A Test Process Model to Evaluate Performance Impact of Privacy Protection Solutions

Victor Mello, Tania Basso, Regina Moraes

Faculdade de Tecnologia – Universidade Estadual de Campinas (UNICAMP)
Caixa Postal 456 – 13484-332 - Campus I – Limeira – SP – Brasil

victorleonel@gmail.com, {taniabasso,regina}@ft.unicamp.br

Abstract. *Organizational Information Systems (IS) collect, store, and manage personal information through web applications and services. Due to regulation laws and to protect the privacy of clients, such information must be kept private. Some solutions were developed to protect privacy personal information. Obviously, this additional resource will produce a performance impact and evaluating it is essential to determine the feasibility of the solution. This paper presents a process model to evaluate the performance impact introduced by privacy protection solutions in web applications. Case study shows the tests were useful to identify the conditions in which the solution under evaluation is able to work with minimal performance impact.*

1. Introduction

Nowadays, applications and services provided via web such as e-commerce, banking and financial services are essential and widely used by society. The provision of these services, performed with the aid of a browser, is only possible due to the support of computers network that allows communication between suppliers and users. Most of time, to use these services, users and customers need to provide personal information. Once sent across the network, the information has become known by the service provider and, often, by other business partners that not even had any interaction or involvement with the users. It means that once personal information is made available they are no longer under control of their owner in respect to how they are used and their consequences. This finding raises privacy concerns.

The need to ensure the security and privacy of personal information handled by web services and applications has led to a significant development of technology. This need arises from regulations laws (the companies and organizations that hold private data have the obligation and responsibility to protect them) and competitive differentials (the more a company protect the privacy of its customers and business partners, the better is its reputation). The privacy policy is a resource often used in this context.

The description of organization's practices on information collection, use, and disclosure is the focus of the internet privacy policies. These privacy policies intend to protect the organization and to signal integrity commitment to site visitors. To guide browsing and transaction decisions, consumers use the stated website policies (Earp *et al.* 2005). They are so important that can influence the organization's credibility: if the privacy policies are clearly and explicitly stated, then the visitor/consumer perceives the organization as more trustworthy (Han and Maclaurin 2002).

Besides the privacy policies definition, mechanisms to enforce them are necessary to make sure companies keep their privacy promises to consumers and business partners. A well-known approach for protecting privacy in scenarios based on web applications and services is to manage data using access control resources, that can be defined as "*a set of rules by which human users, or their representatives, are authenticated and by which access by these users to applications and other services information is granted or denied*" (IETF 2013). Thus, the information access control mechanism must be embedded into privacy-enhancing technologies. Obviously, adding access control to the web application or service will produce a performance impact. It is desired that this impact be small comparing to its nonuse. Evaluating this performance impact (through performance tests) is essential to determine the feasibility of using the privacy solution, as well as ensuring it is appropriate when deployed and used.

To evaluate the performance impact a test process model is required. This process model must support the definition of tests scenarios, their execution and the comparison of the tests results, especially when using and not using the privacy solution. Also, the process allows evaluating the solution's feasibility in different scenarios and different situations of using the web application or service (as, for example, with different amount of records in the database or different amount of simultaneous access by different users). This paper proposes a test process model to evaluate the performance impact of using privacy protection solutions in web applications.

The test process model was applied to the evaluation of a privacy solution integrated in a web application that represents an online book store. Results show that the tests were useful to identify in what conditions the solution under evaluation is able to work with minimal performance impact. Also, it helps to evaluate the scalability in terms of the number of registers in the database (the more registers, the more performance impact). This suggests the situations in which the privacy solution can be used as a simple and effective alternative to privacy protection.

The paper is organized as follows. Section 2 introduces the background and related work. Section 3 contextualizes the privacy protection issue and presents the privacy solution evaluated in this paper. Section 4 presents the proposed test process model. Section 5 shows the case study and the results and discussions. Finally, Section 6 shows the conclusions and future works.

2. Background and Related Work

The system quality is assured by the test activities, which main goal is to find the system failures or to validate the non-functional requirements of a system. Among different types of system test (Myers 1979), the performance test is gaining ground in the Web environments. The main goal of performance testing is to determine if the system performance reaches the restrictions imposed by the owners related to the response average time and throughput, in accordance with the system requirements (Pressman 2009).

Molinari (2003) presented the relationship between test and quality requirements in Web applications and highlights the quality requirements that most compromise the correct operation of these systems if they are not properly tested. In accordance with

Molinari, performance is the quality requirement that should demand more accurate test in Web applications.

The work most close related to ours was presented by Torres-Zenteno et al. (2006), which proposed a testing process model to guide the experiments on a GIS (Geographic Information System) Web application. In that work, the experiments were focused on the more critical use cases of the WebMaps system that helps the users to plan the agricultural distribution in some regions of interest. The performance tests are indispensable in the context of that system to ensure its applicability in its operational phase. The proposed process deals with the specific characteristics of the SIG Web applications, i.e., large volume of data and concurrent users. Our work deals with a completely different application that is an e-commerce Web application based on TPC-W standard (TPC 2014).

The work presented by Basso et al. (2013) proposes a policy model for data privacy protection and a mechanism as a protection layer, which is independent of the web application. The mechanism aims to enforce different policies derived from the model. The solution allows users to define the policies without requiring specific or in-depth knowledge about the web application, even expressing their preferences about each one of their personal information. However, although the model predicts the user preferences in detail, the protection layer enforces the access control in the web application code, leaving the data more vulnerable to attack, once they leave the database in clear. Moreover, there is no process to guide the experiments that were executed in an ad-hoc manner. This paper improves the work presented before, testing a new database framework that was implemented in the database layer, reducing the solution vulnerability. The framework encapsulates the mechanism to express and to enforce polices and it is able to guarantee that the personal privacy preferences will be fulfilled as before. Moreover, a testing process model was defined and was used to guide the experiments.

3. Privacy Protection

Although privacy can be defined in many ways, we use to this work the definition of Bertino et al. (2008), which says that "*privacy is the right of an entity to be secure from unauthorized disclosure of sensible information that are contained in an electronic repository*".The increasing use of personal information in Internet-based applications has raised privacy concerns over the world. Due to the fast advancement of information technology and the Internet, the users have a very low level of control of their information after they are released on the web. Companies and organizations are investing on protection of its customer's personal data privacy as a competitive differential. Also, to support and encourage the privacy protection, governments of different countries are investing in laws and regulations. To contextualize the current scenario of privacy protection regarding the collection and use of personal information, as well as laws that govern privacy on the Internet, some issues are described below.

The value of personal information. Usually, medium or big companies use sophisticated technologies to obtain personal information of their customers or potential customers. This personal information is valuable from the market viewpoint because it allows constructing consumer profiles and, thus, adopting strategies such as

advertisements targeted to their interest profiles. Selling such information to third parties is also common.

Some researches show that, although people approve the collection of their personal information (with their permission and purposes which they agree), they do not trust in many companies and resent when any of them is not clear on their plan to use personal information, or use such information for other purposes (Perkins and Markel 2004). For them, these actions constitute a privacy violation (Reay et al. 2009).

The Truste enterprise (Truste 2013) promoted a research in 2013 to assess and understand the main concerns of the costumers, the costumers trustworthy and business impact related to the online privacy of adults in the United States. More than two thousands internet users were interviewed and 89% revealed to be concerned about the privacy of your information when using the internet. In fact, the users concerns are justified: in a research performed by Accenture (2009), when 5500 business managers in 19 different countries were interviewed, 58% admitted that their enterprises had lost personal information from their customers and clients. Among them, 19% admitted that this event had occurred more than 5 times. Furthermore, 55% of the companies admitted that they had put the personal information available for third-parties or even outsourced the collection or processing of such information.

Privacy as a business competitive advantage. Based on the above reports, there is no doubt that investing in assuring privacy leads companies and organizations achieve a competitive advantage. Perkins and Markel (2004) affirm through a pragmatic argument, that ironically, companies should provide a rigorous protection of personal information of their consumers not only because it is the right thing to do, but for the reason that this protection is part of their larger interests. Innocuous privacy policies are suitable to a short-term business and robust privacy policies are suitable to a long-term business. So, companies and organizations should adopt robust privacy policies because people, in general, hate innocuous privacy policies (Perkins and Markel 2004).

In order to assess the impact of privacy concerns on the result of the use of online advertisements the Ponemom Institute (Ponemon 2010) interviewed, in 2010, 90 organizations that use the internet advertising as the main channel of communication in the United States. More than 70% of them agree that online advertising increases the organization marketing and their sales performance. Furthermore, 98% of the interviewed companies affirm that the privacy concerns limit their investments in online advertising.

Although there is interest by companies and organizations as well as tools and technologies to assist in privacy guarantee, government intervention in the form of laws is needed because the threats are fairly broad, malicious users are many, knowledge levels of the enterprises and organizations are very unequal, and in practice, privacy policies provided by these companies may vary and even may present ethical failures (Cate 2009, Perkins and Markel 2004).

Laws and regulations in different countries. Legislative approaches differ from country to country. Many countries have regulations for privacy information, such as China, India, the countries of the European Union (EU), United States, Canada, among others (Glass and Gresko 2012). Especially when one is dealing with

international business interactions, it is important to know the relevant privacy legislation. The two or more laws and relevant Statutes in several papers in the literature are mainly the European Union and the United States. In Brazil, according to Lemos (2013), there are no specific laws addressing the privacy of information on the Internet in Brazil. However, the Ministry of Justice has been working on drafting a law to protect personal data. The project, entitled "*Marco Civil da Internet*", was inspired by the model of the European Union and is under discussion in Brazilian Congress and still waits for vote (R7 Notícias 2014). A discussion on effectiveness of this project can be found in the article by Torres (2012). A text version of this law, dated from November 2012, which was delivered to the plenary, is available in Convergência Digital (2012).

Some cases of privacy violation. A recent serious example of privacy violation is the case of PRISM, a monitoring program created by the National Security Agency of the United States (NSA), in partnership with the FBI and with most technology companies (Google, Facebook, Microsoft, etc.). The PRISM has the proposal to monitor potential valuable international communications, which could pass by the companies' servers in the United States. With this, U.S. intelligence consulted audios, videos, photos, contents of emails, downloaded files and users' connections, violating their privacy (Veja 2013). The case had a great impact because it allowed spying information inclusive of presidents of several countries.

There are many other cases of privacy violation, as for example, when Google and other giants of the network were able to track users activities through automatic writing cookies in Safari browser used on Iphones, without the knowledge of users (Globonews 2012). And when a law student in Vienna noticed that all his deleted information in Facebook were not really deleted from the social network, making a group of Austrian students protest to press the Facebook to have privacy rules more severe (Youtube 2012).

The cases of privacy violation show that the way the companies and organizations protect and use personal information requires, in addition to ethics, systems and mechanisms for efficient privacy protection. Solutions for defining privacy policies and enforcing them have been proposed. Their feasibility should be evaluated.

3.1. A Database Framework for Expressing and Enforcing Personal Privacy Preferences

This section presents the privacy protection solution we selected to be used in our case study. It is a database framework, designed by Basso et al. (2014), for users to express their preferences about the privacy of their personal information. This selection was done due to the simplicity, ease of use and availability of the solution (it is free). Also, the flexible way it treats the personal privacy preferences is an important resource and is of our interest to evaluate its performance. The solution is described below.

In a broad view, the solution consists of a framework with a set of independent tables that can be added to the application's database. These tables will contain the necessary information to perform the access control according to predefined privacy policies, which consider users preferences about each personal information to be collected, stored and managed. The access control is performed by implemented database packages and has the advantage of filtering the data directly in the database,

contributing to security against possible attacks to the web application. Figure 1 shows a general view of the solution.

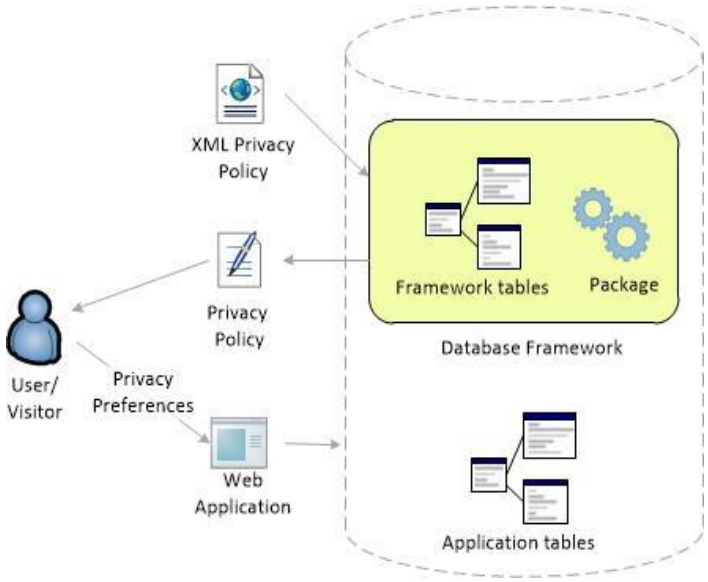

Figure 1. General view of the database framework solution (Basso et al. 2014).

In Figure 1, privacy policies are defined through XML files. These files are based on the policy model from Basso et al. (2013). These policies contain information about the system profiles and the personal data (associated with criticality levels) each profile can access or modify. These criticality levels are a scale of values to define how the information can be protected and will be further explained. A job (i.e., a combination of a schedule and a program, along with any additional arguments required by the program) is executed periodically to verify, automatically, in a specific application directory, the input of new policies. Then, the job maps these policies to the set of framework's tables.

After defining privacy policies, the normal process used by most companies is to present them to users and visitors, to inform them about company's privacy rules. Then, the user or visitor expresses their privacy preferences through the web application and this information are mapped in the both application and framework tables. These privacy preferences are expressed using predefined criticality levels. These criticality levels represent data with different requirements in terms of security, ranging from non-critical data to data that has to be extremely protected against unauthorized access. In order to identify the different levels of criticality and, consequently, how the data has to be protected, we established, for our study, the 5 levels described in the work of Vieira and Madeira (2005). They range from level 1 (non-critical data, i.e., data that does not represent any confidential information.) to level 5 (critical data that has to be exceptionally protected against unauthorized read and modification, using cryptography and auditing) (see Vieira and Madeira (2005) for more details). However, companies and organizations can establish their own levels according to their necessities.

Still in Figure 1, to guarantee the enforcement of privacy policies and, consequently, to respect users privacy preferences, a mechanism was developed and

integrated to the framework. This mechanism is an algorithm integrated to the infrastructure of a relational database system to enforce disclosure control. It provides constructs that allow masking personal information according to the privacy policies and users preferences. The mechanism was implemented using database packages, which are resources to encapsulate related procedures, functions, associated cursors and variables together as a unit in the database.

To better understand the potential and feasibility of the proposed solution in terms of performance impact, performance tests are required. Thus, a test process model was defined to help this activity. It is described in the next section.

4. The Test Process Model

This section describes the test process model that is proposed to guide performance tests when testing the introduction of privacy solutions in web systems. The process is based most on the works of Torres-Zenteno et al. (2006), which consists of a testing process model to guide the experiments on a GIS Web application, and Basso et al. (2013), which proposes a privacy solution integrated in the application layer and performs some performance tests in a not formalized way. Figure 2 shows the proposed test process model, using the notation of UML activity diagram.

In Figure 2, the process starts with the activity of planning environment. It is necessary to establish the tools and resources to be used in the tests. It is important that the test environment reproduces the application environment accurately. Then, the environment must be configured.

The next step in the process refers to choose the number of records to be inserted in the database. This step is important because the number of records can impact the performance of the web application under test. Tests can be done with different amount of records to evaluate the scalability of the privacy solution. Then, it is necessary to populate the database with predefined number of records.

Still in Figure 2, the activity of planning the performance test refers to the identification of the use cases that will be tested. The identification of critical use cases related to privacy protection is vital for achieving a good performance test. Planning the tests is followed by the creation of scenarios. It is important to note that one or more scenarios can be defined. After creating the scenarios, the virtual web users, which represent the concurrent users (or threads), are defined.

To run the tests scenarios, there is a decision activity. As we want to evaluate the performance impact introduced by the privacy solution, tests without the solution are required in order to make a comparison. So, tests can follow two paths: without enabling the privacy solution (NO path) or enabling the privacy solution (YES path). When choosing enabling the privacy solution, an activity to this procedure is represented in Figure 2 as setUseFilter = true. For both paths, the tests scenarios are run and the results are collected and analyzed independently. To evaluate the performance impact, these results must be compared (they should have been executed under the same conditions). Graphics can be created to help the evaluation.

The last activity in the test process model represents the consolidation of the performance tests, where the performance impact can be evaluated and, consequently, the feasibility of using the privacy protection solution.

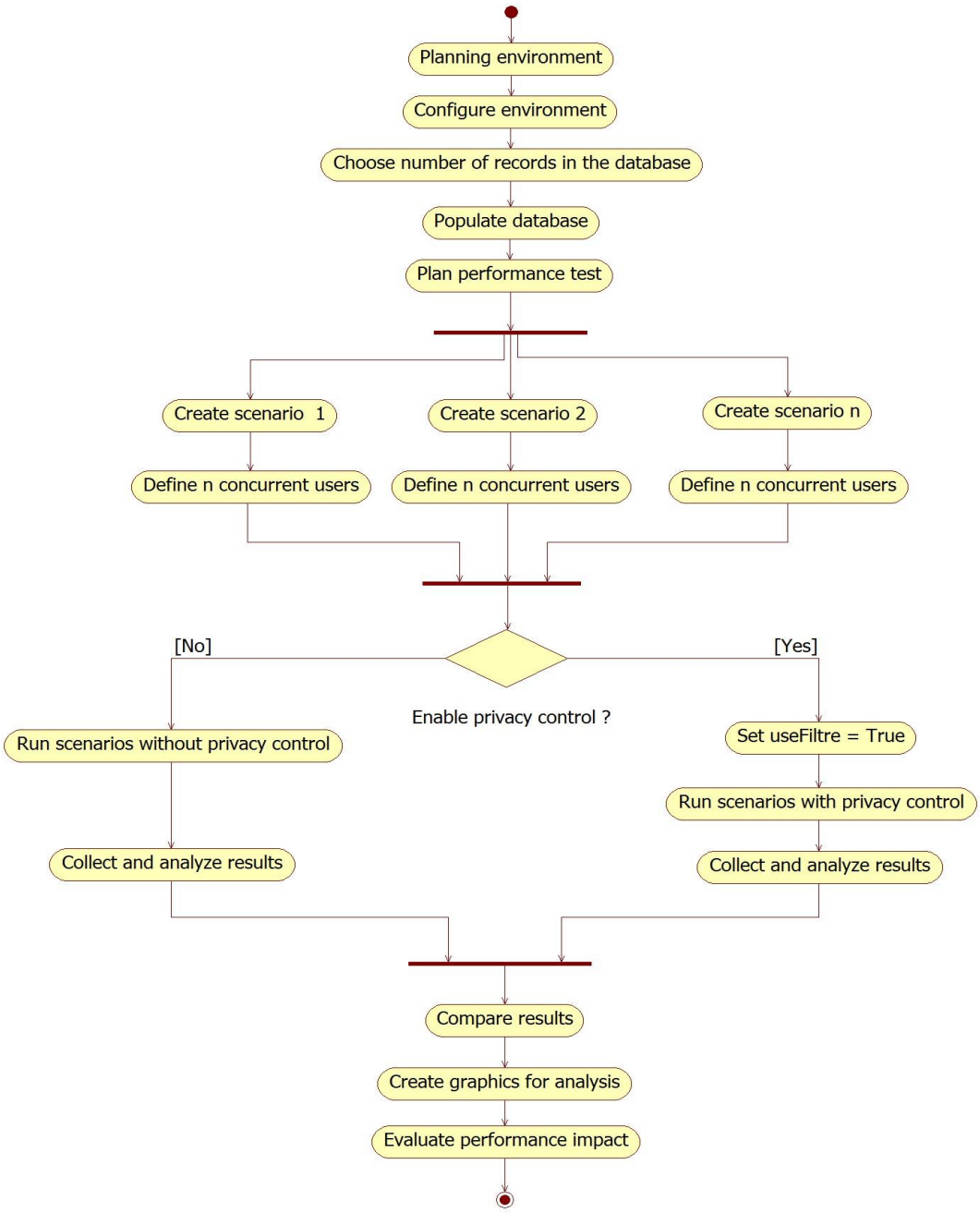

Figure 2. Proposed test process model to evaluate the performance impact of privacy protection solutions in web applications

5. Case Study

To better understand the potential of the selected privacy solution (Basso et al. 2014) and the applicability of our proposed test process model, a case study was performed.

The case study evaluates the scalability and performance impact of the proposed solution and also the correctness of the proposed process. Scalability is expressed in terms of the number of records being processed by the solution, i.e., the goal is to understand how much the number of records in the database application affects the performance. The performance impact can determine advantages or disadvantages of using the solution. For these experiments the performance was characterized by the average response time and throughput.

5.1 . Experimental Setup

The experiments were performed using an Intel Core 2 duo processor, 2 Gb RAM, Windows 7 Professional (32 bits) operating system. The same notebook houses a NetBeans IDE 7.3 and Tomcat 6.0.36. All the resources needs were locally installed for preliminary testing.

The web application used in the experiments is a Java implementation of a TPC-W (TPC 2014), which is a benchmark for web-based transactional systems where several clients access the website to browse, search, and process orders. To this study, the TPC-W implementation simulates a retail online book store. The components of the TPC-W database are defined to consist of a minimum of eight separate and individual base tables. The database engine used in the experiments is Oracle Database 11g Express Edition Release 11.2.0 (Oracle 2014) and the metrics were collected using the JMeter tool version 2.9 (Jmeter 2014).

The application scenario to perform the tests simulates a third-party user, with guest profile, trying to obtain data of a registered customer through a search process. To test including the privacy solution, privacy policies were implemented and the criticality level of each data of each customer was randomly generated through a database script.

For our experimental evaluation it was used, respectively, 500, 5,000, 50,000 and 500,000 records of customers in the database. These records emulate real typical online shopping data. The simulations of threads, that simulate concurrent users connected to the server application, ranged from 1 to 256 users for each set of records. Also, in order to understand the performance impact, the tests were performed without the privacy solution, to obtain baseline indicators. For each run of the experiment, the whole system is returned to its initial state in order to avoid cached data.

5.2. Overall Results Analysis

First of all, the average time was collected to understand the performance degradation due to the amount of data in the Database and the concurrent users (also called threads) of the web application. Figure 3 presents the overall results of the study, showing the average processing time of all requests for the customer search scenario. Presented in Figures 3a, 3c, 3e, the average time is given in milliseconds, representing from 1 up to 256 concurrent users. Also, Figures 3b, 3d and 3f show the throughput results for the same scenarios and amount of concurrent users. Throughput is calculated as the number of requests divided by unit of time. The time is calculated from the start of the first sample to the end of the last sample, including any intervals between them, as it is supposed to represent the load on the server.

Figures 3a, 3c and 3e shows the tests performed with, respectively, 500, 5,000 and 50,000 customers recorded in the database. The same for throughput: Figures 3b, 3d and 3f shows the tests performed with, respectively, 500, 5,000 and 50,000 customers. The use of different number of records can be necessary due to different quantities of information in the database for different companies or organizations sizes. It helps to evaluate the scalability of the privacy solution thinking about applying it in online commercial applications of small and midsize enterprises. Also, we have tried to perform tests with 500,000 customers, but it has exceeded the resources of the computational environment and the solution, making the analysis unfeasible and inaccurate for this case.

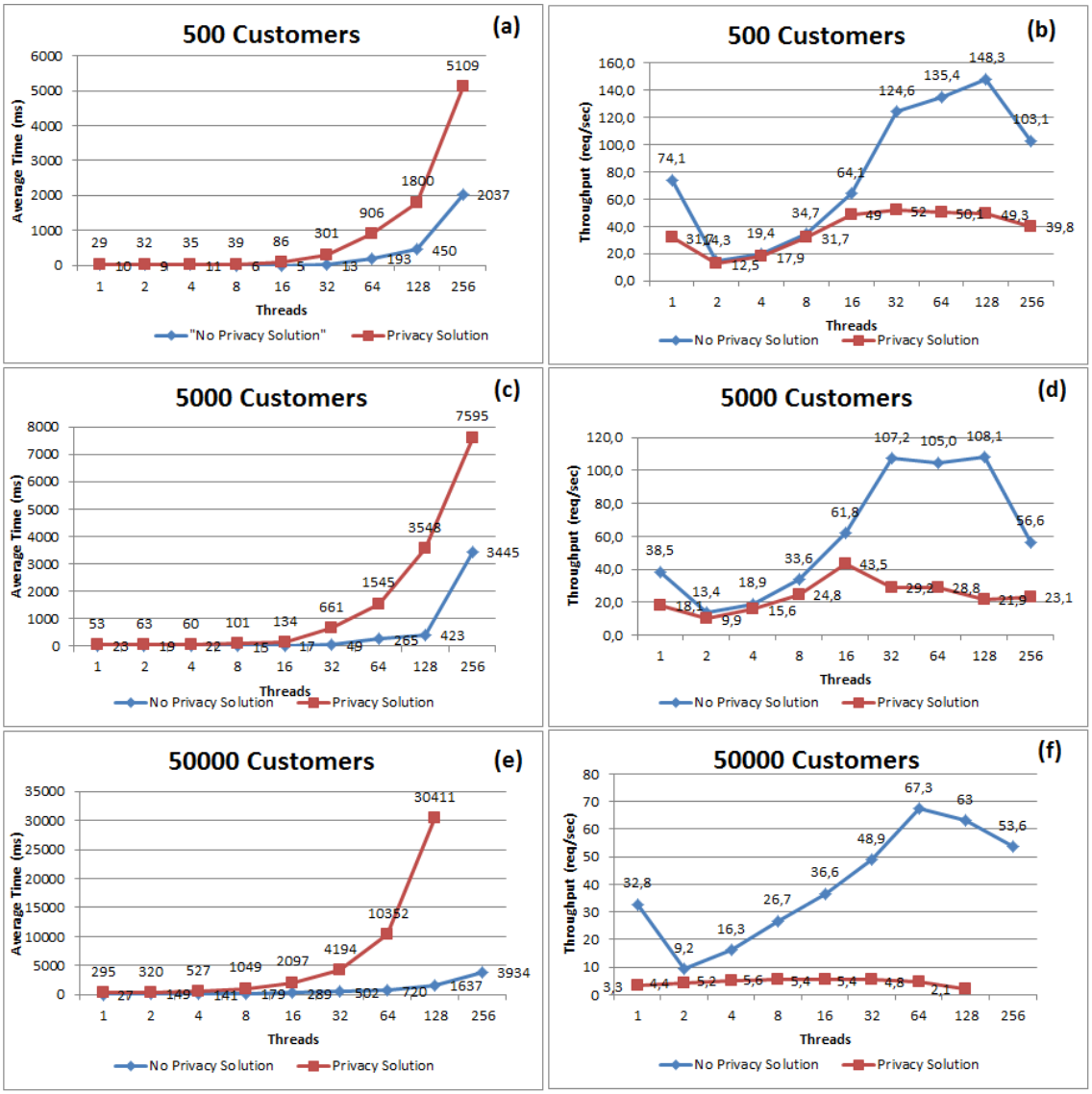

Figure 3. Experiments average time and throughput.

Analyzing the average processing time requests in terms of performance impact, Figures 3a, 3c and 3e shows that the proposed solution has very low impact when few users are using the web application at the same time. Although in some cases the increased time represents a high percentage (for example, in Figure 3a, the average time

for the first sample increases from 10 to 29 ms, representing more than a 100%), the time is milliseconds and this difference is practically irrelevant. So, the average time without the privacy solution is very similar to the other results (applying the privacy mechanism) until around 16 users. As the number of user increases, the differences between both results increase ever more sharply. But, although the inclusion of the privacy solution affects the performance for higher number of users and concurrent access, the system performance is rational for a small to medium enterprises where the number of customers and concurrent access is not too high.

The throughput variation presented in Figures 3b, 3d and 3f is similarly acceptable for the same range: about the 16 first samples the results with and without the proposed privacy solution are similar and the differences arise as it increases. These results reinforce the scalability of the solution for small to medium demands.

Through the analysis of the average processing time requests is possible to observe that, also, the privacy solution is scalable in terms of numbers of records considering the same type of enterprises. Figure 4a consolidates the scalability evaluation experiments, aggregating the average time response results for the respective three amounts of records (50, 5,000 and 50,000 customers) presented in Figures 3a, 3c and 3e, all implementing the privacy protection solution.

In Figure 4a it is possible to observe that the number of records barely affects the system performance for fewer threads. For many threads, the performance is affected in an expected way (the more records, the more processing cost) but the exponential shape brought strong evidence that the mechanism is not feasible to be used in large enterprises and/or high concurrent access situations.

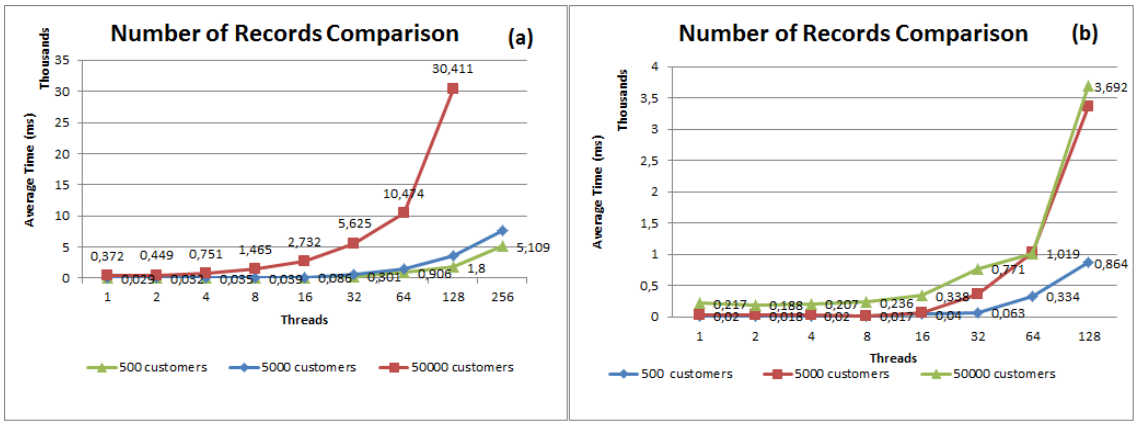

Figure 4. Average time response for different amounts of records implementing privacy solutions.

Figure 4b shows the average time response for the privacy solution of Basso et al (2013). The both solutions have different implementations and respective vantages and disadvantages: in Basso et al. (2013) the authors used AOP (Aspect-Oriented Programming) and the privacy enforcing is done in the application code. The data is recovered from the database and masked in the application. It has the disadvantage of being more vulnerable from the security viewpoint because, face with attacks, the information can be retrieved before masked. Also, it does not consider users preferences for each one of personal information when collecting, storing and using them.

The privacy enforcing mechanism tested in this work is implemented in the database. It is less vulnerable because the data recovered from the database is already masked according to the privacy policies. And it has more resources once it allows users to define privacy preferences for each one of personal information. Although the both solutions were tested in different environments, which influence the results, it is possible to deduce that the current solution produces greater impact on the performance (attention must be taken with the chart scale because, even it is represented on thousands Figure 4a represents 10 times the values in Figure 4b) due to its more elaborated resources.

6. Conclusions and Future Works

Providing efficient and effective privacy policies definition and enforcement for assisting privacy in web applications has long been an open and challenging issue. However, it is critically important for Internet-based data management systems due to privacy protection laws and companies and organizations interests. Introducing solutions for privacy protection in web applications can produce a performance impact, which can determine the feasibility of using the referred solution. So, evaluating this performance impact is essential.

This study presented the definition of a test process model to evaluate the performance impact introduced by privacy protection solutions that were implemented in the database layer. The proposed process is based on performance tests and permits de definition of multiple scenarios, multiple concurrent users (through web virtual users) and different amount of database registers. In comparison with other important process models, our solution has two important features. First, it is generic, i.e., was not developed to a specific type of application and can be used to different web applications segments. Second, it permits performing tests with and without privacy solutions, i.e., permits independent tests and the comparison of the results.

The test process model was validated through experiments involving a web application that simulates an online book store, based on TPC-W benchmark, and a privacy solution that permits users express their preferences about their personal information. The set of tests was useful to allow the identification of under what conditions the use of privacy solution is feasible. A comparison with results of other privacy solution was made and the solution under test was identified as more complete, but with greater performance impact in large scale web systems. This showed that it is more appropriate to be used by companies and organizations where the number of database registers and concurrent access is more limited.

As future work, we intend to complement the tests, evaluating other privacy solutions in the same environment, even to indicate which one is more feasible under the same test conditions. This is one of the areas that we are currently working on.

References

Accenture (2009). “How Global Organizations Approach the Challenge of Protecting Personal Data”. Available: http://www.ponemon.org/local/upload/file/ATC_DPP%20report_FINAL.pdf. Accessed: 19-Mar-2014.

Basso, T., Antunes, N., Moraes, R., Vieira, M. (2013). " An XML-Based Policy Model for Access Control in Web Applications". In proceedings of 24th International Conference on Database and Expert Systems Applications - DEXA, pp. 274-288.

Basso, T., Piardi, L., Moraes, R., Jino, M., Vieira, M. (2014). "A Database Framework for Expressing and Enforcing Personal Privacy Preferences." Paper submitted to The 14th Privacy Enhancing Technologies Symposium – PETS 2014, Amsterdam, Netherlands.

Bertino, E., Lin, D., Jiang, W. (2008) "A Survey of Quantification of Privacy Preserving Data Mining Algorithms". In: Privacy-Preserving Data Mining, vol. 34, C. C. Aggarwal, P. S. Yu, and A. K. Elmagarmid, Orgs. Springer US, pp. 183–205.

Cate, F.H. (2009). "Security, Privacy, and the Role of Law". Security & Privacy, IEEE , vol.7, no.5, pp. 60,63.

Convergência Digital (2012). "Leia a versão do Marco Civil da Internet que foi ao Plenário da Câmara". Portal Convergência Digital, 07 de novembro de 2012. Available: em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm ?infoid=32316&sid=4#.UZvhwMqNAuv. Accessed: 23-may-2013.

Earp, J. B., Antón, A. I., Member, S., Aiman-smith, L., Stufflebeam, W. H. (2005). "Examining Internet Privacy Policies Within the Context of User Privacy Values", IEEE Trans. Eng. Manag., vol. 52, pp. 227–237.

Exame (2012). "Facebook pode revelar mais sobre dados recolhidos de usuários". Available: http://exame.abril.com.br/tecnologia/facebook/noticias/facebook-pode-revelar-mais-sobre-dados-recolhidos-de-usuarios. Accessed: 24-mar-2014.

Glass, L.; Gresko, R. (2012). "Legislation and Privacy across Borders". International Conference on Privacy, Security, Risk and Trust (PASSAT), 2012 and International Confernece on Social Computing (SocialCom) 2012, pp.807,808.

GloboNews (2012). "Google se envolve em invasão de privacidade na internet". Available: http://g1.globo.com/globo-news/globo-news-em-pauta/videos/t/todos-os-videos/v/google-se-envolve-em-invasao-de-privacidade-na-internet/1818480/. Acessed: 24-mar-2014.

Han, P., Maclaurin, A. (2002). "Do consumers really care about online privacy?", Marketing Manage., vol. 11, no. 1, pp. 35-38.

IETF (2013). "Internet Engineering Task Force (IETF)". Available: http://www.ietf.org/. Accessed: 17-sep-2013.

Jmeter (2014). "Apache JMeter - Apache JMeterTM". [Online]. Available: http://jmeter.apache.org/. [Accessed: 09-jan-2014].

Lemos, R. (2013). "Atrasado, Brasil prepara lei de proteção à privacidade". Folha de São Paulo, 14 de janeiro de 2013. Available: http://www1.folha.uol.com.br/fsp/tec/ 88428-atrasado-brasil-prepara-lei-de-protecao-a-privacidade.shtml. Accessed: 12-mar-2014.

Molinari, L. (2003). "Testes de Software: Produzindo Sistemas Melhores e Confiáveis". Editora Érica Ltda, São Paulo.

Myers, G. J. (1979) “The Art of Software Testing”. John Wiley & Sons, Inc, Canada.

Oracle (2014). “Oracle | Hardware and Software, Engineered to Work Together”. Available: http://www.oracle.com/index.html. Accessed: 24-jan-2014.

Perkins, E.; Markel, M. (2004). "Multinational data-privacy laws: an introduction for IT managers". IEEE Transactions on Professional Communication, vol. 47, no.2, pp. 85,94.

Ponemon (2010). “Economic impact of privacy on online behavioral advertising - Benchmark study of Internet marketers and advertisers”. Available: http://www.ponemon.org/local/upload/file/2010_Economic_impact_of_privacy_on_OBA.pdf. Accessed: 22-may-2013.

Pressman, R. S. (2009) “Software Engineering: A practitioner's approach”. 7th Edition, MacGraw Hill.

Reay, I., Dick S., Miller. J. (2009). “A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations”. *ACM Trans. Web* 3, 2, Article 6 (April 2009), 34 pages.

R7 Notícias (2014). “Plenário pode votar Marco Civil da internet nesta semana”. Available: http://noticias.r7.com/brasil/plenario-pode-votar-marco-civil-da-internet-nesta-semana-24032014. Accessed: 24-mar-2014.

Torres, I (2012). “Um ataque contra a sua privacidade”. Revista IstoÉ, Edição 2240, 11 de outubro de 2012. Available: http://www.istoe.com.br/reportagens/245189_UM+ATAQUE+CONTRA+A+SUA+PRIVACIDADE. Accessed: 23-may-2013.

Torres-Zenteno, A.H., Martins, E., Torres, R. S., Cuaresma, J. E. (2006). “Teste de Desempenho em Aplicações SIG Web”. In: Proc. of The Ibero-American Workshop on Requirements Engineering and Software Environments, La Plata, Argentina.

TPC (2014). “TPC-W - Homepage”. Available: http://www.tpc.org/tpcw/. Accessed: 08-jan-2014.

Truste (2013). “Powering Trust In The Data Economy”. Available: http://www.truste.com/. Accessed: 19-Mar-2014.

Veja (2011). “Vida Digital - Congresso dos EUA vai investigar aplicativo para smartphones que 'rouba' dados pessoais”. Revista Veja, 01 de dezembro de 2011. Available:http://veja.abril.com.br/noticia/vida-digital/senador-americano-ira-examinar-escandalo-de-privacidade-envolvendo-smartphones. Accessed: may-2013.

Veja (2013). “EUA: governo vasculha dados de fontes como Google e Facebook”. Available: http://veja.abril.com.br/noticia/internacional/eua-governo-vasculha-dados-de-fontes-como-google-e-facebook. Accessed: 24-mar-2014.

Vieira, M., Madeira, H. (2005). “Towards a security benchmark for database management systems”, in Proceedings, of International Conference on Dependable Systems and Networks, DSN 2005. p p. 592–601.