MMO: A Lightweight Semantic and Trust Model for Metadata

Valentin Mouche
Université de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA
Mont de Marsan, France

Nouha Laamech
University Mohammed VI Polytechnic, COLCOM
Rabat, Morocco
Nouha.laamech@um6p.ma

Manuel Munier
Université de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA
Mont de Marsan, France
Manuel.munier@univ-pau.fr

Abstract

Metadata play a critical role in structuring and contextualizing data, particularly in security systems where provenance, quality, and traceability directly influence the reliability and accountability of downstream models. However, definitions and practices around metadata remain fragmented across domains, limiting their reuse and interoperability. This paper presents a lightweight, extensible ontology for metadata, based on Semantic Web standards, metadata are designed to support secure data exchange, enhance trust through semantic transparency, and enable robust provenance tracking across complex information systems. Covering key metadata dimensions, descriptive, structural, administrative, and temporal, the ontology also incorporates provenance and dynamic metadata, enabling auditable data flows and consistent handling to strengthen data integrity, traceability, and security in critical systems.

CCS Concepts

• **Security and privacy → Formal security models**; **Formal methods and theory of security**.

Keywords

Metadata, Semantic Model, Security and Trust, Knowledge Management

ACM Reference Format:
Valentin Mouche, Nouha Laamech, and Manuel Munier. 2025. MMO: A Lightweight Semantic and Trust Model for Metadata . In *The 6th Workshop on Secure IoT, Edge and Cloud systems (SIoTEC '25), November 10–14, 2025, Seoul, Republic of Korea.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3770740.3771879

1 Introduction

Data-driven applications increasingly depend on the collaboration of multiple stakeholders to achieve their objectives efficiently and reliably. These applications typically involve the integration of heterogeneous information systems that must interoperate seamlessly and share data across organizational or technical boundaries. For instance, in the energy domain, various entities such as smart buildings, industrial facilities, and energy providers exchange consumption data in order to optimize resource allocation, reduce waste, and promote the integration of renewable energy sources. In such distributed environments, the reliability and trustworthiness of shared data become a critical concern, particularly for applications in regulated or security-sensitive sectors [1, 21]. Traditional metrics used to evaluate data quality, namely confidentiality, integrity, availability, and traceability, are necessary but insufficient [14]. These properties do not fully capture the semantic, contextual, or operational characteristics of data that influence its reliability in practice.

To address these limitations, recent research emphasizes the role of metadata for security as a first-class component in assessing data quality [6]. According to the National Information Standards Organization (NISO), metadata are defined as "structured information that describes, explains, locates, or otherwise represents something else" [22]. This definition emphasizes the diverse roles metadata can play, ranging from descriptive and explanatory to locational and representative functions. Crucially, metadata are not static annotations: they are inherently contextual and dynamic, shaped by the nature of the data they describe and the environment in which they are used. For instance, it can be used to enhance decision making [8], the transparency of open data [23], or the basement of machine-learning security algorithms [11].

Metadata do more than only describing data, it enables easier data discovery, and can help increase understanding of a given information. For example, in a smart city, air quality data collected by sensors is accompanied by metadata such as location, timestamp, and sensor status. Additionally, metadata can offer contextual clues that help users better grasp the content and relevance of the data they are examining, ensuring accurate interpretation across information systems [17]. We advocate that detailed, semantically rich metadata can be considerered as security and trust metrics. Beyond describing content or format, metadata must capture operational and contextual information such as provenance, access control, usage constraints, and applied transformations. For instance, being able to trace the lineage of data from raw system logs to processed indicators is critical for validating incident reports, conducting forensic analysis, or ensuring compliance with security policies. Metadata can also support early detection of anomalies, inconsistencies, or policy violations, before they propagate through systems [9]. Although the importance of metadata quality has gained increasing attention in recent years, there is still no universally accepted formalism. Definitions of metadata quality are often highly domain-specific and tend to vary significantly across different domains. Moreover, this lack of standardization challenge interoperability

SIoTEC '25, Seoul, Republic of Korea

ACM ISBN 978-1-4503-XXXX-X/2018/06
https://doi.org/10.1145/3770740.3771879