


Chapter 1

Achieving Balance Between Innovation and Security in the Cloud With Artificial Intelligence of Things: Semantic Web Control Models


R. Sundar

Department of Computer Science and Engineering, Madanapalle Institute of Technology and Science, Madanapalle, India

P. Balaji Srikanth

 <https://orcid.org/0000-0003-4717-7367>
Department of Networking and Communications, SRM Institute of Science and Technology, Kattankulathur, India

Darshana A. Naik

 <https://orcid.org/0000-0001-5103-3089>
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, India


V. P. Murugan

Department of Mathematics, Panimalar Engineering College, Chennai, India

Madhavi Karumudi

Department of Computer Science and Engineering, St. Peter's Engineering College, Hyderabad, India

Sampath Boopathi

 <https://orcid.org/0000-0002-2065-6539>
Department of Mechanical Engineering, Muthayammal Engineering College, Namakkal, India

ABSTRACT

This chapter explores the integration of Semantic Web control models, innovation, and security in cloud computing, especially in the context of AIoT integration. The Semantic Web provides machine-understandable data and offers sophisticated control models that enhance innovation and security in cloud environments. Technologies like RDF, OWL, and SPARQL enable semantic interoperability, while control models focus on access control mechanisms and authentication strategies. The chapter introduces the concept of AIoT, integrating AI with IoT devices and discusses the potential of Semantic Web control models in managing security risks and fostering innovation.

DOI: 10.4018/979-8-3693-1487-6.ch001

INTRODUCTION

The Semantic Web, a concept by Tim Berners-Lee, has revolutionized data management and information retrieval on the internet. It aims to improve the meaning of data, enabling machines to better understand and interpret information. Semantic Web control models govern access, manipulation, and dissemination of semantic data, fostering semantic interoperability, innovation, and security within digital ecosystems. Semantic Web control models use semantic enrichment to annotate data with metadata, enhancing querying, reasoning, and inference, enabling machines to perform complex tasks autonomously (Anwar, 2022). Key technologies include RDF (Resource Description Framework) and OWL (Web Ontology Language), which standardize data representation and linking, and SPARQL (SPARQL Protocol and RDF Query Language) for querying and manipulating RDF data, facilitating seamless access to semantic information (Martinez-Rodriguez et al., 2020).

Semantic Web control models aim to establish robust access control mechanisms for semantic data dissemination. By implementing fine-grained access policies based on user roles, privileges, and contextual attributes, organizations can safeguard sensitive information, promote collaboration, and ensure data integrity constraints and provenance tracking, ensuring the reliability and trustworthiness of semantic data sources. Semantic Web control models are essential for driving innovation by promoting semantic interoperability across diverse data sources and applications (Yahya et al., 2021a). They standardize data representations, enabling seamless integration and facilitating the development of new applications. These models also enable organizations to utilize emerging technologies like artificial intelligence, machine learning, and IoT by providing a coherent framework for data integration and analysis. By leveraging these models, organizations can navigate digital ecosystems confidently, driving value creation and fostering a culture of data-driven decision-making.

The integration of cloud computing has revolutionized the way businesses operate, offering agility, scalability, and cost-effectiveness. However, this has also brought risks such as data breaches, cyberattacks, and compliance violations. To mitigate these risks, organizations must strike a delicate balance between innovation and security. Cloud-native technologies like serverless computing, containerization, and microservices architectures enable rapid application development and deployment, allowing businesses to respond quickly to market changes (Costa Lima et al., 2023; Yahya et al., 2021a). Therefore, organizations must balance their pursuit of innovation with robust security measures to protect against these threats. Cloud environments present inherent security challenges, necessitating proactive risk management strategies. The shared responsibility model, where service providers and customers share responsibility for securing assets, emphasizes collaboration and transparency. Implementing a multi-layered approach to security, including network security, identity and access management, encryption, and continuous monitoring, can fortify defenses against evolving threats while preserving cloud technologies' agility and flexibility.

Achieving a balance between innovation and security in the cloud is crucial for maintaining data integrity and regulatory compliance, especially in highly regulated industries like finance, healthcare, and government. Data privacy regulations like GDPR, CCPA, and HIPAA require robust security controls and privacy-enhancing technologies to safeguard sensitive information and uphold consumer trust (Sepasgozar et al., 2020). Failure to comply can lead to financial penalties, legal liabilities, and eroded brand reputation, emphasizing the importance of prioritizing security alongside innovation. The relationship between innovation and security is crucial for maximizing cloud computing's potential while safeguarding critical assets and ensuring regulatory compli-

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/achieving-balance-between-innovation-and-security-in-the-cloud-with-artificial-intelligence-of-things/347403

Related Content

Ubiquitous Semantic Applications: A Systematic Literature Review

Timofey Ermilov, Ali Khaliliand Sören Auer (2014). *International Journal on Semantic Web and Information Systems* (pp. 66-99).

www.irma-international.org/article/ubiquitous-semantic-applications/113714

Semantic Extension of Query for the Linked Data

Pu Li, Yuncheng Jiang, Ju Wangand Zhilei Yin (2017). *International Journal on Semantic Web and Information Systems* (pp. 109-133).

www.irma-international.org/article/semantic-extension-of-query-for-the-linked-data/189767

Semantic Multimedia Information Anaylsis for Retrieval Applications

Joao Magalhaesand Stefan Ruger (2007). *Semantic-Based Visual Information Retrieval* (pp. 334-354).

www.irma-international.org/chapter/semantic-multimedia-information-anaylsis-retrieval/28934

Towards Practical ABox Abduction in Large Description Logic Ontologies

Jianfeng Du, Guilin Qi, Yi-Dong Shenand Jeff Z. Pan (2012). *International Journal on Semantic Web and Information Systems* (pp. 1-33).

www.irma-international.org/article/towards-practical-abox-abduction-large/70741

Semi-Automatic Ground Truth Annotation for Benchmarking of Face Detection in Video

Dzmitry Tsishkou, Liming Chenand Eugeny Bovbel (2007). *Semantic-Based Visual Information Retrieval* (pp. 187-207).

www.irma-international.org/chapter/semi-automatic-ground-truth-annotation/28927