I.J. Information Technology and Computer Science, **2017, 8, 30-39**
Published Online August 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2017.08.04

Extend Web Service Security Negotiation Framework in Privacy

Amira Abdelatey, Mohamed Elkawkagy, Ashraf Elsisi, Arabi Keshk
Faculty of Computers and Information/Computer Science, Menofia University, Egypt
E-mail: {Amira.mohamed, mohamed.elkhawaga, ashraf.elsisi, arabi.keshk}@ci.menofia.edu.eg.

Received: 02 January 2017; Accepted: 25 March 2017; Published: 08 August 2017

Abstract—Nowadays web service privacy gets high attention especially in the fields of finance and medical. Privacy preserves access rights to personally identifiable information. Different models have been proposed for enforcing privacy in web service environment. Getting a privacy level for protecting data transferred between consumer and provider in a web service environment is still a problem. Negotiation helps participants to get a privacy level. This paper extends web service security negotiation framework in a multilateral web service environment for negotiating privacy. A repaired genetic negotiation framework used to conduct the privacy negotiation. In privacy negotiation, the negotiation communication structure uses a broker for negotiation; where each participant sends its attributes to the broker. Negotiation using this communication structure decreases the number of messages transferred so less execution time. The genetic-based Negotiation is compared to traditional time-based negotiation. Through experimental results, genetic based negotiation outperforms traditional time-based negotiation.

Index Terms—Web service privacy, negotiation, SOA message security, web service negotiation, Web service non-functional properties, Quality of Service attributes.

I. Introduction

Web services can provide a suitable platform for application-to-application interactions over the internet. It is important for building flexible, loosely coupled service oriented applications [1]. Web services constrained by Quality of Service (QoS) requirements for its participants [2]. QoS is one of the non-functional attributes of a web service. Consumer and provider of a web service must be agreed on QoS requirements [3, 4]. Negotiating QoS attributes is the way to get an agreement between web service participants [5]. Besides QoS attributes. A security is an important attribute in a web service environment. And an agreement needs to be reached between web service participants.

A traditional time-based negotiation and a genetic-based negotiation methods are proposed to negotiate security levels of a web service [6]. In this paper, we extend the framework used in negotiating security to negotiate privacy levels of web service. Privacy is important for web service participants. Privacy can be defined as; what data items is collected, who can access each data item? For what purpose, and how long data items stored [7]. For instance, a service provider may use clients' data for illegal purposes. So, there is a need for considering the privacy of data transferred from consumer to provider. To the best of our knowledge, only a few researchers have investigated privacy in web service architecture.

We consider a scenario where a bank carries out a marketing using its credit card holders. And the bank would outsource the marketing project to a marketing company. The protection of personal data for customers must be considered in such case [8]. Web service communication between consumer and provider transferred through three layers; application layer, message layer, and network layer. These three layers are presented in Fig. 1. A point-to-point security of Simple Object Access Protocol (SOAP) messages (the network layer) transferred between bank and marketing company provider is already maintained using network protocols [9]. In contrast to that, end-to-end security and privacy of SOAP messages (the message layer) transferred between consumer and provider is not maintained and must be addressed in any web service architecture. So, a privacy of SOAP messages must be agreed by the two ends; bank and marketing company.

Consumer and provider must be agreed on the privacy of data transferred between them. A negotiation is needed for such a problem. The negotiation between the bank as a consumer and the marketing company as a provider conducted in the privacy of the data transferred as SOAP messages between them.

Negotiation among web services provides an effective way to get an agreement between participants [10]. The goal of web service negotiation is to get an agreement among participants for creating a Service Level Agreement (SLA) between them [11]. In web service architecture, negotiation is conducted in a selection phase [12]. Web service participants negotiate QoS attributes as non-functional attributes. Different models success in negotiating QoS attributes. Other researchers negotiate security for getting an end-to-end security for the data transmitted between participants [13]. The disclosure of data transferred between participants through SOAP messages and getting an agreement between them still a problem.

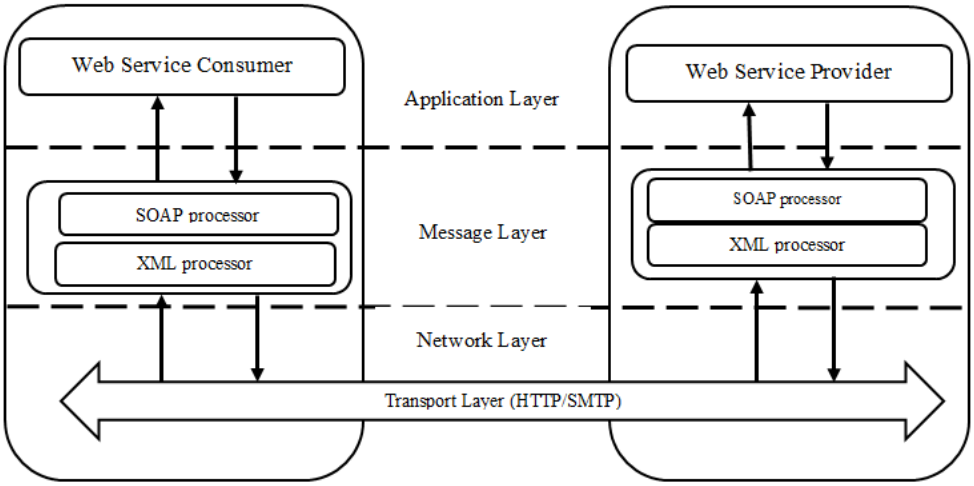

Fig.1. Web service layers

In this paper, First, a different negotiation communication structures between consumer and provider in a negotiation are presented. Second, a traditional time-based negotiation and genetic negotiation used in negotiating security are used in negotiating privacy of consumers' data that transferred between bank and marketing companies. A comparison between the two frameworks is evaluated.

The remainder of this paper is organized as follows: Section II introduces the related works on different privacy models and negotiation frameworks. In section III, web service security Negotiation framework; which is used to negotiate security for a web service participants; is presented. In Section IV, an extension to the security negotiation framework is issued to negotiate privacy and to provide an end-to-end privacy for web service participants. Section V discusses the experimental results of the framework. Section VI provides conclusions and future directions for end-to-end web service privacy negotiation framework.

II. Related Work

Web service privacy is classified into two directions; enforcing privacy on different web service participants and getting an agreed privacy level between web service participants; consumer and provider. This paper will be interested in getting a privacy agreement in a web service environment by negotiation.

In web service privacy, researchers address privacy similarity measure and ranking. Besides, some of them provide frameworks for negotiation. In a web service negotiation, different negotiation models for QoS attributes in a web service architecture is addressed by different researchers such as traditional time-based negotiation strategy and genetic-based approaches [3]. The traditional negotiation strategies use decision functions to get an agreement between participants. Time is the main factor in such negotiation. In Genetic based negotiation, the problem is formulated as a search problem.

Al-aaidroos et al. [14] proposed an agent-based framework for QoS negotiation in web service. A multilateral negotiation is conducted. An exponential time-based utility function is used to generate and evaluate proposals of participants. More than 90% of negotiation are successful.

Costante, et al. [15] studied the privacy of consumer and provider at selection phase of web service. This approach verifies the compliance of privacy policies for web service participants. Also, they rank web services according to privacy level they offer. They use AND/OR tree for representing orchestration of web service composition. They apply the approach to a travel agency case study. In their approach, for each data item, they addressed purpose for using, sensitivity, visibility, and retention time for accessing this data item. Authors through this work proposed only an approach for negotiation and the negotiation process will be implemented as a future work.

Li, et al. [16] proposed similarity measure approach for privacy policies expressed in (eXtensible Access Control Markup Language) XACML. XACML is one of the languages represents the access control policy in a distributed environment [17].The purpose of the approach is to find the cloud service provider which satisfy users' privacy concerns. This means that the approach matches the privacy settings of cloud service provider and user. The similarity measure used to assign a rank for each policy comparing to the user policy.

Li, et al. [18] grabbed an attention that there is no framework to negotiate security policies. Through their paper, authors present only how an agreement can be reached between security policies. They evaluated the relationship between privacy policies by matching them [15]. They stated that negotiation would be the future work.

Sadki, et al. [19] provide an approach for privacy negotiation in a cloud environment. Their proposed approach negotiates health care environment to improve patients' quality of care. Approach for resolving conflicts among privacy requirements of actors is involved. Through the proposed approach for conflict resolving, the patient is an important actor. They compare the two policy requirements. When a conflict occurs between them,

patient as a participant is involved in conducting the negotiation process. Authors intend to develop the negotiation stage as a crucial step of the approach in the future work.

As noted from these works, negotiating privacy still a problem. Most researchers negotiate Quality of Service (QoS) attributes. From the above related work, researchers draw the view of the framework for negotiation and mentioned that negotiation will be addressed as future directions. In this paper, an extension to the security negotiation framework is issued to conduct privacy negotiation [6].

III. Web Service Security Negotiation Framework

A web service security negotiation framework; RGSS-Negotiation; is used to conduct negotiation on security requirements between consumer and different providers [6]. Genetic-based negotiation is used by researchers in negotiating QoS attributes [13, 20]. For the repaired genetic-based negotiation framework; detailed in Fig. 2; consumer and different providers send their attributes to the broker. Then, broker conducts the negotiation process. Offers on a genetic-based negotiation contain eight genes. Fitness value evaluates the fitness of a value of a consumer and provider. Decreasing fitness value means a good solution. A disagreement between provider and consumer value is calculated according to equation 1. The fitness of an offer calculated according to equation 2.

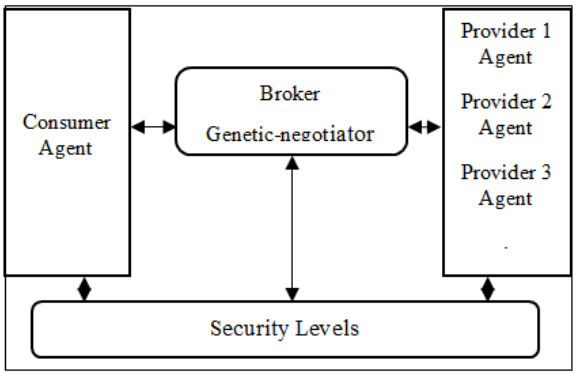

Fig.2. Genetic-based negotiation framework

$$\Delta_{ij} = \frac{C_j - P_{ij}}{C_j} \quad (1)$$

$$f_j = \sum_{j=0}^{n} (wC_j * \Delta_{ij} + WP_{ij} * \Delta_{ij}) \quad (2)$$

Where;

C_j Consumer value of jth attribute,

$C_{j(\min)}$ The min allowed consumer value for jth attribute,

$C_{j(\max)}$ The max allowed consumer value for jth attribute,

wC_j Weight of consumer jth attribute,

P_{ij} The ith provider value for jth attribute,

$P_{ij(\min)}$ The min allowed value for The ith provider value of jth attribute,

$P_{ij(\max)}$ The max allowed for The ith provider value of jth attribute,

WP_{ij} Weight for The ith provider value of jth attribute,

f_j Fitness of solution for participant j.

The algorithm steps of genetic based negotiation are provided in algorithm 1. It is the same steps as classical genetic algorithm except adding a repairing step.

Algorithm1: Genetic-based security negotiation algorithm

1. Initialize the population of the negotiation problem with random solutions
2. Repair each infeasible solution using repairing technique
3. Evaluate the fitness of each solution based on the fitness function defined in equation 1
4. **While** the negotiation termination condition is not reached do
    a. Select the best-fit solutions for survival using roulette-wheel selection.
    b. Apply a uniform crossover operator to generate new solutions using a roulette wheel selection method.
    c. Apply a mutation operator randomly on solutions.
    d. Repair each infeasible solution using repairing technique
    e. Evaluate the fitness function of each solution as expressed in equation 2.
5. **End while**
6. End

This repairing step must be added after the initial population and after conducting genetic algorithm operators. It is used for repairing the solutions to be within the range of values of different participants.

Besides genetic based negotiation, a traditional time-based security negotiation framework is used in negotiating security. It is depending on time as a main factor of negotiation. The traditional time-based negotiation framework is provided in Fig. 3. The negotiation is conducted in broker party of a web service architecture. Consumer and different providers provide their attributes to the broker; which has a function for doing the negotiation. The main parts of the frameworks are:

1. **Decision Making (DM)**: is the module used for decision making for accepting or rejecting the offers.
2. **Negotiation strategy**: which defines how to create an offer, accept the offer and reject the offer for a time-based negotiation strategy.
3. **Security levels:** is the security levels used by both web service participants.

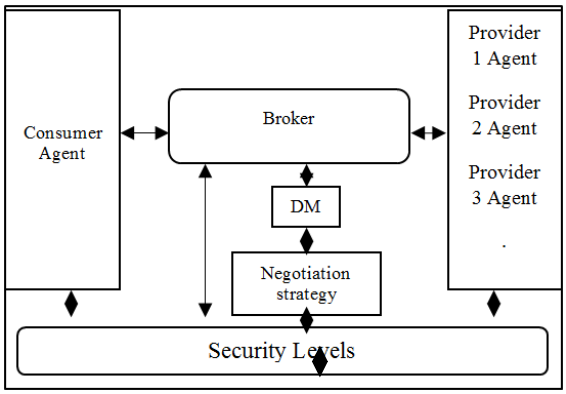

Fig.3. Traditional time-based security negotiation framework

Algorithm 2 details the traditional time-based negotiation algorithm. For the algorithm, some parameters must be defined. t is the bid number. t_{max} is the maximum time. β is the parameter affects the conceding curve $\propto (t)$ defined by a polynomial function or exponential function [21]. A fitness utility function is computed for every offer of the algorithm and according to it an acceptance or rejection of the proposal is issued [21].

Algorithm2: traditional time-based security negotiation algorithm

Input: t_{max}, issues, t=0

Output: Participant proposal

1. Compute β for each issue
2. Compute $\propto (t)$ for each issue
3. currentProposal←getStartingProposal ($\propto (t)$)
4. computeUtiltiyFunction() for each issue
5. currentFitness←computeGlobalUtilityFunction()
6. **While** t < t_{max} **do**
   a. Compute $\propto (t)$ for each issue
   b. tempProposal ← createProposal ($\propto (t)$)
   c. computeUtiltiyFunction() for each issue
   d. tempFitness←computeGlobalUtilityFunction()
   e. **if** tempFitness>=currentFitness **then**
   f. accept(tempProposal)
   g. end if
   h. currentProposal← tempProposal
   i. **if** accept(currentProposal) **then**
   j. **return** currentProposal;
   k. end if
   l. t++ ;
7. **End while**

IV. Extended Web Service Privacy Negotiation Framework

Negotiating privacy requirement of a consumer and provider in a web service environment is still a problem. Besides to that, there is no standard on where the negotiation process must be conducted? On a consumer, provider, or a broker. This paper will address the various communication structures for conducting the negotiation.

The negotiation process between consumer and providers in a multilateral environment may be in two different communication structure as shown in Fig. 4 (A) and (B). In communication structure (A), consumer negotiates with the provider(s) directly. The number of messages transferred between them during the negotiation process is increased. In another side, in the communication structure in B, negotiation process conducted on a broker. Consumer and provider send their attributes to the broker. Then, broker conducts the negotiation process and gets agreed provider with the consumer. In contrast to communication structure (A), there is a little number of messages transferred in this communication structure. The communication structure (B) is used in negotiating privacy. In this paper, negotiation with communication structure (B) is used cause of less execution time.

Privacy can be defined as a person's right to control access to personal information. The privacy level quantifies the risk of disclosure of user information based on three dimensions: visibility, sensitivity and retention time. The negotiation conducted in this paper is a multilateral negotiation between the two sides consumer and many providers. The negotiation process between them depends on a pre-defined privacy level.

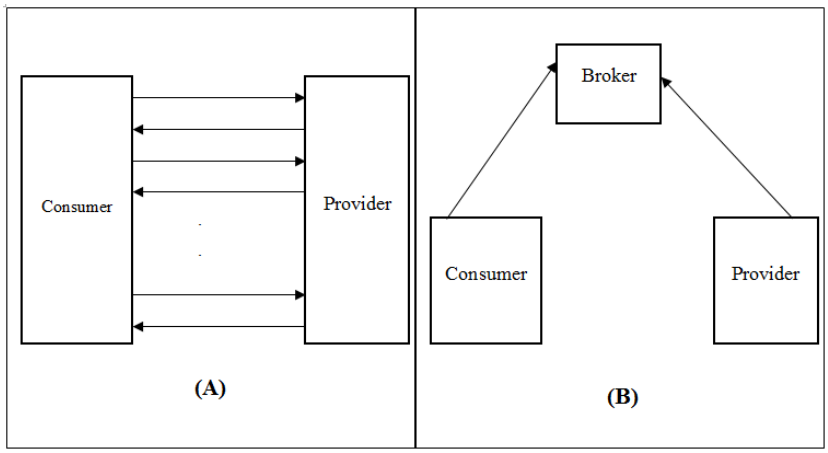

Fig.4. Different negotiation communication structures

With the telemarketing scenario between the bank and different marketing companies, shown in Fig. 5, where Bank sends its credit card holders' information to a marketing company. The consumer needs a privacy of this information, and the marketing companies require using this information as much as possible for other purposes to increase their profit. The bank credit card holders' data must be accessed by the marketing company.

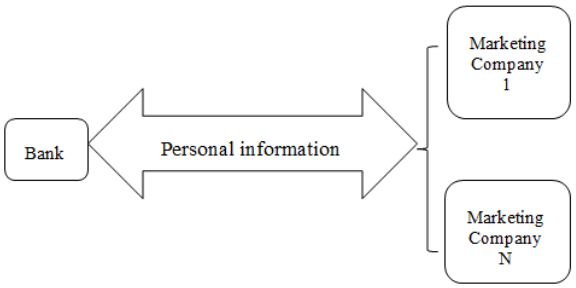

Fig.5. Telemarketing companion

The bank must preserve the privacy of its data. Credit card includes personal information such as Name, Email, Phone, Address, National ID, and Credit card number. The privacy level quantifies the risk of disclosure of user information based on three dimensions: visibility, sensitivity and retention time. Quantifying privacy levels comes from security levels addressed by El-Yamany which quantifies security levels [22]. From privacy definition, we define for each data item, who access it, and for what purpose as the following:

What = (Name, Email, Phone, Address, National ID, Credit card)
Who = (Trusted person, Marketing dept., All)
Purpose = (Marketing project, All)
How long = (short, long, always)

Table 1 shows the proposed taxonomy for privacy access rights. These taxonomies are private, protected, and public [23]. For each of this taxonomy, who, how long, and for what purpose must be defined. Then, we provide this taxonomy to each data item to generate privacy levels. These privacy levels are shown in Table 2. These levels range from less constrained privacy to more constrained privacy. Data items; credit card and national Id; are always private which means that they accessed by trusted person only for the purpose of a marketing project for short period of time. Details of all levels are provided in Table 2. After creating privacy levels; which control access rights to personal information for bank customers; consumer and providers have to negotiate to get an agreement on a privacy level.

Table 1. Privacy Taxonomy

	What	**Who**	**Purpose**	**How long**
Public		All	All	Always
Protected		Marketing dept.	Marketing project	Long
Private		Trusted person	Marketing project	short

Table 2. Privacy levels

Level	**Credit card**	**National ID**	**Address**	**Phone**	**Email**	**Name**
1	Private	Private	Public	Public	Public	Public
2	Private	Private	Protected	Public	Public	Public
3	Private	Private	Protected	Protected	Public	Public
4	Private	Private	Protected	Protected	Protected	Public
5	Private	Private	Protected	Protected	Protected	Protected
6	Private	Private	Private	Protected	Protected	Protected
7	Private	Private	Private	Private	Protected	Protected
8	Private	Private	Private	Private	Private	Protected

There exist two communication structure for negotiation as defined in Fig. 4. Because of decreased number of communication structure of negotiating on a broker, it is chosen as communication structure.

In this paper, A traditional time-based negotiation and genetic is used to negotiate a privacy of web service participants.

Genetic based negotiation framework and traditional time-based negotiation used for negotiating security are extended to negotiate privacy. For privacy negotiation, we must quantify privacy and define privacy levels. Quantifying privacy levels steps are as follows:

1. Define who can access the data, for what purpose, and how long data will be accessed. And provide three taxonomy for them as public, protected, and private.
2. Define privacy levels for data elements depending on the predefined taxonomy.
3. For each consumer and providers, min and max security level must be defined by participants.
4. Define weight of privacy as 1, as there exist only one object to be negotiated.
5. Define the negotiation strategy as genetic-based negotiation or traditional time-based negotiation.
6. Start multilateral genetic-based negotiation between consumer and N providers using genetic-based negotiation or traditional time-based negotiation framework.

A genetic based negotiation and a traditional time-based negotiation gets an agreement on security and privacy only if the requirements of both participants are intersected. In privacy, an issue is addressed as a

modification to the traditional and genetic negotiation. In non-intersected requirements, consider a case, if a consumer needs less privacy level and provider offers more private level. In such case, it is a good chance for the consumer to accept a provider offer without conducting the negotiation.

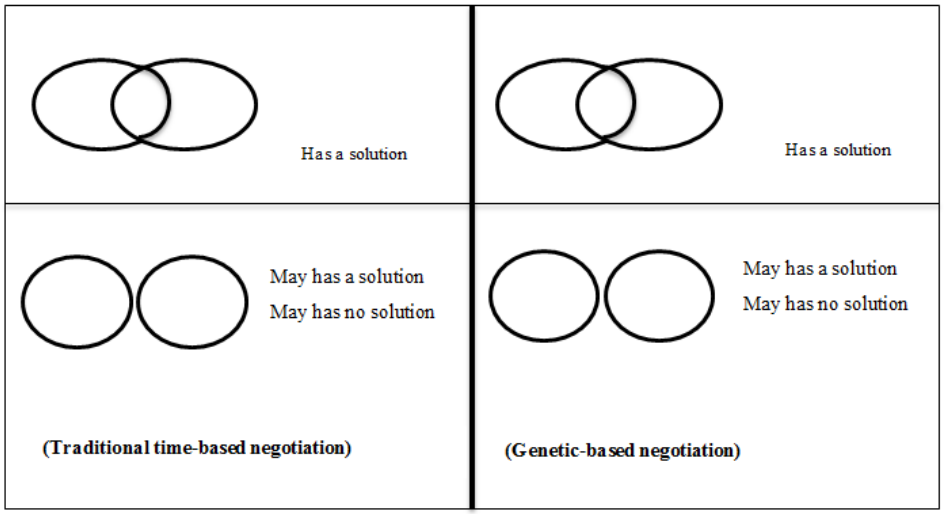

Fig.6. Intersected and non-intersected cases.

The traditional time-based negotiation and genetic based negotiation may have a solution if non-intersected requirements arisen. These cases are shown in Fig. 6. The two frameworks have a solution if they are intersected and may have a solution if they are non-intersected. The check that conducts before applying algorithm 1 and algorithm 2 is as follows:

1. Check intersection between privacy requirements between consumer and each provider
2. If they are not intersected and the requirements of the provider are greater than (more constrained than) consumer requirements, then accept the minimum requirement of the provider.
3. Else if they are not intersected, and the requirements of consumer is (more constrained than) provider requirements, then no result exist/reject the negotiation
4. Else if there is an intersection, then continue with conducting negotiation

V. Experimental Results

We conduct negotiation process between one consumer and 50 providers with different privacy requirements. Genetic based privacy negotiation and traditional time-based negotiation successes in getting an agreement. The framework has been developed using (JADE) Java Agent Development Environment for the multi-agent system. It can be easily deployed with only providing Java 6 Runtime Environment for running the JADE platform. The environment where the framework is conducted is specified in Table 3.

Table 3. Specifications for the environment

Operating System	**Windows 7 Professional (64 bit)**
CPU	Intel Core i3
Clock Speed	Up to 2.13GHz
Memory	3 GB RAM

For the negotiation simulation, sample of Input data for the negotiation is as presented in Table 4. An Id is provided for each participant. Besides, low range and high range of privacy level is provided. This range of privacy is the requirement of participant to get an agreement on that range of privacy levels.

Table 4. Samples of the Input Data

participant ID	**ID**	**Low range**	**High range**
Consumer	0	2	5
Provider1	1	1	3
Provider2	2	1	4
Provider3	3	1	5
Provider4	4	1	6
Provider5	5	2	4
Provider6	6	2	5
Provider7	7	2	6
Provider8	8	2	7
Provider9	9	2	8
Provider10	10	3	8

Firstly, traditional time-based negotiation is analyzed. For a traditional time-based negotiation, different negotiation cases are presented. An example for requirements for both consumer and provider is provided. For a consumer the requirements are {0.0, 2.0, 5.0}and the requirements for the provider 1 are {1.0, 1.0, 3.0}. There exist only one requirement on which a negotiation is conducted. This requirement is privacy. A solution is obtained in bid number 26 as shown in Fig. 7. Although offers of privacy of a provider and consumer are intersected on bid 66 as shown in the figure, the consumer accepts provider offer at bid 26 as the cost/benefit of the accepted offer is greater than or equal to the next offer. Besides, this offer is in range of acceptable privacy levels of the opponent participant.

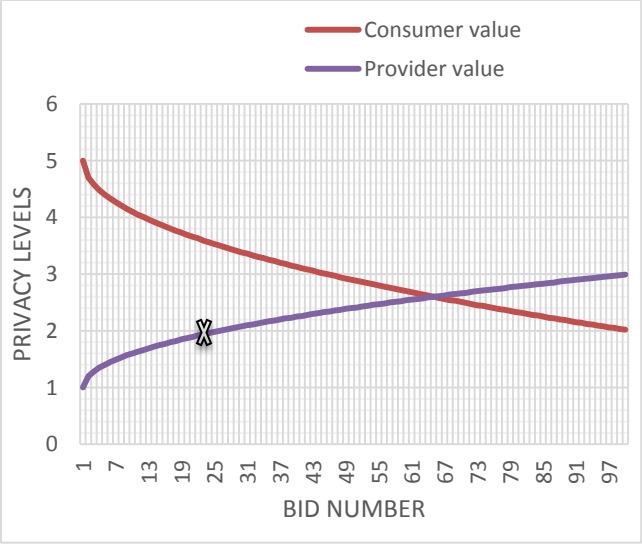

Fig.7. Convergence towards solution-case 1

Different offers for this traditional negotiation case 1 between consumer and provider 1 are provided in Table 5. Offers from the start till offer 25 is not in range of value of the two participants. The first offer that is accepted for the two participants id offer at bid 26 for provider. So, this offer considered the best suitable offer. In such case, the requirements of the consumer and provider are intersected. So, a solution must be obtained with the cost/benefit model of the traditional time-based negotiation technique.

Table 5. Different offers of the opponent participants

Bid number	ID	Value	fitness		ID	Value	Fitness
20	0	3.69	0.56		1	1.87	0.56
21	0	3.66	0.55		1	1.89	0.56
22	0	3.63	0.54		1	1.92	0.54
23	0	3.59	0.53		1	1.94	0.53
24	0	3.56	0.52		1	1.96	0.52
25	0	3.53	0.51		1	1.98	0.51
26	0	3.5	0.5		1	2	0.5
27	0	3.47	0.49		1	2.02	0.49
28	0	3.44	0.48		1	2.04	0.48

Another case with non-intersected requirements of the two participants is analyzed. Consumer required a {0.0, 2.0, 5.0} and provider required a {30.0, 6.0, 7.0}n. From the requirements, no intersection point of the two participants as consumer requires privacy level from "2" to "5" and provider requires privacy level from "6" to "7". In spite of that, traditional time-based negotiation gets an agreement between them as provider offer a more private offer to a consumer. And this is a chance for consumer to secure its data. The coverage towards a solution of the two participants is presented in Fig. 8.

The agreed offer of the two participants is privacy level 6. As for non-intersected cases, the provider provides a more private level than a consumer requires. So, level 6 as a privacy level is a best suitable for the consumer. There is no need to check offers of the two opponent as the agreement is not obtained by negotiation. It is obtained by the check condition added before the negotiation process.

If a consumer requires privacy in range of "6 -7" levels and provider provide a privacy in range of "2 - 5", there is no agreement between them. As, there is no intersection between them. Besides to that, provider provides less privacy level than consumer requires. So, there is no agreement between them.

Secondly, genetic-based negotiation is analyzed. With a genetic-based negotiation, the two participants have an agreement if the requirement of the two participants is intersected. Besides to the intersection, if the provider provides a higher privacy level than consumer without intersection. Consumer accept the provider requirements as it is a good chance for it.

With conducting genetic-based negotiation, the initial populations and new individuals must be within the range of values of participants. For each iteration, the elitism element is gained according to fitness value. An accepted solution is the solution where fitness function value equal "0".

In Fig. 9, the fitness of the best element of each iteration is collected and presented. As shown in the figure, a lot of elitism elements of each iteration has a fitness "0" which means that it is an accepted solution for two

participants. In the addressed case, negotiation is conducted for one object; which is a privacy level. The search space of the presented problem equal to "8^1*50" which equal to "400" solution only where "8" is the levels, "1" is the number of objects we negotiate about, and "50" is the number of participants.

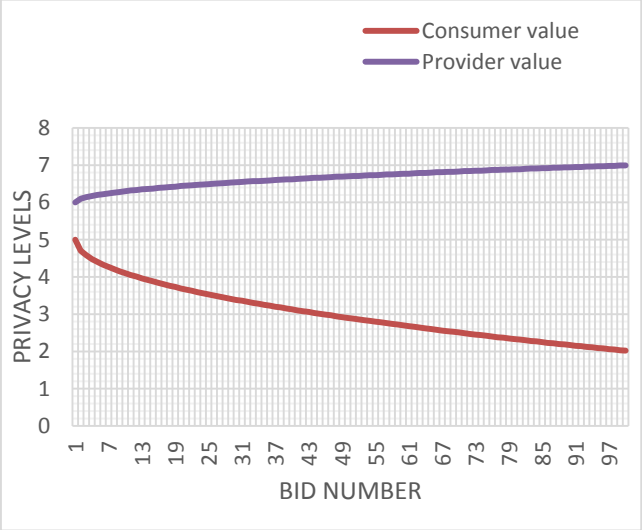

Fig.8. Coverage towards a solution case 2

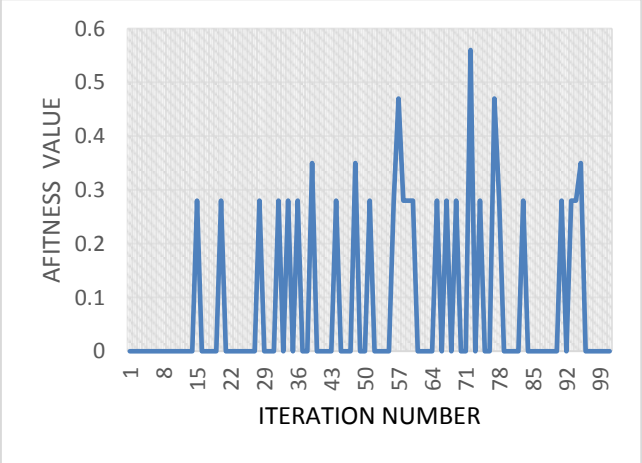

Fig.9. fitness value of elitism elements for 100 iteration

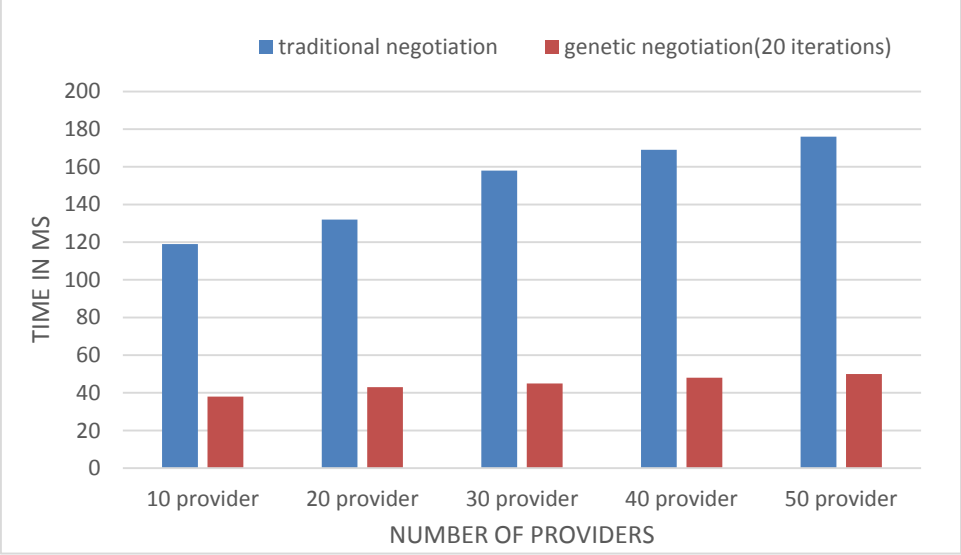

Fig.10. Execution time

Before conducting the genetic-based negotiation, a check is conducted for the non-intersected requirements as presented in the extension for the framework. The check is conducted to check if a provider provides more private level than a consumer. In such case, the consumer is agreed with the provider without the need for conducting negotiation.

Additionaly, The execution time of the traditional time-based negotiation and genetic-based negotiation is evaluated. For genetic-based negotiation, the execution time for the first "20" iterations is computed as a good fitness is obtained in the start set of iterations. For the traditional time-based negotiation is conducted for all participants till the end. For 10, 20, 30, 40, and 50 providers, the execution time of the two negotiation frameworks is evaluated as shown in Fig. 10. The two frameworks communicate with the same communication structure in a web service environment. Genetic based negotiation gets less execution time in contrast to the Traditional time-based negotiation.

Besides execution time, message complexity of the two frameworks; genetic-based and traditional time-based; is analyzed. Message complexity is one of the complexity measurement of a distributed environment [24]. The negotiation problem is affected by communication complexity which can be measured by message complexity. The addressed problem involves one consumer and N providers. For genetic-based negotiation, the negotiation process conducted by the third party. Consumer and providers send their attributes to the third party. Message complexity of the genetic-based negotiation framework can be defined as D(f) which is the number of messages between participants. It can be donated as the following:

$$D(Gentic.NEG) = 3 + N$$

As, N providers send their attributes to the third party. In addition, one message as consumer sends its attributes to the third party. Then, third party conducts the negotiation. And finally, after conducting negotiation, the third party sends two messages to the agreed consumer and provider.

The communication structure of the traditional time-based framework is the same as genetic negotiation communication with the same variables. Each provider and consumer send their attributes to the third party; which conducts the negotiation. The message complexity of traditional time-based negotiation can be represented by the following:

$$D(Trad.NEG) = 3 + N$$

From the above message complexity analysis, the two frameworks have the same message complexity for the communication structure in that distributed environment.

VI. Conclusion and Future Work

A privacy is one of the important a non-functional requirement of a web service. Getting a privacy agreement between participants in a web service using negotiation still a problem. In this paper, the communication structure between participants in a web service environment is addressed. Two communication structure for privacy negotiation is presented; negotiating directly between consumer and different providers and negotiating on a broker as a third-party. Negotiating on a broker is used in negotiation as it decreases the number of messages transferred during negotiation which decreases the execution time of such distributed environment.

An extension to genetic-based security negotiation framework is issued to negotiate privacy. Genetic based negotiation framework outperforms traditional time-based in negotiating security. In a negotiation process, requirements of consumer and providers may be intersected and non-intersected. Different cases for intersected and non-intersected requirements with the two frameworks are tested. Traditional time-based negotiation and genetic-based negotiation gets an agreement for intersected requirements. For non-intersected one, if the requirement of a consumer is less private level and provider provide a more private level of data the two frameworks has a solution with the minimum provided level.

Execution time and message complexity for the genetic based negotiation is evaluated and compared to traditional time-based negotiation. The two frameworks evaluated on the same communication structure. Both negotiation frameworks have the same message complexity. In addition, Genetic based negotiation has a less execution time in contrast to traditional time-based negotiation. This is because of the genetic gets a good fitness function in the start set of iterations. So, the genetic based negotiation outperforms traditional time-based negotiation.

As a future direction, we aim to address the negotiation of security and privacy on a composed web services.

References

[1] M. Alrifai, T. Risse, and W. Nejdl, "A hybrid approach for efficient Web service composition with end-to-end QoS constraints," *ACM Transactions on the Web (TWEB)*, vol. 6, p. 7, 2012.

[2] Z. Zheng, Y. Zhang, and M. R. Lyu, "Investigating QoS of real-world web services," *IEEE Transactions on Services Computing*, vol. 7, pp. 32-39, 2014.

[3] A. Abdelatey, M. Elkawkagy, A. El-Sisi, and A. Keshk, "A Multilateral Agent-Based Service Level Agreement Negotiation Framework," in *International Conference on Advanced Intelligent Systems and Informatics*, 2016, pp. 576-586.

[4] A. Meligy and P. El-Kafrawy, "A Web Service Discovery based on QoS Negotiation Approach," *International Journal of Computer Applications*, vol. 111, 2015.

[5] M. Resinas, P. Fernández, and R. Corchuelo, "A bargaining-specific architecture for supporting automated service agreement negotiation systems," *Science of Computer Programming*, vol. 77, pp. 4-28, 2012.

[6] A. Abdelatey, M. Elkawkagy, A. El-Sisi, and A. Keshk, "RGSS-Negotiation: A Genetic-Based Approach for Web Service Security Negotiation," in *The 11thIEEE International Conference on Computer Engineering and*

Systems (ICCES 2016) 2016, pp. 53-58.
[7] N. Ammar, Z. Malik, E. Bertino, and A. Rezgui, "Dynamic Privacy Policy Management in Services-Based Interactions," in *International Conference on Database and Expert Systems Applications*, 2014, pp. 248-262.
[8] P. C. Hung, D. K. Chiu, W. Fung, W. K. Cheung, R. Wong, S. P. Choi, *et al.*, "Towards end-to-end privacy control in the outsourcing of marketing activities: A web service integration solution," in *Proceedings of the 7th international conference on Electronic commerce*, 2005, pp. 454-461.
[9] A. Ajay, A. Jaiswal, and K. Verma, "Security of Web Applications with short web service: a review Study," in *2015 Fifth International Conference on Advanced Computing & Communication Technologies*, 2015, pp. 569-574.
[10] L. D. Ngan and R. Kanagasabai, "Semantic Web service discovery: state-of-the-art and research challenges," *Personal and ubiquitous computing*, vol. 17, pp. 1741-1752, 2013.
[11] M. Al-Aaidroos, N. Jailani, and M. Mukhtar, "Automated web service SLA negotiation using multiagent system," in *WITPress*, 2014.
[12] C. Di Napoli, P. Pisa, and S. Rossi, "Towards a dynamic negotiation mechanism for qos-aware service markets," in *Trends in Practical Applications of Agents and Multiagent Systems*, ed: Springer, 2013, pp. 9-16.
[13] A. Abdelatey, M. Elkawkagy, A. El-Sisi, and A. Keshk, "A Repaired Genetic Algorithm-based Approach for Web Service Security Negotiation," in *International Conference on Computer Theory and Applications*, 2016.
[14] M. Al-Aaidroos, N. Jailani, and M. Mukhtar, "Agent-based negotiation framework for web service's SLA," in *Information Technology in Asia (CITA 11), 2011 7th International Conference on*, 2011, pp. 1-7.
[15] E. Costante, F. Paci, and N. Zannone, "Privacy-aware web service composition and ranking," in *Web Services (ICWS), 2013 IEEE 20th International Conference on*, 2013, pp. 131-138.
[16] Y. Li, N. Cuppens-Boulahia, J.-M. Crom, F. Cuppens, V. Frey, and X. Ji, "Similarity measure for security policies in service provider selection," in *International Conference on Information Systems Security*, 2015, pp. 227-242.
[17] S. Godik, A. Anderson, B. Parducci, P. Humenn, and S. Vajjhala, "OASIS eXtensible access control 2 markup language (XACML) 3," Tech. rep., OASIS2002.
[18] Y. Li, N. Cuppens-Boulahia, J.-M. Crom, F. Cuppens, and V. Frey, "Reaching agreement in security policy negotiation," in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 2014, pp. 98-105.
[19] S. Sadki and H. El Bakkali, "An approach for privacy policies negotiation in mobile health-Cloud environments," in *Cloud Technologies and Applications (CloudTech), 2015 International Conference on*, 2015, pp. 1-6.
[20] K. Hashmi, A. Alhosban, Z. Malik, B. Medjahed, and S. Benbernou, "Automated Negotiation Among Web services," in *Web Services Foundations*, ed: Springer, 2014, pp. 451-482.
[21] P. Faratin, C. Sierra, and N. R. Jennings, "Negotiation decision functions for autonomous agents," *Robotics and Autonomous Systems*, vol. 24, pp. 159-182, 1998.
[22] H. F. E. Yamany, M. A. Capretz, and D. S. Allison, "Quality of security service for web services within SOA," in *2009 Congress on Services-I*, 2009, pp. 653-660.
[23] E. Zheleva and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in *Proceedings of the 18th international conference on World wide web*, 2009, pp. 531-540.
[24] G. Pandurangan, P. Robinson, and M. Scquizzato, "A Time-and Message-Optimal Distributed Algorithm for Minimum Spanning Trees," *arXiv preprint arXiv:1607.06883*, 2016.

Authors' Profiles

Arabi keshk received the B.Sc. in Electronic Engineering and M.Sc. in Computer Science and Engineering from Menoufia University, Faculty of Electronic Engineering in 1987 and 1995, respectively and received his Ph.D. in Electronic Engineering from Osaka University, Japan in 2001. His research interest includes software testing, software engineering, distributed system, database, data mining, and bioinformatics.

Ashraf El-Sisi received the B.Sc. and M.Sc. in Electronic Engineering and Computer Science Engineering from Menofia University, Faculty of Electronic in 1989 and 1995, respectively and received his Ph.D. in Computer Engineering & Control from Zagazig University, Faculty of Engineering in 2001. His research interest includes cloud computing, privacy preserving data mining, and Intelligent systems

Mohamed Elkawkagy, 1973, male, Faculty of Computers and Information, Menofia University, Egypt, Lecturer, received his Ph.D. in 2012, his research directions include AI-planning, Software Engineering, Planning search strategy , Multi-agent Planning, Web-based planning, Agent Systems and Human-Computer Interaction (HCI)

Amira Abdelatey received the B.Sc. and M.Sc. in computers and information from Menofia University, Faculty of computers and information in 2007 and 2012, respectively. Currently hold Ph.D. student in Faculty of computers and information, Menofia University. Her research interest includes semantic web, web service, intelligent systems, web service security, software engineering and database systems.

How to cite this paper: Amira Abdelatey, Mohamed Elkawkagy, Ashraf Elsisi, Arabi Keshk,"Extend Web Service Security Negotiation Framework in Privacy", International Journal of Information Technology and Computer Science(IJITCS), Vol.9, No.8, pp.30-39, 2017. DOI: 10.5815/ijitcs.2017.08.04