Biomed Tech 2012; 57 (Suppl. 1) © 2012 by Walter de Gruyter · Berlin · Boston. DOI 10.1515/bmt-2012-4412

Service Oriented Architecture Based Web Application Model for Collaborative Biomedical Signal Analysis

Mufti Mahmud [1], M. Mostafizur Rahman [2], Davide Travalin [3], Pawel Raif [4], Amir Hussain [5]
[1] NeuroChip Laboratory, University of Padova, Padova, Italy, mahmud@dei.unipd.it; and Institute of Information Technology, Jahangirnagar University, Dhaka, Bangladesh, muftimahmud@juniv.edu (Corresponding author)
[2] NeuroChip Laboratory, University of Padova, Padova, Italy, rahman@dei.unipd.it
[3] St. Jude Medical Italia S.p.A, Palazzo Andromeda, 16/1, 20864 Agrate Brianza (MB), Italy, dtravalin@sjm.com
[4] Department of Electrical Engineering and Automation, ATH, University of Bielsko-Biala, 43-309 Bielsko-Biala, Poland, pawel.raif@gmail.com
[5] Centre for Cognitive & Computational Neuroscience, University of Stirling, Stirling FK9 4LA, UK, ahu@cs.stir.ac.uk

Abstract

The rapid growth in availability of new biomedical systems and devices capable of acquiring biosignals for disease diagnosis and health monitoring require rigorous processing. Biomedical research by nature depends on integrated problem solving software environment and often involves people located at different geographical positions. The reusability of different personalized tools are limited due to the complex architectural constrains and restricted interoperability among different devices mostly requiring individual tools. Thus, new computational environments are required to provide robust, user friendly, and scalable systems capable of interoperate seamlessly. This work proposes a service oriented architecture (SOA) based web application model for collaborative biosignal analysis and research to facilitate the seamless integration of various existing tools and different Health Information Systems.

1 Introduction

Biomedical signals (e.g., Electrocardiogram, ECG; Phonocardiogram, PCG; Electromyogram, EMG; and Electroencephalogram, EEG) analysis is practiced extensively in disease diagnosis and health monitoring. Mostly these analyses are performed through personalized software tools. To have a common and easily accessible platform unifying the analyses across different clinics and / or research laboratories is a big challenge. This is mainly due to the security and privacy issues related to personalized data, and the amount of experimental data that require sophisticated database management systems in addition to robust analysis algorithms [1, 2]. Non-trivial issues like interconnectivity and interoperability of components and tools, and seamless integration of Health Information Systems (HIS) need to be addressed. Moreover, handing complex biomedical data over the network requires new approaches [3]. To this goal, this paper presents a Service Oriented Architecture (SOA) based web application model to facilitate collaborative biosignal analysis.

The SOA is mainly a toolset for designing robust, reusable, and platform independent applications. Consisting of "services" residing on different machines to perform well-defined tasks are integrated over the internet. Through SOA the services are autonomous which are free to reside on physically separate hardware and usually can perform an independent task for a user. Also, the scalability and performances are expected to increase due to the fact that the SOA provides modular software design with improved adaptability to requirements and services reside in multiple machines and can harness power of resource parallelism.

2 The Model

2.1 Interplayers of the model

To achieve a unified collaborative biosignal analysis platform, our SOA based model emphasizes mainly three interplaying parts: services, users, and contributors (as seen in figure 1). Services are the core individual analysis codes, which upon request performs the predefined analyses. The users are any people who evoke the services at a given time. The contributors are personnel from different laboratories who are core of the development effort and are a special category of users with additional administrative privileges.

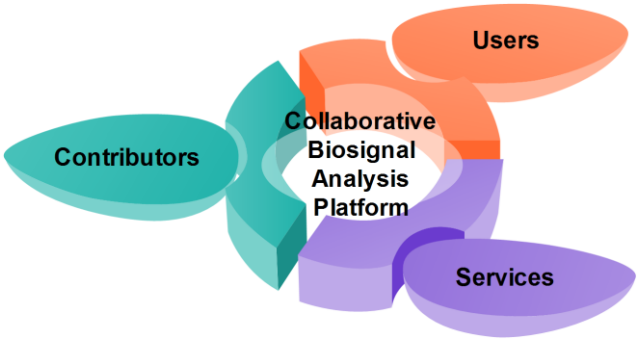

Figure 1 Different interplaying parts of the proposed collaborative biosignal analysis model.

2.2 Architecture

A client-server based three tier architecture is adhered for our model where the tiers are: user interface (client), ser-

vices including the connectivity and control strategies of the services itself (server), and signals (database). As in case of web applications security has been a big concern, the second tier of our model has been designed to contain the services as well as the authentication and access control strategies.

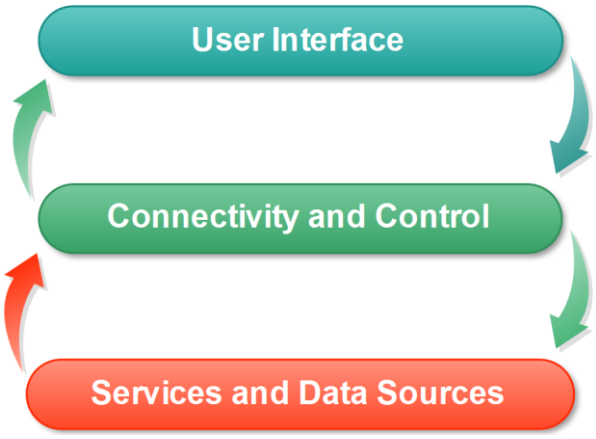

Figure 2 Client-server based three layered architecture of the proposed model.

Figure 2 shows different tiers of the model. The lowest tier termed as services and data sources contains the functions and components to allow the connectivity and control among various services and data. The authentication, access, and organization of services are performed in the middle tier (connectivity and control which otherwise has also been termed as infrastructure). This includes different workflow management, service communication and casting, user administration, resource allocation, and data handling.
In the following design section the system design including the security issues has been discussed.

2.3 Design

One of the major challenges in designing collaborative biomedical platform is tackling the interoperability among the various distributed tools and analysis resources. The other major concern is the secure and efficient access of the available data and resources. No organization would like to have their data flying on the internet without having proper access strategies. Thus, novel, efficient, and secure environment is required which will protect the system from unauthorized access of sensitive health information and proprietary data. Traditionally, in case of collaborative projects databases and analysis tools are hosted at one of the institutions participating in the project. This approach though reduces the security and interoperability issues, yet possesses restrictions in scaling with the increase of collaborators. Also, this approach shows inefficiency in rapid and dynamic creation, and management of shared resources [4].

To achieve a stable, reliable, secure and robust distributed framework, our system is based on user authentication, access control and trust management. Figure 3 depicts the basic design of the system. The users are divided into two distinct categories based on their roles and accordingly the access control policies are set. The first category contains the local users who are mainly the contributors to the distributed services and the second category has the remote users who just use the deployed services for the analysis purpose. The first category is managed using a double authentication process with local authentication service to confirm their role in addition to the usual certificate based authentication. As the second category only evokes the services, it is thought to be sufficient to have a single level of authentication based on their credentials.
The model uses XML for exchanging messages and SOAP for communicating over HTTP. However, the model should be able to tackle security threats for this loosely coupled architecture, service discovery, access control, confidentiality, integrity, privacy, and trust management. While evoking a service from web-based portals many sensitive information are integrated and sent with the request. This makes the access control between portal and Web Service an important issue. SAML (Security Assertion Markup Language) and XACML (eXtensible Access Control Markup Language) developed by OASIS (Organization for the Advancement of Structured Information Standards) have been used to make the model secure [5-8]. SAML and XACML are used in the system for access control. SAML is an XML-based framework used for exchanging authentication and authorization data; on the other hand XACML defines XML files which contain access control policy and the control decision request/response. Due to the fact that SAML has several benefits like - platform neutrality, loose coupling of directories, improved online experience for end user, reduced administrative costs for service providers and risk transference, it may very well be applied in a federated system for Web Single Sign-On, Attribute-Based Authorization, and Securing Web Services [7].
Figure 4 shows a possible solution to handle the identity information between the portal and web services. The Web service handlers are used on both sides to ensure transparent and secure transfer of identity credentials. The handlers create a SAML authentication assertion on the portal side which is attached along with the digital signature of the portal as a XML token to the SOAP header. Whereas, the handlers act as Policy Enforcement Point (PEP) on the Web service side where the received message is intercepted, the signature is verified and the required access control security information is translated to construct a XACML request. This request is then forwarded to the Policy Decision Point (PDP) to take an access decision and return it to the PEP where the XACML response is parsed and the decision on the request to access the web service is provided.

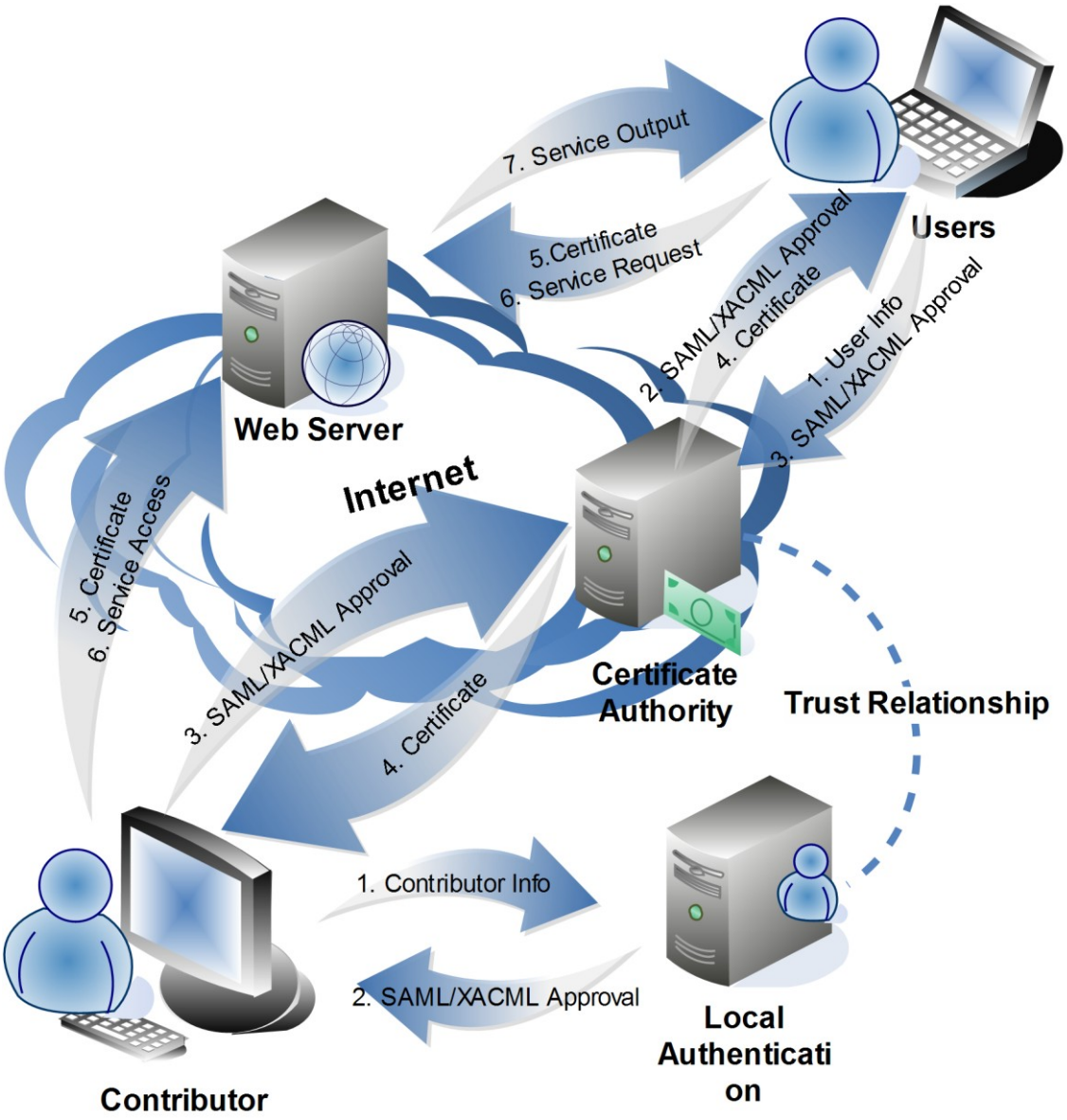

Figure 3 Authentication, access control, and web service evoking of the proposed system.

2.4 Significance

Development of secured infrastructures is critical to the success of large-scale, multi-institutional biomedical research efforts. Future biomedical research needs environments capable of seamlessly integrate data from different sources on-the-fly. Not only data sharing, the environment should be robust enough to address challenging issues like – researchers' collaboration with the option to protect their proprietary data, user friendly allowing users with minimal information technology skills to explore, navigate, and use scientific data and services provided by the environment. The emergence of SOA provides an opportunity to entangle resources that otherwise require more effort. Identification of core components of a model is very necessary to foster collaborative biomedical signal analysis through distributed infrastructure. This type of approach allows for a better representation of different roles taken by users in accordance to their interactions with the system as well as other users in the system. The presented model addresses certain aspects of the concerns on collaborative biomedical research, and may require fine tuning in some aspects based on the technology used in implementation. However, in our opinion, the model is expected to significantly contribute towards:

- Simpler and secure web application design and implementation for biomedical signals.
- Reusability and sharing of codes with adaptability to changing requirements.
- Facilitate easy development and deployment of data intensive applications.
- Secure and protected system.
- Empower researchers to share functionalities that they want to publish.
- Provide building blocks of extendible visual frameworks.

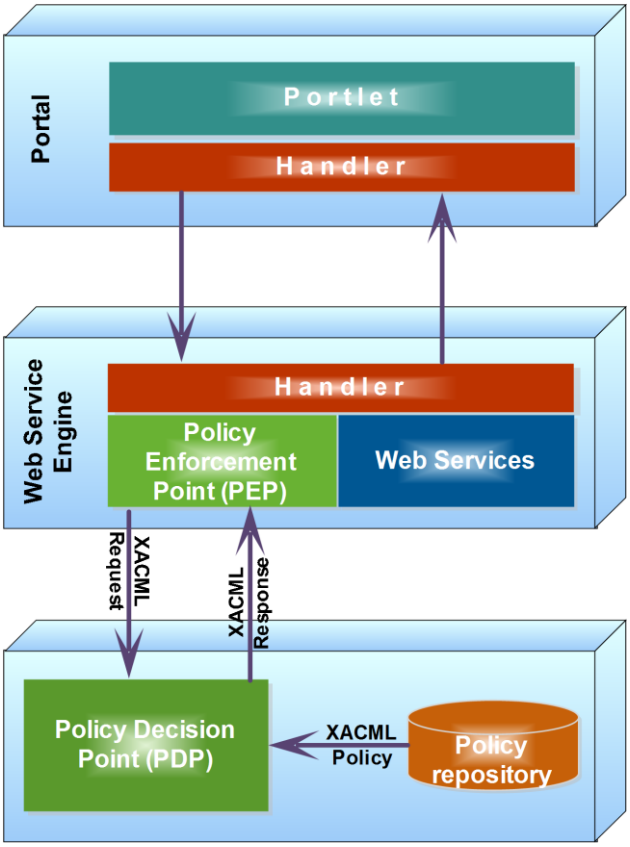

Figure 4 Access control request/response handling architecture using SAML / XACML based system.

3 Conclusion

The SOA facilitates interoperability and foster systems integration with flexibility and efficiency. This paper presents an early report on a SOA based collaborative biomedical signal analysis model where there are limitations which require further polishing and adjustments to be made to reach the final and completely secure system. Also, implementation specific changes may also be necessary. However, we believe, this type of secure SOA based web applications will encourage collaborative research and can bring the industry, health, and research centres even closer.

4 References

[1]. Buetow, K.H.: Cyberinfrastructure: Empowering a "third way" in Biomedical Research. Science, Vol 308, pp. 821-824, 2005.

[2]. Heredia, J.A., Estruch, A., Coltell, O., del Rey, D.P., de la Calle, G., Sánchez, J.P., Sanz, F.: Service Oriented Architecture for Biomedical Collaborative Research. In: Oliveira. J.L. et al. (Eds.): ISBMDA 2005, LNBI 3745, pp. 252–261, 2005.

[3]. Nandakarni, P.M., Miller, R.A.: Service-oriented Architecture in Medical Software: Promises and Perils. J Am Med Inform Assoc, Vol. 14, No. 2, pp. 244 – 246, 2007.

[4]. Langella, S., Hastings, S., Oster, S., Pan, T., Sharma, A., Permar, J., Ervin, D., Cambazoglu, B.B., Kurc, T., Saltz, J.: Sharing Data and Analytical Resources Securely in a Biomedical Research Grid Environment. J Am Med Inform Assoc, Vol. 15, No. 3, pp. 363-373, 2008

[5]. Candolin, C.: A Security Framework for Service Oriented Architectures. IEEE Military Communications Conference 2007 (MILCOM2007), 29-31 Oct. 2007, pp.1-6.

[6]. Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., Scavo, T.: Security Assertion Markup Language (SAML) V2.0 Technical Overview. Committee Draft 02, 25, March 2008. Available at: https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf; accessed on: 01 July 2012.

[7]. Yin, H., Zhou, J., Wu, H., Yu L.: A SAML/XACML Based Access Control between Portal and Web Services. The First International Symposium on Data, Privacy, and E-Commerce 2007 (ISDPE 2007), 1-3 Nov. 2007, pp. 356-360.

[8]. Singhal, A.: Web Services Security: Challenges and Techniques. Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07), 2007, pp.282.