Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security and Privacy for web Databases

Manisha Sharma
Assistant Professor, Department of Computer Science & Technology, Hindu Kanya Mahavidyalaya, Punjab, India

Abstract: Data security has consistently been a major issue in information technology. This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. The database is constructed according to a data model that defines the way in which data and interrelationships between them can be represented. The collection of software programs that provide the functionalities for defining, maintaining, and accessing data stored in a database is called a database management system (DBMS). This paper will mainly focus on security and privacy issues for web databases and services. Finally, some directions toward developing a secure semantic web will be provided.

Keywords: SOAP, WSDL, SDC

I. INTRODUCTION

A semantic web can be thought of as a web that is highly intelligent and sophisticated and one needs little or no human intervention to carry out tasks such as scheduling appointments, coordinating activities, searching for complex documents as well as integrating disparate databases and information systems. While much progress has been made toward developing such an intelligent web there is still a lot to be done. For example, there is little work on security and privacy for the semantic web. However before we examine security for the semantic web we need to ensure that the components such as web databases and web services are secure. This presentation will first focus on security and privacy issues for web databases and then discuss security and privacy for web services. Finally some directions toward developing a secure semantic web will be provided.

File encrypting ransomware has become highly problematic for both regular Internet users and organizations. However, researchers at High-Tech Bridge have spotted a new type of attack that threatens businesses. With the arrival of cloud computing and its model for IT services supported the net and large knowledge centers, the outsourcing of knowledge and computing services is getting a completely unique connation, that is predicted to skyrocket within the close to future. Business intelligence and data discovery services, square measure expected to be among the services amenable to be externalized on the cloud, thanks to their knowledge intensive nature, further because the complexness of knowledge mining algorithms. Thus, the paradigm of mining and management of knowledge as service can presumptively grow as quality of cloud computing grows

II. WEB SERVICES

Web services can be defined as an autonomous unit of application logic that provides either some business functionality features or information to other applications through an Internet connection. They are based on a set of XML standards, namely, the Simple Object Access Protocol (SOAP) [1] – to expose the service functionalities, the Web Services Description Language (WSDL) [1] – to provide an XML-based description of the service interface, and the Universal Description, Discovery and Integration (UDDI) [2] – to publish information regarding the web service and thus making this information available to potential clients. UDDI provides an XML-based structured and standard description of web service functionalities, as well as searching facilities to help in finding the provider(s) that better fit the client requirements. More precisely, an UDDI registry is a collection of entry, each of one providing information on a specific web service. Each entry is in turn composed by five main data structures businessEntity, businessService, bindingTemplate, publisherAssertion, and tModel, which provide di erent information on the web service. For instance, the BusinessEntity data structure provides overall information about the organization providing the web service, whereas the BusinessService data structure provides a technical description of the service.

III. STATISTICAL DISCLOSURE CONTROL

The three papers related to SDC consider different types of data: the first of them is about the classical problem of pro-tecting static tabular data, while the other two refer to on-line queryable databases.

The article ‘‘Adjusting the s-Argus modular approach to deal with linked tables”, by De Wolf and Giessing, is about sta-tistical disclosure control for complex tabular data, namely linked tables. In official statistics, it is common for

statistical agencies to publish multiple tabulations based on the same dataset. Those tabulations are linked through certain linear con-straints; hence, any SDC technique aimed at respondent protection must be applied in a coordinated fashion between tables. Such a coordination can be viewed as protecting a single table of higher dimensionality, which is a computational challenge. This paper considers the secondary cell suppression technique implemented in the s-Argus package and explores a modular approach providing respondent privacy with reasonable information loss and computational cost.[3]

In ‘‘Regression output from a remote analysis server”, O’Keefe and Good analyze the use of remote analysis servers to bal-ance the competing objectives of allowing statistical analysis of confidential data while maintaining appropriate standards of privacy and confidentiality. Several national statistical agencies operate such servers, which do not provide data to users, but rather allow statistical analysis to be carried out remotely. A user submits a statistical query, an analysis is carried out on the original data in a secure environment, then the user receives the results of the analysis. Unless some confidentialization is put in place, the results returned to the user may leak information on the original data on which they have been computed. This article reviews results on remote analysis servers and provides a methodology for confidentializing the output from a single regression query to a remote server.

In ‘‘A Bayesian model for disclosure control in statistical databases”, Canfora and Cavallo propose a novel approach for on-line max and min query auditing. Given a set of past max and min queries and their already disclosed answers, the query auditing system provides the answer to the current query if and only if doing so entails no privacy breach. A Bayesian net-work is used to assist such a decision process. The types of queries considered are substantially simpler than in the case of remote analysis servers, but the added complexity comes from taking into account the log of past queries and answers in the privacy analysis.[3]

IV. SECURITY AND PRIVACY FOR WEB SERVICES

Security and privacy concerns related to web services are receiving today growing attention from both the industry and research community [4]. Although most of the security and privacy concerns are similar to those of many web-based applications, one distinguishing feature of the Web Service Architecture is that it relies on a repository of information, i.e., the UDDI registry, which can be queried by service requestors and populated by service providers. Even if, at the beginning, UDDI has been mainly conceived as a public registry without specific facilities for security and privacy, today security and privacy issues are becoming more and more crucial, due to the fact that data published in UDDI registries may be highly strategic and sensitive. For instance, a service provider may not want that the information about its web services are accessible to everyone, or a service requestor may want to validate the privacy policy of the discovery agency before interacting with this entity. In the following, we thus mainly focus on security and privacy issues related to UDDI registries management. We start by considering security issues, then we deal with privacy.

V. SECURITY FOR WEB SERVICES

When dealing with security, three are the main issues that need to be faced: *authenticity*, *integrity*, and *confidentiality*. In the framework of UDDI, the au-thenticity property mainly means that the service requestor is assured that the information it receives from the UDDI comes from the source it claims to be from. Ensuring integrity means ensuring that the information are not altered during its transmission from the source to the intended recipients and that data are modified according to the specified access control policies. Finally, confiden-tiality means that information in the UDDI registry can only be disclosed to requestors authorized according to some specified access control policies. If a two-party architecture is adopted, security properties can be ensured using the strategies adopted in conventional DBMSs [5], since the owner of the informa-tion (i.e., the service provider) is also responsible for managing the UDDI. By contrast, such standard mechanisms must be revised when a third-party archi-tecture is adopted.

The most intuitive solution is that of requiring the discovery agency to be trusted with respect to the considered security properties. However, the main drawback of this solution is that large web-based systems cannot be easily verified to be trusted and can be easily penetrated. The challenge is then how such security properties can be ensured without requiring the discovery agency to be trusted.

In the following, we discuss each of the above-mentioned security properties in the context of both a two-party and a third-party architecture.

Integrity and confidentiality. If UDDI registries are managed according to a two-party architecture, integrity and confidentiality can be ensured using the standard mechanisms adopted by conventional DBMSs [6]. In particular, an *access control mechanism* can be used to ensure that UDDI entries are accessed and modified only according to the specified access control policies. Basically, an access control mechanism is a software module that filters data accesses on the basis of a set of access control policies. Only the accesses authorized by the specified policies are granted. Additionally, data can be protected during their transmission from the data server to the requestor using standard encryption techniques [6].

If a third-party architecture is adopted, the access control mechanism must reside at the discovery agency site. However, the drawback of this solution is that the discovery agency must be trusted. An alternative approach to relax this assumption is that of using a technique similar to the one proposed in [7] for the secure broadcasting of XML documents. Basically, the idea is that the service provider encrypts the entries to be published in an UDDI registry according to its access control policies: all the entry portions to which the same policies apply are encrypted with the same key. Then, it

publishes the encrypted copy of the entries to the UDDI. Additionally, the service provider is responsible for distributing keys to the service requestors in such a way that each service requestor receives all and only the keys corresponding to the information it is entitled to access. However, exploiting such solution requires the ability of querying encrypted data.

Authenticity. The standard approach for ensuring authenticity is using digi-tal signature techniques [6]. To cope with authenticity requirements, the latest UDDI specifications allow one to optionally sign some of the elements in a reg-istry, according to the W3C XML Signature syntax [8]. This technique can be successfully employed in a two-party architecture. However, it does not fit well in the third-party model, if we do not want to require the discovery agency be trusted wrt authenticity. In such a scenario, it is not possible to directly apply standard digital signature techniques, since a service requestor may require only selected portions of an entry, depending on its needs, or a combination of infor-mation residing in di erent data structures. Additionally, some portions of the requested information could not be delivered to the requestor because of access constraints stated by the specified policies.

In this context (which has been proposed in [9]) is that of applying to UDDI entries the authentication mechanism provided by Merkle hash trees. The ap-proach requires that the service provider sends the discovery agency a summary signature, generated using a technique based on Merkle hash trees, for each en-try it is entitled to manage. When a service requestor queries the UDDI registry, the discovery agency sends it, besides the query result, also the signatures of the entries on which the enquiry is performed. In this way, the requestor can locally recompute the same hash value signed by the service provider, and by comparing the two values it can verify whether the discovery agency has altered the content of the query answer and can thus verify its authenticity. However, since a requestor may be returned only selected portions of an entry, it may not be able to recompute the summary signature, which is based on the whole entry. For this reason, the discovery agency sends the requestor a set of additional hash values, referring to the missing portions, that make it able to locally perform the computation of the summary signature. We refer the interested readers to [9] for the details of the approach.

VI. PRIVACY FOR WEB SERVICES

To enable privacy protection for web services consumers across multiple domains and services, the World Wide Web Consortium working draft *Web Services Ar-chitecture Requirements* has already been defined some specific privacy require-ments for web services [10]. In particular, the working draft specifies five privacy requirements for enabling privacy protection for the consumer of a web service across multiple domains and services:

- the WSA must enable privacy policy statements to be expressed about web services;
- advertised web service privacy policies must be expressed in P3P [10];
- the WSA must enable a consumer to access a web service's advertised privacy policy statement;
- the WSA must enable delegation and propagation of privacy policy;
- web services must not be precluded from supporting interactions where one or more parties of the interaction are anonymous.

Most of these requirements have been recently studied and investigated in the W3C P3P Beyond HTTP task force [10]. Further, this task force is work-ing on the identification of the requirements for adopting P3P into a number of protocols and applications other than HTTP, such as XML applications, SOAP, and web services. As a first step to privacy protection, the W3C P3P Beyond HTTP task force recommends that discovery agencies have their own privacy policies that govern the use of data collected both from service providers and service requestors. In this respect, the main requirement stated in [10] is that collected personal information must not be used or disclosed for purposes other than performing the operations for which it was collected, except with the con-sent of the subject or as required by law. Additionally, such information must be retained only as long as necessary for performing the required operation.

VII. CONCLUSIONS

The strategies outlined above are only some of the enhancements you can make to improve the security of your systems. It is important to recognize that, while it's better late than never, security measures decrease in their effectiveness the longer you wait to implement them. Security cannot be an afterthought and must be implemented from the start alongside the services and applications you are providing.The protection of personal data in a connected world defaults not so much to high-tech applications or hardware, as to careful management of staff and relatively common techniques to ensure the simple, frequent risks are catered for. The determined criminal or government agency will get access somehow, but what matters to doctors is making sure that we take care of the data we collect about patients in a manner appropriate to the twenty-first century.

REFERENCE

[1] World Wide Web Consortium: www.w3c.org.

[2] Universal Description, Discovery and Integration (UDDI): UDDI Version 3.0, UDDI Spec Technical Committee Specification, July, 19th, 2002. Available at: http://uddi.org/pubs/uddi-v3.00-published-20020719.htm.

[3] http://crises2-deim.urv.cat/docs/publications/journals/85.pdf

[4] IBM Corporation : Security in a Web Services World: A Proposed Architecture and Roadmap, White Paper,

Version 1.0, 2002. Available at: www-106.ibm.com/developerworks/library/ws-secroad/.

[5] Castano, S., Fugini, M.G., Martella, G., Samarati, P. : Database Security (1995), Addison-Wesley.

[6] Stallings, W.: Network Security Essentials: Applications and Standards (2000), Prentice Hall

[7] Bertino, E., Ferrari, E.: Secure and Selective Dissemination of XML Documents. ACM Transactions on Information and System Security, 5(3) (2002) 290-331.

[8] World Wide Web Consortium: www.w3c.org.

[9] Bertino, E., Carminati, B., Ferrari, E.: A Flexible Authentication Method for UDDI Registries, Proceedings of the ICWS Conference, (2003), Las Vegas, Nevada, USA.

[10] Gehrke, J.: Research Problems in Data Stream Processing and Privacy-Preserving Data Mining, Proceedings of the Next Generation Data Mining Workshop (2002), Baltimore, MD, USA.

