Research Journal of Applied Sciences, Engineering and Technology 7(4): 673-695, 2014
DOI:10.19026/rjaset.7.304
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: January 21, 2013 Accepted: April 12, 2013 Published: January 27, 2014

Research Article

Novel Security Conscious Evaluation Criteria for Web Service Composition

[1]Homa Movahednejad, [1]Suhaimi Bin Ibrahim, [1, 2]Mahdi Sharifi, [1]Harihodin Bin Selamat,
[3]Arash Habibi Lashkari and [4]Sayed Gholam Hassan Tabatabaei
[1]Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM),
International Campus, Kuala Lumpur, Malaysia
[2]Department of Computer Engineering, Islamic Azad University, Najafabad Branch, Najafabad, Iran
[3]Department of Computer Engineering, Islamic Azad University, Rasht Branch, Rasht, Iran
[4]Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran

Abstract: This study aims to present a new mathematical based evaluation method for service composition with respects to security aspects. Web service composition as complex problem solver in service computing has become one of the recent challenging issues in today's web environment. It makes a new added value service through combination of available basic services to address the problem requirements. Despite the importance of service composition in service computing, security issues have not been addressed in this area. Considering the dazzling growth of number of service based transactions, making a secure composite service from candidate services with different security concerns is a demanding task. To deal with this challenge, different techniques have been employed which have direct impacts on secure service composition efficiency. Nonetheless, little work has been dedicated to deeply investigate those impacts on service composition outperformance. Therefore, the focus of this study is to evaluate the existing approaches based on their applied techniques and QoS aspects. A mathematical-based security-aware evaluation framework is proposed wherein Analytic Hierarchy Process (AHP), a multiple criteria decision making technique, is adopted. The proposed framework is tested on state-of-the-art approaches and the statistical analysis of the results presents the efficiency and correctness of the proposed work.

Keywords: Decision making, factor analysis, Quality of Service (QoS), security, web service composition

INTRODUCTION

In today's society, people face with such familiar concepts including e-government, e-business, e-science and e-health. This happened due to being key enablers who shift human life concepts from the physical to the virtual world. However, the question rises in this regard is: what are the key enablers? Web Services and Service Oriented Computing (SOC) are the most acceptable answers to this question. They make the new world where interconnected services have interaction and communication with sensors, embedded services and human users. Furthermore, the leading technology to realization this migration is undoubtedly a Web. Considering this, the introduction of Web Services has been a conspicuous progression and emerges the new concept called Service-oriented Web (Service Web) (Malik and Bouguettaya, 2009). In fact, enabling use of Web Services as independent components to organizing automated consumer-demand formed services without human intervention is the ultimate aim of Web Service technology (Brahim *et al.*, 2003). They strongly support the development of low-cost, rapid, massively, evolvable and interoperable distributed applications as major goal of SOC through defined XML-based standards such as Web Service Description Language (WSDL) and Simple Object Access Protocol (SOAP). Nonetheless, being unknown parties or the ones with unpredictable level of trustworthiness raise an argument in the global e-society members recently whether they can trust such type of services. It leads to claim that there is still a missing point to be optimistic to SOC. In this regard, one of the keywords that should be highlighted is "security" which can be viewed as an imperative component of internet-based interaction and service oriented environments. Compared to existing computer systems, providing security for service oriented environments is much more challenging. It happened, owing to the dynamic and adaptable nature of these environments where are often large scale and across domains (Bajaj *et al.*, 2006). Therefore, it can be claimed that Web services technology has not achieved

Corresponding Author: Homa Movahednejad, Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM), International Campus, Kuala Lumpur, Malaysia

its authentic performance and full potential yet. Furthermore, as IBM and Microsoft (2002) stated in their technical report security has been a key factor that holds companies back from adopting Web services. Particularly, this rationale grows in the computer society that Service revolution cannot eventuate unless security issues are resolved. As an instance, the success of Web service based marketplaces still faces critical impediment and lack consumers' trust whether or not they are secured. On the other hand, the real power of web services cannot be realized unless service composition is efficiently employed. Ramakrishnan and Tomkins (2007) mentioned service composition has brought about a change in the Web from being a "read-only" repository of Web pages to a Web of services that can be enriched and composed. In order to address security issue, the related parameters as subset of non-functional properties i.e., Quality of Service (QoS) are considered along with functional properties. The aim of involving QoS in service deployment process is enhancing and optimizing service oriented processes. Considering security issues in QoS can also help to more realizing this aim. Although providing security for single Web services is a demanding task, securing service composition process seems to be more challengeable. Regarding the former case, security requirements of users and Web services should be matched together while in the latter one security coordination and compatibility between services components have to be taken into account. That is, security requirements between service components, the composer and the user need to be considered. Concerning security in service composition is important from two viewpoints: service consumer and service provider. Regarding the former view, satisfying desired goals by reliable and reputable candidate service is so important since personal information may be transferred between involved parties. In contrast, it is very high importance to latter view i.e., service provider as composer to choose the closest and most reliable services for composition which have no negative impact on his reputation in the future. Recently, the bulk of research has been conducted on Web service security in both industry and academia whereas, few number of researches have been presented with regards to security in service composition. Nonetheless, there is a lack of appropriate review on investigating the role of security in Web services composition. This study aims to present a new mathematical based evaluation method for service composition with respects to security aspects (based on our prior work (Movahednejad *et al*., 2011)). In this regard, firstly a taxonomy of Web service composition solution which is an extension of our prior work (Movahednejad *et al*., 2011) is presented and existing approaches are classified in respective categories. In order to do that, rigorous review of existing literature has been conducted and most relevant and updated literature has been selected and analyzed. After that, evaluation criteria with respect to service composition, QoS and security are gathered and applied. Next, these criteria are mathematically demonstrated applying decision making techniques and new security conscious evaluation formulation is introduced for service composition approaches. The gathered approaches are evaluated based on the proposed formula to prove its correctness. Finally, the achieved results demonstrate how a service composition approach addresses security aspects.

CLASSIFICATION OF STATE-OF-THE-ART WEB SERVICE COMPOSITION APPROACHES

In this section, a new classification regarding service composition approaches is introduced and all the existing approaches are classified from two major points of view: syntactic-based and semantic-based. The first category is divided to two sub categories namely information flow control based and access control based approaches. The hierarchical classification of the security-aware Web Service Composition (WSC) approaches is illustrated in Fig. 1. For each category, a brief explanation along with respective approaches is provided. It should be noted that there are no predefined strictly boundaries between these classification aspects.

Syntactic-based approaches: The approaches which are based on XML like BPEL-based composition are classified in syntactic based service composition approach. There are two major approaches in syntactic-based WSC realm namely WS orchestration and WS choreography. In the former approach, a central coordinator i.e., the orchestrator is devised to invoke and combine the atomic activities and compose available WSs. While in the latter, a central coordinator is substituted and complex tasks are defined through the definition of the conversation which each participant should take on (Ter Beek *et al*., 2007). Web Service Business Process Execution Language (WS-BPEL) and Web Service Choreography Description Language (WS-CDL) are two representative languages that mostly use for orchestration and chorography, respectively.

Besides, for the purpose of assuring secure composition and having convenience design and analysis, secure orchestration and choreography as a demanding and critical means are needed (Xu *et al*., 2008). Therefore, the latter points out a simple form of equations for secure WSC: Secure Web services composition is equal to secure orchestration accompanied with secure choreography (Secure WSC = Secure Orchestration + Secure Choreography). In this research, syntactic-based approaches- that are XML-based approaches as well- are reviewed from security point of view. An approach is classified as security-aware solution as long as it can address at least one of

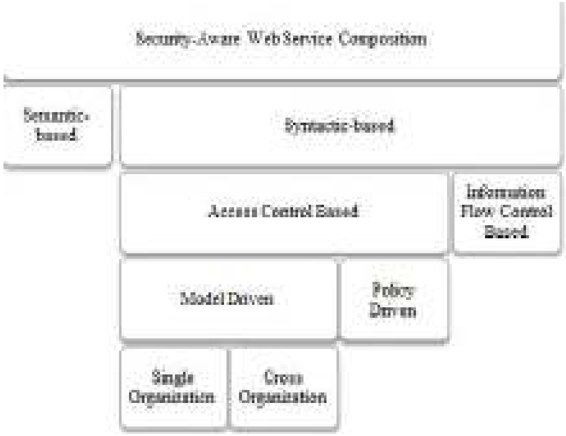


Fig. 1: Hierarchical classification of WSC approaches

the security criteria. In this regards, the state-of-the-art approaches are summarized and discussed below.

Information flow control-based: Non-functional aspects modelling of service oriented systems and utilizing them for the purpose of analysis and deployment are presented by Gilmore *et al*. (2010). In the proposed work, SOA profile so-called UML4SOA is employed to modelling service composition in UML. Moreover, the Non-Functional extension of UML4SOA (UML4SOA-NFP) and the MARTE profile can represent non-functional properties of service-oriented systems as well. The annotation of models is facilitated through Modelling and Analysis of Real-Time and Embedded systems (MARTE) profile and can be used to execute specific analysis (more concentrated on performance and schedulability analysis). Considering this, modelling of performance, security and reliable messaging are enabled as well. In addition, authors discussed formal analysis of model and considered reliability analysis and performance estimation applying "Stochastically Timed Process Algebra" (PEPA) as the underlying analytical engine. From the security perspective, the approach addresses confidentiality and integrity and provides authentication using security token. The user privacy is also protected since all requests have been encrypted.

Charfi and Mezini (2007) utilized WS-Policy and WS-Security to propose a secure framework for the sake of securing BPEL compositions. In order to achieve it, XML-Encryption is employed to cover confidentiality, XML-Signature is used to providing integrity and security token is given to support authentication. The process container which is implemented by a set of aspects in AO4BPEL is the main component of proposed framework. AO4BPEL is an aspect-oriented extension for BPEL which supports more adaptable and modular WSs. In the proposed approach, AO4BPEL is implemented as an aspect-aware orchestration engine for BPEL. As another work in the context of secure WSC, Boger *et al*. (2009) proposed a model wherein existing standards are combined and it is tried to provide a practical and consistent solution for secure service composition. According to the approach, WS-Policy is utilized to specify policies and supports not only the orchestration language (WS-BPEL), but also the business processes description language (WS-CDL).

Moreover, an approach to build processes in accordance with consumer security requirements and provider capabilities is proposed in Garcia and Felgar de Toledo (2008). In order to express these characteristics, the suggested approach utilizes Web Ontology Language (OWL) ontology and Web Services Policy Framework (WS-Policy) policies. Moreover, a framework presented by Biskup *et al*. (2007) is proposed to execute composite Web service in a decentralized manner and enable secure execution as well. The main component of framework is a data structure called container which is passed among the participating web services in the composition process. The container is encrypted and authenticated so that the execution flow is secured and a set of relevant security requirements are addressed. Besides, an automated service composition considering security policies of component services is presented in a novel approach (Chevalier *et al*., 2008). As discussed in latter, the approach amounts to constraints collection from parameters, messages and control flow of the components services as well as the goal service requirements. As a novelty of the approach, a constraint solver is introduced to check the probability of the composition-i.e., feasibly adaption of the message structure and the semantics preserving simultaneously- and presents the service composition as a message sequence chart. Besides this, authors modelled composed web services in the HLPSL language that has originally designed for security protocols specification in cryptography. In addition, a composite web service solution is proposed by Chafle *et al*. (2005) which is grounded on decentralized orchestration. The proposed approach considers the "business defined data flow constraints" as well. Lastly, an open, fine grained and end-to-end framework is pointed out by Singaravelu and Pu (2007). The proposed framework leverages WS-Security to preserve confidentiality and integrity in WSC.

Access control based approaches: One of the key components in secure systems is access control. The main responsibility of access control is answering these types of questions: which subject can do which action under which circumstances on the protected resources (Bertino *et al*., 2009). According to this approach, a method to encode an access control policy is given in an access control model and all the conditions which should be satisfied to grant an access request are stated in the model as well. In the service composition scope, access control had not been seriously considered in the past. As an instance, BPEL doesn't provide access control mechanism itself and there is no condition to invoke service in BPEL-based process. Consequently, a security model to support access control function for BPEL should be necessitated. As discussed by Rossebø and Bræk (2006), authentication and authorization patterns can be integrated to grant access rights as well.

In this study, access control based approaches are classified with respects to different perspectives including Model Driven vs. Policy Driven, Single Organization vs. Cross Organization and User based vs. Service based. The first perspective i.e., model vs. policy driven is discussed in the following. Regarding the second one, the former refers to providing inter-organizational access control comprising a small or enterprise organization, whereas the latter applies to presenting access control between some different organizational domains which intend to have connections together. Considering the last perspective, the latter refers to set limitations on service-to-service interactions while the former relates to restricting services access by users.

Policy-driven approaches: As Sodiya *et al*. (2009) state policy refers to "the statement of what is and what is not allowed". The policy-driven approach is about how the needed rules in access control can be expressed. In this regard, Rouached and Godart (2007) proposed a framework to mange authorization policies for WSC. A logic based approach is utilized to specify authorization policies and detect the resulting conflicts. In WS environments, conflicts come from the combination of various kinds of authorization and constraint policies. Rather than static detection of policy, the method can be used to correct the policies. Moreover, a formal based approach for specifying authorization policies is proposed by Bertino *et al*. (2006). The formalism technique utilized in the approach is based on Event Calculus (EC) and SPIKE is also used as automated theorem prover to verify whether a provided policy is conflict-free and prove that there are no imposed conflicts during adding and removing operations. In another presented framework (Rossebø and Bræk, 2006), a policy-driven approach is integrated with Authentication and Authorization patterns (AA-patterns) to compose services and restrict service access to only authorized users. The authors point out that the approach is applicable considering both static and dynamic composition of services. According to the approach, UML 2.0 is employed to specify AA-patterns as well as Object Constraint Language (OCL) that is used for specifications of semantic interfaces annotated with policies. Further, the authors concentrate on definition of organizational policies like RBAC.

Model driven approaches: Regarding the model definition, Sodiya *et al*. (2009) state that "the model is the formal representation of the security policies enforced by the system". According to the same reference, the model can be useful to prove the theoretical limitations of a system. In the field of access control, the model-driven approaches are concerned with execution of rules and policies. The famous types of access control like Role Based Access Control (RBAC) are classified as model-driven. In the following, some representatives of this category are discussed briefly:

- **Role Based Access Control (RBAC):** RBAC also known as non discretionary access Control inspires a real world approach more to structure access control. Considering the RBAC mechanism, permissions are firstly assigned to particular roles in an organization. Following this, users are assigned to that particular role. Then, access is granted based on users' job function within the organization and same permissions are defined for the specified role. That is, no individual user can be assigned more permissions than the defined ones for his role. In the service computing realm, RBAC widely utilized to enforce access control. There is a wealth of research in service composition about employing RBAC access control and WSC approaches which some of them are briefly explained in the following. RBAC-WS-BPEL is proposed to tackle the problem of WSC (Paci *et al*., 2009). In fact, BPEL itself has no support for access control mechanism and RBAC-WS-BPEL is an extension of WS-BPEL language to support access control in service composition. According to the proposed approach, role hierarchy which reflects the organizational structure, permission role assignment relation and a set of permissions representing the ability to perform activities are included in the authorization information. The main components of the proposed architecture are the XACML policy store, history store, BPCL constraints store repositories, the RBAC-WS-BPEL enforcement service and WS-BPEL engine.
  According to the presented architecture, scheduling and synchronizing the various activities of business process with regards to the specified activity dependencies are responsibilities of WS-BPEL engine. Further, it should invoke the associated WS operations for activities. Compared to the previous architecture which presented by Bertino *et al*. (2006), the history store is added as a new component to record the users who have performed an activity and verify whether the execution of the activity has been successful. In addition, RBAC-WS-BPEL enforcement service is responsible to support the WS-BPEL process administrators at

both deployment time and at runtime. The XACML and BPCL are also utilized in the proposed approach to encode the authorization information and describe authorization constraints such as separation of duty respectively. Moreover, this work is extended by Paci *et al.* (2008b) wherein the new types of authorization constraints such as binding of duty and resiliency are introduced and used to restrict the roles and users who can execute the activities in the business process.

Besides, another RBAC access control model for WSC is proposed by Srivatsa *et al.* (2007). In this study constraints are expressed via access control rules. These constraints may include separation of duty constraints and past histories of service invocations constraints which can also be dependent on one or more parameters associated with a WS invocation. In order to represent access control rules, a Pure-Past Linear Temporal Logic language (PPLTL) is used. In addition, role translations enforce access control and they are defined in a form of a table to map roles among different involved organizations in the composition process. After that, if the user having a certain role invokes an operation of the composite Web service, the role translation is carried out through the enforcement system and a composite role is created. A composite role includes a temporally ordered sequence of roles and services involved in the invocation.

Moreover, an integrated access control model for Web service oriented architecture is presented by Emig *et al.* (2007) wherein Attribute-Based Access Control (ABAC) model is combined with hierarchical RBAC. From the ABAC perspective, the proposed approach inherits the way service requestors are authenticated i.e., identification of a set of attributes whereas, from the RBAC point of view, it inherits a set of permissions i.e., the role hierarchy and policies definition. As a result, access control policy include not only the integration of combined permissions of an object (either an operation or the whole Web service) but also a set of attributes which should be provided by requestor and environmental state constraints (any other attribute not related to the object or service requestor e.g. date and time). Compared to the RBAC, the permissions are associated with a set of attributes of the service requestor rather than a role and it identifies a set of the service requestor's attributes rather than a business role. Furthermore, Klarl *et al.* (2009) proposed an extension of the previous model to support composite service wherein policy is enforced by composite service. This policy is a combination of the policies which protect the operations invoked in the composition process.

- **Task Based Access Control (TBAC):** TBAC framework is an extension of RBAC introduced by Thomas and Sandhu (1998) which is known as an active security model (Xu *et al*., 2008). As stated by Kerschbaum and Robinson (2009), "TBAC authorizations are granted and revoked based on when tasks are scheduled and performed. Therefore, capabilities are valid only for the duration of a task". In addition, Ji-Bo and Fan (2003) discuss that TBAC as new security model can: adopt the service-oriented perspective; build security model; realize security mechanism from the task viewpoint; and provide dynamic real-time security administration during the task processing. Considering TBAC in service computing, workflow can be modelled from the task view and permissions can be dynamically administrated with regards to the task and its status. Likewise, Ji *et al.* (2007) discuss TBAC is suitable to be utilized in distributed workflow processing and decision making for transaction management system. TBAC can be also considered as kind of context-based access control model that gives flexible security mechanism to be used in business process.

  Since activating and deactivating of permissions are based on current state of the tasks in TBAC, it provides the tracking of overall task progress and as a result secure workflow management can be supported by TBAC. In addition, TBAC can be employed for the purpose of security modelling and enforcement and has its advantages over the system-centric approach in subject-object systems. Nonetheless, for the majority of collaborative environments, TBAC should be used along with other access control (Bhatti *et al*., 2005). One of the research directions in access control technology is concentrated on integration of RBAC and TBAC (Thomas and Sandhu, 1998). Moreover, a TBAC model suitable for service composition is proposed by Ji *et al.* (2007) wherein BPEL and TBAC model are integrated together. The basic structure and functions of each main component of the TBAC engine is presented as well.
- **Credential Based Access Control (CBAC):** According to Agarwal *et al.* (2004), "Credentials are digitally signed documents, which can be transmitted by un-trusted channels like the Web". In CBAC, defined rules by access control policies state that only subjects having credentials fulfilling specific conditions are eligible to invoke a provided operation of the WS. A logical framework for CBAC was proposed by Koshutanski and Massacci (2005). In the proposed approach, an interactive algorithm based on negotiation of credentials is presented and used in stateful business process. The proposed algorithm is an extension of the previous one which supports

stateless processes. An automatic composition synthesis technique grounded on satisfiability reduction using Propositional Dynamic Logic (PDL) was proposed by Cheikh *et al*. (2006). In the suggested approach, the component services have their own authorization constraints and credential based access control. In addition, the issued credentials by other component services may or may not be trusted and the possible conversations between services and clients are used to model the service behavior.

- **Attribute Based Access Control (ABAC):** According to Yuan and Tong (2005), there are different kinds of attributes. Considering the concept of subject (such as application, user and process), the associated attributes can be the characteristics and identity of the subjects such as name, role and job title. Regarding resource, environment and context, attributes can be considered as Dublin Core metadata elements, operational, technical, or situational environment information and the access information such as current date, time and threat level respectively. In regards to service computing, an access control model is proposed by She *et al*. (2009) through which services of service chain are enabled to control their sensitive information flow. In the proposed model, information flow control is supported via a back-check procedure and pass-on certificates as well as the basic mechanism is based on the attribute certificate. During the access decision, the attribute certificates of the requesting services along with the properties of the requested resources are evaluated against the security policies. An attribute certificate of a service indicates service properties like service provider or service name, clearance level and role.

Semantic-based approaches: The representation and exchange of information in a meaningful way is one of the advantages which are allowed in Semantic Web as well as automated processing of descriptions is facilitated through it on the web (Lee *et al*., 2001). Indeed, the ultimate aim of the Semantic Web is transforming the data stored in the web to interpretable knowledge which can be understood by both machines and humans (Zhu *et al*., 2006). The key enablers to achieve this goal are ontologies which provide knowledge structure of the semantic web. Ontologies as backbone of Semantic Web helps to support interoperability as an impressive requirement of Web service environments. Due to taking care security requirements, ontologies can be extended with additional message security techniques and technologies. In order to achieve it, new classes and properties should added (Garcia and Felgar de Toledo, 2008). While an approach can address at least one of the security requirements, it goes under security-aware approaches. In the following, brief explanations of the state-of-the-art approaches relevant to this category are provided.

A semantic web service composition approach namely SCAIMO with respect to security issues is presented by Tabatabaei *et al*. (2010). In the SCAIMO framework, a secure task matchmaker is introduced to its previous work i.e., AIMO-it is based on AI-planning and Web Service Modelling Ontology (WSMO)-to match tasks with operators and methods as well as take care security requirements of both service provider and requester. To achieve this aim, three different constrains including security related goal, choreography and orchestration are defined and checked during matchmaking process. Furthermore, a recent study by Kuter and Golbeck (2009) involved an effort to generate trustworthy Web service composition. To achieve this goal, they present a new formalism for Web service composition considering available user ratings as well as a novel service composition algorithm called Trusty. Moreover, three trust computation strategies for Trusty are defined; namely overly-cautious, overly-optimistic and average. In their approach, the Hierarchical Task Network (HTN) planner SHOP2 is advanced in order to generate trustworthy service composition by incorporating reasoning mechanisms for social trust. The trust information is used as input for this new procedure and as a result, the most trustworthy composition is produced to solve a service composition problem. A WSC approach Based on Service-Ontology is reported by Liquan *et al*. (2009) and authors integrated the proposed approach with intelligent smart transcript repository. Besides, considering service composition process, Maamar *et al*. (2006) concentrate on problem of context heterogeneity of WSs and as a result, they propose an ontology based approach using OWL-C language to tackle the problem. They aim to develop a new language to manage contexts of Web services and their language is inspired by OWL-S. This new language i.e., OWL-C stands for “Ontology Web Language-based Context Ontology”. According to the suggested approach, each Web service is subject to have multiple constraints such as strategy for selecting the ontology or maximum number of Web service instances for concurrent use. In addition, security constraints as one of the multiple constraints for WSs are focused and among them, the integrity of the context of Web services and achieving it is more concentrated.

THE PROPOSED EVALUATION FRAMEWORK

For the purpose of security-aware evaluation, following framework has been presented. As it can be seen in Fig. 2, there are five defined steps which should be followed respectively.

Table 1: Evaluation criteria proposed for web service composition approaches

Criteria	Description
Composition criteria	
Composition Language (CL)	For the purpose of service composition, there are several languages developed by several organizations such as BPEL4WS, OWL-S, WSMO.
Static/Dynamic composition (S/D)	Static composition refers to constructing an abstract process model prior to the composition planning whereas, dynamic composition creates process model and selects atomic WSs in an automatic manner.
Automatic composition (A)	Automatic composition promises many improvements for service composition approaches including safer reusability, faster application development and facilitating user interactions through complex service sets.
QoS criteria	
Security Constraints (SC)	Specified to restrict the activity execution for roles or users.
Security policy/Constraint Language (SCL)	Constraints like separation and binding of duty can be specified through these languages to limit the execution of activities for users.
Reliability (R)	The ability of a WS to perform its functions is represented by reliability. Applying formal method increases the reliability of WS applications (Ter Beek *et al*., 2007).
Performance (P)	Performance represents how fast a web service request can be completed. In addition, employing AI-planning or agents in WS application, improves the performance of process (Jian Feng and Kowalczyk, 2006; Sirin, 2006).
Correctness (C)	The correctness verifiability can be identified directly with regards to the specifications of WSC (Ter Beek *et al*., 2007). Considering this, complicated web service systems might be formed through WSC wherein the behavior accuracy will be the feature of such systems. Applying AI-planning, UML and formal methods can improve correctness of WSC (Gilmore *et al*., 2010; Sirin, 2006).
Privacy (PR)	Privacy means the identity and personal data of a client is not revealed to non-authorized bodies.
Availability (AV)	The probability that a WS is available at any given time, measured as the percentage of time a WS is available over an extended period of time. Moreover, based on (Chafle *et al*., 2005) those approaches which are agent-based can increase WS availability.
Validation (V)	Verification of WSC at runtime refers to validation.
Stateless/Stateful (SL/SF)	Stateful systems are systems where the status of the current state depends on the status of the system in past conditions.
Security criteria	
Confidentiality (CO)	It means that information during transit cannot be read by unauthorized entities.
Integrity (I)	Information cannot be changed or tampered with during transit by unauthorized entities.
Authentication (AU)	The process of verifying or testing that the claimed identity is valid.
Authorization (AUT)	The process of establishing what someone who has been authenticated is allowed to do.

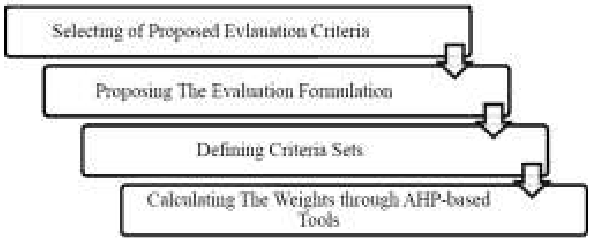

Selecting of Proposed Evlauation Criteria
Proposing The Evaluation Formulation
Defining Criteria Sets
Calculating The Weights through AHP-based Tools

Fig. 2: The proposed framework for security-conscious evaluation of web service composition

Table 2: Values of security-aware evaluation of service composition criterion

Qualitative measure of evaluation criterion	Assigned value
Exceptionally Low (XL)	0.045
Extremely Low (EL)	0.135
Very Low (VL)	0.255
Low (L)	0.335
Below Average (BA)	0.410
Average (A)	0.500
Above Average (AA)	0.590
High (H)	0.665
Very High (VH)	0.745
Extremely High (EH)	0.865
Exceptionally High (XH)	0.955

Table 3: Pair-wise comparison value

Score	Response to the question
1	Equal importance or preference
2	Equal to moderate importance or preference
3	Moderate importance or preference of one over another
4	Moderate to strong importance or preference
5	Strong or essential importance or preference
6	Strong to very strong importance or preference
7	Very strong or demonstrated importance or preference
8	Very strong to extreme importance or preference
9	Extreme importance or preference

Evaluation criteria: In this section, the criteria which are used to compare WSC approaches are presented and briefly discussed in Table 1 (first step of evaluation framework). In the comparative table, some of the criteria are assigned symbols as "✓" or "×". The former symbol indicates that the respective criterion either is supported or improved by the desired approach. On the contrary, the latter one applies in case of the required criterion neither is nor supported neither enhanced via the demanded approach. In addition, informative explanations are provided along with symbols whenever it is needed. Besides, some terms are presented in Table 2 including "Model Driven", "Formal Method" and "Agent Based" which are explained here, respectively. Model Driven Architecture (MDA) as an approach to software development is centered on the creation of models rather than program code (such as UML). Making separation between design and architecture is one of its major goals. Regarding the second term, Dillon *et al.* (1997) states "A formal method manipulates a precise mathematical description of a software system for the purpose of establishing that the system does or does not exhibit some property, which is itself precisely defined". The last term refers to a piece of code that acts on behalf of a user with authority to decide for the best action for the user.

Mathematical formulation: The second step of the proposed evaluation framework is mathematically evaluation formulation. Multi Criteria Decision Making (MCDM) has remarkable impact in the situations facing different alternative options and decision criteria. In this study, since different criteria with various values affect

Table 4: Regulated data set for evaluation criteria

Derived regulations to assign data set to evalaution criteria					References
CL_k=	0.255	VL	if	Has not been applied composition language	Mokhtar *et al*. (2006), Ter Beek *et al*. (2007), Charfi and Mezini (2007), Rouached and Godart (2007), Xu *et al*. (2008), Rao and Su (2005), Hristoskova *et al*. (2009), Kuter and Golbeck (2009) and Xiaochuan and Kochut (2004)
	0.335	L	if	Language = BPEL4WS	
	0.410	BA	if	Language = BPEL4WS + WSDL	
	0.500	A	if	Language = BPEL4WS + AO4BPEL (an engine)	
	0.590	AA	if	Language = OWL-S	
	0.745	VH	if	Language = WSMO	
A_k=	0.045	XL	if	The approach is not automatic	Sirin *et al*. (2004), Rao and Su (2005), Ter Beek *et al*. (2007), Van Der Aalst (2005), Sivasubramanian *et al*. (2009), Timm and Gannod (2007) and Foerster *et al*. (2008)
	0.410	BA	if	The approach is automatic because of applying factors support automation along with BPEL such as agent/formal method/AI planning/intelligent service/UML	
	0.500	A	if	The approach supports automation owing to use of semantic	
	0.590	AA	if	The approach supports automation due to using factors support automation along with semantic	
	0.665	H	if	The approach supports automation because of applying UML and OCL with semantic or applies HTN along with DL	
D_k=	0.045	XL	if	The approach is not dynamic	Ter Beek *et al*. (2007), van der Aalst (2005) and Sivasubramanian *et al*. (2009)
	0.410	BA	if	The approach supports dynamism because of applying factors support dynamism along with BPEL such as UML/AI planning /formal method/ intelligent service	
	0.500	A	if	The approach supports dynamism owing to use of semantic	
	0.590	AA	if	The approach supports dynamism due to applying factors support dynamism along with semantic	
SC_k=	0.135	EL	if	It is not proposed security constraint	Tabatabaei *et al*. (2010) and Mokhtar *et al*. (2006)
	0.500	A	if	The proposed security constraints consider only service provider or requester or web service side	
	0.590	AA	if	The proposed security constraints consider only two of service provider or requester or web service sides	
	0.665	H	if	The proposed security constraints consider all three of service provider or requester or web service sides	
P_k=	0.335	L	if	In case of no points with regards to the performance in the approach	Chafle *et al*. (2005), Dersingh *et al*. (2008), Jian Feng and Kowalczyk (2006), Rao and Su (2005) and Sirin *et al*. (2004)
	0.410	BA	if	The approach just claims to increase performance but no offers validation	
	0.500	A	if	The approach validates its claimed performance improvement	
	0.590	AA	if	The approach applies formal method/agent/AI planning/UML technique to improve its performance	
	0.665	H	if	The approach applies AI planning along with DL to improve its performance	
AV_k =	0.500	VL	if	There is no applied standards or methods to improve availability	Dersingh *et al*. (2008) and Timm and Gannod (2005)
	0.590	AA	if	The approach applies agent-based technique to improve availability	
PR_k =	0.255	VL	if	There is no applied standards or methods to address privacy	Proposed by authots
	0.590	AA	if	The approach applies standards or methods to address privacy	
C_k =	0.410	BA	if	The proposed approach is semantic or syntactic based without applying techniques to improve correctness	Ter Beek *et al*. (2007), Foerster *et al*. (2008), Zhengdong *et al*. (2009) and Gilmore *et al*. (2010)
	0.590	AA	if	The proposed approach is applied techniques to improve correctness such as AI-planning, formal method and UML	
	0.665	H	if	The proposed approach is applied AI-planning with DL to improve correctness	
V_k =	0.255	VL	if	The approach proposes no implementation for its claim	Proposed by authots
	0.500	A	if	The approach employs programming as a implementation	
	0.665	H	if	The approach applies mathematical technique to implement its claim	
SF_k =	0.255	VL	if	The approach support no stateful aspect	Proposed by authots
	0.500	A	if	The approach supports stateful aspect	
R_k =	0.410	BA	if	Formal method is not applied in the approach	Ter Beek *et al*. (2007)
	0.590	AA	if	Formal method is applied in the approach	

on the evaluation process, it is needed to utilize one of the MCDM techniques. Analytical Hierarchical Process (AHP) proposed by Saaty (1994) as one of the most famous MCDM techniques is preferred to apply for the proposed evaluation process. Employing this technique provides opportunities to assign different values i.e., weights to different criteria so that they can have an effect on evaluation in a proper manner.

For evaluating web service composition approaches we introduce QoS-aware Service Composition (QSC) which is a metric to measure how well (efficient) are service compositions approaches based on the proposed criteria. QSC values are computed based on the following equations:

$$QSC_k = CoM_k + QoS_k \tag{1}$$

$$CoM_k = \sum_{i=1}^{3} w_i * i \tag{2}$$

$$QoS_k = \sum_{j=1}^{13} w_j * j \tag{3}$$

Table 5: Regulated data set for evaluation criteria

Derived regulations to assign data set to evalaution criteria					References
CO_k and I_k =	0.045	XL	if	The approach applies no standard or method to provide data integrity or confidentiality.	Charfi *et al.* (2005), Chevalier *et al.* (2008), Garcia and Felgar de Toledo (2008), Carminati *et al.* (2007) and Dersingh *et al.* (2008)
	0.135	EL	if	The approach just claims to support integrity or confidentiality but no proof how it provides.	
	0.255	VL	if	The proposed composition language is syntactic and proposes no security constraint language.	
	0.335	L	if	The proposed composition language is syntactic based and the security constraint language isn't even applied along with UML, mathematic or ontology.	
	0.410	BA	if	The proposed composition language is syntactic based and is applied along with an engine to support QoS criteria as well as security constraint language is applied without ontology.	
	0.500	A	if	The proposed composition language is OWL-S or WSMO but applies no security constraint language.	
	0.590	AA	if	The proposed composition language is syntactic based (BPEL) and security constraint language is applied along with UML, mathematic or ontology.	
AU_k =	0.045	XL	if	The approach applies no standard or method to provide authentication.	Ji-Bo and Fan (2003), Agarwal *et al.* (2004), Sodiya *et al.* (2009), Yuan and Tong (2005) and Rouached and Godart (2007)
	0.135	EL	if	The approach just claims to support authentication but no proof how it provides.	
	0.255	VL	if	The proposed composition language is syntactic and proposes no security constraint language.	
	0.335	L	if	The proposed composition language is syntactic based and the security constraint language isn't even applied along with UML, mathematic or ontology.	
	0.410	BA	if	The proposed composition language is syntactic based and is applied along with an engine to support QoS criteria as well as security constraint language is applied without ontology. Credential applies to provide authentication.	
	0.500	A	if	The proposed composition language is OWL-S or WSMO but applies no security constraint language. Credential applies to provide authentication.	
	0.590	AA	if	The proposed composition language is syntactic based (BPEL) and security constraint language is applied along with UML, mathematic or ontology. Credential applies to provide authentication.	
AUT_k =	0.255	VL	if	The proposed composition language is syntactic and offers no engine and security constraint language.	Ji-Bo and Fan (2003), Agarwal *et al.* (2004), Sodiya *et al.* (2009), Yuan and Tong (2005) and Rouached and Godart (2007)
	0.335	L	if	The proposed composition language is syntactic based (without any engine) and the security constraint language is offered. Attributes are used to support authorization.	
	0.410	BA	if	The proposed composition language is syntactic based (without any engine) and the security constraint language is offered. Roles are used to support authorization.	
	0.500	A	if	The proposed composition language is syntactic based and formal method, UML or ontology is utilized to define security constraint language. Credential are used to support authorization.	
	0.590	AA	if	The proposed composition language is syntactic based and formal method, UML or ontology is utilized to define security constraint language. Roles are used to support authorization.	
SCL_k =	0.255	VL	if	The approach proposes no languages to define policy or constraint.	Carminati *et al.* (2007), Tabatabaei *et al.* (2010) and Chevalier *et al.* (2008)
	0.500	A	if	The proposed language supports no semantic.	
	0.665	H	if	The proposed language supports semantic or defined in UML or mathematic based.	

Table 6: Primary assessment of web service composition approaches

							QoS				
							Security				
Work/criteria			CL	SCL	D/S	A	CON	I	AU	AUT	SF
Syntactic -based	Information flow control-based	[1]	BPEL	WS-policy+ OWL	S	×	WS-security: XML encryption	WS-security : XML signature	×	×	×
		[2]	BPEL	×	S	✓agents	WS-security: XML encryption	WS-security: XML signature	×	×	×
		[3]	BPEL	×	S	×	WS-security: XML encryption	WS-security: XML signature	×	×	×
		[4]	BPEL	XACML	S	✓agent	✓	×	×	×	×
		[5]	BPEL	×	D/process algebra	✓model transformation /formal method	XML encryption	XML signature	Security token: user name	×	×
		[6]	BPEL	HLPSL	D/HLPSL	✓	XML encryption	×	Digital signature	×	×
		[7]	BPEL+ AO4BPEL	WS-policy	S	×	WS-security: XML encryption	WS-security: XML signature	Security token: user name	×	×
		[8]	BPEL/ WS-CDL	WS-policy	S	×	WS-security: XML encryption	×	×	×	×
		[9]	BPEL	SAML+ OWL	S	×	×	×	Credential	×	×
	Access control-based	[10]	BPEL	×	S	×	×	×	Attributes	Role	×
		[11]	BPEL	Pol.: XACML Con: BPCL	S	×	×	×	Credential	Role	✓
		[12]	BPEL	×	S	×	×	×	Credential	✓	✓
		[13]	BPEL	×	S	×	×	×	N/A	Task	×
		[14]	BPEL	XACML	S	✓ agent	×	×	Attribute	✓	×
		[15]	BPEL	PDL	D (PDL)	✓ PDL	×	×	Credential	✓	×
		[16]	BPEL	×	S	×	×	×	N/A	Role	✓
		[17]	×	UML/ OCL	S	×	×	×	Credential	Role	×
		[18]	×	EC (formal method)	S	×	×	×	Credential	✓	×
Semantic-based		[19]	WSMO	×	D/semantic/ AI planning	Semantic/AI planning: HTN-DL	×	×	X.509	×	×
		[20]	OWL-S	×	D/semantic	Semantic	×	×	×	×	✓
		[21]	OWL-S	×	D/semantic	Semantic	×	✓	×	×	×
		[22]	OWL-S	×	D/semantic/ AI planning	Semantic/AI planning: HTN planner SHOP2	×	×	Service credential	×	✓

			QoS						
Work/criteria			R	P	C	AV	PR	V	SC
Syntactic-based	Information flow control-based	[1]							
		[2]	×		×	×	×	×	×
		[3]	×	✓ agents	×	✓ agent	✓	×	×
		[4]	×	✓ claim	×	×	✓	Program	×
		[5]	×	✓ agents	×	✓ agent	×	Program	×
		[6]	✓ process algebra	✓ process algebra	✓ process algebra	×	✓	Program	×
		[7]	×		✓ HLPSL	×	×	Mathematic	×
		[8]	×		×	×	×	Program	×
		[9]	×		×	×	×	Program	×

Table 6: (Continue)

	Access control-based	[10]	×		×	×	×	Program	×
		[11]	×	✓ claim	×	×	×	Program	×
		[12]	×	✓ claim	×	×	×	Program	Separation/ binding of duty
		[13]	×	✓ claim	×	×	×	Program	Separation of duty
		[14]	×	×	×	×	×	Program	×
		[15]	×	✓ agent	×	✓ agent	×	Program	×
		[16]	×		✓ PDL	×	×	Mathematic	×
		[17]	×	Claim	×	×	×	Program	Composition history, separation of duty, inter-organizational roles
		[18]	×	×	✓ UML	×	×	Program	×
Semantic-based		[19]	×	×	✓ EC	×	×	Mathematic	×
		[20]	×	✓ AI planning	✓ AI planning	×	×	Program	Security-related goal, choreography, orchestration constraints
		[21]	×	×	×	×	×	Program	×
		[22]	×	×	×	×	×	Program	Maximum number of web service instances to make available for concurrent use
			×	✓ AI planning	✓ AI planning	×	×	Program	×

$$QSC_k = \sum_{i=1}^{3} w_i * i + \sum_{j=1}^{13} w_j * j \tag{4}$$

$$CoM_k = \{CL_k, D_k, A_k\} \tag{5}$$

$$QoS_k = \begin{Bmatrix} SC_k, R_k, P_k, C_k, V_k, PR_k, AV_k, SF_k, \\ SCL_K, CO_K, I_K, AU_K, AUT_K \end{Bmatrix} \tag{6}$$

where, the CoM_k and QoS_k are composition and QoS criteria for approach k respectively and comprise two important parts of the proposed evaluation formula Eq. (1) and (4). They compute based on their comprised criteria as presented in Eq. (2) and (3). K is the number of compared approaches which equals to 22 in this study. i and j indicate the respective criterion as described as follows:

$$i = \begin{cases} CL_k & \text{if} \quad i = 1 \\ D_k & \text{if} \quad i = 2 \\ A_K & \text{if} \quad i = 3 \end{cases}$$

$$j = \begin{cases} SC_k & \text{if} \quad j = 1 \\ R_k & \text{if} \quad j = 2 \\ P_K & \text{if} \quad j = 3 \\ C_K & \text{if} \quad j = 4 \\ V_K & \text{if} \quad j = 5 \\ PR_K & \text{if} \quad j = 6 \\ AV_K & \text{if} \quad j = 7 \\ SF_K & \text{if} \quad j = 8 \\ SCL_K & \text{if} \quad j = 9 \\ CO_K & \text{if} \quad j = 10 \\ I_K & \text{if} \quad j = 11 \\ AU_K & \text{if} \quad j = 12 \\ AUT_K & \text{if} \quad j = 13 \end{cases}$$

The next step in evaluation framework is defining criteria sets. In order to do this, Table 2 proposed by Chen *et al.* (1992) is utilized to assign values to respective criteria considering their all possible situations.

Considering this table, a designated set to each criterion is demonstrated in Table 4 and 5. It can be noted here that these data sets are derived through the exhaustive literature review.

Lastly, final step in the proposed evaluation framework is computing the weights for evaluation criteria. This step is based on pair-wise comparisons of criteria suggested by AHP methodology to determine criteria weights. Therefore as major contribution of AHP, subjective assessments of relative importance is converted to numerical values i.e., weights and a matrix for evaluation of criteria importance is proposed (as depicted in Fig. 3). In the matrix, f is the number of criteria and cells above the diagonal of the matrix are specified through an answer to the question of "how important is criterion C$_i$ compared with criterion C$_j$?" (which could be one from the Table 3). On a diagonal, the cells are equal to 1 and the rest of them are reciprocal. The weights for criteria come from this matrix.

In order to do that, an AHP based tool called "Expert Choice" is utilized to calculate the appropriate each criterion with respect to received feedbacks from experts. Number of experts and academics has been

Table 7: Mathematical evaluation of security aware web service composition approaches

							QoS				
							Security				
Work/criteria			CL	SCL	D/S	A	CO	I	AU	AUT	SF/SL
Syntactic - based	Information flow control-based	[1]	0.335	0.665	0.045	0.045	0.590	0.590	0.045	0.255	0.255
		[2]	0.335	0.255	0.045	0.410	0.255	0.255	0.045	0.255	0.255
		[3]	0.335	0.255	0.045	0.045	0.255	0.255	0.045	0.255	0.255
		[4]	0.335	0.500	0.045	0.410	0.135	0.045	0.045	0.255	0.255
		[5]	0.335	0.255	0.410	0.410	0.255	0.255	0.255	0.255	0.255
		[6]	0.335	0.665	0.410	0.410	0.590	0.045	0.590	0.255	0.255
		[7]	0.500	0.500	0.045	0.045	0.335	0.335	0.335	0.255	0.255
		[8]	0.410	0.500	0.045	0.045	0.335	0.045	0.045	0.255	0.255
		[9]	0.335	0.665	0.045	0.045	0.045	0.045	0.590	0.255	0.255
	Access control-based	[10]	0.335	0.255	0.045	0.045	0.045	0.045	0.255	0.255	0.255
		[11]	0.335	0.500	0.045	0.045	0.045	0.045	0.335	0.410	0.500
		[12]	0.335	0.255	0.045	0.045	0.045	0.045	0.255	0.255	0.500
		[13]	0.335	0.255	0.045	0.045	0.045	0.045	0.135	0.255	0.255
		[14]	0.335	0.500	0.045	0.335	0.045	0.045	0.335	0.335	0.255
		[15]	0.335	0.665	0.410	0.500	0.045	0.045	0.590	0.500	0.255
		[16]	0.335	0.255	0.045	0.045	0.045	0.045	0.135	0.255	0.500
		[17]	0.255	0.665	0.045	0.045	0.045	0.045	0.590	0.590	0.255
		[18]	0.255	0.665	0.045	0.045	0.045	0.045	0.590	0.500	0.255
Semantic-based		[19]	0.745	0.255	0.590	0.665	0.045	0.045	0.500	0.255	0.255
		[20]	0.590	0.255	0.500	0.500	0.045	0.045	0.045	0.255	0.500
		[21]	0.590	0.255	0.500	0.500	0.045	0.135	0.045	0.255	0.255
		[22]	0.590	0.255	0.590	0.590	0.045	0.045	0.500	0.255	0.500

			QoS						
Work/criteria			R	P	C	AV	PR	V	SC
Syntactic - based	Information flow control-based	[1]	0.410	0.335	0.410	0.500	0.045	0.255	0.135
		[2]	0.410	0.590	0.410	0.590	0.590	0.255	0.135
		[3]	0.410	0.410	0.410	0.500	0.590	0.500	0.135
		[4]	0.410	0.590	0.410	0.590	0.045	0.500	0.135
		[5]	0.590	0.590	0.590	0.500	0.590	0.500	0.135
		[6]	0.410	0.335	0.590	0.500	0.045	0.665	0.135
		[7]	0.410	0.335	0.410	0.500	0.045	0.500	0.135
		[8]	0.410	0.335	0.410	0.500	0.045	0.500	0.135
		[9]	0.410	0.335	0.410	0.500	0.045	0.500	0.135
	Access control-based	[10]	0.410	0.410	0.500	0.500	0.045	0.500	0.135
		[11]	0.410	0.410	0.500	0.500	0.045	0.500	0.500
		[12]	0.410	0.410	0.500	0.500	0.045	0.500	0.500
		[13]	0.410	0.335	0.500	0.500	0.045	0.500	0.135
		[14]	0.410	0.590	0.500	0.590	0.045	0.500	0.135
		[15]	0.410	0.335	0.665	0.500	0.045	0.665	0.135
		[16]	0.410	0.410	0.500	0.500	0.045	0.500	0.590
		[17]	0.410	0.335	0.665	0.500	0.045	0.500	0.135
		[18]	0.410	0.335	0.665	0.500	0.045	0.665	0.135
Semantic-based		[19]	0.410	0.665	0.665	0.500	0.045	0.500	0.665
		[20]	0.410	0.335	0.410	0.500	0.045	0.500	0.135
		[21]	0.410	0.335	0.410	0.500	0.045	0.500	0.500
		[22]	0.410	0.590	0.590	0.500	0.045	0.500	0.135

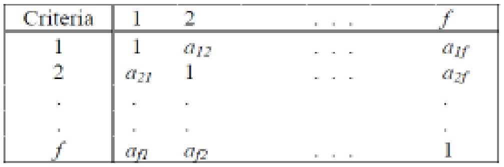
requested to provide their feedbacks on proposed evaluation attributes to make pair-wise comparison matrix. To achieve accurate result, the geometrical mean of individual evaluations are computed through Eq. (7). It should be noted here that the importance of expert is considered to be equal. The obtained weights for the criteria are presented in Fig. 4 and the Consistency Ratio (CR) is equal to 0.1:

$$\bar{a}_{\text{ij}} = (\prod_{k=1}^{N} a_{ij}^{(k)})^{1/N}$$

where,

$$\begin{cases} a_{ij}^{(k)} \text{ is } k\text{th expert's opinion to compare attribute } i \text{ to attribute } j \\ N \text{ is the number of involved experts} \end{cases} \quad (7)$$

Primary assessment: The aforementioned approaches in section (Classification of state-of-the-art web service composition approaches) are comparatively evaluated with respects to presented criteria in the third section



Criteria	1	2	. . .	f
1	1	a_{12}	. . .	a_{1f}
2	a_{21}	1	. . .	a_{2f}
.	.	.		.
.	.	.		.
f	a_{f1}	a_{f2}	. . .	1

Fig. 3: Matrix for evaluation of criteria importance

and the results based on extracted information from review of respective approaches are illustrated in Table 6. This table concerns on descriptive data derived from each approach. In the next step, this information with regards to defined formula in above section is utilized to mathematically evaluate those approaches.

Mathematical based evaluation: In this section, the comparative table presented in previous section i.e., Table 6 is transformed from descriptive mode to mathematical-based style with the help of Table 2, 4 and 5 discussed in section (Mathematical formulation). As a result, a new diagram i.e., Fig. 5 is produced wherein the value of each criterion with respect to each approach is illustrated.

Considering the presented results in Fig. 5 and aforementioned formulation, comparative evaluation for all proposed categories is in more precisely manner performed and each approach is ranked through the obtained results. Moreover, the definition of “Low”, “Average” and “High” approach is inferred from the achieved approaches ranking. According to the definition depicted in Fig. 6, an approach is considered as a “Low”, if its achieved value (x) is less than 0.335 ($x \le 0.335$). In case of an approach obtains a value between 0.335 and 0.450 ($0.335 < x \le 0.450$), it is considered as an “Average”. Finally, an approach is considered as a “High” if its gained value is more than 0.450 ($x > 0.450$).

RESULT ANALYSIS

In this section, discussion and analysis with respects to each category is provided. The comparative evaluation of state-of-the-art approaches are presented in Table 7. This table is the mathematical version of Table 6 demonstrated as primary assessment. In the following, the respective explanation with regards to each classification is provided.

Comparative evaluation of syntactic-based approaches: In this section, security-aware syntactic-based approaches are compared with respects to two sub categories namely information flow control-based and access control-based. The result of these comparisons is presented as follows.

Information flow control-based: Regarding information flow control-based category, works proposed by Chevalier *et al.* (2008) and Gilmore *et al.* (2010) are evaluated as “Average” approaches while the rest of them are marked as “Low” ones. It also can be noted all the existed approaches in this comparison mainly concern confidentiality and integrity of exchanged message in WSC. From the perspective of composition language, all the approaches except the work presented by Boger *et al.* (2009) have considered BPEL to provide only secure orchestration and have not dealt with secure choreography. Nevertheless, being secure orchestration and choreography together is needed to ensure secure service composition. Therefore, integration of conversation specification languages such as WS-CDL along with BPEL can be considered as advantage of proposed work by Boger *et al.* (2009). Furthermore, all compared approaches except proposed work by Chevalier *et al.* (2008) and Gilmore *et al.* (2010) are contemplated as static service composition

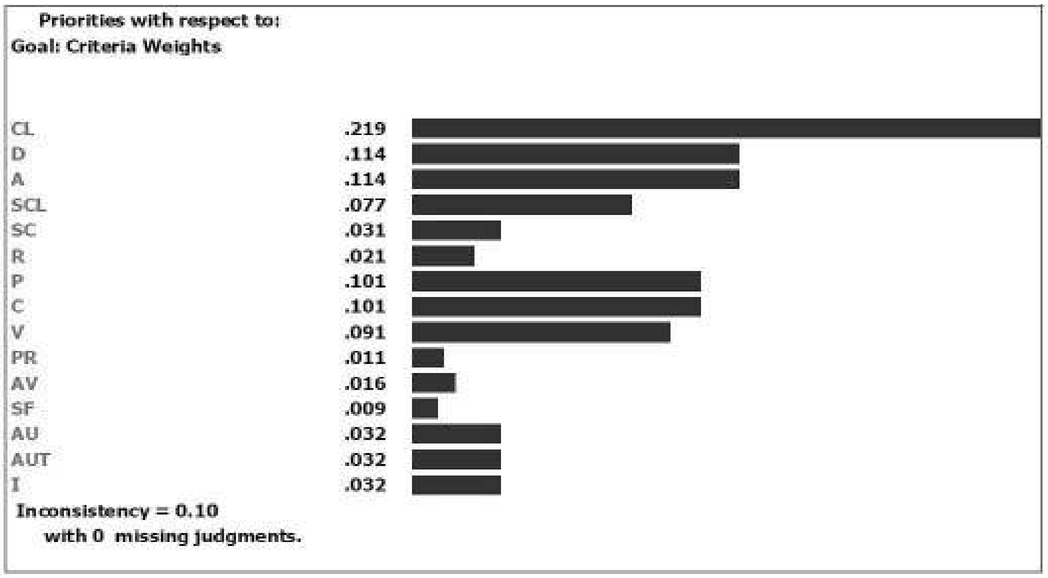


Fig. 4: Weight of evaluation attributes

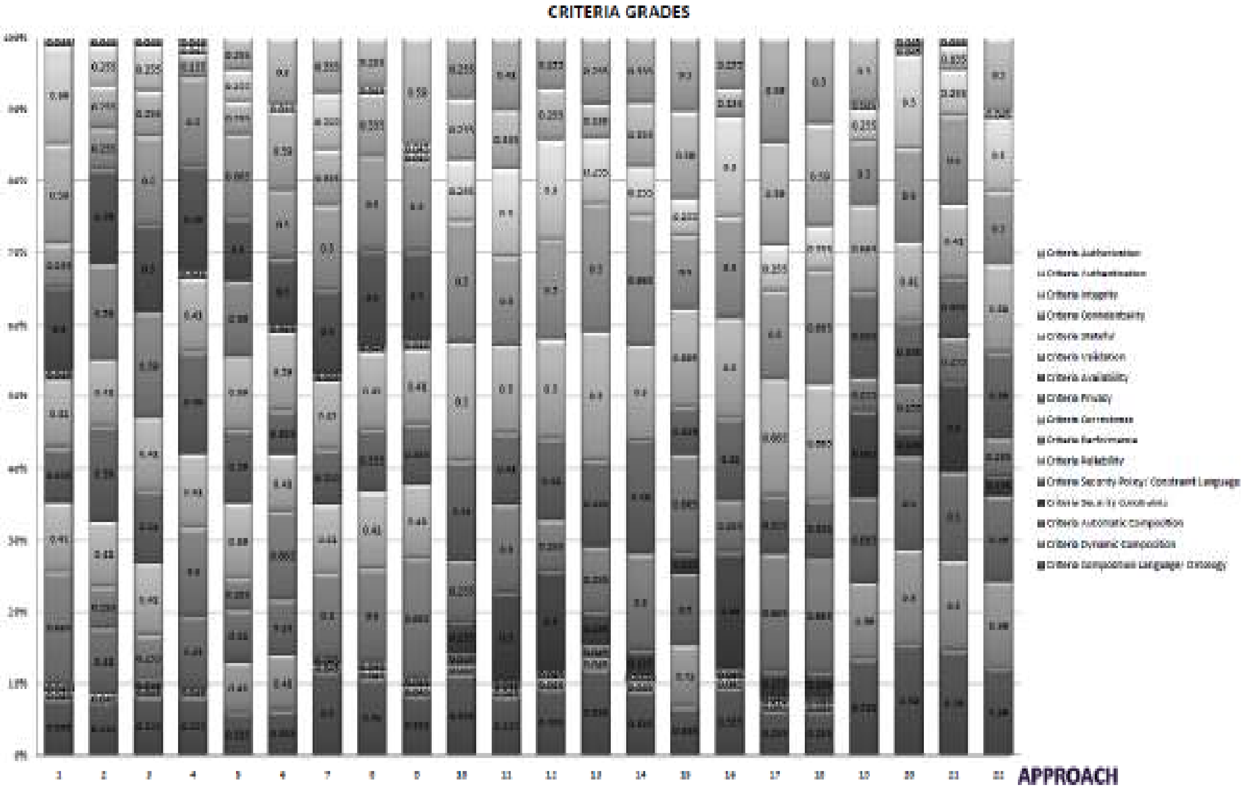


Fig. 5: Mathematical-based evaluation of web service composition approaches

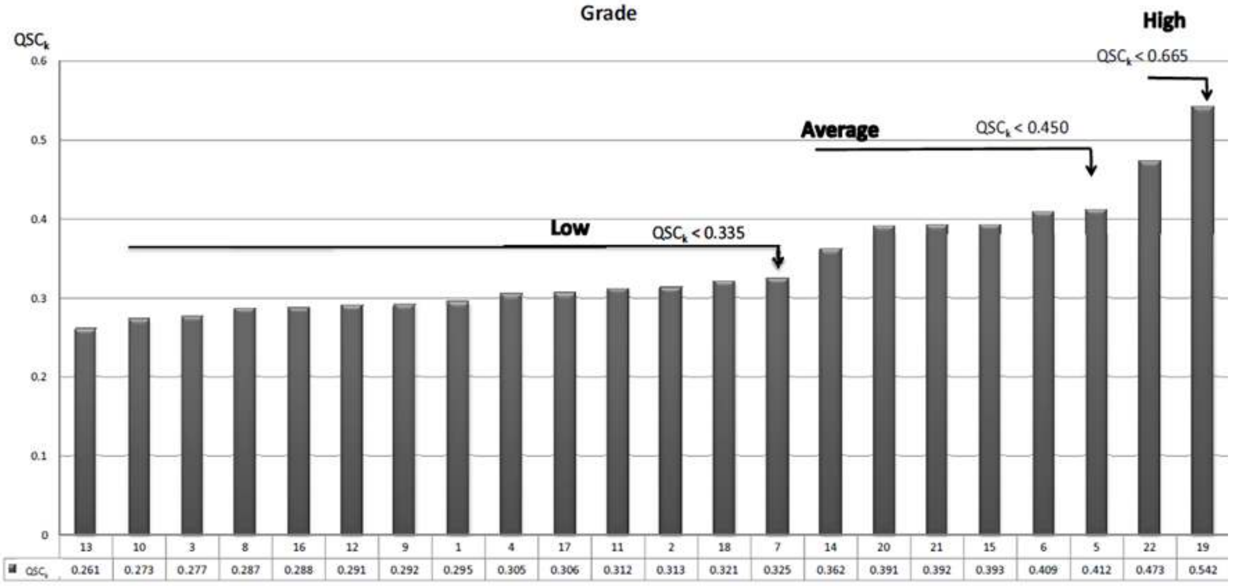


Fig. 6: QoS-aware web service composition ranking

approaches, since BPEL and WS-CDL lack the semantic knowledge. However, those exception works provide dynamic composition applying HLPSL and UML, respectively. Likewise, approaches presented by Charfi *et al*. (2005), Boger *et al*. (2009), Garcia and Felgar de Toledo (2008) and Singaravelu and Pu (2007) can provide no automatic WSC due to being based on BPEL. On the other hand, proposed works by Biskup *et al*. (2007), Chafle *et al*. (2005), Gilmore *et al*. (2010) and Chevalier *et al*. (2008) are considered as automatic service composition approaches owing to applying agent-based technique, UML and HLPSL respectively. In addition, construction of BPEL specification from UML diagrams has been facilitated by Gilmore *et al*.

(2010) through model transformation. Besides, it has estimated and analyzed reliability, correctness and performance using timed Process Algebra namely PEPA. The work presented by Chevalier *et al*. (2008) is also evaluated as "Above Average" quality with respect to correctness since the approach used mathematical-based (cryptographic tools) technique. Regarding performance, Singaravelu and Pu (2007) claimed that acceptable performance is provided while proposed works by Chafle *et al*. (2005) and Biskup *et al*. (2007) have improved their performance due to using agent based technique. Moreover, they enhanced availability of services during service composition via utilizing agent based technique. It is also claimed that privacy has been addressed using data encryption in works presented by Biskup *et al*. (2007), Singaravelu and Pu (2007) and Gilmore *et al*. (2010). From security point of view, WS-Security has been utilized by Charfi *et al*. (2005), Singaravelu and Pu (2007), Biskup *et al*. (2007), Garcia and Felgar de Toledo (2008) and Boger *et al*. (2009) to address security issues including confidentiality and integrity. Nevertheless, basic security functionalities can only be provided through WS-Security and there is no enough support provided in those approaches to ensure security for WSC (Biskup *et al*., 2007). In addition, Chafle *et al*. (2005) claimed that confidentiality of message can be provided utilizing decentralized (agent based) approach. According to latter, WSs may impose some restrictions on data flow and these data constraints present obstacles for centralized coordinator in orchestration-based service composition. Moreover, authentication has been provided by Charfi *et al*. (2005), Chevalier *et al*. (2008) and Gilmore *et al*. (2010) through security token (username) and digital signature respectively. With respect to security policy languages, XACML and WS-Policy languages are employed to specify WS security policies by Chafle *et al*. (2005), Charfi *et al*. (2005) and Boger *et al*. (2009) respectively. However, WS-Policy and XACML lack semantics. It in turn impedes the effectiveness of computing the compatibility between the policies.

Moreover, since applying WS-Policy and XACML as syntactic approaches may restrict the selection of suitable WSs, the use of ontology to overcome this limitation is essentially needed. Therefore, ontology based policy annotations are added to WS-Policy by Garcia and Felgar de Toledo (2008) to offer a flexible approach to support interoperability as a key requirement in service computing environments. In addition, according to the latter, additional message security techniques and technologies can be extended to WS-policy utilizing new classes and properties. Considering this, the proposed approach enables building processes in accordance with provider capabilities and consumer security requirements which is expressed through WS-Policy along with OWL. Despite that, flexibility and extensibility of this approach has been limited due to inherent deficiencies of WS-Policy. Besides, security policies should be enforced through the orchestration engine (Charfi *et al*., 2005). Since current BPEL engines have not provided this, an aspect-aware orchestration engine (as extension to BPEL engine) so-called AO4BPEL is proposed by Charfi *et al*. (2005) to support more adaptable and modular WSC. Nonetheless, there are still some remaining problems in that proposed approach as follows. Firstly, although the dynamic adaptability and modularity have been provided in AO4BPEL towards service composition, it still suffers lack of semantic description for business processes and rules and security aspects. Thus, conflicts detection and policy negotiation are infeasible for secure WSC. Secondly, the approach lacks flexibility since service composition aspect is considered at the deployment time rather than runtime. Moreover, Chevalier *et al*. (2008) utilized HLPSL language to specify security constraints. With regards to validation, proposed approach by Gilmore *et al*. (2010) has been marked as "High" due to using formal methods while approaches proposed by Garcia and Felgar de Toledo (2008) and Biskup *et al*. (2007) have been evaluated as "Very Low" since they provide no validation proofs. The rest of compared approaches are marked as "Average" owing to presenting prototypes. Finally, since there are no formal semantics in BPEL and WS-CDL, they can provide no formal reasoning regarding process behavior. On the other hand, better service discovery as well as easier service interoperation and composition will be enabled through semantically described services. In that case, in order to enable semantically meaningful execution, there must be certain rules and mapping formalisms between ontologically described knowledge about business process on one side and BPEL and WS-CDL definitions of business process on another side.

Access control-based: Considering access control-based classification, proposed approaches by Rossebø and Bræk (2006), Cheikh *et al*. (2006), Rouached and Godart (2007) and She *et al*. (2009) are evaluated as "Average" while the rest of compared approaches are evaluated as "Low". With respects to composition language, all the compared approaches selected BPEL as their composition language however, approaches presented by Rossebø and Bræk (2006) and Rouached and Godart (2007) just claim they are syntactic-based and clarify no languages used in their works. Likewise, all of these works except Cheikh *et al*. (2006) are contemplated as static approaches to support service composition owing to use of BPEL language. On the other hand, Cheikh *et al*. (2006) proposed dynamic technique towards service composition due to utilizing PDL as logic based approach along with BPEL. Moreover, among compared approaches only the presented works by Cheikh *et al*. (2006) and She *et al*. (2009) are classified as an automatic service composition since they employed agent-based technique and mathematic approach (PDL) respectively. Besides, latter approach claimed that it has acceptable performance by applying agents in its work.

Regarding correctness, approaches proposed by Cheikh *et al.* (2006), Rossebø and Bræk (2006) and Rouached and Godart (2007) are evaluated as "High" since they utilize PDL, EC and UML, respectively. From the security perspective, presented works by Koshutanski and Massacci (2005), Srivatsa *et al.* (2007) and Paci *et al.* (2009) are considered as stateful approaches due to keeping user or service histories for future decisions. Moreover, approaches proposed by Emig *et al.* (2007) and She *et al.* (2009) provide authentication through user and service attributes respectively. In addition, authentication is addressed via user credentials in works proposed by Koshutanski and Massacci (2005), Rossebø and Bræk (2006) and Paci *et al.* (2009) whereas service credentials are utilized by Cheikh *et al.* (2006) and Rouached and Godart (2007) for the purpose of authentication.

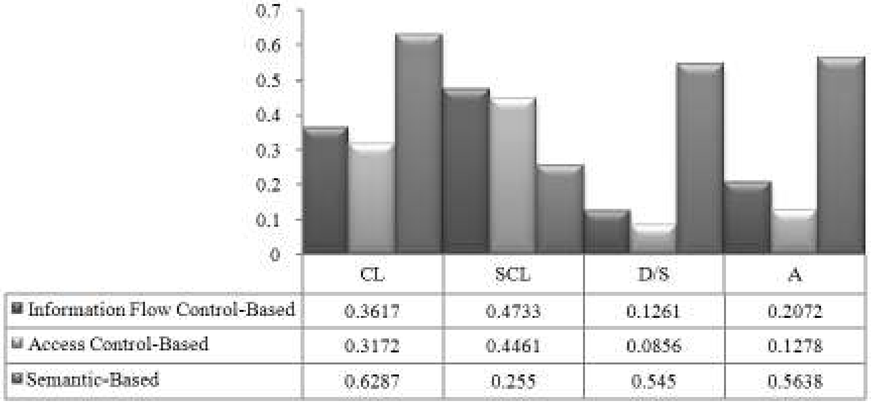
With regards to authorization, role-based technique is used by Rossebø and Bræk (2006), Emig *et al.* (2007), Srivatsa *et al.* (2007) and Paci *et al.* (2009). However, RBAC is insufficient method to be used in service composition due to the following reasons: firstly, RBAC as an inactive security model cannot dynamically administrate permissions in the executing states of working progress and thus the requirements of BPEL-based access control cannot properly addressed. Following this, RBAC suffers the inability for specifying a fine-grained control in collaborative environments. Next, RBAC provides no abstraction to capture a set of collaborating users which operate in different roles. Lastly, RBAC sometimes faces difficulties for encapsulation of all permissions to perform a job function.

To address RBAC problems in BPEL, Ji *et al.* (2007) suggests replacing TBAC with RBAC. It caused to provision of more flexibility for secure business processes. However, better support to understand context semantics is provided in semantic based approaches compared to the BPEL. Likewise, semantic based approaches provide better reasoning for complicated relations among contextual concepts. Moreover, approaches proposed by Koshutanski and Massacci (2005), Cheikh *et al.* (2006), Rouached and Godart (2007) and She *et al.* (2009) proposed authorization technique based on user/service attribute or credential. According to section Model Driven Approaches, it is concluded that attribute-based access control is more perfect than credential-based one. With regards to security constraints or policy language, presented approaches by Paci *et al.* (2009) and She *et al.* (2009) utilized XACML to define their security policies as well as BPCL (Business Process Constraint Language) is used in the former approach as a constraint language. In fact, the BPCL is proposed in this approach since RBAC is insufficient to address all the authorization requirements of workflow systems like separation and binding of duty constraints. Despite that XACML is a good approach to specify policy in a designated domain, it suffers some limitations as follow: Firstly, the issue of enforcing access control has not been addressed properly and it has not been considered to include in composition phase. After that, XACML faces with lack of semantics for high-level security requirements and this affects on effectiveness of the compatibility computing among the policies and thus it results in false negative (Rouached and Godart, 2007). Lastly, no explicit constructs is provided in XACML to reason about transactional histories (Srivatsa *et al.*, 2007). Manual definition and verification of authorization policies is error-prone and cumbersome. Thus, it is needed to have an automated analysis to make sure policies are conflict-free at first time and during adding or removing new authorization policies. In order to address it, Cheikh *et al.* (2006) utilize PDL to automate defining and verifying authorization policies as a part of composition process. Likewise, security policies are carried out dynamically by Rossebø and Bræk (2006) and Rouached and Godart (2007) applying UML as model driven technique and EC as formal method respectively. Moreover, proposed approaches by Cheikh *et al.* (2006) and Rouached and Godart (2007) increase the reliability due to using formal methods. With regards to verification, these two approaches are evaluated as "High" due to presenting mathematical-based proof while the rest of compared approaches are marked as "Average" owing to proposing prototypes for their works. However, those works which use syntactic-based approaches cannot be fully applicable since their completeness depends on syntactical restrictions.

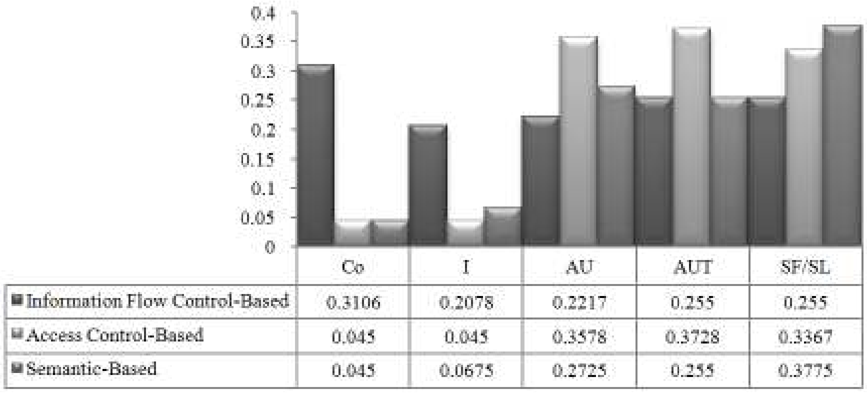
Comparative evaluation of semantic-based approaches: Regarding semantic-based classification, proposed work by Kuter and Golbeck (2009) and Tabatabaei *et al.* (2010) are evaluated as "High", whereas the rest of the approaches are marked as "Average". All the approaches classified in this category support automatic and dynamic service composition owing to using ontologies (Liquan *et al.*, 2009). Considering these approaches, the composition language used by Tabatabaei *et al.* (2010) is WSMO while the rest of composition languages are based on OWL-S. With regards to supporting non-functional properties, WSMO is superior than OWL-S. The reason is that non-functional properties in OWL-S are more restricted than WSMO. While the latter supports them in any WSMO elements, the former provides non-functional properties in service profile (Kuter and Golbeck, 2009). Furthermore, proposed works by Kuter and Golbeck (2009) and Tabatabaei *et al.* (2010) present more automation composition due to applying AI planning. The former approach utilizes HTN planning as an AI technique to automate WSC while the latter one employs HTN-DL for automation of service composition. Although HTN is suitable approach for service composition and HTN planner is more efficient compared to other planning languages, there are some limitations when a HTN planner is used for service composition by itself. It faces limitations such as: no formalization, lack of an interactive WS environment, no function to cover additional scheduling information or satisfaction of general problems, lack of autonomy and no proper non-functional properties support. Consequently, integration of Description Logic (DL) with HTN is proposed to solve most of aforementioned limitations, specially supporting non-functional properties such as performance and correctness in proper way (Sirin, 2006). Considering this, Tabatabaei *et al*. (2010) applied HTN-DL to automate WSC. In the light of correctness and performance, those two works have improved the correctness and performance of composition process using AI planning. Moreover, the proposed approach by Tabatabaei *et al*. (2010) provides more correctness and performance than the Kuter and Golbeck's work (2009) due to using HTN along with DL. As a result, HTN-DL can be considered as optimized AI planning technique for WSC.

From the security perspective, approaches presented by Kuter and Golbeck (2009) and Liquan *et al*. (2009) are state full approaches. Generally speaking, keeping a past history of service invocations i.e., being state full can be a key feature to support access control for service composition to make suitable access decisions (Liquan *et al*., 2009). Furthermore, authentication is provided through X.509 and service credential in these two works respectively. It should also be noted that the privacy of service credential in the former work needs to be provided. In addition, Maamar *et al*. (2006) claim that their proposed approach supports the integrity to secure WS interactions. Security constraints must be carefully considered during WSC. In this regard, only the presented approaches by Maamar *et al*. (2006) and Tabatabaei *et al*. (2010) take security constraints into account with service composition process. Finally, all the approaches discussed in this comparison proposed prototype to validate their approaches and with regards to definition of validation criterion they marked as "Average".

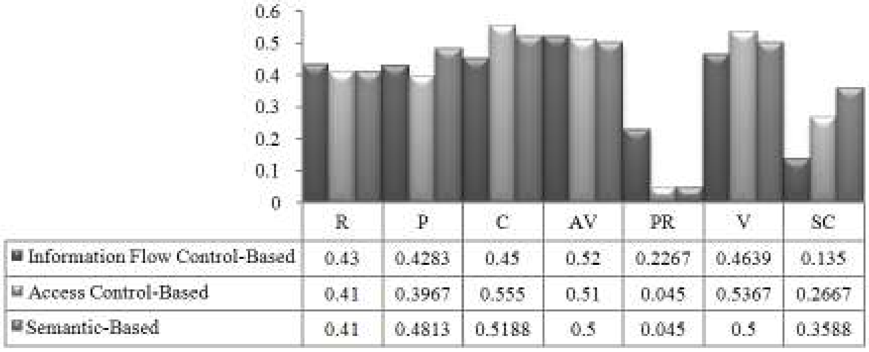
An statistical approach to study security conscious web service composition: In this part, statistical analysis results based on existing data are presented. First statistic technique used is the mean of all 16 characteristics with respect to three categories as presented in Table 8. Comparing among all approaches was done using one way Analysis of Variance (ANOVA) for all criteria. Results of this test (Table 9) indicated a significant difference among Mean score of some criteria including CL, D/S, A, CO, I, AUT and SF/SL at 0.05 level but the other criteria did not show significant differences among approaches (p>0.05). Semantic based approaches are significantly higher than others with respects to CL characteristic. As discussed before, first diagram in Fig. 7 proves that semantic based approaches support much more automation and dynamism in service composition compared to other approaches.



	CL	SCL	D/S	A
▪ Information Flow Control-Based	0.3617	0.4733	0.1261	0.2072
▪ Access Control-Based	0.3172	0.4461	0.0856	0.1278
▪ Semantic-Based	0.6287	0.255	0.545	0.5638



	Co	I	AU	AUT	SF/SL
▪ Information Flow Control-Based	0.3106	0.2078	0.2217	0.255	0.255
▪ Access Control-Based	0.045	0.045	0.3578	0.3728	0.3367
▪ Semantic-Based	0.045	0.0675	0.2725	0.255	0.3775



	R	P	C	AV	PR	V	SC
■ Information Flow Control-Based	0.43	0.4283	0.45	0.52	0.2267	0.4639	0.135
■ Access Control-Based	0.41	0.3967	0.555	0.51	0.045	0.5367	0.2667
■ Semantic-Based	0.41	0.4813	0.5188	0.5	0.045	0.5	0.3588

Fig. 7: Difference level of means between three groups

Table 8: Mean of criteria for approaches

	Criteria							
Group	CL	SCL	D/S	A	CO	I	AU	AUT
Information flow Control-based	0.3617	0.4733	0.1261	0.2072	0.3106	0.2078	0.2217	0.2550
Access control-based	0.3172	0.4461	0.0856	0.1278	0.0450	0.0450	0.3578	0.3728
Semantic-based	0.6287	0.2550	0.5450	0.5638	0.0450	0.0675	0.2725	0.2550
Group	SF/SL	R	P	C	AV	PR	V	SC
Information flow Control-based	0.2550	0.4300	0.4283	0.4500	0.5200	0.2267	0.4639	0.1350
Access control-based	0.3367	0.4100	0.3967	0.5550	0.5100	0.0450	0.5367	0.2667
Semantic-based	0.3775	0.4100	0.4813	0.5188	0.5000	0.0450	0.5000	0.3588

Table 9: ANOVA table

Criterion	M.S.	F-value	p-value
CL	0.141	49.365	0
SCL	0.070	2.422	0.116
D/S	0.319	18.177	0
A	0.271	9.460	0.001
CO	0.188	13.296	0.000
I	0.065	4.414	0.027
AU	0.042	0.860	0.439
AUT	0.037	5.084	0.017
SF/SL	0.026	2.735	0.090
R	0.001	0.702	0.508
P	0.010	0.719	0.500
C	0.025	3.094	0.069
AV	0.001	0.569	0.575
PR	0.088	2.807	0.086
V	0.012	1.273	0.303
SC	0.080	2.854	0.082

M.S.: Mean square

Table 10: Total variance explained

Total variance explained			
Rotation sums of squared loadings			
Component	Total	% of variance	Cumulative (%)
1	3.887	22.468	22.468
2	3.524	17.716	40.184
3	2.257	15.472	55.655
4	1.696	12.419	68.074
5	1.379	11.571	79.645

According to the presented diagrams in Fig. 7, the most level of confidentiality is provided by information flow-control based while access control-based approaches provide much more authentication and authorization compared to other categories. The second statistical analysis utilized in this work is factor analysis. The role of factor analysis is describing variability between observed, correlated variables considering unobserved latent variables called factors. The number of criteria used to evaluate service composition approaches reduced from 16 parameters to 5 linear functions where previous parameters are classified in those five dimensions based on their similarity and co-linearity. Varimax rotation was applied for clearing all dimensions and an examination of the Kaiser-Meyer in measure of sampling adequacy suggested that the sample was factorable (KMO = 0.347). The initial Eigen values presented that the first factor explained 22.468% of the variance and the second, third, fourth and fifth factor 17.716, 15.472, 12.419 and 11.571% of the variance, respectively. As indicated in Table 10, the most important function is the first one called “Accountability and Accuracy” explained 22.46% of the variance. A brief explanation for each factor is provided below.

First of all, three criteria loaded onto Factor 1 which is labeled “Accountability and Accuracy”. As it can be clearly seen from Table 11, these four criteria relate to level of correctness and validation provided by approach as well as countermeasure proposed for authentication and authorization. Three criteria load onto a second factor labeled as “Automation and Dynamism” relate to automatic and dynamic composition and the composition language used in approach. After that, the four criteria that load onto Factor 3 relate to confidentiality level, being stateless or

Table 11: Rotated component matrix

	Component				
Criteria	Accountability and accuracy	Automation and dynamism	Secrecy and security controls	Credibility and privateness	Productivity and accessibility
C	0.873				
AU	0.861				
V	0.765				
AUT	0.763				
D/S		0.924			
A		0.871			
CL		0.862			
Co			0.739		
SF/SL			-0.734		
SC			-0.684		
SCL			0.646		
R				0.887	
PR				0.809	
AV					0.928
P					0.724
I					

Extraction method: Principal component analysis; Rotation method: Varimax with Kaiser normalization: Rotation converged in 7 iterations

stateful, proposed security constraints and the language used to define those security constraints. This factor is labelled as “Secrecy and Security Controls”. Next factor i.e., forth factor is labeled as “Credibility and Privateness” which two criteria including privacy and reliability load onto it. Lastly, criteria loaded for Factor 5 relates to level of performance and availability in an approach and this factor is labeled as “Productivity and Accessibility”. According to the rotated component matrix depicted in Table 11, the most important factor in security evaluation does “Accountability and Accuracy” comprise Correctness (C), Authentication (AU), Validation (V) and Authorization (AUT) parameters. It can be concluded that all 16 criteria categorized in these five factors (dimensions) have overall 79.645% effect on security evaluation. That is, there are some other effective factors on security evaluation which are unknown for us in this study.

DISCUSSION

A comparative evaluation of state-of-the-art security conscious WSC approaches with respects to all categories of WSC taxonomy is proposed. In this section, it is tried to highlight the most salient advantages and strengths of evaluated approaches to achieve (guideline) principle for researchers to evaluate service composition approaches and take advantages of this evaluation to enhance strengths and lessen deficiencies of desired approach.

The approaches with the highest achieved rank are selected as the best representative of each classification. The approaches proposed by Gilmore *et al*. (2010), Cheikh *et al*. (2006) and Tabatabaei *et al*. (2010) are picked out as the representative of information flow control-based, access control based and semantic-based category, respectively. Considering the obtained results with respect to being dynamic and automatic service composition, it can be claimed that applying formal methods has a significant impact to support these characteristics. Applying formal methods along with UML by Gilmore *et al.* (2010) not only supports automatic and dynamic composition but enhance the level of correctness and reliability. Cheikh *et al*. (2006) propose PDL (mathematic based language) to provide automation, dynamism and high level of correctness in composition process. Moreover, being semantic helps to support dynamic composition (such as proposed work by Tabatabaei *et al*. (2010)). Generally speaking, employing formal methods in service composition offers several advantages as follows: It enhances the correctness and reliability of service composition regardless of being syntactic or semantic; it improves the level of automation and dynamism; and it provides strong validation for service composition because of its being intrinsic mathematic-based. Regarding the composition language, it is recommended orchestration and choreography are considered together in service composition such as work proposed by Tabatabaei *et al*. (2010). This work uses WSMO as semantic solution to support this issue, whereas those two works employ BPEL to address it. In fact, lack of semantic leads to impede the effectiveness of the compatibility computing among the policies and causes some restrictions for service selection (Charfi and Mezini, 2007). As a result, it can be taken as deficiency into account for those approaches which apply no semantics.

With respects to security issues, only Cheikh *et al*. (2006) specify security constraint language while Tabatabaei *et al*. (2008) propose security constraints including goal, choreography and orchestration constraints. To gain the real power of security in service composition, it is advised to address its aspects as much as possible. As an instance, the security aspects are addressed in the aforementioned approaches comprises confidentiality, integrity, authentication and

Appendix: Studies included in this study (Table 6, 7)

ID	Reference	ID	Reference
[1]	Garcia and Felgar de Toledo (2008)	[12]	Koshutanski and Massacci (2005)
[2]	Biskup *et al*. (2007)	[13]	Ji *et al*. (2007)
[3]	Singaravelu and Pu (2007)	[14]	She *et al*. (2009)
[4]	Chafle *et al*. (2005)	[15]	Cheikh *et al*. (2006)
[5]	Gilmore *et al*. (2010)	[16]	Srivatsa *et al*. (2007)
[6]	Chevalier *et al*. (2008)	[17]	Rossebø and Bræk (2006)
[7]	Charfi *et al*. (2005)	[18]	Rouached and Godart (2007)
[8]	Boger *et al*. (2009)	[19]	Tabatabaei *et al*. (2010)
[9]	Carminati *et al*. (2007)	[20]	Liquan *et al*. (2009)
[10]	Emig *et al*. (2007)	[21]	Maamar *et al*. (2006)
[11]	Paci *et al*. (2008a)	[22]	Kuter and Golbeck (2009)

authorization. It is worth noting that credential based authentication and authorization such as provided by Cheikh *et al*. (2006) and Tabatabaei *et al*. (2010) is more powerful than username and password styled ones like proposed work by Gilmore *et al*. (2010). Moreover, being stateful can facilitate security through keeping previous records but none of those aforementioned approaches are stateful. Besides, data encryption has an apparent effect on supporting privacy (like work presented by Gilmore *et al*. (2010)).

Furthermore, AI-Planning techniques outperform service composition performance (like work proposed by Tabatabaei *et al*. (2010)). As it is discussed before, HTN-DL is most preferred AI-Planning based techniques since it significantly improves the correctness and performance of service composition. Utilizing UML-based techniques in service composition also leads to enhance the level of correctness and performance (such as proposed approach by Gilmore *et al*. (2010)). In addition, applying formal methods as utilized by latter approach and proposing programming by Cheikh *et al*. (2006) and Tabatabaei *et al*. (2010) support validity of service composition approach, however stronger validation is provided by the former technique compared to the latter one.

CONCLUSION

Web service composition has been gained lots of attentions since emerging service computing. The importance of this issue is highlighted whenever users' desires have not been satisfied by single services. In such situations, it is needed to be a new added value service which can satisfy service consumers' request. The raison d'être of service composition is to address such scenarios. Besides, security has been investigated from the emergence of service computing as an inevitable factor to adopt service based business applications. Security conscious service composition is a challenging demand which tries to address security issues between candidate service components, service composer and service users. In this regard, there is a lack of appropriate and comprehensive review on investigating the role of security along with QoS in Web services composition. This study presents a comparative evaluation of state-of-the-art approaches in security conscious service composition. A taxonomy of service composition approaches is introduced and each classification of the proposed taxonomy including their respective approaches is illustrated in details. The new security-aware evaluation formulation is proposed. In order to do that, evaluation criteria with respect to service composition, QoS and security are gathered and defined mathematically by means of decision making techniques. The classified approaches are evaluated as "Low", "Average" and "High" with respects to those criteria. The statistical analysis results prove that the proposed evaluation formula works properly and can be considered as principle to help researchers to evaluate the service composition approaches from security and QoS points of views. They indicate that proposed formula considers the effective factors with approximately confidence 80%. There are several directions for future work to further enhance evaluation formulation. One thread in our future work can be looking into other non-functional aspects in WSC such as trust for the proposed formula.

ACKNOWLEDGMENT

This research is supported by the SERG group of RMC-RAKE, Universiti Teknologi Malaysia (UTM) under Vote No: 01J56/00H68. We wish to thank Mahmoud Danaee for his assistance and constructive suggestions to enhance the quality of this paper.

REFERENCES

Agarwal, S., B. Sprick and S. Wortmann, 2004. Credential based Access Control for Semantic Web Services, pp: 44-52. Retrieved from: citeseerx.ist. psu. edu/view doc/download? doi...1... -United States.

Bajaj, S., D. Box, D. Chappell, F. Curbera, G. Daniels, P. Hallam-Baker, M. Hondo, C. Kaler, D. Langworthy and A. Nadalin, 2006. Web Services Policy 1.2-framework (WS-policy). W3C Member Submission, April 25, 2006. Retrieved from: www.w3.org/Submission/WS-Policy/.

Bertino, E., J. Crampton and F. Paci, 2006. Access control and authorization constraints for WS-BPEL. Proceeding of the International Conference on Web Services (ICWS '06).

Bertino, E., L. Martino, F. Paci and A. Squicciarini, 2009. Security for Web Services and Service-oriented Architectures. Springer-Verlag Inc., New York.

Bhatti, R., E. Bertino and A. Ghafoor, 2005. A trust-based context-aware access control model for web-services. Distrib. Parallel Dat., 18: 83-105.

Biskup, J., B. Carminati, E. Ferrari, F. Muller and S. Wortmann, 2007. Towards secure execution orders for composite web services. Proceeding of the IEEE International Conference on Web Services (ICWS 2007).

Boger, D., J. Fraga, P. Mafra and M. Wangham, 2009. A model to verify quality of protection policies in composite web services. Proceeding of the World Conference on Services-I.

Brahim, M., B. Athman and K.E. Ahmed, 2003. Composing web services on the semantic web. VLDB J., 12: 333-351.

Carminati, B., E. Ferrari, R. Bishop and P.C.K. Hung, 2007. Security conscious web service composition with semantic Web support. Proceeding of the IEEE 23rd International Conference on Data Engineering Workshop, pp: 695-704.

Chafle, G., S. Chandra, V. Mann, M.G. Nanda and I.C. Soc, 2005. Orchestrating composite web services under data flow constraints. Proceedings of the 2005 IEEE International Conference on Web Services (ICWS 2005).

Charfi, A. and M. Mezini, 2007. Ao4bpel: An aspect-oriented extension to bpel. World Wide Web, 10: 309-344.

Charfi, A., M. Mezini and I.C. Soc, 2005. Using aspects for security engineering of web service compositions. Proceedings of the 2005 IEEE International Conference on Web Services (ICWS 2005).

Cheikh, F., G. de Giacomo and M. Mecella, 2006. Automatic Web Services Composition in Trustaware Communities. Retrieved from: citeseerx.ist.psu. edu/viewdoc/download? doi...1...-United States.

Chen, S.J.J., C.L. Hwang, M.J. Beckmann and W. Krelle, 1992. Fuzzy Multiple Attribute Decision Making: Methods and Applications. Springer-Verlag Inc., New York.

Chevalier, Y., M.A. Mekki and M. Rusinowitch, 2008. Automatic composition of services with security policies. Proceedings of the IEEE Congress on Services Pt I, pp: 529-537.

Dersingh, A., R. Liscano, A. Jost, M. Ahmad, V. Saxena, K. Kurn, M. Baumgarten, M. Mulvenna, K. Greer and C. Nugent, 2008. Context-aware access control using semantic policies. Ubiquitous Comput. Commun. J. (UBICC) Special Issue on Autonomic Computing Systems and Applications, 3: 19-32.

Dillon, L.K., A.K. Richard and S. Sankar, 1997. Special issue on formal methods in software practice. IEEE T. Softw. Eng., 23(5).

Emig, C., F. Brandt, S. Abeck, J. Biermann and H. Klarl, 2007. An access control metamodel for web service-oriented architecture. Proceeding of International Conference on Software Engineering Advances (ICSEA 2007), pp: 57.

Foerster, T., J.M. Morales and J.E. Stoter, 2008. A classification of generalization operators formalised in OCL. Proceedings of the 6th Geographic Information Days, 32: 141-156.

Garcia, D.Z.G. and M.B. Felgar de Toledo, 2008. Ontology-based security policies for supporting the management of web service business processes. Proceeding of the IEEE International Conference on Semantic Computing, Aug. 4-7, pp: 331-338.

Gilmore, S., L. Gönczy, N. Koch, P. Mayer, M. Tribastone and D. Varró, 2010. Non-functional properties in the model-driven development of service-oriented systems. Softw. Syst. Model., 10(3): 287.

Hristoskova, A., B. Volckaert and F. De Turck, 2009. Dynamic composition of semantically annotated web services through QoS-aware HTN planning algorithms. Proceeding of 4th International Conference on Internet and Web Applications and Services (ICIW '09), pp: 377-382.

IBM and Microsoft, 2002. Security in a Web Services World: A Proposed Architecture and Roadmap. IBM, Microsoft.

Ji, G.F., Y. Tang, F. Huang, P. Wang and G.B. Wu, 2007. An Access Control Model for Service Composite. Proceedings of the 11th International Conference on Computer Supported Cooperative Work in Design, 1-2: 852-857.

Ji-Bo, D. and H. Fan, 2003. Task-based access control model. J. Softw., 14: 76-82.

Jian Feng, Z. and R. Kowalczyk, 2006. Agent-based Dis-graph planning algorithm for web service composition. Proceeding of International Conference on Computational Intelligence for Modelling, Control and Automation, 2006 and International Conference on Intelligent Agents, Web Technologies and Internet Commerce. Nov. 28-Dec. 1, pp: 258.

Kerschbaum, F. and P. Robinson, 2009. Security architecture for virtual organizations of business web services. J. Syst. Architect., 55: 224-232.

Klarl, H., F. Marmé, C. Wolff, C. Emig and S. Abeck, 2009. An MDA-based environment for generating access control policies. Comput. Inform. Sci., 5695: 115-126.

Koshutanski, H. and F. Massacci, 2005. Interactive credential negotiation for stateful business processes. Hermann, P., V. Issarny and S. Shiu (Eds.), Proceedings of the 3rd International Conference onTrust Management.

Kuter, U. and J. Golbeck, 2009. Semantic web service composition in social environments. Proceedings of the Semantic Web- Iswc 2009, 5823: 344-358.

Lee, T., J. Hendler and O. Lassila, 2001. The semantic web. Sci. Am., 284: 34-43.

Liquan, H., X. Zhongyu and Y. Qing'an, 2009. An Approach to web service composition based on service-ontology. Proceeding of the 6th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD '09), pp: 173-177.

Maamar, Z., N.C. Narendra and S. Sattanathan, 2006. Towards an ontology-based approach for specifying and securing web services. Inform. Softw. Technol., 48: 441-455.

Malik, Z. and A. Bouguettaya, 2009. Trust Management for Service-oriented Environments. Springer, US.

Mokhtar, S., D. Fournier, N. Georgantas and V. Issarny, 2006. Context-aware service composition in pervasive computing environments. Lect. Notes Comput. Sc., 3943: 129-144.

Movahednejad, H., S.B. Ibrahim, M. Sharifi, H.B. Selamat and S.G.H. Tabatabaei, 2011. Security-aware web service composition approaches: State-of-the-art. Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services. Ho Chi Minh City, Vietnam, ACM.

Paci, F., E. Bertino and J. Crampton, 2008a. An access-control framework for WS-BPEL. Int. J. Web Serv. Res., 5: 20-43.

Paci, F., R. Ferrini and E. Bertino, 2009. Identity attribute-based role provisioning for human WS-BPEL processes. Proceeding of the IEEE International Conference on Web Services (ICWS 2009).

Paci, F., R. Ferrini, Y.Q. Sun and E. Bertino, 2008b. Authorization and user failure resiliency for WS-BPEL business processes. Proceedings of the 6th International Conference on Service-oriented Computing (ICSOC 2008).

Ramakrishnan, R. and A. Tomkins, 2007. Toward a PeopleWeb. Computer, 40: 63-72.

Rao, J. and X. Su, 2005. A survey of automated web service composition methods. Lect. Notes Comput. Sc., 3387: 43-54.

Rossebø, J. and R. Bræk, 2006. A policy-driven approach to dynamic composition of authentication and authorization patterns and services. J. Comput., 1: 13.

Rouached, M. and C. Godart, 2007. Reasoning about events to specify authorization policies forweb services composition. Proceeding of the IEEE International Conference on Web Services (ICWS 2007). July 9-13, pp: 481-488.

She, W., I. Yen, B. Thuraisingham and E. Bertino, 2009. The SCIFC model for information flow control in web service composition. Proceeding of the IEEE International Conference on Web Services (ICWS 2009), pp: 1-8.

Singaravelu, L. and C. Pu, 2007. Fine-grain, end-to-end security for web service compositions. Proceeding of the IEEE International Conference on Services Computing (SCC 2007).

Sirin, E., 2006. Combining description logic reasoning with ai planning for composition of web services. Ph.D. Thesis, University of Maryland at College Park, College Park, MD, USA.

Sirin, E., B. Parsia, D. Wu, J. Hendler and D. Nau, 2004. HTN planning for web service composition using SHOP2. J. Web Semantics, 1: 377-396.

Sivasubramanian, S.P., E. Ilavarasan and G. Vadivelou, 2009. Dynamic web service composition: Challenges and techniques. Proceeding of International Conference on Intelligent Agent and Multi-Agent Systems (IAMA 2009), July 22-24, pp: 1-8.

Sodiya, A., A. Onashoga and N. Abeokuta, 2009. Components-based access control architecture. Issues Inform. Sci. Inform. Technol., Vol. 6.

Srivatsa, M., A. Iyengar, T. Mikalsen, I. Rouvellou and J. Yin, 2007. An access control system for web service compositions. Proceeding of the IEEE International Conference on Web Services (ICWS 2007). Salt Lake City, UT, pp: 1-8.

Tabatabaei, S.G.H., W.M.N. Kadir and S. Ibrahim, 2008. Semantic web service discovery and composition based on AI planning and web service modeling ontology. Proceeding of the IEEE Asia-Pacific Services Computing Conference (APSCC '08). Dec. 9-12, pp: 397-403.

Tabatabaei, S., A. Dastjerdi, W. Kadir, S. Ibrahim and E. Sarafian, 2010. Security conscious AI-planning-based composition of semantic web services. Int. J. Web Inform. Syst., 6: 203-229.

Ter Beek, M., A. Bucchiarone and S. Gnesi, 2007. Web service composition approaches: From industrial standards to formal methods. Proceeding of the 2nd International Conference on Internet and Web Applications and Services (ICIW '07). May 13-19, pp: 15.

Thomas, R. and R. Sandhu, 1998. Task-Based Authorization Controls (TBAC): A family of models for active and enterprise-oriented authorization management. Database Security, 11: 166-181.

Timm, J. and G. Gannod, 2005. A model-driven approach for specifying semantic web services. Proceeding of IEEE International Conference on Web Services (ICWS 2005), pp: 313-320.

Timm, J.T.E. and G.C. Gannod, 2007. Specifying semantic web service compositions using UML and OCL. Proceeding of IEEE International Conference on Web Services (ICWS 2007), July 9-13, pp: 521-528.

Van Der Aalst, W., 2005. Pi calculus versus petri nets: Let us eat" humble pie" rather than further inflate the" pi hype". BP Trends, 3: 1-11.

Xiaochuan, Y. and K.J. Kochut, 2004. A CP-nets-based design and verification framework for Web services composition. Proceeding of IEEE International Conference on Web Services, July 6-9, pp: 756-760.

Xu, D.H., Y. Qi, D. Hou, G.Z. Wang and Y. Chen 2008. A novel formal framework for secure dynamic services composition. Proceeding of the 8th IEEE International Conference on Computer and Information Technology. Sydney, NSW, pp: 694-699.

Yuan, E. and J. Tong, 2005. Attributed based access control (ABAC) for Web services. Proceedings of the IEEE International Conference on Web Services, (ICWS 2005).

Zhengdong, Z., L., Ronggui, M. Ruifang and C. Yanping, 2009. Describing and verifying semantic web service composition with MDA. Proceeding of International Conference on E-business and Information System Security (EBISS '09), May 23-24, pp: 1-6.

Zhu, J.Q., Y. Zhou and W.Q. Tong, 2006. Access control on the composition of Web services. Proceedings of the International Conference on Next Generation Web Services Practices (NWeSP 2006). Seoul, pp: 89-93.