2009 Sixth International Conference on Information Technology: New Generations

Is Continuous Compliance Assurance Possible?

Joseph M. D'Alessandro[1] Cynthia D. Tanner[1] Bonnie W. Morris[2] Tim Menzies[1]

[1]West Virginia University – LCSEE
PO Box 6109
Morgantown, WV 26506-6109

[2] West Virginia University – CB&E
PO Box 6025
Morgantown, WV 26506-6025

Abstract

The increased threat of legal sanctions or fines for failure to comply with laws and regulations make it imperative that auditors assess the level of compliance with information sharing policies and regulations in a timely manner. Embedding a monitoring mechanism, such as our Continuous Compliance Assurance (CCA) module, into a technology solution for inter-organizational information sharing, if not too costly in processing, would ensure appropriately timed compliance enforcement. A test-bed, which incorporated our CCA module, was built to capture realistic processing statistics. Through this test-bed, we have observed a limiting factor imposed by XML based processing. The feasibility of CCA rests on the reduction of these limiting factors. Accordingly we present two approaches to mitigate these issues.

Key Words: Embedded Audit Process, Monitored Information Exchange, Regulatory Compliance, XML Based Processing

Today more and more businesses, government agencies and international agencies are sharing information. The body of regulations covering this exchange of information is growing profoundly. For example, many countries have laws regarding the exchange of personal information such as Gramm-Leach-Bliley Act and HIPAA in the U.S., the European Union's 1995 and 1997 Directives on Data Protection and Privacy, and Canada's PIPEDA [1]. Furthermore, organizations have internal policies that govern the distribution and sharing of sensitive or confidential organizational information. Information technology systems are being developed to enable seamless information exchange and these systems must conform to and enforce the growing body of regulations. These emerging policies and regulations regarding information exchange suggest the need for an embedded in-stream monitoring system to ensure regulatory compliance.

The inclusion of our Continuous Compliance Assurance (CCA) mechanism provides existing information sharing facilities with an internal audit capability. CCA is a policy driven process which accepts an XML message containing the information to be shared, verifies that all applicable regulatory polices are conformed with and routes the verified message to its recipient. At any point in the process, if non-compliance is detected, user determined resolution steps are taken. The mechanism creates an audit log of the message which allows both external independent ex-post facto auditing and examination of data access and exchange.

A prototype CCA system has been implemented at West Virginia University. The prototype has been incorporated into a test-bed environment which simulates data sharing between various trading partners. Through this test-bed, we have observed a limiting factor imposed by XML based processing. We propose that the feasibility of an automated internal audit process is directly reliant on the reduction of the limiting effects imposed by XML based processing. Data from the test-bed indicates that this type of processing consumes 70% of the total processing time required by our CCA mechanism. There are two approaches that we feel will best reduce the time cost of compliance assurance. These two approaches are: intra-process optimization using an algorithm called MinContext [3] and pre-process optimization using a document size reduction technique called Type Based Document Projection [4].

References

[1] American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants 2006. *Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* New York.

[2] Debreceny, R. S., G. L. Gray, J-J Ng, Kevin Lee, and W-F Yau. 2005. Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Functionality. *Journal of Information Systems*. Fall. 19 (2): 7-28.

[3] Gottlob, G., Koch, C., and Pichler, R. 2005. Efficient algorithms for processing XPath queries. *ACM Trans. Database Syst.* 30, 2 (Jun. 2005), 444-491.

[4] Benzaken, V., Castagna, G., Colazzo, D., and Nguyên, K. 2006. Type-based XML projection. In *Proceedings of the 32nd international Conference on Very Large Data Bases* (Seoul, Korea, September 12 - 15, 2006

978-0-7695-3596-8/09 $25.00 © 2009 IEEE
DOI 10.1109/ITNG.2009.270