I.J. Modern Education and Computer Science, **2016, 10, 49-55**
Published Online October 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2016.10.07

Web Services Privacy Preserving Based on Negotiation and Certificate Authorities

A. Meligy
Math and Computer Science Department, Faculty of Science, Menoufia University, Egypt
Email: meligyali@hotmail.com

Emad Elabd
Information System Department, Faculty of computers and Information, Menoufia University, Egypt
Email: emadqap@gmail.com

Sahar Kotb
Math and Computer Science Department, Faculty of Science, Menoufia University, Egypt
Email: soso.kotb@gmail.com

***Abstract*—**Nowadays, Web services are the leading solution for solving the problem of information systems' integration. Web services are based on the service oriented architecture (SOA). Preserving privacy of web services is one of the main challenges during their interaction. Therefore, minimizing the number of the disclosed credentials that are required for accessing the web services resources during the interaction is a desirable behavior. Credentials generalization and substitution and credentials encryption can be used for privacy preserving. To the best of our knowledge, in the current privacy preserving approaches for web services, there is no technique that uses the negotiation for credential generalization and substitution between the consumer and the provider in conjunction with the credentials encryption using certificate authority as a third party. In this paper, a proposed approach for web services privacy preserving is proposed. This approach is based on the negotiation, encryption, and certificate authorities as third parties. The proposed approach is implemented and tested. The results show that the number of disclosed sensitive credential is the minimum number of credentials that can be disclosed to guarantee the accessing of the service.

***Index Terms*—**Web services (WS), Service oriented architecture (SOA), Privacy, Negotiation.

I. Introduction

Recently, the web services are widely used in many fields to perform easily and fast a lot of tasks. More and more e-learning, electronic and agile businesses, e-commerce and e-governance projects tend to apply Web services to build systems. Dozens of people can share by their sensitive information to perform tasks through web services. Generally, web service is identified by URL just like any other website, but the different is the type of interaction that they can provide. It is a software application that can be accessed remotely using XML-based languages. XML [1] provides a language which can be used between different platforms and programming languages and still express complex messages and functions and the HTTP protocol is the most used Internet protocol. These services have two types of uses: Reusable application-components that can offer application-components (like currency conversion, weather reports, or even language translation as services) and Connect existing software that can help to solve the interoperability problem by giving different applications a way to link their data.

The Web services is defined as software designed to support interoperable machine-to-machine interaction over a network by W3C. Its interface is described in a machine-process able format called Web Services Description Language (WSDL). In other words, it is a software application that provides business functionality or information to other applications through an Internet connection using different XML-based languages such as Universal Description Discovery and Integration (UDDI), Web Services Description Language (WSDL), and Simple Object Access Protocol (SOAP). SOAP, WSDL and UDDI are the platform elements of web service [2]. These web languages are designed to define standards for service discovery, description, and messaging protocols.

In some situation, services (consumers and providers) are prone to attack by corrupted ones. Due to the features of web services, it is not easy to guarantee the reliability of the services in cooperation, thus it is possible for consumer's sensitive information to be collected or disclosed illegally [3]. Privacy refers to the ability of users to control the collection, use, retention and distribution of themselves [4]. In order to meet the needs of privacy, a strict control mechanism is required to protect the consumer's private data.

Privacy in web services is one of the most important challenges that many researches concentrate on it. In most web services systems, sensitive information is required to access these services. We focus on solving this problem by

using negotiation among services to reduce the information and using encryption technique to encrypt the rest of the credentials that have not certificate authorities as a third parties.

The current privacy preserving techniques for web services do not study the effect of using the negotiation for credential generalization and substitution between the consumer and the provider in conjunction with the credentials encryption using certificate authority as a third party. The main contribution of this paper is a proposal of an approach for minimizing the privacy disclosure. This approach is based on the negotiation, encryption, and certificate authorities as third parties.

The remainder of the paper as follows: Section II discusses the related works that handle the privacy problem in web services. Section III illustrates the proposed approach with an example of a web service online shopping. Section IV presents the implementation and the analysis of the proposed approach. The conclusion and future work are list in Section V. Finally, the references are list.

II. Related Work

Many of works discussed the web services security and privacy through many technologies and latest mechanisms[4,5,6,7,8,9,10,11, 12]. A set of these approaches concentrates on securing the Web services resources [6,7] and the other approches are related to preserving privacy in Web services[4,8,9,10,11,12,13].

Jiang at al. [6] developed an enhanced mechanism to secure the web services based systems, especially; to secure accesses of Web resources. This mechanism is based on the combination of these modules (Identity Authentication, Authorized Access and Secure Transmission) to improve the web service systems. In that paper, they studied one of web service systems called VeePalms which is a representative web service based system that provides multi-discipline virtual experiments for massive learners. It also faced diverse web security vulnerabilities such as illegal changes of the experimental data, falsifications of students' experimental scores and important resources exposed to unauthenticated users. To solve these weaknesses, they gave an overview on two points: the web services security and access control level.

Kabir et al. [7] explained and developed a Conditional Purpose-Based Access Control (CPBAC) model where more information can be extracted while preserving privacy at the same time. It allows users to associate some data with certain conditions and multiple purposes with each data element. To expand the CPBAC with RBAC, they implemented the extension of CPBAC with roles that are called Role-involved purpose-based access control (RPAC). In this paper, they help enterprises to circulate a clear privacy promise and to collect and manage the user preferences.

Squicciarini et al. [8] study the privacy implications due to the exchange of large amount of potentially sensitive data required by optimized strategies for service-discovery. They present a comprehensive framework to uniformly protect users' and service providers' privacy requirements, at the time of service discovery. They provide a solution that allows matching of the search criteria against the Web services attributes in a private fashion such that both criteria and service attributes are kept private during the matching. In addition, they propose an approach to protect service provisioning rules from unwanted disclosure, both from the user and the service provider's perspective.

Tbahriti et al. [9] propose a formal privacy model to extend DaaS descriptions with privacy capabilities. The service can define the privacy policy and a set of privacy requirements and policies in DaaS composition. The negotiation mechanism is proposed that makes it possible to dynamically reconcile the privacy capabilities of services when incompabilities arise in a composition. They studied the PAIRSE project that is supported by French National Research. It deals with the privacy preservation issue in P2P data sharing environment. The privacy model is described for DaaS. Every service has a privacy policy and privacy requirements. They defined two privacy levels: data and operation. The data deals with data privacy, but the operation copes with the privacy about operation's invocation. The sensitivity of a resource may be defined according to several dimensions called privacy rules. They define its rule by a topic, domain, level and scope. The services will use privacy rules to define the privacy features of their resources.

Linyuan Liu et al. [5] explain how to satisfy the minimal privacy disclosure while achieving the functional objectives through role mechanisms. To do this, first they proposed a revised role-based framework for privacy-aware services collaborations to effect on the reputation degree, then they designed the privacy behaviors of services by extending the interface automata to support privacy semantics. They proposed and applied a revised role-based framework for privacy-aware services collaborations (RBPSC) through the minimal privacy delegation. They applied the reputation degrees in addition to the interface automata.

Yee et al. [4] designs privacy controllers together with user privacy policies in order to protect privacy. But they do not addresses the issue of enforcing privacy that confirms to emerging industry standards.

Li et al. [10] present a graph-transformation based framework to check whether an internal business process that is implemented using the Web service composition language BPEL adheres to the organization's privacy policies. There framework combines the advantages of an intuitive visual framework with rigorous semantically foundation that allows consistency checking between a business process and privacy policy. They use set of rules to build the system state for the privacy consistency verification framework.

Aldhafferi et al. [13] presented a study that can be used as a base for developing a new privacy system which will help users control their personal information in an easy way from different devices, including mobile Internet devices and computers. Their results show that the majority the use of smart phones for web services but the

current privacy settings for online social networks need to be improved to support different type of mobile phones screens.

Padam Gulwaniet al. [14] studied the privacy preservation problem in database caused by data mining technology and proposed an approach for hiding sensitive data in association rules mining.

Emad and Hacid [15] investigate the impact of users' profiles and previously issued queries by the users in case of concurrent queries on the privacy in location based services. Then, they present an approach for privacy presering of the user information in the location based services.

III. The Proposed Approachr

The proposed approach aims to reduce the set of disclosed credentils the minimum number during Web services interaction based on trust negotiation and encryption techniques.

In the traditional interaction process between two Web services, the consumer satisfies the policies that are required for accessing the provider's resources when the authentication and authorization are achieved. The proposed model attemps to achieve the provider's policies through the negotiation and encryption of the unavoidable sensitive credentials based on a third party. The third party is the certificate authority(CA) issuer. For instance, the banks are the certificate authorities for credit cards and the edutctional insituties including universities are the certificate authorities for the graduation certificates credentials.

The negotiation between the consumer and the provider in the proposed approach is based on two main privacy preserving approaches: substitution and generalization. Substitution replaces the credential with another one that has less or non-sensitive information but may provide the required information for the provider. Generalization replaces the credential with another none that contains more general information that the original credentials. Fig. 1 represents the proposed model.

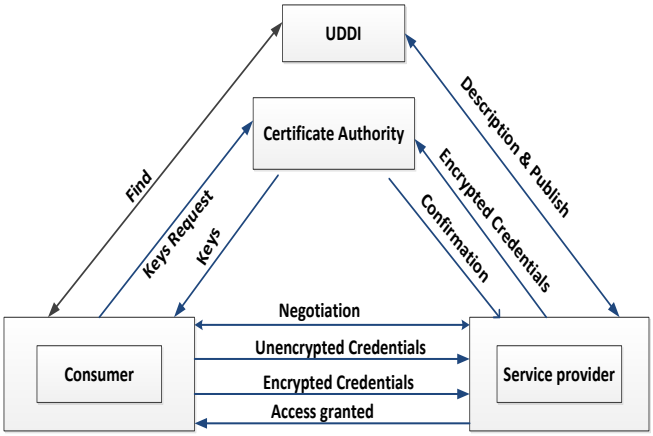

Fig.1. Proposed model

Fig. 1 shows the proposed model which is based on the SOA. The proposed approach is designed for privacy preserving for mimimum policies and credentials disclosure based on negotiation. This model consists of four partenetrs: Web service provider, Consumer, Third party, and UDDI. The Web service provider offers the services to consumers. These services or resources have a set of access policies. The consumer can access the services (resources) using his credentials. The credentials of the consumer or the provider may have disclosure policies. For instance, a credit-card credential may have a policy say that "Certificate from the issuer bank" which states that the only person who has a certificate from the credit-card issuer bank can see the credit-card credential. Therefore, the service provider and consumer may have resources and policies. The third party is the certificate issuer and the UDDI is the repository for storing the of functional and non-functional descriptions of Web services.

The proposed approach works as follows : The consumer searches for the required service in the UDDI using the functional and/or non-functional description of the service. A list of services is nominated to the consumer. After that, the consumer starts to select and bind the suitable service provider. Finally, a negotiation process is started between the consumer and the provider for minimal privacy disclosure. This process includes the exchange of policies to create an agreed trusted sequence. During the negotiation process the generalization technique for replacing policies can be used. This generalization increases the privacy level. For instance, if the policy asks for the address and the consumer doesn't want to provide his address in details (flat number, street number, city, country), so he can ask the provider to give him a more general policy which can be his city for example. Then the consumer shows the provider credentials for his city. As shown the generalization technique in this step contributes in preserving privacy of the consumer or provider during the negotiation phase. Besides, the policy substitution can be used for preserving

privacy. In other words, the consumer asks the service provider to provide him with alternative policies for accessing the required resource.

The consumer and the provider starts to exchange the credentials based on the agreed trusted sequence. The consumer can exchange the required credentials with or without encryption. The encryption decision of credntials is based the existence of the credential issuer as a third party and the sensitivty level of the credential in terms of privacy. The sensitivty level of the credential is determined by the consumer. Finally, if the credential is high senstive in terms of privacy and the issuer is exist as a third party then the credential is encrypted using the third party and the consumer. In this situation, the credential issuer encrypts the credential and the consumer sends the encrypted version to the service provider and the service provider forward this encrypted credential to the third part to verify of the correctness of the credentials data. For example, if the bank is one of the third parties then the bank encrypted the consumer credit-card data including the provider data and the required amount of money. The service provider forwards this encrypted message to the bank after assigning his data (name, amount of money required, resource…). The bank will verify the data and perform the operation and inform the service consumer and provider by the results.

As shown in the encryption process that the only two category of the disclosed credential are the credential with low sensitively in terms of privacy and the credentials that have not credentials issuers as third parties and the provider refused the substitution and generalization for them. Therefore, the set of the credentials that are disclosed in the approach is restricted to credential that cannot be avoided (minimum number of credentials disclosure). Fig. 2 shows the detailed flowchart of the proposed approach.

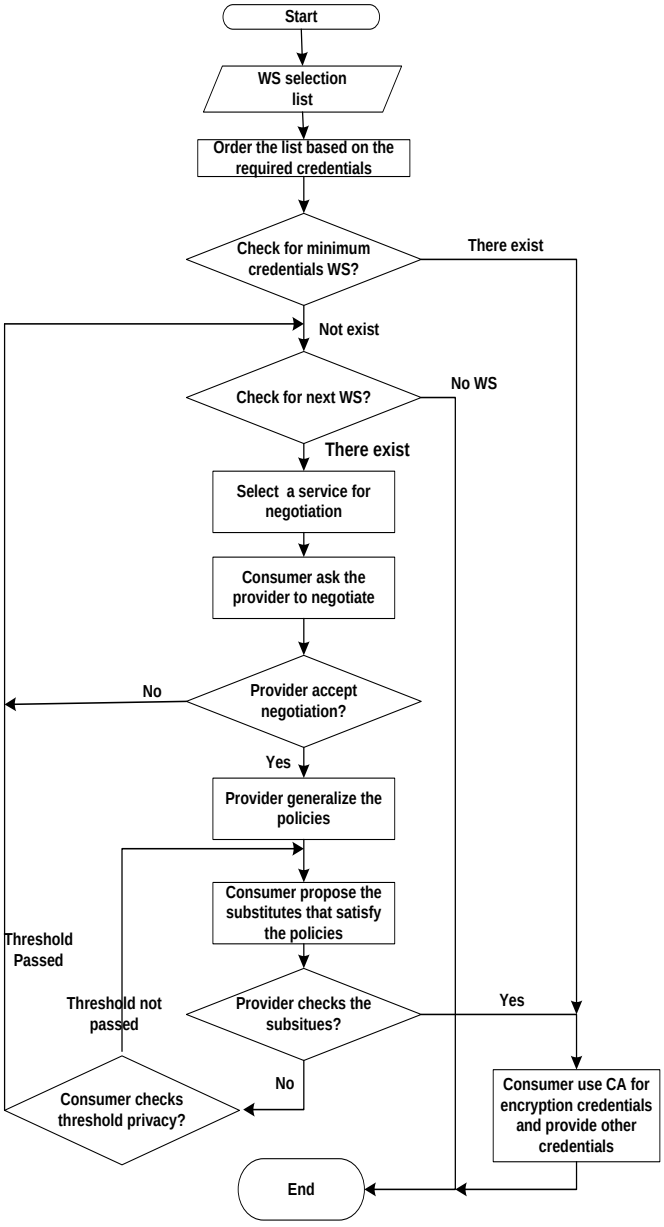

Fig.2. Flowchart of proposed approach

A. An example

An online shopping scenario is an example that can be used to indicate our contribution. In this scenario, there are four web services play roles: buyer, banker, seller and shipper as shown in Fig 3.

The process starts by checking the service that has a minimum credentials from the list that is disclosed and ordered by UDDI. If this service already has the minimum credentials, the buyer will use the certificate authority for encrypted credentials (these credentials that needs the bank such as credit-card details) and provide other credentials; otherwise, the buyer searches for another Web service in the ordered list. If there is another service, the negotiation process starts between the seller and the buyer; otherwise, the connection is terminated.

The negotiation process starts between the Buyer and Seller to agree on a trust sequence. The buyer asks the seller to negotiate; the seller may refuse this negotiation, in this case the buyer will search another one in the list, but if the seller accepts the negotiation, the seller will generalize his policies. After that the buyer proposes the substitutes that satisfy the policies. When the seller accepts the buyer's substitutes, the buyer will send to the bank to encrypt the CA credentials and send the others that the seller can see it. The buyer can not disclose all substitutes to the seller specially the financial information, but the buyer used the encryption to solve this problem, s/he sends a request to the banker to encrypt the credit-card information or bank account details.

If the seller doesn't accept the buyer's substitutes, The buyer checks his threshold privacy level to decide whether s/he will continue of terminate the connection. S/he starts to check if s/he can propose others substitutes, s/he will return to propose the others; otherwise, go to check the order list again for another service.

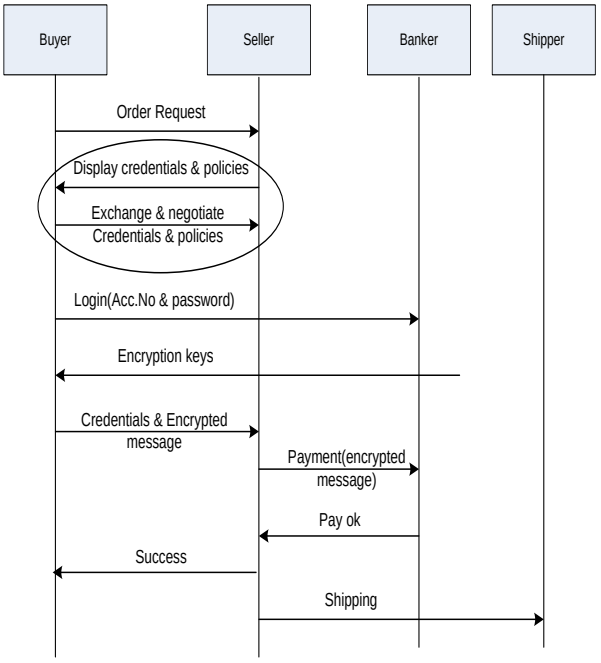

Fig.3. Online Shopping Scenario Transaction

IV. Implementation and Analysis

In order to test the performance of the proposed approach, we have tested a real set of Web services varies between educational web services, online web services and financial web services etc. Each service has a specific policies and substitutes of each policy that are required to satisfy these policies. The consumer can negotiate with the web service if this service accepts the negotiation. Each consumer can accept or refuse these credentials or substitutes according to the sensitivity in his opinion. A consumer may refuse all providers' substitutes that are required, but another one may accept one of them that s/he sees that it is less sensitive one. Using the encryption makes some sensitive credentials looks as non-sensitive credentials because of sending them to the provider in an encrypted form and using negotiation convert sensitive to non-sensitive because of replacing the credentials with general one or substitute of it that doesn't contain more information. There are two types of credentials, the first type is the credentials that have CA as third party and the second one includes the credentials that have not CA.

After testing the proposed approach using the previous data sets, Fig. 4 and Fig. 5 shows the effect encryption technique in the existence of certificate authorities as third parties. In Fig. 4, a comparison between the average percentage of the number of disclosed credentials in the traditional approach and the percentage of the average disclosed sensitive credentials without applying the negotiation is shown. In Fig. 5, a comparison between the percentage of the disclosed credentials in the traditional approach and the percentage of the average encrypted sensitive credentials (i.e., the credentials that have certificate authorities as third parties) without applying the negotiation.

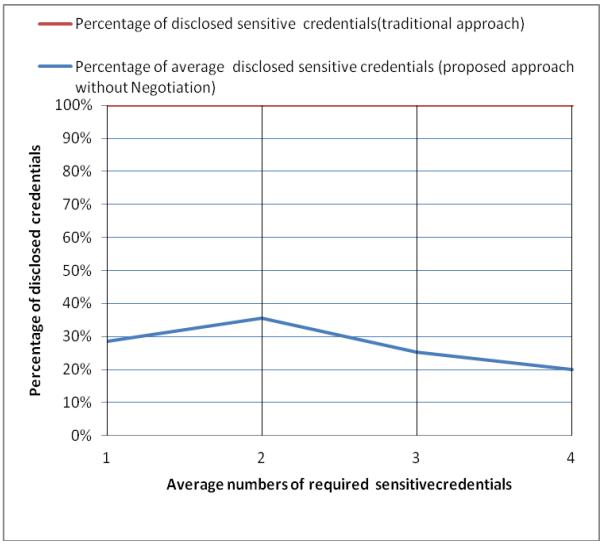

Fig.4. Percentage of disclosed sensitive credentials without applying negotiation.

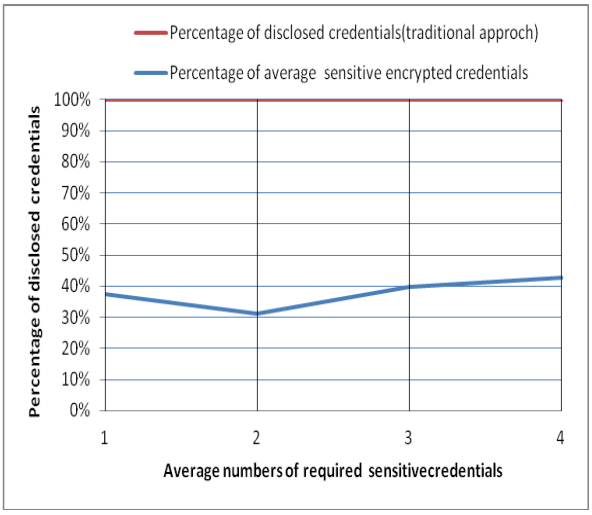

Fig.5. Percentage of undisclosed sensitive credentials without applying negotiation.

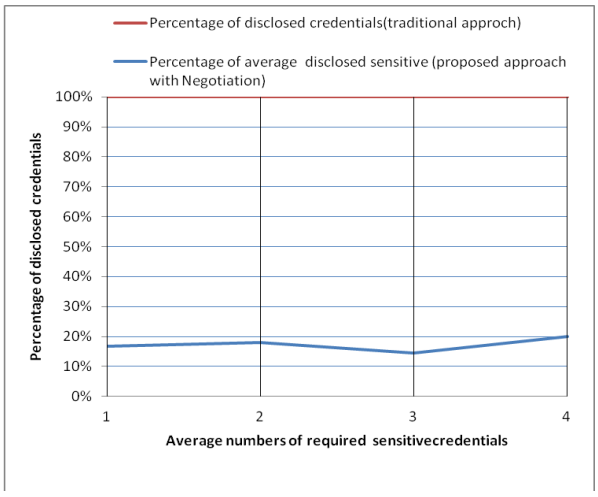

Fig.6. Percentage of disclosed sensitive credentials after applying negotiation.

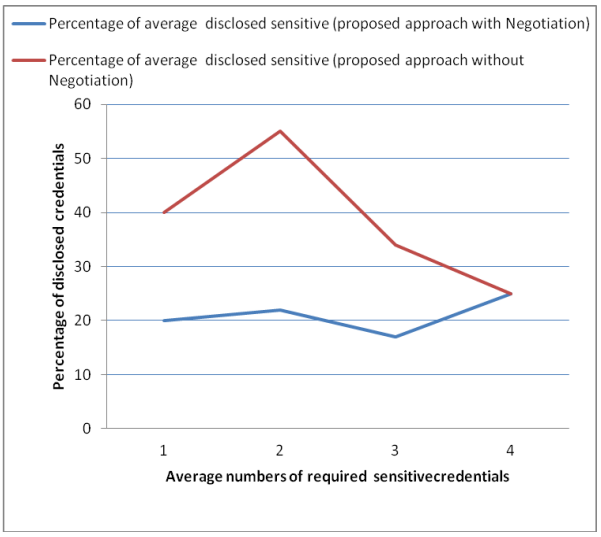

Fig.7. Percentage of disclosed sensitive credentials with and without applying negotiation.

The results in all the previous figures indicate that the proposed approach has a positively effect on the privacy by disclosing only the minimum number of sensitive credentials. The combination between the encryption and the negation which is based on generalization and substitution guarantees a minimal privacy disclosure.

V. Conclusions and Future Work

In this paper, an approach for minimum credentials disclosure of Web services interaction is presented. This approach preseves the privacy between the cooperated Web services. This approach is based on the negotiation and encryption of sensitive credentials in conjunction with certificates authoriies as third parties. The results shows that the new approach provides the minimal privacy disclosure for Web service interaction. In the future work, a formal model is presented and the effect of new parameters such as the time in privacy is tested.

References

[1] Alaa Hussein Al-Hamami, Handbook of Research on Threat Detection and Countermeasures in Network Security. Amman Arab University, J. a.-S. October, 2014.

[2] Stephen Potts, M. K. Web Services in 24 Hours. Sams Publishing. 2003.

[3] Guarda, P. a. Towards the Development of Privacy-aware Systems. Inf. Software. Technol., 51, 337—350, 2009.

[4] Yee, G. O. A privacy controller approach for privacy protection in web services. Proceedings of the 2007 ACM workshop on Secure web services, 44-51.

[5] Liu, L. a. Analysis of the minimal privacy disclosure for web services collaborations with role mechanisms. Expert Syst. Appl., 38, 4540—4549, 2011.

[6] Jiang, W. a. An enhanced security mechanism for web service based systems. Proceedings of the 2012 international conference on Pervasive Computing and the Networked World, 282--296.

[7] Kabir, M. E. A role-involved purpose-based access control model. Information Systems Frontiers, 14, 809—822, 2012.

[8] Squicciarini, A.; Carminati, B.; Karumanchi, S., "A Privacy-Preserving Approach for Web Service Selection and Provisioning," Web Services (ICWS), 2011 IEEE International Conference on, vol., no., pp.33,40, 4-9 July 2011.

[9] Mrissa, S.-E. T. Privacy-Enhanced Web Service Composition. IEEE Transactions on Services Computing, 99, 1, 2013.

[10] Li, Y. H.-Y. Formal consistency verification between BPEL process and privacy policy. Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, 26:1--26:10.

[11] Xu, W. a. A Framework for Building Privacy-Conscious Composite Web Services. Proceedings of the IEEE International Conference on Web Services, 655—662, 2006.

[12] Emad Elabd, Hatem Abdulkader, and Ahmed Mubark. "L–Diversity-Based Semantic Anonymaztion for Data Publishing." I.J. Information Technology and Computer Science (IJITCS), 2015, 10, 1-7.

[13] Aldhafferi, N.; Watson, C. & Sajeev, A. S. M. "Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices", International Journal of Security, Privacy and Trust

Management (IJSPTM) vol 2, No 2, April 2013.
[14] P. Gulwani, "Association rule hiding by positions swapping of support and confidence," International Journal of Information Technology and Computer Science (IJITCS), vol. 4, no. 4, p. 54, 2012.
[15] Emad Elabd, Mohand-Said Hacid:" Concurrent Queries in Location Based Services". International conference of availability, reliability, and security (ARES), University of Fribourg, Switzerland, September 8th - 12th, 2014, 134-139.

Authors' Profiles

Ali M. Meligy a full professor of computer science at the Menoufia University in Egypt. Previously, he was the head of computer science and information technology departments at Al-Hussein Bin Talal University in Jordan. His research interests include parallel processing and applications, distributed systems, Petri nets, and reuse-based software engineering.

Dr. Emad ELABD: An Assistant Professor, Dept. of Information Systems, Menoufia University, Egypt. He got his Ph.D. in the field of Web services compliance over high-level specifications at LIRIS, University Lyon1, France, July 2011. He received bachelor ́s degrees in Electronic Engineering from Menoufia University, Egypt where he did his master ́s studies in computer science also. His research interests include Web services modeling and analysis with access control and time aspects, Web services (specification, composition), Semantic Web, and Information retrieval.

Sahar Kotb a Master student at Menoufia University. She received bachelor ́s degrees in Computer science from Menoufia University, Egypt. Her research interests include Web services security and privacy.