International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **9**, September **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 3787–3817

SCMAS: A DISTRIBUTED HIERARCHICAL MULTI-AGENT ARCHITECTURE FOR BLOCKING ATTACKS TO DATABASES

Javier Bajo[1], Juan M. Corchado[2], Cristian Pinzón[2]
Yanira De Paz[2] and Belén Pérez-Lancho[2]

[1]Universidad Pontificia de Salamanca
Compañía 5, 37002, Salamanca, Spain
jbajope@upsa.es

[2]Departament of Computer Science
University of Salamanca
Plaza de la Merced s/n, 37008, Salamanca, Spain
{ corchado; cristian_ivanp; yanira; lancho }@usal.es

Received February 2009; revised June 2009

Abstract. *One of the main attacks on databases is the SQL injection attack which causes severe damage both in the commercial aspect and the confidence of users. This papers presents a novel strategy for detecting and preventing SQL injection attacks consisting of a multi-agent based architecture called SCMAS. The SCMAS architecture is structured in hierarchical layers and incorporates SQLCBR agents with improved learning and adaptation capabilities. The SQLCBR agents presented within this paper have been specifically designed to classify SQL injection attacks and to predict the behaviour of malicious users. These agents incorporate a new technique based on a mixture of neural networks and a technique based on a temporal series. This paper begins with a detailed explanation of the SCMAS architecture and the SQLCBR agents. The results of their application to a case study are then presented and discussed.*
Keywords: Multi-agent, Case based reasoning, Security database, SQL injection, Intrusion detection system

1. **Introduction.** For several years, databases have been a key element of the technology components in organizations. Nevertheless, security is a serious problem for databases and it has become a complex task due to continuous threats and the emergence of new vulnerabilities [7]. In addition, the recent emergence of mobile technologies such as the Personal Digital Assistant (PDA), Smart Phone and laptop computer, as well as greater interconnection of networks across wireless networks, have caused a revolution in the supply of services [27]. This new philosophy of communication allows users to access information anywhere and anytime. The problem of open environments is the complexity of providing full protection. Over the last years, one of the most serious security threats around databases has been the SQL Injection attack [25]. In spite of being a well-known type of attack, the SQL injection remains at the top of the published threat list. The solutions proposed so far seem insufficient to block this type of attack because the vast majority are based on centralized mechanisms [26, 29, 30] with little capacity to work in distributed and dynamic environments. Furthermore, the detection and classification mechanisms proposed by these solutions lack the learning and adaptation capabilities for dealing with attacks and variations of the attacks that may appear in the future.

This study presents SQL-CBR Multi-agent System (SCMAS), a distributed hierarchical multi-agent architecture for blocking database attacks. SCMAS proposes a novel strategy