An ontology-based secure design framework for graph-based databases

Manuel Paneque[1], María del Mar Roldán-García[1], Carlos Blanco[2], Alejandro Maté[4], David G. Rosado[3], and Juan Trujillo[4]

[1] ITIS Software, Department of Computer Science and Programming Languages, University of Málaga, Spain
{mpaneque,mrgarcia}@uma.es
[2] ISTR Research Group, Department of Computer Science and Electronics, University of Cantabria, Spain
carlos.blanco@unican.es
[3] GSyA Research Group, Department of Information Technologies and Systems, University of Castilla-La Mancha, Spain
david.grosado@uclm.es
[4] Lucentia Research Group, Department of Software and Computing Systems, University of Alicante, Spain
{amate@,jtrujillo}@dlsi.ua.es

Keywords: Ontology, Security, Reasoning, Knowledge extraction, Healthcare
Published in: Computer Standards & Interfaces, Vol. 88, pp. 103801, 2024
Impact Factor: JCR 5.00 - Q1 - Position: 17/108 - Area: COMPUTER SCIENCE / SOFTWARE ENGINEERING
DOI: https://doi.org/10.1016/j.csi.2023.103801

Abstract. Graph-based databases are concerned with performance and flexibility. Most of the existing approaches used to design secure NoSQL databases are limited to the final implementation stage, and do not involve the design of security and access control issues at higher abstraction levels. Ensuring security and access control for Graph-based databases is difficult, as each approach differs significantly depending on the technology employed. In this paper, we propose the first technology-ascetic framework with which to design secure Graph-based databases. Our proposal raises the abstraction level by using ontologies to simultaneously model database and security requirements together. This is supported by the TITAN framework, which facilitates the way in which both aspects are dealt with. The great advantages of our approach are, therefore, that it: allows database designers to focus on the simultaneous protection of security and data while ignoring the implementation details; facilitates the secure design and rapid migration of security rules by deriving specific security measures for each underlying technology, and enables database designers to employ ontology reasoning in order to verify whether the security rules are consistent. We show the applicability of our proposal by applying it to a case study based on a hospital data access control.