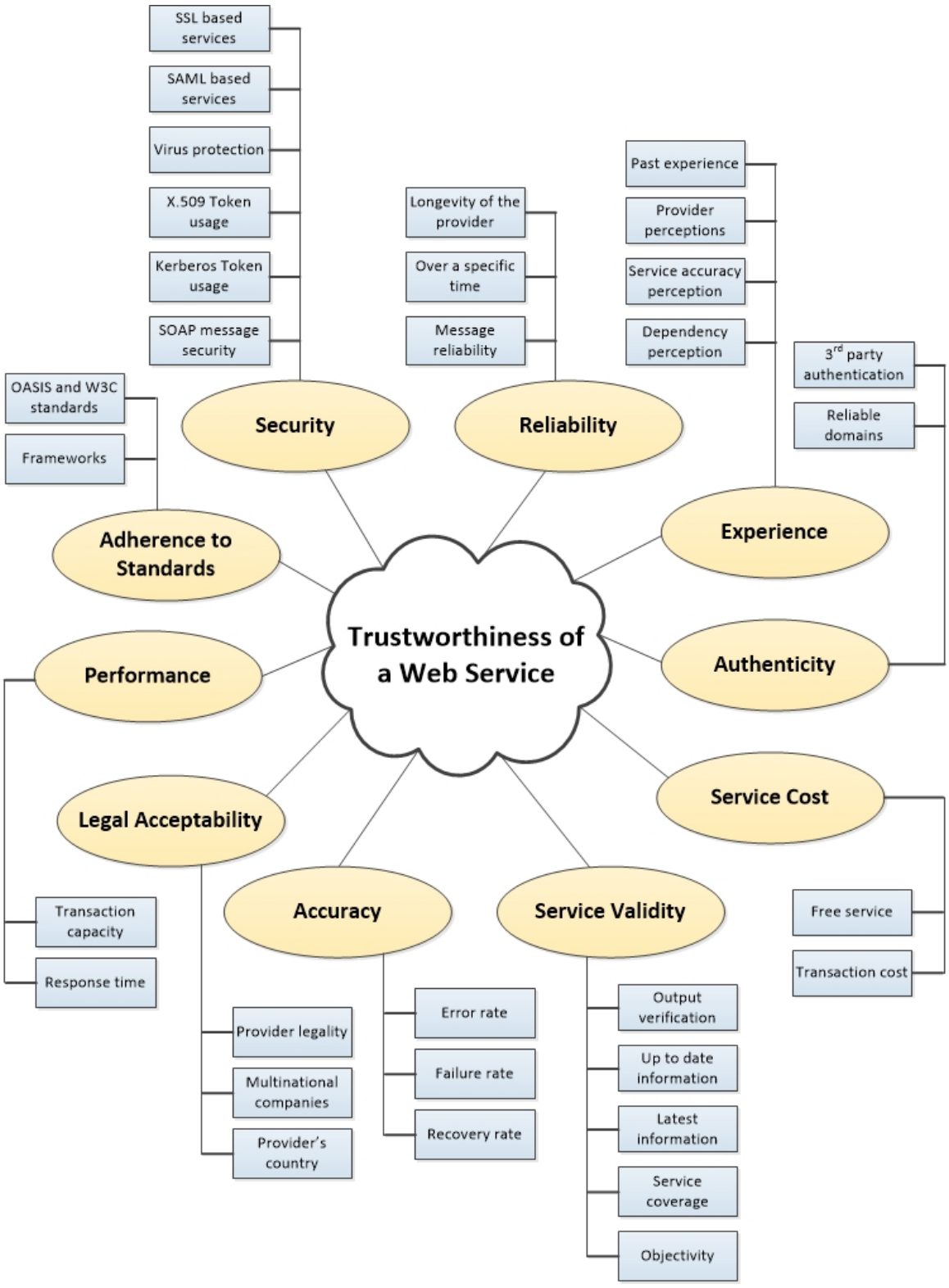

Figure 2. Conceptual Model

The following are the major factors that influence trustworthiness of a web service.

3.1 Security

One of the important trustworthiness concepts that have been vastly acknowledged within the literature is the security of the web service. Security is considered as a major aspect for web service development as the service is made available via the Internet. In general, a service can be accessed by two ways, either through an intranet or through the World Wide Web where anyone can access the service for a business or a personal need. The focus of this thesis is on the publically available services via World Wide Web. The sub-factors relevant to the security group are following: SSL (Secure Socket Layer), SAML (Security Assertion Markup Language), virus protection, X.509_token profile, Kerberos-token profile, SOAP message security, and risk factors on security.

In an attempt to measure the security related factors, the proposed tool in this thesis will read the WSDL document of the web service, the server where the service is hosted, the security details in the service URL, and other similar related information to assess the level of security offered by the service.

3.1.1 SSL Usage

SSL (Secure Socket Layer) offers the basic security for a communication between a client and a server, or between any two entities or among multiple entities. The message is

encrypted so that it cannot be easily deciphered by the other parties during the transmission. Hence, in web service methodology, SSL plays a vital role for the secured interaction between the clients and the servers. Without security, web services cannot be considered for business transactions.

3.1.2 SAML Usage

SAML (Security Assertion Markup Language) standard is an open source standard offered by OASIS. In online transactions, there are two elements that are vital to implementing security. These elements are authentication and authorization. During transactions between clients and servers, the knowledge of the above elements needs to be shared among the parties that are involved in the transaction.

In general, a third party is involved to make sure that the clients and servers are legitimate parties and they have the required access to handle the transaction the way the business requirements demand. SAML standard paves way to carry out these authentication and authorization in the defined XML format that can be shared among the parties in safe and secure ways.

3.1.3 Virus Protection

One of the major threats on the security side of the business transactions is the risk from virus attacks. To alleviate this problem, most of the web service providers use a proxy

service in front of the provider component that will take care of such risks. If we make sure that a typical proxy is used in front of the provider that mitigates these kinds of dangers then the environment would be more safe and secure. Typical proxy services for the web services are provided by major companies like IBM. Leveraging these services will enhance the trustworthiness of the provider.

3.1.4 X.509 Token Profile Usage

The standard for the key exchanges during the encryption and decryption of the secured messages (TurnerNadalin, et al., 2012a) is named X509. This is important in web service transactions, as online transactions need to be encrypted to ensure safety and security of the message content. Encryption and decryption involves the usage of keys. The X509 standard specifies the format for exchanging the key certificates and attribute certificates. It is imperative that this standard be followed while exchanging the certificates and other keys among involved parties within a transaction.

3.1.5 Kerberos Token Profile Usage

Kerberos essentially defines a mechanism for authentication protocol among various parties involved in a transaction to securely transfer each party's identification and subsequently transfer business information in a secure manner (TurnerMonzillo, et al., 2012). This protocol involves a third party which ensures that the involved parties are sharing their real identities during the authentication phase of the transactions.

In a typical client server authentication model, the clients need to establish their identities during their requests to the servers. In order to get the identities the clients reach the KDC (Key Distribution Center) and collect their authentication tickets. In general, the Kerberos makes sure that both the client and the server establish their secure network connections before proceeding to share their business information.

3.1.6 SOAP Message Security

SOAP message security is a part of WS-Security. SOAP message security ensures the SOAP messages are transmitted with confidentiality and integrity (TurnerNadalin, et al., 2012b). This specification offers three components: provision to protect messages from false disclosures, frameworks to attach the security tokens along with the messages while the transmission takes place, and a way to increase protection from the eavesdropping by intruders during the transmission of these secured messages. Components of SOAP message security can be applied altogether or individually while the transmission takes place.

3.2 Reliability

Reliability is a required measurement in assessing any software component's trustworthiness as it ensures dependable service offering. In the context of web services, reliability indicates an efficient service offering with minimal downtime. Thus, it is

imperative to measure level of the reliability of a web service as a part of its trustworthiness assessment. The sub-factors relevant to reliability are: how long the service provider has been in the market, how reliable the service is in a specified time period, what the failure rate of the service is, and message reliability (whether the message can be delivered without a failure and if failed whether the message can be recovered).

3.2.1 Longevity of the Provider

This particular sub-concept is very important to the consumer as it indicates whether the service provider is a well-established or a well-known organization. If the provider is established in the service market for a considerable amount of time with known reliability then this fact increases the trustworthiness of the provider. For example, if the provider of the service is Microsoft or IBM, then the consumer will have higher level of trust for the services offered by these providers.

3.2.2 Reliability in a Specific Time Period

This concept means identifying the reliability of the provider in the recent past. It is because many providers would have offered their services in the market and those services would have been used by many consumers successfully. However due to the technological changes or market issues the same services might not have been more reliable in the recent past. Therefore, while selecting a service for a business requirement, it is important to ensure the reliability of the service at the current period is stable and dependable.

3.2.3 Message Reliability

Message reliability can be attributed to the reliability of the business content provided by the service. This may not be critical for many business requirements, but for transactions oriented requirements, the business content cannot be lost due to many financial implications. Some services offer transaction coordination to make sure that the services roll back if the transaction is not completed for some reasons.

3.3 Experience

Experience is one of the most influential factors affecting trustworthiness. A favorable experience with a service provider certainly increases the trust associated with service offered by the provider. Thus, a good experience on a service increases the probability of better service in the future. Therefore, past experience with a service and service provider must be accounted for in the assessment of trustworthiness. The sub-factors relevant to experience are: level of service satisfaction from past experiences, perception of the provider, percentage of accuracy, percentage of dependency, and percentage of reliability.
In the tool proposed in this thesis, a provision for the user will be available to enter the satisfaction level of a provider with the organization. The values input will be used while we evaluate the trustworthiness of a web service.

3.3.1 Past Experience with the Provider

Past experience with the provider is vital and important for making a decision to select a new service offered by the provider. In assessing the trustworthiness of a service, if we have a database containing a satisfactory rating for the service provider, then this information can be leveraged in assessing the trustworthiness of the new service offered by the provider.

3.3.2 Users' Perception of the Providers

In some cases, the user may not have the past experience with the provider of the service. At those specific junctures, the perception of the providers in the market can be utilized while deciding the usage of the services offered by the providers. If the providers are well established in the market with a reliable track record then that information can obviously increases the trustworthiness of those sources.

3.3.3 Market's Perception of the Service Accuracy

Information collected on various providers of their service accuracy can be leveraged in making a decision of using a particular vendor's services. If the market feedback on the providers is good certainly it increases the trustworthiness of the services they offer.

3.3.4 Percentage of Dependability

This dependability factor can be ascribed to the experience of the client or by the other clients while using the services offered by the major providers or vendors. However, the client's personal experience with the provider obviously plays a vital role in deciding the choice of using the services. Dependability increases with reliability. The importance of reliability and dependability may be related to the requirements and clients' preference. Sometimes the client may be looking for a service to satisfy an immediate business requirement, and hence may not consider dependability and reliability as important. On the other hand, clients may consider dependability and reliability as very important factors if they are looking for a long term solution.

3.4 Authenticity

Authenticity of a web service is considered to be a stepping stone for building trust as it guarantees the service provider is real and does not have hidden agenda behind the services offered. It is important to include authenticity as a part of trustworthiness assessment, as it is helpful in identifying services that can be potentially fraudulent. Authenticity of a web service can be measured in many ways, including whether it is certified by third party authentication organizations like VeriSign, or whether it is a government service, or it is from a reputed major organization.

3.4.1 Third Party Authentication

Third party authentication can be identified from the certificate information that has been handed over to the client from the server. This is similar to 3rd party authentication like Verisign authentication. If the certificate is from one of the authentic 3rd party certifiers then the name of the guarantor can be added in the database for the assessment.

3.4.2 Government Service or from Other Reliable Domains

Services from user provided list of domains and services provided by government domains can be considered to be authentic and reliable, thus, increasing its trustworthiness.

3.5 Cost of the Service

The concept of cost may not be a part of trustworthiness evaluation but in general cost can affect how a client perceives the service and how well it is maintained. As long as the service is maintained it might increase the trustworthiness of the service. The cost of the service is an important factor for small organizations as they might be a little more cost conscious. Large organizations may not have a constraint on the cost of the web services but even then if the cost is based on a transaction usage they may think otherwise. An organization that expects millions of transactions may not want to be tied on the transaction

count based pricing as that could very well go beyond their budget for their business process implementation.

In this thesis cost is introduced as an optional factor to be included as a part of trustworthiness assessment, if needed by the user; the cost will not be incorporated as a part of trustworthiness assessment in the proposed tool. If there is a desire to add this in future, the user will be able to include this value in the trustworthy index calculations. If the user has intentions of buying the services within a particular cost range then the tool can match the cost of the services that fall into the user's cost range.

3.5.1 Free Service

The user can access information regarding the cost of service in the provider's site or in service description pages. The user can enter information on whether the service is free to use or not in the knowledge database to calculate the cost/benefit ratio. In general, if a service is offered by the provider on cost basis that would increase accountability on the provider side in offering services. This in turn might increase the trustworthiness of a service.

3.5.2 Cost per Transaction

When the provider offers services on cost per transaction basis, the user can enter this information into the knowledge database to calculate the cost/benefit ratio while comparing the services from different types of vendors.

3.6 Validity of the Service

A web service that offered high quality service in the past does not necessarily mean currently offers a similar level of service. As a web service is in the online arena, the validity of a service can be hindered for many reasons. For example, the service's certificate might have expired; the service might have been broken because of high frequency usage; or the service might go out of order because the technology has changed in the recent past. Some of the validation techniques that can be used to check whether the service is currently valid are by verifying whether the service is rendering the desired output at this point of time, whether the information about the service is up to date, when the information was updated, coverage of the service, and the objectivity of the service.

3.6.1 Verifying Output Rendered

One of the simple validation techniques is just to check whether the service is rendering the desired output at this point of time. There could be other validation checks to make sure whether the service is based on a specific standard and on a specific optimized technology.

3.6.2 Whether the Information is Up To Date

Since there are too many online services available, most of the times the information given by the providers offer these services could be outdated. When a client makes a decision to go ahead and choose a specific web service the present values of the web service need to be up to date. This is because the technology keeps changing rapidly and the current information of the web service is absolutely essential to take a proper decision.

3.6.3 Latest Date of the Information Availability

If the client feels the information received from the provider is old or outdated there needs to be a validation mechanism in choosing the date ranges like how far behind the information can be accepted to be in compliance with the client's requirements and mandates.

3.6.4 Coverage of the Service

Coverage is one of the additional subgroups of concepts of validity which involves verification of whether information provided by the service is valid only for certain date (Murley, 2006). It is possible that the information offered by the vendor could be valid for a limited time range and beyond that time range the offered information could be invalid. While choosing the services this needs to be checked before the selection is made to ensure whether the ongoing usage of the service will not be impacted by the given time range for the validity.

3.6.5 Objectivity

The cost/benefit calculation of the enterprise is driven by the objectivity of the business requirement. The objectivity is also one of the vital elements that drive the decision in deciding the trustworthiness of a web service based on the cost/benefit ratio. The cost/benefit ratio is discussed under the cost concept as well and it is up to the user to consider this factor while the choice is being made for a suitable service to the organization.

3.7 Accuracy

Accuracy of a web service is one of the paramount measures to be taken into consideration while choosing a service for desired business functionality. The accuracy of a service output can be tested by the clients while using the service but it is a challenge to measure the same from the initial available resources. However, by measuring the error rate of the service along with the failure rate and recovery rate, the accuracy of the service can be determined.

3.7.1 Percentage of Error Rate

The error rate of the service is the measurement of the service response errors when invoked by the clients. This can be assessed by invoking the web service. The rate of the errors can be measured as the ratio of number of failures to the number of successful invocations.

3.7.2 Percentage of Failure Rate

The failure rate of the service is the measurement of the service response failures when invoked. The rate of the failures can be measured as ratio of number of failures and number of times service invoked.

3.7.3 Percentage of Recovery Rate

The recovery rate of the service is the measurement of the successful responses after the failures when invoked by the clients. The rate of the recovery can be measured as the ratio of the number of successes to the number of failures.

3.8 Legal Acceptability

Legality of the service provider such as nationality, geographical location, trade embargo, and security protocol/policies are main concerns for some organizations in the health care and financial industries. For these organizations, selection of services is limited by legal constraints. In the proposed tool, we will identify the origins of the service and utilize the user's input on the provider's legality to assess trustworthiness of the service.

3.8.1 Service Provider Legality

Service provider legality is the main concern in current scenarios with various organizations (particularly in the healthcare sector). Due to the recent past security violations, the provider's legal acceptability, nationality, and geographical location are getting much attention these days. As far as web services are concerned, service provider legality has gained more importance and significance. In the tool proposed in this thesis, the users should be able to identify the origins of the service or allow user to input

information based on their knowledge on the provider to measure the trustworthiness of the offered service.

3.8.2 Provider's Status as a Multinational Company

The term multinational company is used here to emphasize the company's criteria to adhere to the international standards to run a business across the global platform. This acceptance by the universal regulations apparently increases the trustworthiness of the vendor and this factor can be utilized while evaluating the trustworthiness of a web service.

3.8.3 Validation of Preferred Countries

Choice of providers from preferred countries plays a vital role in choosing a service for various reasons such as stability, security, dependability etc. due to the recent developments in the global political environment. Understandably, this solely depends upon the client's requirements in the business domain.

3.9 Performance

Efficiency of a software component is typically measured based on its performance. Since web service is essentially a software component, its efficiency will be measured. If a service doesn't perform well then obviously it should not be selected. The proposed tool

would be designed to capture most of the criteria related to the performance of the service. Thus the tool needs to have provisions for measuring the performance of a web service and to log measured information for arriving at an index of trustworthiness.

3.9.1 Transaction Handling Capacity

Measurement of the transaction capacity in a specific period of time establishes more trustworthiness when the service is able to handle the client's requests at any point in time. If the service is able to serve many clients at a particular time then the client can depend upon the service more realistically.

3.9.2 Service Response Time During Critical Volume Conditions

This is the response time of the service when it is accessed by the client. In most cases, when there is high volume of requests, then the response time from the service gets increased. From the perspective of a client to the service, it may not be possible to compromise the response time at critical junctures based on many business impacts. Even though the service can handle high volumes at a certain period, as long as the response time doesn't get impacted significantly the trustworthiness of the service will not be affected.

3.10 Adherence to Web Service Standards

Web service standards play critical role in ensuring services are interoperable. Thus, inappropriate or lack of usage of standards, would impact reliable usage of the service. The proposed tool includes provisions to check whether appropriate standards are used for the relevant web service context areas.

In the software life cycle, a component needs to adhere to common accepted industry standards and frameworks. By and large in the software industry, maintaining software is a nightmare unless it has been designed and built on some specific standards. As the technology changes very rapidly, if a component is not built on an accepted framework or a standard then it might not be able to exchange information or be integrated with other software components. The proposed tool should then include provisions to check and validate whether the web services are using the required standards while communicating with the client. The tool needs to make sure at least the OASIS and W3C web service standards are implemented by the services.

3.10.1 OASIS and W3C standards

OASIS and W3C provide the basic standards for a web service for the online commerce applications. These organizations also provide the guidelines and specifications for running any e-commerce application that requires essential fundamental security, compliance to industry domain standards and other similar related features.

3.10.2 Web Service Resource Framework

WSRF (web service resource framework) gives guidelines to web services if they want to be maintained in an acceptable condition due to some specific business requirements (Banks, 2006). Eventually this all depends upon the client's requirement and can be taken into consideration if it is essential for the implementations.

All of the above concepts that are involved in the conceptual model need to be measured in assessing the total trustworthiness of a service. Figure 3 provides cause and effect diagram for web services trustworthiness developed based on the conceptual model.

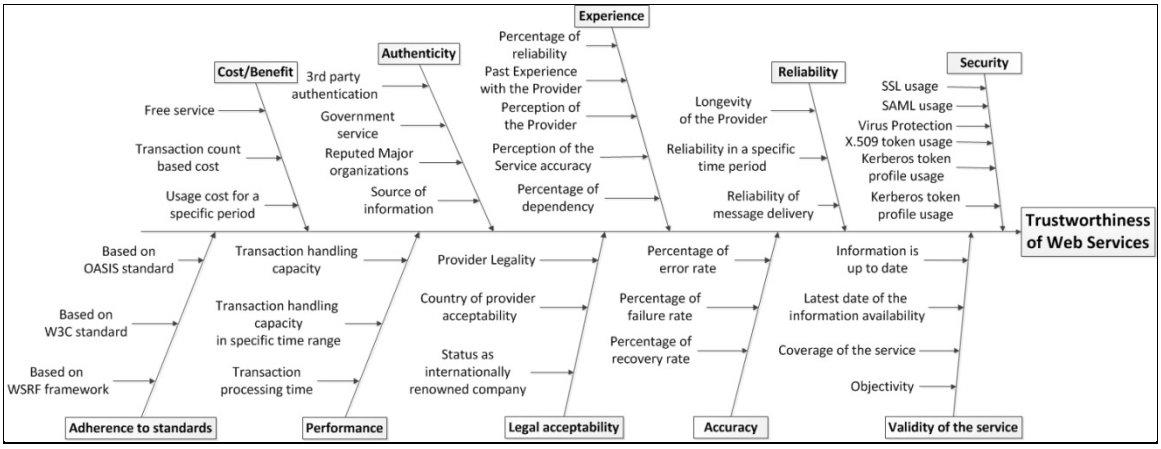

Figure 3. Cause and effect diagram for web service trustworthiness

Chapter 4

METHODOLOGY TO CALCULATE TRUSTWORTHINESS

This chapter provides details on how the data for sub-concepts identified in the conceptual model are gathered, and how the gathered data will be utilized to calculate a trustworthiness index as a measure of web service trustworthiness.

4.1 Security

4.1.1 SSL Usage

Usage of SSL can be identified from the URL of the web service. If the web service uses the HTTPS protocol instead of the regular HTTP then it can be determined that the web service is using the SSL for the communication. In other words, the web content cannot be obtained from the regular port 80; instead the port 443 need to be opened by the server for the client to receive the load and the security certificates are used to encrypt and decrypt the business content. The presence of the SSL usage will be noted as value '1' while the absence of SSL usage will be noted as value '0' for our measurements during the calculations.

4.1.2 SAML Usage

The indication of the SAML usage can be determined from the server reply content while it directs the client to a 3rd party authentication and authorization server. The usage of the SAML tokens will inform us whether the server leverages the facilities provided by the SAML protocol. The presence of the SAML usage will be noted as value '1' while the absence of SAML usage will be noted as value '0' for our measurements during the calculations. An aggregated average value of the security concepts will then be used in total trustworthiness based on the corresponding weights.

4.1.3 Virus and Other Security Threats Protections

The defensive mechanisms against virus attacks will generally be deployed by the service providers on the proxy servers. Some providers might use proxy server mechanisms like data power from IBM for instance to filter all offensive threats. Thus, virus and security threat protection can be detected by the presence of a proxy server. Identifying the proxy server's existence can solidify the protection from the offensive threats like virus attacks and other similar assaults. The presence of the proxy server usage will be noted as value '1' while the absence of proxy server usage will be noted as value '0' for our measurements during the calculations.

4.1.4 Usage of X509 Standards

The usage of X509 standards in key distributions may be detected from the contents received from the server while the clients interact with the services. The manifestation of this standard can be detected within the SOAP message. The presence of X509 tag usage will be noted as value '1' while the absence of X509 tag usage will be noted as value '0' for our measurements during the calculations.

An aggregated average value of the security sub-concepts will be used as a security group value in total trustworthiness index calculations based on the corresponding weights.

4.2 Reliability

4.2.1 Longevity of the Provider

This element measures how long the provider is in the market and doing business. The values can be received from the knowledge database that has been updated by the user based on consumer- forums, technical journals and other similar related sources. This will be aggregated in reliability concept values based on the 1 (low) to 5 (high) ratings. The accumulated final value will be used based on the weights applied.

4.2.2 Measurement of the Reliability of the Service in a Specified Time Period

Opinions of the reliability of the service in the recent past will influence the decision process. After using a service, the user will be asked to rate the service. The user rating response will be stored in the knowledge database. This value can be assessed from our own experience database if there is any for the service in the past. The concept values will be in the range from 1 (low) to 5 (high) ratings.

The combined value reliability sub-concepts will finally be used along with the corresponding weight in determining the total trustworthiness.

4.3 Experience

4.3.1 Past Experience with the Provider

The values of ratings on past experiences of a service can be assessed from our own experience database, if any exists. Users would be requested to rate a service after they use it or input it from any of the web service user forums, if available. The concept values will be in the range from 1 (low) to 5 (high) ratings and the combined value with the other experience concept values will be finally used along with the corresponding weight in determining the total trustworthiness.

4.3.2 Measurement of Accuracy

Partial values for accuracy can be assessed by invoking the web service URL and recording whether response was received. However the accuracy of the business functionality would need to be measured by the user and recorded later after the usage of the service. If the user has past experience of the service then that information can be leveraged from the experience database for the future considerations. Accuracy concept value will be in the range from 1 (low) to 5 (high) ratings. This graded value will be used in the accrued value.

4.3.3 Measurement of Dependability

Dependability rating value can be assessed from the experience database, if the client has inputted rating based on some previous experience with the provider. A range of values between 1 (low) to 5 (high) will be used in assessing the dependency concept.

4.3.4 Measurement of Reliability

This can be assessed from our own testing procedures from our user interface. This also can be assessed from the experience database if the client has some previous experience with the provider. If not, the values that are available from the knowledge database can be used to assess this measurement. The reliability concept will be measured using rating values from 1 (low) to 5 (high).

4.4 Authenticity

4.4.1 Third Party Authentication

Usage of 3rd party authentication can be identified from the certificate information that has been handed over to the client from the server. If the certificate is from one of the authentic 3rd party certifier then the name of the guarantor can be added in the database for our assessment. There are many 3rd party certificate providers like VeriSign and TWCA are available for authentication purposes.

The presence of the third party authentication usage will be noted as value '1' while the absence of the same will be noted as value '0' for measurements during the calculations. An aggregated average value of the authenticity sub-concepts will then be used in total trustworthiness based on the matching weights.

4.4.2 Government Service

Whether a service is provided by the government can be identified from the URL of the web service. If the URL ends with ".gov" then it can be assessed as a government entity. On the other hand, if the URL ends with ".edu," then it will be assessed as an educational institution. Government service will be weighed three times (a chosen weight > 1) as much as a commercial service in the calculation of trustworthiness index.

4.4.3 From a Reputed Major Organization

The user would be requested to input to the knowledge base a list of URL domains for reputed major organizations. Thus, whether a service is provided by reputed organization can be identified from the knowledge database. This sub-concept value will be measure in range from 1 (low) to 5 (high) ratings. This graded value will be used in the accrued value.

4.4.4 Source of Information

This is mainly to identify the fraudulent web services and to eliminate them from the trustworthiness process. The knowledge database needs to be utilized to identify the genuineness of the provider. This sub-concept value will be in range from 1 (low) to 5 (high) ratings like other concepts. This graded value will be used in the accrued value.

4.5 Cost/Benefit

4.5.1 Whether the Service is Free to Use

Whether a service is free to use can be assessed when we start using the web service. The information such as whether a service is free or it is on a charge basis can be entered into the knowledge database to calculate the cost/benefit ratio. The user needs to enter the

values of the cost of the service in the knowledge database. The concept values are calculated based on the range again like the earlier range values from 1(low) to 5 (high).

4.5.2 Cost of the Service is per Transaction Base or Time Base

The user can assess the service cost when they start using the service or from the service description, if available. The user will have to input cost structure information into the knowledge database along with rating of the cost structure. Similar to above, this sub-concept will be also measured with range values from 1 (low) to 5 (high).

4.6 Validity

4.6.1 Whether the Service Functionality and Information is Up-To-Date

Whether a service is up-to-date or not can be assessed by getting the latest service update date and comparing the date with the present date. The information collected can be entered into the knowledge database and used for the assessment. If the service is up to date the value will be '1' while if it is old then the value will be noted as '0' for measurements during the calculations.

4.6.2 Coverage

Coverage can be assessed if a blatant coverage is given by the provider in any of the technical journals and seminars. The user can input available information into the knowledge database to assess this concept value. If coverage is available then the value will be taken as '1' and if not the value will be assessed as '0' for the calculation purposes.

4.6.3 Objectivity

The objectivity is one of the vital elements that influence the trustworthiness and the subsequent selection of a web service. The objectivity of a service is driven by the cost/benefit ratio calculation based on a specific business requirement. Some services would be considered based on long term requirements and some could be based on short time requirements by the user's organization. Since this is the information from the customer's organization, the users will be requested to input objectivity information for the business requirement into the knowledge database. The user has to enter the inputs to validate the cost of the web service. If service objectivity is validated then the value will be taken as '1' and if not the value will be assessed as '0' for the calculation purposes.

4.7 Accuracy

4.7.1 Percentage of Error Rates

Percentage of error rates can be assessed while invoking the web service. The rate of the errors can be measured as a ratio of number of successes to failures. The service will be invoked multiple times and the error rates will be calculated. The values will be used in accuracy calculation and in the reliability calculation as well. The higher the error rate the lower the percentage of reliability will be.

4.7.2 Percentage of Failure Rate

Percentage of failure rate can be assessed while invoking the web service. The rate of the failures can be measured as the ratio of the failed invocations to the total invocations. The values will be used in accuracy calculation and in reliability calculation as well. The failure rate increase will decrease the percentage of reliability.

4.7.3 Percentage of Recovery Rate

Percentage of recovery rate can be measured as the rate of successful invocations after a failure has occurred. This value will be used in the accuracy and in the reliability calculations. The higher the recovery rate the higher the percentage of reliability will be.

4.8 Legal Acceptability

4.8.1 Provider Legality

The user will be requested to input a list of URLs of providers banned by the user's organizations for the purpose of business partnerships. Thus, the list of these banned providers will be available in the knowledge database which can be leveraged by the tool while validating the legality of the providers. The presence of the legal status will be noted as value '1' while absence of the same will be noted as value '0' for the measurements during the calculations.

4.8.2 Legality of the Provider's Country

A list of acceptable countries for service providers will be entered into to the knowledge database by the user. From the knowledge database, the information to know whether the provider's country is acceptable according to the user organization's restrictions can be obtained. The presence of services from acceptable countries will be noted as value '1' while absence of the same will be noted as value '0' for measurements during the calculations.

4.8.3 Status as an Internationally Renowned Company

Many international companies have earned the reputation of doing a trustworthy business in the online environment. The knowledge database needs to be updated with this kind of information and used in assessing the trustworthiness of the service. The presence of the international status will be noted as value '1' while absence will be noted as value '0' for measurements during the calculations.

4.9 Adherence to Standards

4.9.1 Service Built based on OASIS Standards

OASIS standard specification utilized to offer a service can be received from the WSDL information of the web service. The namespace inclusions would indicate the specifications utilized in the construction of the web service. The presence of the standards will be noted as value '1' while absence will be noted as value '0' for measurements during the calculations.

4.9.2 Service based on Frameworks like WSRF

Information regarding the utilization of a framework like WSRF can be received from the service WSDL. The namespace inclusions would indicate framework specifications

utilized while constructing the web service. The presence of the WSRF usage will be noted as value '1' while absence will be noted as value '0' for measurements during the calculations.

4.9.3 Service based on W3C Standards

W3C standard specification utilized to offer a service can be obtained from service WSDL. The namespace inclusions would indicate the W3C specifications utilized in the construction of the web service. The presence of the W3C standard will be noted as value '1' while absence will be noted as value '0' for measurements during the calculations.

Appendix A – Concepts and collection sources provides a summarized list of sub-concepts and sources from where relevant information about the concept will be gathered.

4.10 Calculating Trustworthiness Index

The algorithm to measure trustworthiness has to encompass all of the concepts identified and their weights into the final derivation of the trustworthiness index. It can be a simple addition of weights of various group concepts that contribute to trustworthiness index based on their importance and participation in deriving a total trust outcome.

An analysis needs to be made on all of the components to bring out their corresponding weight to the attribution. This could vary based on the given business requirement and

domain. In essence, the user who will be selecting the service should be in the position to vary the weight percentage based on the domain and business requirements. For example, some organizations would give more weight to the security concept compared to the cost. Some business sector can compromise on security if the cost can be reduced. In the same way, some concepts that attribute to trustworthiness will not be considered by the user in calculating total trustworthiness for their business. In those particular scenarios, the user can assign zero for weight so that the component will not impact the final trustworthiness calculated for their business. Thus, weights of concepts can be obtained as user inputs varying in range of zero to hundred. Forced distribution method will be used to obtain user input on concept weight, i.e., combined total weight for all concepts should be equal to 100. Thus, the trustworthiness index will be calculated based on a function of group concepts along with their weight assigned by the user's preference.

4.10.1 Algorithm to Compute Trustworthiness Index

Suppose the total trustworthiness is denoted by T_t. The individual Concept Groups can be denoted as CG with the suffix of an alphabet and a numeric value. The corresponding weight value for that group concept can be denoted as W_{cgs1}. Thus the total contribution of that group concept in the total trustworthiness calculation can be denoted as the multiplication of these two factors: W_{cgs1} and CG_{s1}.

For instance, suppose the security group concept is denoted by CG_{s1} and the group concept of reliability is denoted by CG_{s2}. Each group concept can be arithmetic mean of collection

of sub concepts under that group, i.e., CG_{s1} is average of the individual sub concepts (SG_1 to SG_n) that are available under the security group concept. Then the following equation describes the calculation of the total trustworthiness index of a particular web service:

$$T_t = W_{cgs1} \text{ x } CG_{s1} + W_{cgs2} \text{ x } CG_{s2} + \cdots + W_{cgs(n-1)} \text{ x } CG_{s(n-1)} + W_{cgsn} \text{ x } CG_{sn} \quad (1)$$

In the above equation, W_{cgsn} is the last value of the applicable percentage and CG_{sn} is the last group concept. It should be noted that the sum of the weight for each sub-concept must be always 100.

$$W_{cgs1} + W_{cgs2} + \cdots + W_{cgs(n-1)} + W_{cgsn} = 100 \quad (2)$$

Each group concept is average of the collection of sub concepts in that group. Hence the following will be a typical collection group. The subscript k stands for the k^{th} group concept and the subscript m_k stands for the number of the sub concepts under the k^{th} group concept.

$$CG_{sk} = \frac{SG_1 + SG_2 + \cdots + SG_{(m_k-1)} + SG_{m_k}}{m_k} \quad (3)$$

4.10.2 Confidence Level on the Calculated Trustworthiness Index

In the calculations of trustworthiness, trust index value of a service will be found to rank the services that are under study based on the indexes. However, the data collected on each service will vary based on many reasons. For some services, there may be sufficient data available while for some services the data availability may not be to an adequate level.

For instance, if 20 concept values are needed in a particular domain, then all of 20 values may not be available for all the services that are under consideration. For some services, only 10 values may be available while for others 15 may be. It is obvious that the more sub-concept values gathered, the more dependable the calculated trustworthiness index will be. This property can be attributed to the Confidence Level (C_f) of the assessment of the trustworthiness index.

The confidence level will be calculated as a simple ratio of number of sub-concepts for which data was gathered to the total number of sub-concepts considered. If the total number of concept values is 20 (based on user inputs on weight) and if only 15 values may be obtained from various sources for a service, then the confidence level may be calculated as 15 out of 20, or 75%. Similarly, if only 10 concept values are available out of the required 20 values the confidence level is 10 out of 20, or 50%.

Once the trustworthiness index value and the corresponding confidence level are calculated, then the services may be ranked. The total trustworthiness index of a particular

web service calculated as shown below can be used to rank and order the list of services considered:

$$T_t = C_f \left(W_{cgs1} \text{ x } CG_{s1} + W_{cgs2} \text{ x } CG_{s2} + \cdots + W_{cgs(n-1)} \text{ x } CG_{s(n-1)} + W_{cgsn} \text{ x } CG_{sn}\right) \qquad (4)$$

Chapter 5

RESEARCH METHODOLOGY

The research methodology followed in this thesis consists of four steps: (a) developing a conceptual model of concepts influencing and impacting trustworthiness of a web service, (b) developing a methodology to assess trustworthiness, (c) developing a proof of concept system incorporating the methodology to assess trustworthiness, and (d) evaluating the proof of concept system to demonstrate the utility of the methodology. The first step involves reviewing relevant literature to identify concepts related to the trustworthiness of web services and developing a conceptual model based on the identified concepts. The second step involves analyzing the conceptual model to determine the contribution of concepts related to trustworthiness, applying appropriate weight of these concepts based on user inputs, bringing in the preferences of the end user's perspective into the calculations, and eventually developing an algorithm to measure the total trustworthiness of a web service. The third step involves building a proof of concept system to assess the trustworthiness of web services. Finally, the fourth step involves evaluating the accuracy of the trustworthiness measurement by the proof of concept system.

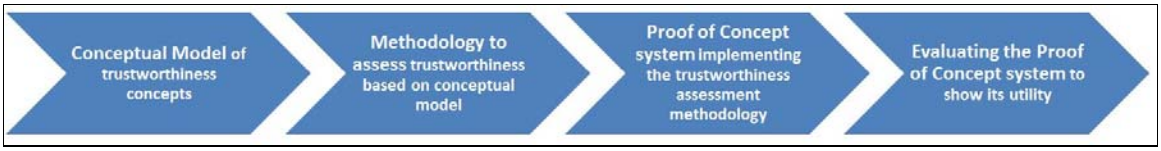

Figure 4. Research Methodology Steps

5.1 Proof of Concept System

A simple Proof of Concept (POC) system was built with the basic MVC pattern (Model View Controller). The POC system was built using the ASP.NET technology platform. The ASP.NET platform was selected due to author's familiarity and experience. The MVC pattern is an industry accepted best practice for building web applications using ASP.NET as it aids developers with separating different concerns of a web application. A basic MVC framework contains Models, Views and Controllers. Models simply represent the business data while the views represent various screens the customer can use to view business data with corresponding flavors. The controller is the in-between component that really interacts between the user's screens and the model objects based on the framework.

The MVC pattern could be framed with multiple layers. In the POC, the presentation layer poses two types of presentations to the end user. The first one would be providing the user the ability to invoke available web services to study their performance in relation to the trustworthiness concepts. The second one provides the user interface for the persistent layer of this framework. In such schemes, models may contain the business data that may be available for the analysis. In the POC system, the model layer consists of classes for analyzing the trust worthiness of web services. A typical class diagram of this POC is shown in the figure 5. This has the various Controllers and Models that are used in this development.

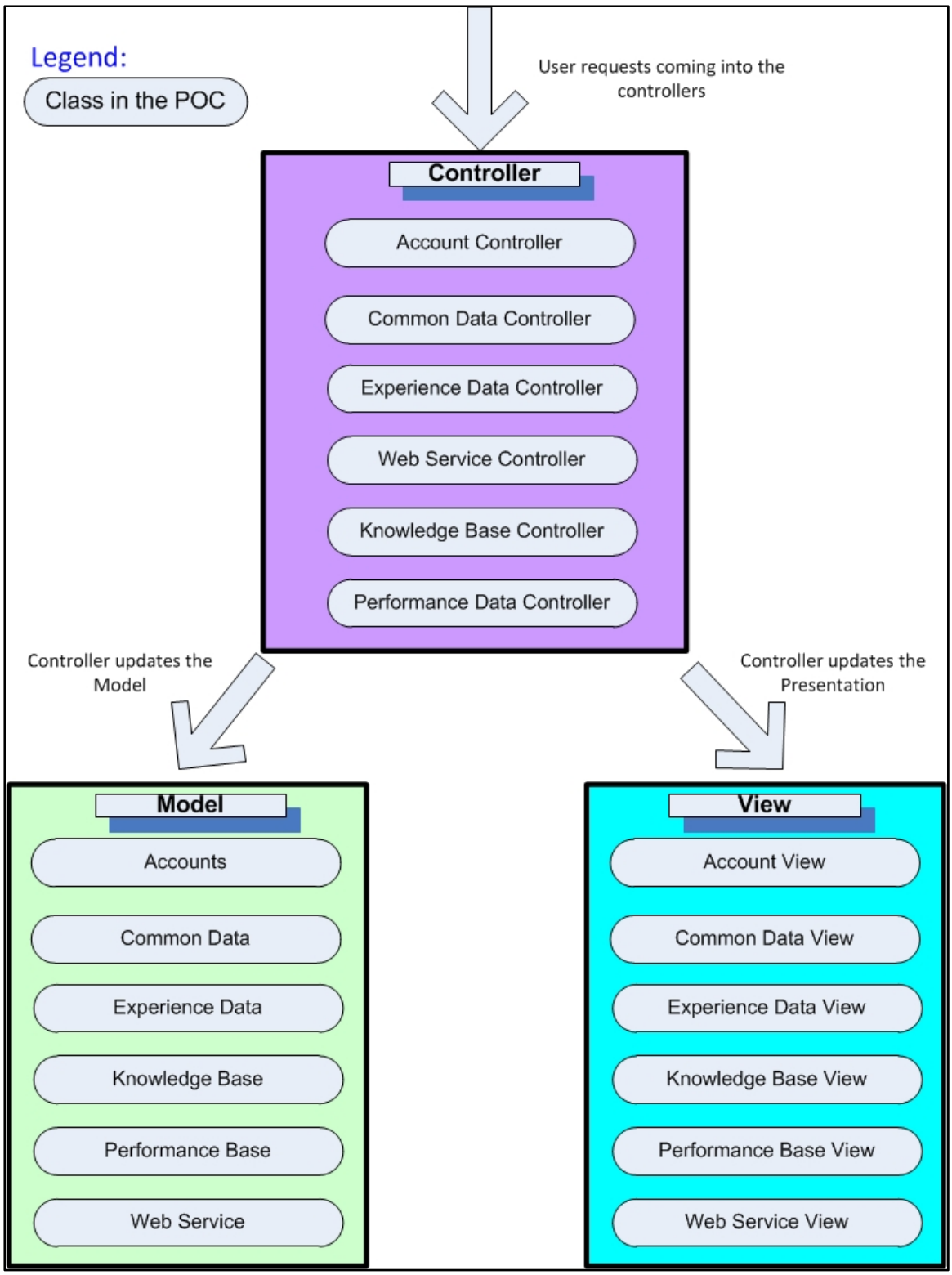

Figure 5. A POC designed following the MVC Pattern

5.2 Obtaining Trustworthiness Concept Values

The POC system will obtain relevant information of trustworthiness concepts from the available web services. There are many ways in which these concept values may be collected. For instance, the POC system should provide a provision for collecting the base concept values from the URL of the web service. Some values such as the usage of frameworks that are used in web services like a WSRF based frame work and the usage of specifications like WS-Security can be obtained from a WSDL of the web service.

The POC system will not collect trustworthiness concept values from Universal Description, Discovery and Integration (UDDI) registries. While concept values such as the provider names and their credentials can be obtained from the web service UDDI registries, collecting the required values from the UDDI was excluded as the UDDI registries are not used by majority of the web services. Most of the information relevant to trustworthiness concepts can be collected from other resources apart from the UDDI such as data from the servers, URL, and WSDL.

Similarly, other concepts such as provider's reliability and integrity can be collected from the past experience sources if they are made available. The POC system does not have provisions to directly collect data for above mentioned concepts from the market, technical articles, or journals. However, the knowledge of the various providers and their services can be entered into the POC system by the users, and these user inputs can be used as knowledge database to take some of the decisions based on the data provided. The POC

system will also request the user to enter data on their previous experience from the web services under consideration as well as their experience with the various providers. This experience database subsequently can be used for calculating trustworthiness.

There are also other resources available, like the content received from the web service server and the content received while redirecting the service client to a 3rd party application for purposes like authentication. These resources also can be used to get some of the concept values required to assess the trust worthiness of the services. The concepts along with their collection methods are summarized in the Appendix A.

Chapter 6

EVALUATION

6.1 Evaluation Objectives

Evaluating the proposed tool and the trustworthiness mechanism to determine whether they meet desired expectations of potential users is a necessity for a research project that involves a designed artifact (Hevner et al., 2004). The objective of this evaluation is to show the utility of the prototype that implements the methodology for calculating the trustworthiness of a web service. We exhibit the utility of the prototype to calculate the trustworthiness index by demonstrating following:

1. Trustworthiness index is a multidimensional concept, and existence (or non-existence) of these concepts can be verified and subsequently collected for assessing the trustworthiness of a web service.
2. Total trustworthiness index value, generated by the prototype can be meaningfully interpreted to aid in the selection of a suitable web service for a stated requirement.

One of the major contributions of this thesis is the development of the conceptual model to measure the total trustworthiness of a web service. Thus, the first objective focuses on demonstrating that the various concepts elaborated in the model can be verified and

collected in a systematic way to calculate the trustworthiness index value for a given business requirement criterion. The second objective focuses on the prototype tool that has been built on these foundations. The prototype tool was tested to make sure that the resulting calculated values can be meaningfully interpreted in making a decision of selecting a suitable web service based on the business requirements criteria.

6.2 Scenario-based Evaluation

The prototype tool and the trustworthiness mechanism were evaluated using a scenario-based analysis method. Scenario-based evaluation is an appropriate technique to determine whether a software system meets a set of desired quality attributes (Kazman et al., 1996). Scenario-based evaluation involves the following steps: scenario development, performing scenario evaluations and analysis, and interpreting scenario analysis results. In this thesis, a set of scenarios is used to illustrate the methodological use of the prototype to select a service based on its trustworthiness. A scenario is a brief description of desired behaviors of a system (Kazman, et al., 1996). For this thesis, scenarios are essentially the business requirements that need to be satisfied by the selected web service. The prototype tool was used to invoke services identified for each scenario. Outputs generated by the prototype tool were used for evaluation. The following are the outputs that were generated by the prototype:

1. The values for concepts related to the trustworthiness of the service as identified in the conceptual model.

2. The Trustworthiness index value calculated based on the collected concept values, the business requirements, and concept weights stated in the scenarios.

The above two outputs can be meaningfully interpreted to select a suitable service for three stated business scenarios.

6.3 Scenarios Used for Evaluation

Scenario-based evaluation comprises of using the prototype system and generating a total trustworthiness index value for a given set of web services and business scenarios. For this purpose, we used both publically available services and a few custom developed web services. We leverage these services to exhibit practical usage and robustness of the prototype as well as to exhibit the methodology to calculate the trustworthiness index. We develop custom web services to exhibit multi-dimensionality of trustworthiness. The custom built web services were developed to complement randomly selected publically available services during the testing process.

In order to aid this evaluation, we identified three business scenarios. The first business scenario deals with the requirement of displaying local weather conditions for visitors to a major health care organization's retail center. The second scenario deals with the requirement of visitors submitting potentially sensitive information relevant to their health during a registration process with emphasis on security features. The third scenario is same as the second scenario but emphasizes the availability and precision features of the service.

The tool needs to identify a suitable web service for each requirement and present the results.

6.3.1 Scenario #1

A leading Healthcare company wants to encourage customers visiting the company web pages to visit local Retail Centers established by the company at various locations. To aid the customers with choosing their timings at the retail centers, the local weather information is displayed for the location of each Retail Center for a period of time. Hence, the company needs a weather web service to aid in displaying the local weather on the web pages to enable the customers choose their timings to visit a retail center.

The healthcare company needs a weather web service with the following criteria:

Mandatory requirements:

1. The service response time needs to be at an accepted level < 500 ms.
2. The provider needs to be from inside the country USA according to the HIPPA regulations.
3. The provider should not be listed in the restricted providers list according to the business legal constraints.
4. The Trustworthiness index needs to be calculated with weight at equal distribution and also needs to be calculated with 40% weight over precision and availability concepts compared to the other weight concepts.
5. High availability is required to be more than 95%.

Optional requirements:

6. SSL/Data encryption
7. Government service or a service from a renowned organization
8. Services built on standard web service frameworks

For the purpose of the evaluation, the following public web services will be used for scenario #1:

Weather–Service 1 →http://www.restfulwebservices.net/wcf/WeatherForecastService.svc

Weather–Service 2→http://graphical.weather.gov/xml/SOAP_server/ndfdXMLserver.php

Weather–Service 3 → http://www.webservicex.net/globalweather.asmx

Weather–Service 4 → http://wsf.cdyne.com/WeatherWS/Weather.asmx

Weather–Service 5 → http://www.lostsprings.com/weather/WeatherService.asmx

Weather–Service 6 → http://trial.serviceobjects.com/fw/FastWeather.asmx

Most of the searches for free publicly available web services were made using Google search. The following are the major sites that contributed to the collection of freely available web services for our testing purposes:

http://www.service-repository.com/

http://msdn.microsoft.com/en-us/magazine/cc164049.aspx

http://www.webservicex.net/WS/wscatlist.aspx

http://free-web-services.com/web-services/geo/weather/

http://wiki.cdyne.com/?title=CDYNE_Weather

http://free-web-services.com/

http://www.weather.gov

http://docs.serviceobjects.com

Weather – Service 1 and Service 3 were found from Google search for weather web service along with WCF (Windows Communication Foundation) framework. It is a RESTful web service. Weather – Service 2 was located from the site http://www.weather.gov. Weather – Service 4 was found from the site http://www.service-repository.com. Similarly Weather – Service 5 was found from the site http://free-web-services.com. Weather – Service 6 was collected from the http://docs.serviceobjects.com.

Sufficient precautions were taken to avoid unsafe and deceptive web services. Services from search result set were invoked to test for genuineness and legitimacy. We have leveraged the recommendations and guidance in selecting web services from major magazines and periodicals like PCWorld.

In general, the requirements specified in the scenarios were instrumental in the selection of the web services. For example, in the first scenario, we need to choose a web service where the provider is from USA. Hence the shortlisted web services needed to be from other countries as well to make sure that the prototype chooses a service from USA according to the stated requirement. Similarly, to select a highly available web service, we need to make sure at least some of the shortlisted web services have poor availability status. Given the above context, we decided to select six web services to ensure that we have sufficient number of services to adequately test the prototype.

6.3.2 Scenario #2

A leading healthcare company wants potential customers visiting its website to register and create a user profile. It is mandated to secure data flows within the website as it requires the customer to provide health related information which is PHI (Protected Health Information as per Health Care Act HIPPA privacy Rules) along with other sensitive data like social security number. The company needs the registration service to be always available to the customers. The company does not want to lose a potential a customer due to the non-availability of the web page services. The healthcare company needs a registration web service with the following criteria:

Mandatory requirements:

1. The service response time needs to be at an accepted level < 500 ms.
2. The provider needs to be from inside the country USA according to the HIPPA regulations.
3. The provider should not be listed in the restricted providers list according to the business legal constraints.
4. Data encryption - required along with SSL connectivity.
5. The Trustworthy index needs to be calculated with weight at equal distribution and also needs to be calculated with 60% weight over security concepts compared to the other weight concepts.
6. High Availability is required to be 90% or more.
7. Reliability of the service availability is needed over consecutive invocations.

Optional requirements:

8. Response time < 200 ms.
9. SAML based web service.
10. Services built on standard web service frame-works.

For the purpose of the evaluation, the following web services will be used for scenario #2:

Registration–Service 1 → http://localhost:6004/ServiceProvider/RegistrationService.asmx

Registration–Service 2 → http://localhost:54304/RegistrationService1.asmx

Registration–Service 3 → http://lightbulb.saml2.com/lb/register.php

Registration–Service 4 → http://www.lundachark.se/Register.asmx

The above scenario #2 requirements need the web services to have high security features built-in like SSL and SAML. It is very rare to see publicly available and free web services having all these built-in security features. A couple of web services given above, Service 3 and 4 were chosen from Google search as these services contained registration functionalities. Service 3 is an openSSO Extension that has the SAML methodology. This service can be leveraged for our evaluation as it is a PHP based web service that has incorporated the security mechanism. Service 4 is another web service that has been selected as it has the built-in registration functionality but does incorporate security features. As per the given requirement, we need to get a web service that has been built with more robustness on the areas of safety and security. To cater to this need custom built web services were also developed for testing purposes. Hence the selection of the public web services and custom-built web services was used for scenario #2. Web service

Registration – Service 1 is a secured service built with SSL and SAML while the Registration – Service 2 will be a non-SSL and non-SAML web service.

6.3.3 Scenario #3

In the same Healthcare Company as in scenario #2, another division of the company wants to emphasize 60% weight on Precision and Availability of the service rather than the emphasis on the security as in scenario #2. In this case, we need to select the best suitable web service for this division's requirement among the four available registration services. Thus, the division in the Healthcare Company needs a registration web service with the following criteria:

Mandatory requirements:

1. The service response time needs to be at an accepted level < 500 ms.
2. The provider needs to be from inside the country USA according to the HIPPA regulations.
3. The provider should not be listed in the restricted providers list according to the business legal constraints.
4. The trustworthiness index needs to be calculated with 60% weight over precision and availability concepts compared to the other concepts.
5. The service needs to be highly available.
6. Reliability of the service availability is needed over consecutive invocations.

Optional requirement:

7. Services built on standard web service frameworks.

For the purpose of the evaluation, same four registration services listed under scenario #2 will be used for scenario #3 as well.

6.4 Trustworthiness Concept Values Data Collection

Each web service identified for the above scenarios will be invoked to acquire values for trustworthiness concepts. The trustworthiness index will be calculated based on the collected concepts with equal distribution percentages for concept groups. The calculated trustworthiness index value for each of identified services for a given scenario will be compared to select a service. Following that, the trustworthiness index will be calculated based on the user preferred concept group distribution percentages and subsequently a service will be selected. A combination of equal distribution and user preferred distribution is used to demonstrate the importance of user preference within the process of calculating the trustworthiness index.

6.4.1 Comparison of Weather Services for Scenario #1

Appendices B to G exhibit the collected values of each Weather Service for the scenario #1. Table 1 exhibits the condensed concept group values with the calculated trustworthiness index and the confidence levels of each Weather Service along with even weight distribution, as shown below:

- Security: 20%

- Standards: 20%
- Precision & Availability: 20%
- Authenticity: 20%
- Reliability: 20%

Web service URLs	Security Group Concept Value	Standards Group Concept Value	Precision and Availability Group Concept Value	Authenticity Group Concept Value	Reliability Group Concept Value	Confidence level	Trustworthiness Index value
Weather – Service 1	0.83	2	5.75	3.8	5.83	**63%**	**2.29**
Weather – Service 2	0.83	0	10.00	5.8	8.33	**65%**	**3.24**
Weather – Service 3	0.83	2	9.00	3.8	8.5	**65%**	**3.14**
Weather – Service 4	0.83	2	9.50	3.8	8.67	**65%**	**3.22**
Weather – Service 5	0.83	2	9.00	3.2	8.17	**55%**	**2.55**
Weather – Service 6	0.83	0	9.25	4.4	9.17	**74%**	**3.50**

Table 1. Trustworthiness index values for Scenario #1 with default distribution

Based on the above test results with equal weight distribution, the web service **Weather – Service 6** was found to be more trustworthy than the other web services, as it has the highest trustworthiness index and confidence level values. From table 1, it can be noted that all six services attained 0.83 for security group concept value. All six services had partial score for mutual trust concept and none for other security sub-group concepts, thus, receiving 0.83 for security group concept. Mutual trust subgroup is verifying whether both server and client is being fully authenticated or just server is authenticating itself to the client.

However, based on the scenario #1 requirements, we need to apply 40% weight over precision and availability concept. Rest of the concepts weight was even distributed to 15%, so that, combined total weight is100%. Hence each web service was invoked one more time with the changed weight distribution based on the weight requirement as given in Appendices B to G:

- Security: 15%
- Standards: 15%
- Precision & Availability: 40%
- Authenticity:15%
- Reliability: 15%

Web service URLs	Security Group Concept Value	Standards Group Concept Value	Precision and Availability Group Concept Value	Authenticity Group Concept Value	Reliability Group Concept Value	Confidence level	Trustworthiness Index value
Weather – Service 1	0.83	8	9.00	3.8	6.83	**68%**	**4.43**
Weather – Service 2	0.83	0	9.75	5.8	8.33	**65%**	**3.99**
Weather – Service 3	0.83	2	9.00	3.8	8.67	**65%**	**3.83**
Weather – Service 4	0.83	2	9.5	3.8	8.67	**65%**	**3.96**
Weather – Service 5	0.83	2	9.00	3.2	8.17	**55%**	**3.15**
Weather – Service 6	0.83	0	6.25	4.4	7.83	**71%**	**3.17**

Table 2. Trustworthiness index values for Scenario #1 with user distribution

Table 2 exhibits condensed concept group values with the calculated trustworthiness index and the confidence levels for scenario #1 requirements. Based on the above test results during this invocation the Weather – Service 1 was found more trustworthy compared to

the other web services. From table 2, it can be noted that **Weather – Service 1** meets 6 out of 8 requirements listed for scenario#1. Table 3 provides status on requirements that are met and not met. Service 1 satisfies stated requirements as it has notched 377 mille seconds as the average response time which is less than 500 mille seconds. The location of the service provider is from USA which satisfies the HIPPA regulation as mentioned in the requirements. The provider has also been identified as not existing in the banned/restricted vendor short list. Apart from these the service has been available at 100% during the various invocations of the testing times which satisfies the availability to be more than 95%. The services also utilizes WCF standards framework. Two requirements that were not met are optional requirements which are SSL and government/renowned service requirements.

Requirements	Status
Mandatory Requirements	
The service response time needs to be at an accepted level < 500 ms.	Met
The provider needs to be from inside the country USA according to the HIPPA regulations.	Met
The provider should not be listed in the restricted providers list according to the business legal constraints.	Met
Trustworthy index needs to be calculated with weight at default distribution and also needs to be calculated with 40% weight over precision and availability concepts compared to the other weight concepts.	Met
High Availability is required to be more than 95%.	Met
Optional Requirements	
SSL/Data encryption	Not Met
Government service or a service from a renowned org.	Not Met
Services built on standard web service frame works.	Met

Table 3. Scenario #1 – Weather Service 1 Requirements Satisfaction Status

For scenario #1 with even concept group distribution, Service 6 was selected based on the trustworthiness index. However, when user preferred distribution was applied Service 1 was selected as a more suitable web service. For user preferred distribution, importance was placed on the precision and availability concepts and the services were invoked again thus favoring Service 1 for our selection. Selection of different services based on user preferred distribution validates and demonstrates importance of incorporating user preference as a part of the process to calculate the trustworthiness index for a service.

6.4.2 Comparison of Registration Services for Scenario #2

Appendices H to K exhibit the collected values of the each Registration Service. Table 4 exhibits the condensed concept group values with the calculated trustworthiness index and the confidence levels of each registration service along with even weight distribution, as shown below:

- Security: 20%
- Standards: 20%
- Precision & Availability: 20%
- Authenticity: 20%
- Reliability: 20%

Web service URLs	Security Group Concept Value	Standards Group Concept Value	Precision and Availability Group Concept Value	Authenticity Group Concept Value	Reliability Group Concept Value	Confidence level	Trustworthiness Index value
Registration – Service 1	9.17	2	6.25	6	8.50	**91%**	**5.81**
Registration – Service 2	0.83	2	9.50	5	9.33	**85%**	**4.53**
Registration – Service 3	0.83	0	5.00	3	3.83	**82%**	**2.08**
Registration – Service 4	0.83	2	8.75	3	9.33	**85%**	**4.06**

Table 4. Trustworthiness index values for Scenario #2 with default distribution

Based on the above test results with even weight distribution, **Registration – Service 1** has been found to have the highest trustworthiness index; thus it is more trustworthy compared to the other web services. From table 4, it can be observed that service 1 attained 9.17 and the rest of the services attained 0.83 for security group concept. A combination of service 1 and service 2 values yields 10, the maximum attainable value for the security group concept by service. This pattern is incidental. Service 1 received values for all security sub-group concepts, whereas, other services received value for only mutual trust (only partial score) sub-group concept.

However, based on the scenario #2 requirements, we need to apply 60% weight for security concept. The weights for the rest of the concepts were even distributed to 10%, so that, combined total weight is 100%. Hence each web service was invoked one more time with the changed weight distribution based on the weight requirement as given above from Appendices H to K:

- Security: 60%

- Standards: 10%
- Precision & Availability: 10%
- Authenticity:10%
- Reliability: 10%

Table 5 exhibits the condensed concept group values with the calculated trustworthiness index and the confidence levels for scenario #2 requirements. Based on the above test results, the web service **Registration – Service 1** was found more trustworthy compared to the other web services. From table 11, it can be noted that Registration – Service 1 meets all of the 10 requirements listed for scenario #2. Table 6 provides status on requirements that are met. The service response time was observed as 155 ms, which is less than 500 ms. It has even satisfied the optional response time of less than 200 ms. Service has been identified by the tool that the provider is from inside of the country USA along with legal requirements. The service uses SSL encryption for the data transfer which is one of the mandatory requirements. It has also been identified that the service uses SAML security standards as per the requirement. The availability of the service has been found as 90% which satisfies the availability requirement. It also noticed that the service has used some web service basic framework standards.

Web service URLs	Security Group Concept Value	Standards Group Concept Value	Precision and Availability Group Concept Value	Authenticity Group Concept Value	Reliability Group Concept Value	Confidence level	Trustworthiness index value
Registration – Service 1	9.17	2	6.25	6	8.17	**91%**	**7.05**
Registration – Service 2	0.83	2	9.50	5	9.67	**85%**	**2.65**
Registration – Service 3	0.83	0	5.50	3	3.83	**82%**	**1.42**
Registration – Service 4	0.83	2	8.75	3	9.17	**85%**	**2.37**

Table 5. Trustworthiness index values for Scenario #2 with user distribution

Requirements	Status
Mandatory Requirements	
The service response time needs to be at an accepted level < 500 ms.	Met
The provider needs to be from inside the country USA according to the HIPPA regulations.	Met
The provider should not be listed in the restricted providers list according to the business legal constraints.	Met
Data encryption - required along with SSL connectivity.	Met
Trustworthy index needs to be calculated with weight at default distribution and also needs to be calculated with 60% weight over security concepts compared to the other weight concepts.	Met
High Availability is required to be 90% or more.	Met
Optional Requirements	
Response time < 200 ms.	Met
SAML based web service.	Met
Services built on standard web service frameworks.	Met

Table 6. Scenario #2 – Registration Service 1 Requirements Satisfaction Status

The above scenario results elicit that the total trustworthiness is a multidimensional concept. It includes all aspects of a web service in bringing out the selection process more transparent to the user while choosing a proper web service for the given requirements. During the equal weight distribution the Service 1 was chosen as a more suitable service.

Equal weight distribution treats trustworthiness as a multidimensional concept as all concepts are valued equally. With a user preferred distribution which gave higher weight for security, Service 1 was again selected as the suitable service. The process of running prototype with equal distribution and user preferred distribution provides confidence with users' selection of a service using the trustworthiness index. For scenario #2 requirements, Service 1 was selected for both equal distribution and for user preferred distribution, thus giving more assurance to the user.

6.4.3 Comparison of Registration Services for Scenario #3

For scenario #3 requirements, we need to apply 60% weight for precision and availability concept. Rest of the concepts weight was evenly distributed to 10%, so that, combined total weight is 100%. Hence each web service was invoked one more time with the changed weight distribution based on the weight requirement as given in the Appendices H to K with Scenario #3 columns:

- Security: 10%
- Standards: 10%
- Precision & Availability: 60%
- Authenticity:10%
- Reliability: 10%

Web service URLs	Security Group Concept Value	Standards Group Concept Value	Precision and Availability Group Concept Value	Authenticity Group Concept Value	Reliability Group Concept Value	Confidence level	Trustworthiness index value
Registration – Service 1	9.17	2	6.25	6	8.00	**91%**	**5.70**
Registration – Service 2	0.83	2	9.50	5	9.50	**85%**	**6.32**
Registration – Service 3	0.83	0	5.75	3	3.83	**82%**	**3.46**
Registration – Service 4	0.83	2	8.75	3	9.17	**85%**	**5.74**

Table 7. Trustworthiness index values for Scenario #3 with user distribution

Table 7 exhibits condensed concept group values with the calculated trustworthiness index and the confidence levels for scenario #3 requirements. Based on the above test results the web service **Registration – Service 2** was found more trustworthy compared to the other web services. From table 7, it can be noted that Registration – Service 2 meets 6 out of 7 requirements listed for scenario #3. Table 8 provides status on the requirements that are met and not met. The service response time was observed as 76 ms, which is less than 500 ms. The service provider is from USA along with legal requirements. The availability of the service has been found as 100% which satisfies the availability requirement. It also noticed that the service does not use web service basic framework standards.

A comparison of scenario #2 and #3 shows that changes in business requirements could change which service can be considered more trustworthy. It demonstrates that a web service that has been identified as a suitable web service for one department's requirement in an organization may not be the suitable service for a different department's requirement in the same organization.

Requirements	Status
Mandatory Requirements	
The service response time needs to be at an accepted level < 500 ms.	Met
The provider needs to be from inside the country USA according to the HIPPA regulations.	Met
The provider should not be listed in the restricted providers list according to the business legal constraints.	Met
Trustworthy index needs to be calculated with 60% weight over precision and availability concepts compared to the other concepts.	Met
The service needs to be highly available.	Met
Reliability of the service availability is needed over consecutive invocations.	Met
Optional Requirements	
Services built on standard web service frameworks.	Not met

Table 8. Scenario #3 – Registration Service 2 Requirements Satisfaction Status

6.5 Evaluation Conclusion

From the acquired test results, it can be observed that the total trustworthiness is a multidimensional concept. Trustworthiness of a web service is not based on single concept like security, availability, service-level agreements, or other functional or non-functional aspects. Rather, it is based on variety of concepts as identified in the conceptual model presented in the chapter 3. Data collection of concept values for services identified for three evaluation scenarios demonstrates that the existence of concept values within a given service can be verified and collected methodically. We have exhibited how concept values collected can be used to calculate the trustworthiness index for a service. Thus, we achieved the first evaluation objective by demonstrating that trustworthiness of a web service is a multi-dimensional concept whose values can be collected to calculate trustworthiness index value.

We have also exhibited how trustworthiness index values can be meaningfully compared to select a service for a given requirement. Through three evaluation scenarios, we have demonstrated how each potential service can be compared based on stated business requirements. We also demonstrate how trustworthiness index values can be used for selecting the most trustworthy web service for given requirements. We also demonstrated the importance of calculating the trustworthiness index with and without concept value weight distribution based on business requirement and user preferences. Evaluation scenario results show that a web service that has been identified as trustworthy service for a given requirement is not necessarily the most trustworthy service another similar requirement. Hence, trustworthiness mechanisms should provide for selection of suitable web services based on user preference for a specific requirement, rather than treating each concept value on equal weights.

Through the three evaluation scenarios, we have shown that trustworthiness is multidimensional concept and outputs generated by the prototype tool can be meaningfully interpreted to select a suitable web service based on the user preferences and constraints of the requirement. Thus, we have demonstrated usefulness of the conceptual model and the prototype tool that implements the trustworthiness mechanism. Table 9 provides summarized view of the scenario based evaluation.

Scenario and Concept Weight Distribution	Selected Service	Most Influential Concepts	Confidence Level	Trustworthiness Index
Scenario#1 with equal distribution	Weather – Service 6	Precision and Availability Group (9.25) and Reliability Group (9.17)	74	3.50
Scenario#1 with user distribution	Weather – Service 1	Precision and Availability Group (9.25) and Standards Group (8.00)	68	4.43
Scenario#2 with equal distribution	Registration – Service 1	Security Group (9.17) and Reliability Group (8.50)	91	5.81
Scenario#2 with user distribution	Registration – Service 1	Security Group (9.17) and Reliability Group (8.17)	91	7.05
Scenario#3 with user distribution	Registration – Service 2	Precision and Availability Group (9.50) and Reliability Group (9.50)	85	6.32
		Demonstrates first objective – **Trustworthiness is multidimensional concept.**	Demonstrates second objective – **Trustworthiness index value can be meaningfully interpreted.**	

Table 9. Summary of evaluation objectives and scenario analysis

Chapter 7

CONCLUSION

7.1 Concluding Remarks

This thesis demonstrates that the total trustworthiness is a multi-dimensional concept. This work makes several contributions to the field. A conceptual model for quantifying and measuring the total trustworthiness of a web service utilizing multiple facets has been developed. Also a simple proof-of-concept online tool has been built to measure the various concepts that have been identified by the conceptual model to quantify and calculate the trustworthiness index values for web services. The online tool can help the end users to select the most suitable service for their business requirements contexts. Finally the utility of the tool was demonstrated by conducting scenario-based evaluation. Industries can leverage the tool and the conceptual model developed in this thesis to measure the trustworthiness of a service while choosing a suitable and/or analyzing the feasibility of a web service for their business requirements.

7.2 Future work

Future work would involve more extensive analysis and addition of new concepts that are involved in deciding the comprehensive trustworthiness of a web service. As it is well known that information technology is growing in leaps and bounds, new technologies are

produced on a daily basis that would change the outlook of total trustworthiness of a web service going forward. The conceptual model has to evolve along with the changes in the industry. The tool can be modified to accommodate the newly emerging concepts and can be optimized for a better performance and better user interface with a wide-ranging solution in mind. Every year a set of standards come into play and hence a close watch needs to be applied to cope up with the changing standards as well.

REFERENCES

Alonso, G., Casati, F., Kuno, H., & Machiraju, V. (2004). *Web Services: Concepts, Architectures and Applications*. Berlin: Springer-Verlag.

Banks, T. (2006). Web Services Resource Framework (WSRF) – Primer Retrieved July 1, 2014, from http://docs.oasis-open.org/wsrf/wsrf-primer-1.2-primer-cd-02.pdf

Christensen, E., Curbera, F., Meredith, G., & Weerawarana, S. (2001, 15 March). Web Service Description Lanaguage (WSDL) Retrieved June 25, 2014, from http://www.w3.org/TR/wsdl

Gudgin, M., Hadley, M., Mendelsohn, N., Moreau, J.-J., Nielsen, H. F., Karmarkar, A., & Lafon, Y. (2007, April 27). SOAP Version 1.2 Part 1: Messaging Framework Retrieved June 25, 2014, from http://www.w3.org/TR/soap12-part1/

Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., & Savio, D. (2010). Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services. *IEEE Transactions on Services Computing, 3*(3), 223-235. doi: 10.1109/tsc.2010.3

He, H., Haas, H., & Orchard, D. (2004). Web Services Architecture Usage Scenarios Retrieved June 25, 2014, from http://www.w3.org/TR/ws-arch-scenarios/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75-105.

Infonetica. (2006). Trustworthiness of WebSites Retrieved April 24, 2013, from http://www.infoneticainc.com/~ideas/articles/trustworthiness.pdf

Iwasa, K., Durand, J., Rutt, T., Peel, M., Kunisetty, S., & Bunting, D. (2004, 24 August). Web Services Reliability (WS-Reliability) Retrieved June 25, 2014, from http://docs.oasis-open.org/wsrm/2004/06/WS-Reliability-CD1.086.pdf

Jin, K., Zhu, J., & Fan, G. (2011, 9-11 Oct. 2011). *MET: Multi-party E-Commerce Transaction Model.* Paper presented at the IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, Boston, Massachusetts, USA.

Kazman, R., Abowd, G., Bass, L., & Clements, P. (1996). Scenario-based analysis of software architecture. *IEEE Software, 13*(6), 47-55. doi: 10.1109/52.542294

Lawrence, K., Kaler, C., Nadalin, A., Goodner, M., Gudgin, M., Barbir, A., & Granqvist, H. (2007). Web Services Security Policy Retrieved June 25, 2014, from http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html

Mehdi, M., Bouguila, N., & Bentahar, J. (2012, 24-29 June 2012). *Trustworthy Web Service Selection Using Probabilistic Models.* Paper presented at the IEEE International Conference on Web Services (ICWS), Honolulu, HI.

Microsoft-XMLWS. (2014). Anatomy of an XML Web Service Lifetime Retrieved June 25, 2014, from http://msdn.microsoft.com/en-us/library/x05s00wz(v=vs.71).aspx

Murley, D. (2006, August). Evaluating and Rating Websites and Other Information Resources Retrieved June 25, 2014, from http://www.law.siu.edu/lawlib/guides/eval.pdf

Parnas, D. L., Schouwen, A. J. v., & Kwan, S. P. (1990). Evaluation of safety-critical software. *Communications of the ACM, 33*(6), 636-648. doi: 10.1145/78973.78974

Pasternack, J., & Roth, D. (2010). *Comprehensive Trust Metrics for Information Networks.* Paper presented at the Army Science Conference (ASC), Orlando, Florida.

Sun, Y., He, S., & Leu, J. Y. (2007). Syndicating Web Services: A QoS and user-driven approach. *Decision Support Systems, 43*(1), 243-255. doi: http://dx.doi.org/10.1016/j.dss.2006.09.011

Toma, C. L. (2010). *Perceptions of trustworthiness online: the role of visual and textual information.* Paper presented at the ACM conference on Computer Supported Cooperative Work, Savannah, Georgia, USA.

Turner, D., Monzillo, R., Kaler, C., Nadalin, A., Hallam-Baker, P., & Milono, C. (2012). Web Services Security Kerberos Token Profile Retrieved May 18, 2012, from http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-KerberosTokenProfile-v1.1.1.html

Turner, D., Nadalin, A., Kaler, C., Monzillo, R., Hallam-Baker, P., & Milono, C. (2012a, May 18). Web Services Security X.509 Certificate Token Profile Retrieved June 25, 2014, from http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-v1.1.1.html

Turner, D., Nadalin, A., Kaler, C., Monzillo, R., Hallam-Baker, P., & Milono, C. (2012b). Web Services Security: SOAP Message Security Retrieved June 26, 2014, from http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.html

Umapathy, K., & Purao, S. (2010). Systems Integration and Web Services. *Computer, 43*(11), 91-94.

Wang, L., Liu, F., Li, G., Gu, L., Zhang, L., & Xie, B. (2009). Assisting Trustworthiness Based Web Services Selection Using the Fidelity of Websites. In L. Baresi, C.-H. Chi & J. Suzuki (Eds.), *Service-Oriented Computing* (Vol. 5900, pp. 429-436). Berlin Heidelberg: Springer

WS-Security. (2006, 28 November). Web Services Security Retrieved June 25, 2014, from http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Xiong, K., & Perros, H. (2008). Trustworthy Web services provisioning for differentiated customer services. *Telecommunication Systems, 39*(3-4), 171-185. doi: 10.1007/s11235-008-9126-9

Zhang, D. (2004). Web services composition for process management in e-Business. *Journal of Computer Information Systems, 45*(2), 83-91.

Zhang, J. (2005). Trustworthy Web services: actions for now. *IT Professional, 7*(1), 32-36.

Zhao, W., Sun, H., Huang, Z., Liu, X., & Kang, X. (2010). A User-Oriented Approach to Assessing Web Service Trustworthiness. In B. Xie, J. Branke, S. M. Sadjadi, D. Zhang & X. Zhou (Eds.), *Autonomic and Trusted Computing* (Vol. 6407, pp. 195-207). Berlin Heidelberg: Springer

APPENDIX A: CONCEPTS AND COLLECTION SOURCES

Trustworthiness Concepts	Source from where concepts value will be obtained	Categorical Values
SSL Usage	From the web service URL	'0' or '1'
SAML Usage	From the web server redirect content	'0' or '1'
Virus and other security threats protection	Identifying the redirects to proxy servers from the web server redirect content.	'0' or '1'
X509 standard usage	From the web server traffic content	'0' or '1'
Longevity of the Provider	From the knowledge database that has been updated by the user input	1 (low) to 5 (high)
Reliability of the service in a specific range of time	From the experience database that has been entered by the user	1 (low) to 5 (high)
Reliability of the Message Delivery	From the test results of invoking the service and collecting the success and failure rates for the initial response.	1 (low) to 5 (high)
Percentage of Reliability	By invoking the web service URL	1 (low) to 5 (high)
Past experience with the Provider	From the experience database that has been maintained by the user based on the experiences	1 (low) to 5 (high)
Measurement of Dependability	From the values received by invoking the web service URL.	1 (low) to 5 (high)
Perception of the Provider	From the knowledge database that has been updated by the user input	1 (low) to 5 (high)
Measurement of Accuracy	From the values entered by the user. If the customer has the past experience of the service used then that information can be leveraged from the experience database.	1 (low) to 5 (high)
3rd party authentication	From the redirect content of the web service server	'0' or '1'
Source of Information	From the knowledge database that has been updated by the user input	1 (low) to 5 (high)
Government service	From the web service URL	1 (low) to 5 (high)
Reputed Major Organization	From the knowledge database that has been updated by the user input	1 (low) to 5 (high)
Service cost	From the information received from the web service provider	1 (low) to 5 (high)
Transaction	From the information received from the web	1 (low) to 5 (high)

Trustworthiness Concepts	Source from where concepts value will be obtained	Categorical Values
count based cost	service provider	
Usage cost for a specific period	From the information received from the web service provider	1 (low) to 5 (high)
Up to date service information	From the knowledge database that has been updated by the user input.	'0' or '1'
Latest date of Information Availability	From the knowledge database that has been updated by the user input.	'0' or '1'
Coverage for a credible period of length	From the experience database that has been entered by the user	'0' or '1'
Objectivity	From the knowledge database that has been updated by the user input	'0' or '1'
Error Rate	From the values received by invoking the web service URL	± 0% to 100%
Failure Rate	From the values received by invoking the web service URL	± 0% to 100%
Recovery Rate	From the values received by invoking the web service URL	± 0% to 100%
Provider Legality	From the knowledge database that has been updated by the user input	'0' or '1'
Country acceptability of the Provider	From the knowledge database that has been updated by the user input based on consumer-forums, technical journals and other similar related sources.	'0' or '1'
Status as Internationally accepted	From the knowledge database that has been updated by the user input based on consumer-forums, technical journals and other similar related sources.	'0' or '1'
Web service response Handling Capacity	From the values received by invoking the web service URL	± 0% to 100%
Web service response Capacity in a specific time range	From the values received by invoking the web service URL	1 (low) to 5 (high)
Web service response Processing Time	From the values received by invoking the web service URL	1 (low) to 5 (high)
OASIS Standard usage	From the WSDL of the web service	'0' or '1'

Trustworthiness Concepts	Source from where concepts value will be obtained	Categorical Values
Other accepted frame work standards usage	From the WSDL of the web service	'0' or '1'

APPENDIX B: WEATHER – SERVICE 1 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Security					
SSL Usage	'0' or '10'	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5
Average value for Security →			**0.83**		**0.83**
Standard					
SOAP1.2 usage	'0' or '10'	No	0	Yes	10
ebXML usage	'0' or '10'	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	Yes	10
WS-Security frame work standards usage	'0' or '10'	No	0	Yes	10
WCF framework usage	'0' or '10'	Yes	10	Yes	10
Average value for Standard→			**2**		**8**
Precision & Availability					
Availability of the Service	'0' or '10'	No	0	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	463ms	8	377ms	8
Document/RPC type	Document - 8 RPC -10 None -5	None	5	Document	8
SSL usage	Value '0' or '10'	No	10	No	10
Average value for Precision and Availability→			**5.75**		**9**
Authenticity					
Cert authentication	'0' or '10'	No	0	No	0
Government service	Value '20' or '0' count -2	No	0	No	0
Org type organization	'0' or '10'	No	0	No	0

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
3rd party authentication	'0' or '10'	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Perception of Authenticity from knowledgebase	'0' or '10'	3	6	3	6
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10
Average value for Authenticity →			**3.8**		**3.8**
Reliability					
Document/RPC type	Document - 10 RPC -8 None -5	None	5	Document	10
Success count/Attempted count rate	Value '20' or '0' count -2	4/9	8	5/10	10
Availability Response time variation	1 (low) to 10 (high)	168ms	8	344ms	7
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8
Average value for Reliability →			**5.83**		**6.83**
Calculated Trustworthy Index value →			**2.29**		**4.43**

APPENDIX C: WEATHER – SERVICE 2 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Security					
SSL Usage	'0' or '10'	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5
Average value for Security →			**0.83**		**0.83**
Standard					
SOAP1.2 usage	'0' or '10'	No	0	No	0
ebXML usage	'0' or '10'	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0
Average value for Standard→			**0**		**0**
Precision & Availability					
Availability of the Service	'0' or '10'	Yes	10	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	200 ms	10	220 ms	9
Document/RPC type	Document -8 RPC -10 None -5	RPC	10	RPC	10
SSL usage	Value '0' or '10'	No	10	No	10
Average value for Precision and Availability→			**10**		**9.75**
Authenticity					
Cert authentication	'0' or '10'	No	0	No	0
Government service	Value '20' or '0' count -2	Yes	20	Yes	20
Org type organization	'0' or '10'	No	0	No	0

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
3rd party authentication	'0' or '10'	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Perception of Authenticity from knowledgebase	'0' or '10'	3	6	3	6
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10
Average value for Authenticity →			**5.8**		**5.8**
Reliability					
Document/RPC type	Document -10 RPC -8 None -5	RPC	8	RPC	8
Success count/Attempted count rate	Value '20' or '0' count -2	100%	20	100%	20
Availability Response time variation	1 (low) to 10 (high)	173 ms	8	187 ms	8
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8
Average value for Reliability →			**8.33**		**8.33**
Calculated Trustworthy Index value →			**3.24**		**3.99**

APPENDIX D: WEATHER – SERVICE 3 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Security					
SSL Usage	'0' or '10'	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5
Average value for Security →			**0.83**		**0.83**
Standard					
SOAP1.2 usage	'0' or '10'	Yes	10	Yes	10
ebXML usage	'0' or '10'	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0
Average value for Standard→			**2**		**2**
Precision & Availability					
Availability of the Service	'0' or '10'	Yes	10	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	424 ms	8	445 ms	8
Document/RPC type	Document -8 RPC -10 None -5	Document	8	Document	8
SSL usage	Value '0' or '10'	No	10	No	10
Average value for Precision and Availability→			**9**		**9**
Authenticity					
Cert authentication	'0' or '10'	No	0	No	0
Government service	Value '20' or '0' count -2	No	0	No	0

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Org type organization	'0' or '10'	No	0	No	0
3rd party authentication	'0' or '10'	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Perception of Authenticity from knowledgebase	'0' or '10'	3	6	3	6
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10
Average value for Authenticity →			**3.8**		**3.8**
Reliability					
Document/RPC type	Document -10 RPC -8 None -5	Document	10	Document	10
Success count/Attempted count rate	Value '20' or '0' count -2	100%	20	100%	20
Availability Response time variation	1 (low) to 10 (high)	279 ms	7	195 ms	8
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8
Average value for Reliability →			**8.5**		**8.67**
Calculated Trustworthy Index value →			**3.14**		**3.83**

APPENDIX E: WEATHER – SERVICE 4 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Security					
SSL Usage	'0' or '10'	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5
Average value for Security →			**0.83**		**0.83**
Standard					
SOAP1.2 usage	'0' or '10'	Yes	10	Yes	10
ebXML usage	'0' or '10'	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0
Average value for Standard→			**2**		**2**
Precision & Availability					
Availability of the Service	'0' or '10'	Yes	10	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	174 ms	10	191 ms	10
Document/RPC type	Document -8 RPC -10 None -5	Document	8	Document	8
SSL usage	Value '0' or '10'	No	10	No	10
Average value for Precision and Availability→			**9.5**		**9.5**
Authenticity					
Cert authentication	'0' or '10'	No	0	No	0
Government service	Value '20' or '0' count -2	No	0	No	0

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Org type organization	'0' or '10'	No	0	No	0
3rd party authentication	'0' or '10'	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Perception of Authenticity from knowledgebase	'0' or '10'	3	6	3	6
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10
Average value for Authenticity →			**3.8**		**3.8**
Reliability					
Document/RPC type	Document -10 RPC -8 None -5	Document	10	Document	10
Success count/Attempted count rate	Value '20' or '0' count -2	100%	20	100%	20
Availability Response time variation	1 (low) to 10 (high)	104 ms	8	159 ms	8
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	3	6	3	6
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8
Average value for Reliability →			**8.67**		**8.67**
Calculated Trustworthy Index value →			**3.22**		**3.96**

APPENDIX F: WEATHER – SERVICE 5 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Security					
SSL Usage	'0' or '10'	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5
Average value for Security →			**0.83**		**0.83**
Standard					
SOAP1.2 usage	'0' or '10'	Yes	10	Yes	10
ebXML usage	'0' or '10'	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0
Average value for Standard→			**2**		**2**
Precision & Availability					
Availability of the Service	'0' or '10'	Yes	10	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	471 ms	8	372 ms	8
Document/RPC type	Document -8 RPC -10 None -5	Document	8	Document	8
SSL usage	Value '0' or '10'	No	10	No	10
Average value for Precision and Availability→			**9**		**9**
Authenticity					
Cert authentication	'0' or '10'	No	0	No	0
Government service	Value '20' or '0' count -2	No	0	No	0

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Org type organization	'0' or '10'	No	0	No	0
3rd party authentication	'0' or '10'	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	2	4	2	4
Perception of Authenticity from knowledgebase	'0' or '10'	2	4	2	4
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	2	4	2	4
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10
Average value for Authenticity →			**3.2**		**3.2**
Reliability					
Document/RPC type	Document -10 RPC -8 None -5	Document	10	Document	10
Success count/Attempted count rate	Value '20' or '0' count -2	100%	20	100%	20
Availability Response time variation	1 (low) to 10 (high)	217 ms	7	250 ms	7
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	2	4	2	4
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8
Average value for Reliability →			**8.17**		**8.17**
Calculated Trustworthy Index value →			**2.55**		**3.15**

APPENDIX G: WEATHER – SERVICE 6 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Security					
SSL Usage	'0' or '10'	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5
Average value for Security →			**0.83**		**0.83**
Standard					
SOAP1.2 usage	'0' or '10'	No	0	No	0
ebXML usage	'0' or '10'	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0
Average value for Standard→			**0**		**0**
Precision & Availability					
Availability of the Service	'0' or '10'	Yes	10	No	0
Web service performance based on response Time	1 (low) to 10 (high)	207 ms	9	186 ms	10
Document/RPC type	Document -8 RPC -10 None -5	Document	8	None	5
SSL usage	Value '0' or '10'	No	10	No	10
Average value for Precision and Availability→			**9.25**		**6.25**
Authenticity					
Cert authentication	'0' or '10'	No	0	No	0
Government service	Value '20' or '0' count -2	No	0	No	0

Trustworthiness Concepts	Categorical Values	Scenario #1 Default Distribution		Scenario #1 User Preferred Distribution	
		Received value	Effective value	Received value	Effective value
Org type organization	'0' or '10'	No	0	No	0
3rd party authentication	'0' or '10'	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	4	8	4	8
Perception of Authenticity from knowledgebase	'0' or '10'	4	8	4	8
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	4	8	4	8
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10
Average value for Authenticity →			**4.4**		**4.4**
Reliability					
Document/RPC type	Document -10 RPC -8 None -5	Document	10	None	5
Success count/Attempted count rate	Value '20' or '0' count -2	100%	20	9/10	18
Availability Response time variation	1 (low) to 10 (high)	65 ms	9	186 ms	8
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	4	8	4	8
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8
Average value for Reliability →			**9.17**		**7.83**
Calculated Trustworthy Index value →			**3.5**		**3.17**

APPENDIX H: REGISTRATION – SERVICE 1 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
Security							
SSL Usage	'0' or '10'	Yes	10	Yes	10	Yes	10
SAML Usage	'0' or '10'	Yes	10	Yes	10	Yes	10
Usage of the proxy server detection	'0' or '10'	Yes	10	Yes	10	Yes	10
X509 standard usage	'0' or '10'	Yes	10	Yes	10	Yes	10
SOAP encoding	'0' or '10'	Yes	10	Yes	10	Yes	10
Mutual trust	'0' or '5'	No	5	No	5	No	5
Average value for Security →			**9.17**		**9.17**		**9.17**
Standard							
SOAP1.2 usage	'0' or '10'	No	0	No	0	No	0
ebXML usage	'0' or '10'	No	0	No	0	No	0
OASIS Standard usage	'0' or '10'	Yes	10	Yes	10	Yes	10
WS-Security frame work standards usage	'0' or '10'	No	0	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0	No	0
Average value for Standard→			**2**		**2**		**2**
Precision & Availability							
Availability of the Service	'0' or '10'	Yes	10	Yes	10	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	113 ms	10	155 ms	10	137 ms	10
Document/RPC type	Document -8 RPC -10 None -5	None	5	None	5	None	5
SSL usage	Value '0' or '10'	Yes	0	Yes	0	Yes	0
Average value for Precision and Availability→			**6.25**		**6.25**		**6.25**
Authenticity							
Cert authentication	'0' or '10'	None	0	None	0	None	0
Government service	Value '20' or '0' count -2	No	0	No	0	No	0
Org type organization	'0' or '10'	No	0	No	0	No	0
3rd party authentication	'0' or '10'	Yes	10	Yes	10	Yes	10
Reputation from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
Perception of Authenticity from knowledgebase	'0' or '10'	5	10	5	10	5	10
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10	Yes	10
Average value for Authenticity →			**6**		**6**		**6**
Reliability							
Document/RPC type	Document - 10 RPC -8 None -5	None	5	None	5	None	5
Success count/Attempted count rate	Value '20' or '0' count -2	90%	18	90%	18	10/11	18
Availability Response time variation	1 (low) to 10 (high)	17 ms	10	178 ms	8	235 ms	7
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8	Good	8
Average value for Reliability →			**8.5**		**8.17**		**8.0**
Calculated Trustworthy Index value →			**5.81**		**7.05**		**5.7**

APPENDIX I: REGISTRATION – SERVICE 2 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
Security							
SSL Usage	'0' or '10'	No	0	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5	No	5
Average value for Security →			**0.83**		**0.83**		**0.83**
Standard							
SOAP1.2 usage	'0' or '10'	Yes	10	Yes	10	Yes	10
ebXML usage	'0' or '10'	No	0	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0	No	0
Average value for Standard→			**2**		**2**		**2**
Precision & Availability							
Availability of the Service	'0' or '10'	Yes	10	Yes	10	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	82 ms	10	76 ms	10	76 ms	10
Document/RPC type	Document -8 RPC -10 None -5	Document	8	Document	8	Document	8
SSL usage	Value '0' or '10'	No	10	No	10	No	10
Average value for Precision and Availability→			**9.5**		**9.5**		**9.5**
Authenticity							
Cert authentication	'0' or '10'	No	0	No	0	No	0
Government service	Value '20' or '0' count - 2	No	0	No	0	No	0
Org type organization	'0' or '10'	No	0	No	0	No	0
3rd party authentication	'0' or '10'	No	0	No	0	No	0
Reputation from	2 (low) to 10	5	10	5	10	5	10

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
knowledgebase	(high)						
Perception of Authenticity from knowledgebase	'0' or '10'	5	10	5	10	5	10
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Legal acceptability of the Country of the Provider	'0' or '10'	USA	10	USA	10	USA	10
Legality of the provider	'0' or '10'	Yes	10	Yes	10	Yes	10
Average value for Authenticity →			**5**		**5**		**5**
Reliability							
Document/RPC type	Document - 10 RPC -8 None -5	Document	10	Document	10	Document	10
Success count/Attempted count rate	Value '20' or '0' count - 2	100%	20	100%	20	100%	20
Availability Response time variation	1 (low) to 10 (high)	178 ms	8	9 ms	10	53 ms	9
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8	Good	8
Average value for Reliability →			**9.33**		**9.67**		**9.5**
Calculated Trustworthy Index value →			**4.53**		**7.05**		**6.32**

APPENDIX J: REGISTRATION – SERVICE 3 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
Security							
SSL Usage	'0' or '10'	No	0	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5	No	5
Average value for Security →			**0.83**		**0.83**		**0.83**
Standard							
SOAP1.2 usage	'0' or '10'	No	0	No	0	No	0
ebXML usage	'0' or '10'	No	0	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0	No	0
Average value for Standard→			**0**		**0**		**0**
Precision & Availability							
Availability of the Service	'0' or '10'	No	0	No	0	No	0
Web service performance based on response Time	1 (low) to 10 (high)	754ms	5	659ms	7	419ms	8
Document/RPC type	Document -8 RPC -10 None -5	None	5	None	5	None	5
SSL usage	Value '0' or '10'	No	10	No	10	No	10
Average value for Precision and Availability→			**5**		**5.5**		**5.75**
Authenticity							
Cert authentication	'0' or '10'	No	0	No	0	No	0
Government service	Value '20' or '0' count -2	No	0	No	0	No	0
Org type organization	'0' or '10'	No	0	No	0	No	0
3rd party authentication	'0' or '10'	No	0	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
Perception of Authenticity from knowledgebase	'0' or '10'	5	10	5	10	5	10
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Legal acceptability of the Country of the Provider	'0' or '10'	Germany	0	Germany	0	Germany	0
Legality of the provider	'0' or '10'	No	0	No	0	No	0
Average value for Authenticity →			**3**		**3**		**3**
Reliability							
Document/RPC type	Document - 10 RPC -8 None -5	None	5	None	5	None	5
Success count/Attempted count rate	Value '20' or '0' count -2	0%	0	0%	0	0%	0
Availability Response time variation	1 (low) to 10 (high)	n/a	0	n/a	0	n/a	0
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8	Good	8
Average value for Reliability →			**3.83**		**3.83**		**3.83**
Calculated Trustworthy Index value →			**2.08**		**1.42**		**3.46**

APPENDIX K: REGISTRATION – SERVICE 4 DATA VALUES COLLECTED BY PROTOTYPE

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
Security							
SSL Usage	'0' or '10'	No	0	No	0	No	0
SAML Usage	'0' or '10'	No	0	No	0	No	0
Usage of the proxy server detection	'0' or '10'	No	0	No	0	No	0
X509 standard usage	'0' or '10'	No	0	No	0	No	0
SOAP encoding	'0' or '10'	No	0	No	0	No	0
Mutual trust	'0' or '5'	No	5	No	5	No	5
Average value for Security →			**0.83**		**0.83**		**0.83**
Standard							
SOAP1.2 usage	'0' or '10'	No	10	No	10	No	10
ebXML usage	'0' or '10'	No	0	No	0	No	0
OASIS Standard usage	'0' or '10'	No	0	No	0	No	0
WS-Security frame work standards usage	'0' or '10'	No	0	No	0	No	0
WCF framework usage	'0' or '10'	No	0	No	0	No	0
Average value for Standard→			**2**		**2**		**2**
Precision & Availability							
Availability of the Service	'0' or '10'	Yes	10	Yes	10	Yes	10
Web service performance based on response Time	1 (low) to 10 (high)	617ms	7	617ms	7	586ms	7
Document/RPC type	Document -8 RPC -10 None -5	Document	8	Document	8	Document	8
SSL usage	Value '0' or '10'	No	10	No	10	No	10
Average value for Precision and Availability→			**8.75**		**8.75**		**8.75**
Authenticity							
Cert authentication	'0' or '10'	No	0	No	0	No	0
Government service	Value '20' or '0' count -2	No	0	No	0	No	0
Org type organization	'0' or '10'	No	0	No	0	No	0
3rd party authentication	'0' or '10'	No	0	No	0	No	0
Reputation from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10

Trustworthiness Concepts	Categorical Values	Scenario #2 Default even Distribution		Scenario #2 User Preferred Distribution		Scenario #3 User Preferred Distribution	
		Received Value	Effective Value	Received Value	Effective Value	Received Value	Effective Value
Perception of Authenticity from knowledgebase	'0' or '10'	5	10	5	10	5	10
Authenticity of source of information from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Legal acceptability of the Country of the Provider	'0' or '10'	Sweden	0	Sweden	0	Sweden	0
Legality of the provider	'0' or '10'	No	0	No	0	No	0
Average value for Authenticity →			**3**		**3**		**3**
Reliability							
Document/RPC type	Document - 10 RPC -8 None -5	Document	10	Document	10	Document	10
Success count/Attempted count rate	Value '20' or '0' count -2	100%	20	100%	20	100%	20
Availability Response time variation	1 (low) to 10 (high)	130 ms	8	359 ms	7	315 ms	7
Longevity of the Provider from knowledgebase	2 (low) to 10 (high)	5	10	5	10	5	10
Reliability experienced	2 (low) to 10 (high)	Good	8	Good	8	Good	8
Average value for Reliability →			**9.33**		**9.17**		**9.17**
Calculated Trustworthy Index value →			**4.06**		**2.37**		**5.74**

VITA

Britto N. Arockiasamy has a Bachelor's degree in Electrical and Electronics Engineering and around 30 years of industrial experience. He also holds a diploma in Business Administration. He is certified in multiple technologies from key IT companies like IBM, Microsoft, and Oracle. He has worked in various business domains including service, manufacturing, financial, sales network, and healthcare. His experience spans many multinational major companies and several turnkey projects; he has produced several state-of-the-art products as well. For the past 13 years, he has been working at a well-known healthcare company in Florida. He is a Senior Administrator in WebSphere application domain. His current passion is to explore the latest Government regulations applicable to the healthcare industry. Currently, he lives in Jacksonville, Florida.