ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 8, No. 3, 2013, *pp*.183-208

Design and Implementation of RESTful Non-repudiation Services

Saman Barakat
Department of Computer Sciences, University of Zakho,
Duhok, Kurdistan-Region, Iraq
saman.barakat@gmail.com

(*Received October 30, 2012, accepted April 4, 2013*)

Abstract. Security issues can be a barrier to make successful online businesses because the Internet can make critical information vulnerable [1, 2]. Non-repudiation is a security feature that is related to integrity and authenticity [3]. Providing non-repudiation for online communication is a key factor to achieve a successful electronic business [2]. Non-repudiation should ensure that each involvement in an online interaction cannot be denied. Besides, non-repudiation, fairness between the parties also plays an important role to achieve successful electronic businesses. One solution used to achieve fair non-repudiation services is by using a trusted third party (TTP) that implements fair non-repudiation protocols [4]. This project uses work that has been done by Cook et al in 2006 [5] as a starting point, which was a non-repudiation service project that uses SOAP web service technology. However, this project aims to implement non-repudiation services using Representational State Transfer (REST) architecture style principles in order to obtain significant advantages that REST technology provides such as scalability and simplicity.

Keywords: *Non-repudiation services, Non-repudiation protocols, Fair exchange protocols, Resful web services, REST.*.

1. Introduction

The Internet has become one of the major ways of conducting business. It makes accessing new and larger business easier. It also enables integration between different businesses and services using different types of programming middleware and web services easier [6]. Web services have been used to implement and integrate web applications. Web applications might be e-commerce business, banking service, e-voting, electronic trading, digital contract exchanging, and so on [3]. As a result, many businesses have migrated to the Internet taking advantage of its efficiency and low cost [2].

Security concerns can be an impediment to achieve successful online business since online transactions across insecure environment such as the Internet can make valuable information vulnerable [1, 2]. Consequently, security issues such as confidentiality, integrity, and authenticity have been studied in order to establish successful online businesses [3].

An aspect related to integrity and authenticity is non-repudiation [3]. Providing non-repudiation for online communication is a key factor in building a successful electronic business [2]. Non-repudiation should ensure that each involvement in an online interaction cannot be denied. For instance, if Alice and Bob are two parties that want to make an online transaction or exchange an electronic document, neither Alice nor Bob can deny their involvement in the exchange. Therefore, the non-repudiation of origin should be generated for the receiver and the non-repudiation of the receipt should be generated for the originator or sender [3].

In addition to non-repudiation, fairness between the parties also plays an important role in establishing successful electronic businesses. Fairness between participants within online businesses means that each online transaction between participants must be fair at the end of the transaction under any circumstances. For example, if Alice and Bob have been involved in an electronic transaction either both obtain what they expect or neither of them gains any advantage over the other.

One possible solution for non-repudiation and fairness issues is to use non-repudiation services. Non-repudiation services provide electronic evidence such as digital signatures entitled to all parties involved in online transactions [2]. Non-repudiation services implement fair non-repudiation protocols to guarantee both non-repudiation for the actions and fairness for each party involved in a particular transaction [3]. The

accountability of participating in a transaction can be guaranteed by using the two types of non-repudiation evidences which are non-repudiation of origin (NRO) and non-repudiation of receipt (NRR) [1]. The NRO is digital evidence generated by the originator and entitled to the recipient; while the NRR is digital evidence generated by the recipient and entitled to the originator.

One approach used to achieve fair non-repudiation services is by using a trusted third party (TTP) that implements fair non-repudiation protocols [4]. The trusted third parties have three main types; inline TTP, online TTP and offline TTP [2, 3]. These types of TTPs will be discussed in details in section 2.

This project uses work that has been done by Cook et al in 2006 [5] as a starting point, which was a non-repudiation service project that uses soap web service technology. However, this project aims to implement a non-repudiation service using Representational State Transfer (REST) architecture style principles in order to obtain significant advantages that REST technology provides such as scalability and simplicity.

Representational State Transfer (REST) is an architecture style for distributed web applications introduced in 2000 by Roy Fielding in his doctoral dissertation [10]. REST architecture style deals with data on the web service as resources and uses Uniform Resource Identifiers (URIs) to access these resources which is a unique identifier for each resource on the web [11-13]. The REST architectural style introduces several roles and constrains for distributed web applications.

The most significant benefit of designing the system as a RESTful web service is scalability. By applying REST constraints, the system will be highly scalable. First, by decoupling the client side concerns from server side concern, the developers do not need to worry about the server implementation only they need to focus on the client side and this can help clients to integrate the system with their business quickly. Secondly, the scalability of the system increased by applying the hierarchy constraint [10]. In this case, the system can be scaled by adding intermediaries to the system in order to balance the load between machines on the network.

Another advantage of using a RESTful web service is simplicity. Clients' requests will be stateless [10]; therefore, the system does not require managing and maintaining request state across multiple client requests. Moreover, request messages are fully descriptive and can be understood by intermediaries and the ultimate service. REST will be discussed in depth in section 2.

The aim of this project is to design and implement RESTful Non-Repudiation Services. It will implement three types of fair exchange protocols; inline, online and offline protocol. The interactions are between only two clients; Alice and Bob. Therefore, in order to achieve this aim, the project is divided into several objectives as follows:

1. Implement Inline Protocol: The first objective is to design the project using inline TTP protocol [2, 3, 7] for two clients Alice and Bob, in order to understand the basic functionality of Non-Repudiation Services and the interactions between clients.

2. Implement Online and Offline Protocols: The second objective is to implement both online TTP and offline TTP protocols [2, 3]. The main reason of implementing online and offline protocol is to reduce trusted third party's responsibility and move it to clients in which clients will do verification of signatures as well as storing information. The other reason of implementing online and offline protocol is to show the scalability of the Non-Repudiation
Services to adapt to different protocols.

3. Using Proxies: The next objective is to use proxies in the system [14-16]. The main reason of using proxies is to execute non-repudiation protocols instead of clients. In addition, the proxy will keep clients away from implementation details such as signing, encryption and decryption [5]. The other advantage of using proxies is to provide more security in the system by using SSL within insecure communications.

4. Testing and Evaluating the System: The final objective to complete the project is to provide testing and evaluation of the project. Testing section is necessary in order to show that every method is working properly. The evaluation is to evaluate the overall project and show whether the project has achieved its main aim or not.

By achieving the aim and objectives, the project will provide clients the flexibility to choose between different types of non-repudiation protocols. In addition, the project will provide REST properties such as scalability and simplicity.