Analysis of Security and Performance Service in Service Oriented Architecture (SOA) and Data Integration

Erick Fernando
Informatics engineering
STIKOM Dinamika Bangsa
Jambi, Indonesia
Erick.fernando_88@yahoo.com

Pandapotan Siagian
Computer System
STIKOM Dinamika Bangsa
Jambi, Indonesia
Siagian.p@gmail.com

Hetty Rohayani. AH
Computer System
STIKOM Dinamika Bangsa
Jambi, Indonesia
hetty_mna@yahoo.com

Derist Touriano
Informatics engineering
STIKOM Dinamika Bangsa
Jambi, Indonesia
Amuntai9@ovi.com

Abstract— Nowdays, the use of web services in the world of education is very much particular services and information provided in the form of the transaction until the payment - the payment and security in a system that is built in the form of a website. This system does not yet have a system that is integrated with each other and the security that is necessary to develop a system that leads towards it. Services provided requires an integrated system of all related system, the Service Oriented Architecture (SOA) to be used as an efficient solution for integrating distributed applications. In SOA-based environment that focuses on quality of service called WSARCH (Web Services Architecture). With this paper can then propose a system that uses a Service Oriented Architecture (SOA) with Web Services Architecture to resolve accurately than techniques that have a lower negative impact in terms of service performance and security.

Keywords: Service Oriented Architecture (SOA), Data Integration, Operational, Data, Web Services, Security, Performance , Encryption

1. INTRODUCTION

Service-Oriented Architecture (SOA) is growing an popular mechanism for achieving the interoperability between systems and for reusing the functionality at the business level and becoming the key concept of next generation systems [16]. In a business viewpoint, another advantage of SOA is that it is possible to obtain business flexibility by dividing processes as services at the fine-grained level [8].

SOA also can be considered as an IT strategy reorganizing enterprise applications into basic services which can be assembled, reused and collaborated so as to find a quick solution according to business demands.

The service-oriented has allowed applications that can be built through a network of collaboration which crosses the boundaries of universities and organizations to intergration data. The basic idea of Service-Oriented Architecture (SOA) has received significant attention and concern from the community of software design and development for a systems who will to use in universities and organizations. As a result of this attention, there has been a proliferation of many conflicting definitions of SOA. Thus, various types of service-oriented architectures have emerged, and among them, Web services have been the most commonly used ones in development systems.

This a web services enable interoperability of applications due to a series of standards that have been created based on standard XML (eXtensible Markup Language). However, this Web services do not have predefined clients and therefore must be adaptable to different contexts and are, somehow, a type of client/server system especially structured to make the best use of Web standards.

Web-Oriented Architecture (WOA) is recently appeared with The core concept of WOA is that an appropriate incorporation of the existing Web 2.0 technologies can make it easier to achieve what SOA have promised such as reusability, flexibility, and complexity reduction [7]. Specifically, the existing standards such as HTTP (Hyper Text Transfer Protocol), REST (Representational State Transfer), and URI (Uniform Resource Identifier), which have already been used successfully in the current Internet, are employed in WOA without defining additional standards.

In this paper, we propose a novel integrated model that can take the strong points of both SOA and WOA simultaneously. When designing a new service, it applies a SOA or WOA approach selectively depending on the characteristics of the service. For instance, it applies a SOA approach to design a

service that requires data transformations dan intergrated handled among multiple components.

On the contrary, it applies a WOA approach for a service that just presents data as it is or collectively. Also, we make use of a SOA approach for a service accessed by the external users, that necessitates a relevant security quality.

To validate the proposed model, we design a systems to development transaction service , one is based on our proposed model and the other is based on the legacy SOA model.

Then, we compare two systems using the function point analysis, which allows us to infer the complexity to actually develop the systems [11, 17]. Estimation results have shown that the function point of the integrated model based system is lower than that of the legacy SOA model based system, by designing some services using a WOA approach. In addition, we have observed that the integrated model can assure the quality of services, especial security and reliability, by applying a SOA approach when required. Finally, the experimental results have proven that the SOA and WOA based services can coexist seamlessly without any performance degradation and additional complexity.

2. SERVICE ORIENTED ARCHITECTURE (SOA)

Service Oriented Architecture (SOA) is a collection of services that communicate with each other to fulfill a particular business process. This paradigm passes data between service consumer and service provider either simply or complicatedly. SOA is a popular strategy to provide an integrated, flexible, and cost efficient (Web) Service-based enterprise. It promises interoperability, reusability, loose coupling, and protocol independency of services as core principles of SOA. Normally, this standard- based approach uses Web Services as building block to support particular business tasks. Web Services are published with Web Services Description Language (WSDL) interface and they use Simple Object Access Protocol (SOAP) as a communication protocol. Figure 1 shows the operation that each component can perform.

3. WEB SERVICES

According to, Web Services are loosely coupled computing services that can reduce the complexity of building business applications, save costs, and enable new business models. Web Services are application components that using open protocols to communicate and they are self-contained and self describing. Web Service can be discovered using UDDI and used by other applications. Extensible Markup Language (XML) is the basic for Web Services. Web Services can be able to publish the functions and data to the rest of the world. A Web Service is a software interface that describes a collection of operations that can be accessed over the network through standardized XML messaging. It uses protocols based on the XML language to describe an operation to execute or data to exchange with another Web Service.

4. SOA AND WEB SERVICES

Although much has been written about SOA and Web services, there still is some confusion be-tween these two terms among software developers. SOA is an architectural style, whereas Web services is a technology that can be used to implement SOAs. The Web services technology con-sists of several published standards, the most important ones being SOAP and WSDL. Other technologies may also be considered technologies for implementing SOA, such as CORBA. Al-though no current technologies entirely fulfill the vision and goals of SOA as defined by most authors, they are still referred to as SOA technologies. The relationship between SOA and SOA technologies is represented in Figure 1. Much of the technical information in this report is related to the Web services technology, because it is commonly used in today's SOA implementations.

5. WSARCH (WEB SERVICES ARCHITECTURE)

The WSARCH (Web Services Architecture) [7] is an architecture which allows accessing Web services using a combination of functional and non-functional aspects of Quality of Service (QoS). These QoS aspects aim at evaluating the performance of Web services in order to achieve QoS in a service-oriented architecture. These QoS attributes were mapped to the components participating in a service-oriented architecture that incorporates quality of service. The architecture provides the monitoring of service providers and the data obtained are used to locate the most appropriated service. A prototype for the WSARCH allows performance evaluation studies being conducted considering different components of the architecture, algorithms, protocols and standards. By now, we want include security attributes in this architecture involving all. the components (UDDI, Broker, clients and providers). The WSARCH and its components are presented in Figure 2.

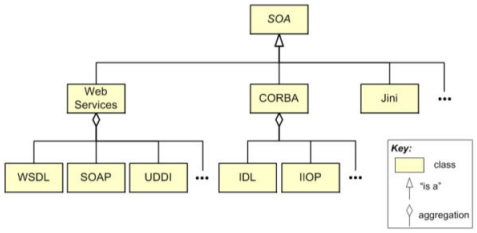

Figure 1: SOA and SOA Technologies

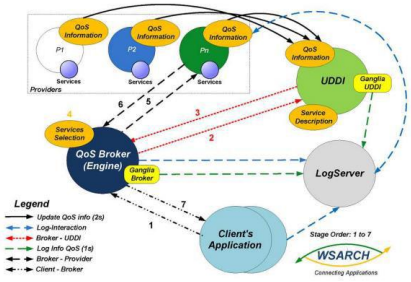

Figure 2. WSARCH

6. ACCESS CONTROL MODELS

So far various models have been proposed to solve accesses control problem that each one has its own advantages and disadvantages. In this section, some examples of such models are dealt with.

6.1. Identity-Based Access Control

Under this Model, permissions to access a resource is directly associated with a subject's identifier (e.g., a user name). Access to the resource is only granted when such an association exists. An example of IBAC is the use of Access Control Lists (ACL), commonly found in operation systems and network security services [7].The concept of an ACL is very simple: each resource on a system to which access should be controlled, referred to as an object, has its own associated list of mappings between the set of entities requesting access to the resource and the set of actions that each entity can take on the resource.

6.2. Role-Based Access Control

The RBAC model restricts access to a resource based on the business function or the role the subject is playing. The permissions to access a resource are then assigned to the appropriate role(s) rather than being directly assigned to subject identifiers [8]. When a user changes jobs, another user is allowed to take on that role. No ACL changes are needed. Of course, sometimes only a few of the user's rights change. In that case, a new role needs to be introduced. Often the rights associated with a role depend on which user is acting in that role. In that case, too, a new role needs to be introduced[9]. The RBAC reference model is defined in terms of four model components: Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, and Dynamic Separation of Duty Relations [10]. Although RBAC may take slightly different forms, a common representation as defined in [11] that is depicted in Fig. 3.

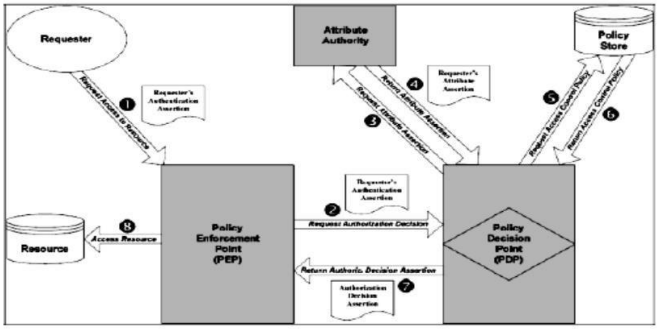

Figure 3: Role-based access control model

6.3. Attribute-Based Access Control

Policy Based Access Control (PBAC), which is called Attribute-Based Access Control (ABAC) in the US Defense Department jargon, extends RBAC to a more general set of properties [1]. Unlike IBAC and RBAC, the ABAC model [9] can define permissions based on just about any security relevant characteristics, known as attributes. For access control purposes, we are concerned with three types of attributes:

- Subject Attributes (S). Associated with a subject that defines the identity and characteristics of that subject.
- Resource Attributes (R). Associated with a resource, such as a web service, system function and or data.
- Environment Attributes (E). Describes the operational, technical, or situational environment or context in which the information access occurs.

ABAC clearly provides an advantage over traditional RBAC when extended into SOA environments, which can be extremely dynamic in nature. ABAC policy rules can be custom-defined with respect to semantic context and are significantly more flexible than RBAC for fine-grained alterations or adjustments to a subject's access profile. ABAC also is integrated seamlessly with XACML, which relies on policy defined attributes to make access control decisions. One additional benefit behind web service implementations of ABAC lies in the nature of the loose definition of subjects. Because ABAC provides the flexibility to associate policy rules with any actor, it can be extended to web service software agents as well [10].

One additional advantage of ABAC web service implementations is related to the nature of the loose definition of the subjects. Because ABAC provides the flexibility to associate policy rules with any actor, it can be extended to web service software agents as well. Figure 4 illustrates how an ABAC attribute authority (AA) can be integrated into a SAML framework. In this diagram, the AA generates attribute assertions containing all attributes necessary for an ABAC policy-based access control decision written in XACML. The PDP uses the attribute assertions, the authentication assertion, and the XACML policy to generate an authorization decision assertion [2].

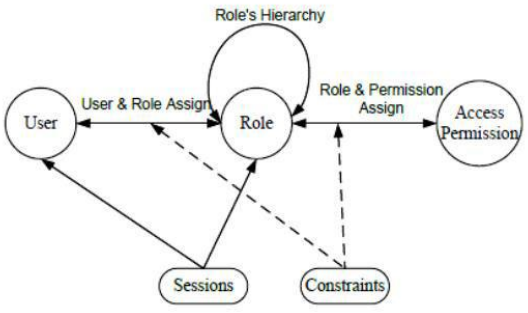

Figure 4: Use of SAML and XACML in implementing ABAC

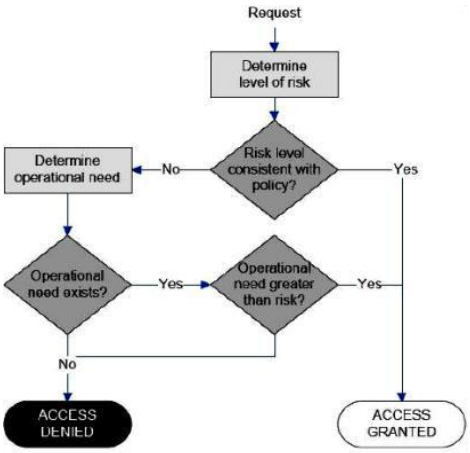

Figure 5: RAdAC Decision Tree

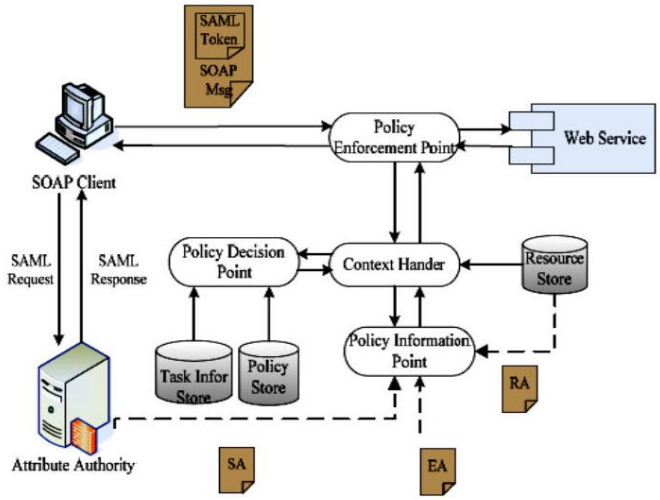

Figure 6: WABAC Access Control Framework

6.4. Risk Adaptive Access Control

Risk Adaptive Access Control (RAdAC) [13] is another variation access control method. Unlike IBAC, RBAC and ABAC, however, Radii makes access control decisions on the basis of a relative risk profile of the subject and not necessarily strictly on the basis of a predefined policy rule. Fig.3 illustrates the logical process governing RAdAC, which uses a combination of a measured level of risk the subject poses and an assessment of operational need as the primary attributes by which the subject's access rights are determined

6.5. WABAC Access Control Framework

The model of WABAC can realize fine-grained access control of cross-domain system; also it can manage subject's permissions dynamically. This model is suitable for access control of SOA, especially workflow based distributed computing system [6]. Fig.3 depicts the access control view of WABAC. The following will discuss the implementation of WABAC model and present an access control framework. With Web services implemented and the inclusion of their security policies, experiments and data collection were performed for this analysis. Thus, the performance of a Web service without security with other Web services using the WS-Security to add encryption and digital signatures in SOAP messages exchanged in communication have been compared. Furthermore, the results obtained with the WS-Security were compared with results obtained in an experiment where the Web service using the SSL security standard. As could be seen, despite having a relatively lower response time, SSL does not guarantee end-to-end security. Due to the inherent characteristics of the protocols that make up a service-oriented architecture, security becomes a key item. Thus, studies and performance evaluation of the inclusion of security in this environment are important, since such inclusion causes a considerable reduction in the performance of a service-oriented architecture. The study presented in this paper demonstrates that in addition to encryption factor, the number of concurrent clients requesting a particular service confirms the performance degradation.

7. CONCLUSION

In this paper, the necessity behind paying attention to accesses control in distributed environments such as services based on service–oriented architecture is dealt with. Software development, as a whole, is a complex process and on top of it, the requirements keep changing during the development phase. Software configuration management happens to be the most critical part as it necessitates doing considerable modification in the software design and code.

In the following, some samples of access control models in the architecture based on service are analyzed with model WABAC. Software development process provides a solution to such a changing environment. model WABAC use an incremental approach to develop high quality software within time, cost and other associated constraints through several iterations.

There are some prominent factors in software project management e.g., scope, cost, time and quality. Software engineering explores constructive and dynamic ways to manage the entire project lifecycle. Change in the requirements is a critical phase in any of the software development process and managing the requirement change is an open issue in the literature for many decades.

According to the analysis conducted, regarding that WABAC model has dynamic & higher flexible structure compared with the other models, it's concluded that this models more appropriate for dynamic environments such as service–oriented architecture environment and a system intergrated where use in transaction system .

REFERENCES

[1] A.H.Karp and J. Li, "Solving the Transitive Access Problem for Service-Oriented Architecture", IEEE International Conference on Availability, Reliability and Security, DOI 10.1109/ARES.2010.

[2] A. Singhal, T. Winograd and K. Scarfone, "Guide to Secure Web Services", National Institute of Standards and Technology Special Publication. .2007.

[3] D.F. Ferraiolo and D.R. Kuhn. "Role Based Access Control", 15th National Computer Security Conf.: 554-563. 1992.

[4] D.Smith,"Migration of legacy assets to service-oriented architecture environments," in Proceedings of the 29th International Conference on Software Engineering, 2007, pp. 174-175.

[5] E.Yuan and J. Tong. "Attributed Based Access Control (ABAC) for Web Services", IEEE International Conference on Web Services (ICWS'05). 2005.

[6] G. Zhang and J. Liu, "A Model of Workflow-Oriented Attributed Based Access Control" , I. J. Computer Network & Information Security,1, 47-53.2011.

[7] G. Thies and G. Vossen, "Web-oriented architectures: On the impact of web 2.0 on service-oriented architectures," in Proceedings of IEEE Asia-Pacific Services Computing Conference, 2008, pp. 1075-1082.

[8] I. Jorstad, S. Dustdar, and D. Thanh, "A service oriented architecture framework for collaborative services," in Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise, 2005, pp. 121- 125.

[9] J. C. Estrella, R. T. Toyohara, B. T. Kuehne, T. C. Tavares, R. C. Santana, M. J. Santana, and S. M. Bruschi. "A Performance Evaluation for a QoS-Aware Service Oriented Architecture". IEEE Congress on Services, pp. 260-267. 6th World Congress on Services, 2010.

[10] J. Tong, "Attribute Based Access Control: New Access Control Approach for Service- Oriented Architectures", Workshop on New Challenges for Access Control, Ottawa, Canada, Apr.2005.

[11] M. Beadley, "Function point counting practices manual, release 4.1," International Function Point Users Group (IFPUG), 1999.

[12] 12. Mohammad Mahdi Shafiei , Homayun Motameni and Javad Vahidi. "Analyzing Access control Models Dynamic Level and Security In Service–Oriented ArchitectureEnvironment" International Journal of Mechatronics, Electrical and Computer Technology Vol. 4(11), pp. 470-484, ISSN: 2305-0543, Apr. 2014

[13] P.C. Cheng, P.Rohatgi, and C. Keser, "Fuzzy MLS: Experiment on Quantified Risk- Adaptive Access Control", IEEE Symposium on Security and Privacy, PP. 222-230.2007.

[14] Phil Bianco, Rick Kotermanski and Paulo Merson. "Evaluating a Service-Oriented Architecture", Software Architecture Technology Initiative, Carnegie Mellon University, September 2007

[15] [8] R. S.Sandhu et al, "Role-Based Access Control Models. IEEE Computer", pp. 38-47. 1996.

[16] R Kuhn, American National Standards Institute. 2003.

[17] S. Balasubramaniam, G. Lewis, E. Morris, S. Simanta, and D. Smith, "Challenges for assuring quality of service in a service-oriented environment," in Proceedings of ICSE Workshop on Principles of Engineering Service Oriented Systems, 2009, pp. 103-106.

[18] T. Uemura, S. Kusumoto, and K. Inoue, "Function point analysis for design specifications based on the unified modeling language," Journal of Software Maintenance and Evaluation, Vol. 13, 2001, pp. 223-243.