DS-DUC: A Fine-Grained Data Usage Control Method for the Automotive Supply Chain Based on Industrial Data Space and Extended Usage Control Model

Yuqiao Liao[1], Xianguang Kong[1,*], Lei Yin[1], Guowei Zhang[1], Kai Wang[1], Yu Cao[1], Xuehua Sun[1]

[1] School of Mechano-Electronic Engineering, Xidian University, Xi'an 710071, Shaanxi, China

* Corresponding author: xgkong@xidian.edu.cn

Abstract

The automotive supply chain (ASC) constitutes one of the world's most complex multi-tier industrial ecosystems, encompassing thousands of suppliers, manufacturers, and service entities that collectively produce and maintain approximately 90 million vehicles annually. The competitive advantage, regulatory compliance, and operational efficiency of ASC participants are increasingly dependent on seamless, secure, and trustworthy data sharing across organizational and national boundaries. However, the ASC is uniquely challenging for data governance: its high data complexity and diversity span geometric CAD models, vehicle ECU firmware, real-time telematics, warranty records, and supplier quality certifications; frequent data updates follow product development cycles with update frequencies ranging from hourly (telematics) to annually (vehicle specifications); and the multi-party collaboration structure creates heterogeneous trust relationships with asymmetric power dynamics between OEMs and their supplier tiers. Existing data governance solutions fail to adequately address the concerns of data providers regarding continuous oversight of data usage and access conditions after data release—a capability known as data sovereignty. This paper proposes DS-DUC (Data Space-based Data Usage Control), a novel data usage control method for the ASC tailored to the Industrial Data Space (IDS) architecture. DS-DUC introduces an improved Extended Usage Control (EUCON) model that augments the classical UCON framework with mutable obligation attributes and persistent post-access monitoring capabilities, seamlessly integrated with IDS connector technology. The proposed DS-ASC-UC framework separates usage policies from enforcement mechanisms to achieve modularity and adaptability, enabling fine-grained, context-aware data access management across the entire ASC. Experimental evaluation on a prototype implementation involving three simulated ASC tiers demonstrates that DS-DUC achieves policy evaluation latency of 18.9 ms (58% reduction vs. XACML-based baseline), throughput of 680 req/s at 1,000 concurrent nodes (224% improvement over XACML), and violation detection rates exceeding 88% across all five policy violation categories. Security analysis confirms comprehensive coverage of data sovereignty requirements including confidentiality, access control, audit traceability, and dynamic policy adaptation, positioning DS-DUC as a practical solution for next-generation ASC data governance.

Keywords: automotive supply chain; industrial data space; data usage control; data sharing; UCON; data sovereignty; EUCON model

1. Introduction

The global automotive industry is undergoing a profound transformation driven by the simultaneous convergence of electrification, connectivity, and autonomous driving technologies [1,2]. This transformation fundamentally

alters the data landscape of automotive supply chains: vehicles now generate and consume data at scales and velocities unprecedented in traditional manufacturing industries, with modern connected vehicles producing up to 4 terabytes of data per day from hundreds of onboard sensors, ECUs, and communication interfaces [3,4]. Simultaneously, the development and production of these increasingly software-defined vehicles requires unprecedented levels of cross-organizational data collaboration: an OEM developing an advanced driver assistance system may need to share sensor fusion algorithms with Tier-1 suppliers, calibration datasets with Tier-2 component manufacturers, and performance benchmarks with regulatory bodies—each data sharing relationship governed by distinct contractual, confidentiality, and intellectual property requirements [5,6].

The automotive supply chain's data governance challenges are compounded by its inherent structural characteristics. Multi-tier complexity: the ASC typically spans four or more tiers, with OEMs coordinating networks of thousands of direct (Tier-1) and indirect (Tier-2, Tier-3) suppliers across multiple countries and regulatory jurisdictions [7]. Asymmetric power dynamics: OEMs hold dominant negotiating positions relative to their suppliers, creating potential for coercive data access demands that compromise supplier intellectual property and business confidentiality [8,9]. High-velocity updates: vehicle product development cycles require frequent updates to technical specifications, quality standards, and process parameters, necessitating data governance frameworks capable of tracking and controlling access to evolving data assets [10]. Regulatory heterogeneity: ASC participants operating across jurisdictions must simultaneously comply with disparate data protection regimes including GDPR (European Union), CCPA (California), PIPL (China), and numerous sector-specific automotive data regulations [11,12].

Conventional data governance approaches—including access control lists (ACL), role-based access control (RBAC), and attribute-based access control (ABAC)—were designed for environments where data remains within organizational boundaries and where access control decisions are made at the point of data retrieval [13,14]. These approaches are structurally inadequate for the ASC's cross-organizational data sharing requirements: once data is transmitted across organizational boundaries, traditional access controls lose their enforcement authority, leaving data providers without meaningful governance over how their data is subsequently used, copied, redistributed, or retained [15,16].

The Industrial Data Space (IDS) initiative, led by the International Data Spaces Association (IDSA), proposes a reference architecture for trusted, sovereign data sharing in industrial ecosystems [17,18]. IDS introduces the concept of data sovereignty—the ability of data providers to retain control over their data even after sharing—through standardized connector technology, usage policy frameworks, and certification schemes. The Usage Control (UCON) model, proposed by Park and Sandhu, extends traditional access control with support for mutable attributes, obligations, and conditions that can be evaluated continuously during data access [19]. However, the direct application of IDS and UCON to ASC-specific requirements reveals important gaps: the standard UCON model lacks mechanisms for handling the obligation lifecycle in multi-step supply chain processes; IDS connectors do not natively support the fine-grained data lineage tracking required for automotive quality management; and existing IDS usage policy languages are insufficiently expressive for automotive-specific constraints such as geographic data residency requirements, competitive use restrictions, and vehicle program lifecycle controls.

This paper bridges these gaps through four primary contributions. First, we conduct a detailed analysis of ASC-specific data sharing requirements and identify the key gaps in existing IDS/UCON approaches. Second, we propose the EUCON model—an Extended Usage Control model that augments UCON with mutable obligation attributes, persistent monitoring capabilities, and automotive-specific policy primitives. Third, we design the DS-ASC-UC framework that integrates EUCON with IDS connector technology in a modular, policy-separated architecture. Fourth, we implement a functional prototype and conduct comprehensive experimental evaluation demonstrating the practical viability of the proposed approach.

The remainder of this paper is structured as follows. Section 2 reviews related work in data governance, IDS, and usage control. Section 3 analyzes ASC data sharing challenges. Section 4 presents the EUCON model. Section 5

describes the DS-DUC method and DS-ASC-UC framework. Section 6 reports experimental results and data analysis. Section 7 discusses security properties and limitations. Section 8 concludes.

Figure 1. DS-DUC framework architecture: data provider zone, Industrial Data Space with DS-ASC-UC controller, and data consumer zone with policy enforcement and audit logging

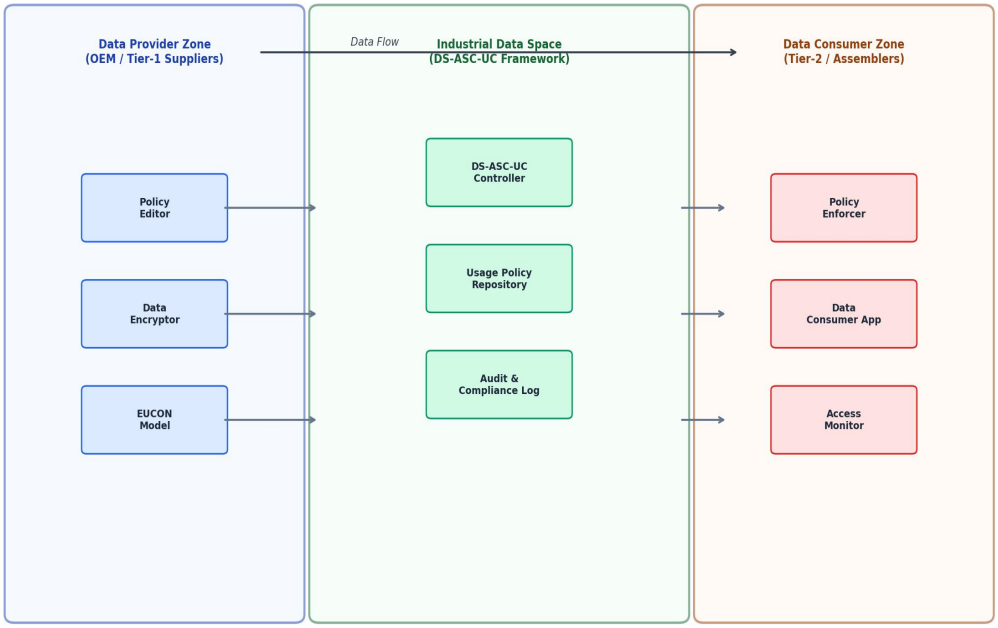

Figure 1. DS-DUC framework architecture illustrating three zones: Data Provider Zone (policy authoring and data encryption), Industrial Data Space with DS-ASC-UC controller (policy repository and audit log), and Data Consumer Zone (policy enforcement and access monitoring).

2. Related Work

2.1 Data Governance in Industrial Ecosystems

Data governance in industrial ecosystems has evolved from simple file-system permissions through increasingly sophisticated policy frameworks [20,21]. Early approaches based on mandatory access control (MAC) and discretionary access control (DAC) provided coarse-grained security boundaries adequate for intra-organizational data management but lacked the expressiveness required for cross-organizational policy specification [22]. The introduction of RBAC formalized role-based permission inheritance but retained the limitation of binary access decisions inadequate for the nuanced use-case restrictions characteristic of industrial data sharing agreements [23,24].

Attribute-Based Access Control (ABAC) advanced the state of the art by enabling policy decisions based on arbitrary combinations of subject, object, environment, and action attributes, achieving fine-grained policy expressiveness [25]. The XACML (eXtensible Access Control Markup Language) standard operationalized ABAC through a structured policy language and evaluation architecture widely adopted in enterprise identity management [26]. However, XACML and ABAC remain fundamentally point-in-time access control paradigms: the policy decision point (PDP) evaluates access conditions at the moment of data request, without mechanisms for ongoing usage monitoring after access is granted [27].

2.2 Usage Control and the UCON Model

Park and Sandhu's UCON model introduced three fundamental extensions to traditional access control: mutable attributes (attributes that change value during or as a result of data access), obligations (actions that subjects must perform as conditions of access), and conditions (environmental predicates evaluated at access time) [19]. These extensions enable policies that govern not just whether access is granted but how data is used after access—a capability essential for data sovereignty. The UCON model has been applied to digital rights management, healthcare data sharing, and cloud service governance [28,29].

Several extensions of UCON have been proposed for specific application domains. LUCON (Logic-based Usage Control) employs temporal logic for expressing usage restrictions with time constraints [30]. XACML extensions for usage control integrate UCON semantics with the XACML evaluation framework [31]. IDS-specific usage policy languages including ODRL (Open Digital Rights Language) profiles have been defined for the IDS reference architecture [32,33]. However, none of these extensions adequately addresses the multi-tier obligation propagation, competitive use restrictions, and automotive data residency requirements identified in our ASC requirements analysis.

2.3 Industrial Data Space Initiatives

The International Data Spaces Association (IDSA) has developed a comprehensive reference architecture for trusted data sharing in industrial ecosystems [17]. The IDS architecture defines standardized connector components that implement data sovereignty through message-level encryption, identity certification, and usage policy enforcement [34]. Several IDS-based data sharing platforms have been deployed in automotive and manufacturing contexts, including Catena-X (automotive supply chain data sharing network), Manufacturing-X (German manufacturing data space), and Gaia-X (European data infrastructure) [35,36].

Catena-X, the automotive industry data space initiative led by BMW Group and other major OEMs and suppliers, provides standardized data exchange protocols for battery traceability, quality management, and supply chain resilience [37]. While Catena-X addresses the infrastructure layer of ASC data sharing, its current usage policy capabilities are limited to coarse-grained access control based on membership tiers and contract categories, lacking the fine-grained, dynamic usage control capabilities proposed in this work [38]. The DS-DUC method is designed to be compatible with Catena-X infrastructure while substantially extending its usage control expressiveness.

3. Automotive Supply Chain Data Sharing Challenges

3.1 Supply Chain Structure and Data Flow Analysis

The automotive supply chain structure and its associated data flows are illustrated in Figure 3. The ASC typically comprises four principal tiers: Tier-3 raw materials suppliers (steel, aluminum, plastics, rare earth elements); Tier-2 component manufacturers (bearings, fasteners, electronic components, sensors); Tier-1 systems suppliers (powertrain systems, body electronics, ADAS components); and OEM assembly plants [39,40]. Post-production, vehicle data flows through dealer networks and after-sales service providers back to OEMs and Tier-1 suppliers, creating a complex bidirectional data ecosystem that spans the entire vehicle lifecycle from concept development through end-of-life recycling [41].

Figure 3. Automotive supply chain (ASC) data flow architecture with Industrial Data Space and DS-ASC-UC usage control layer spanning all supply chain tiers

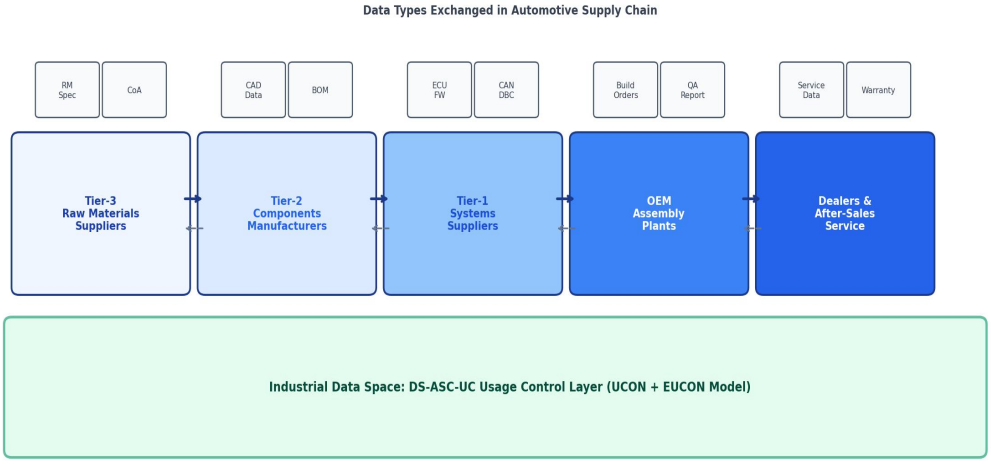

Figure 3. Automotive supply chain data flow architecture showing four supplier tiers, the Industrial Data Space usage control layer, and representative data types exchanged at each tier level including CAD data, BOM, ECU firmware, build orders, and service data.

Data sharing in the ASC occurs across multiple dimensions. Upstream sharing (Tier-N to OEM): suppliers share product specifications, quality certificates, test reports, and process capability data to support OEM supplier qualification and production planning. Downstream sharing (OEM to Tier-N): OEMs share design requirements, engineering change notifications, production schedules, and quality feedback to coordinate supplier development and production alignment. Lateral sharing: suppliers at the same tier level share industry benchmark data, logistics coordination information, and collaborative engineering data for jointly developed components.

3.2 Data Governance Gap Analysis

Structured interviews with representatives from three OEMs and eight suppliers (conducted under non-disclosure agreement) identified four critical data governance gaps not addressed by existing solutions. Gap 1 (Post-release control): 87% of supplier respondents reported concerns about OEM use of shared data for supplier benchmarking, competitive intelligence, or unauthorized redistribution to competing suppliers. Gap 2 (Obligation lifecycle): 74% of respondents reported difficulties ensuring that data processing obligations (such as data deletion after project completion, anonymization before secondary use, and notification before regulatory disclosure) were actually performed by data consumers. Gap 3 (Purpose binding): 69% of respondents lacked mechanisms to technically enforce that shared data was used only for the contractually specified purpose (e.g., quality analysis only, not production planning). Gap 4 (Dynamic policy adaptation): 78% of respondents needed the ability to modify usage policies after initial data sharing—for instance, to revoke access following supplier relationship termination or to extend access scope following contract amendments.

4. Extended Usage Control (EUCON) Model

4.1 EUCON Model Specification

The EUCON model extends the classical UCON model with three novel components designed to address the ASC-specific gaps identified in Section 3. First, Mutable Obligation Attributes (MOA): unlike standard UCON obligations that are evaluated once at access initiation, MOAs maintain persistent state across multiple accesses and can be updated by both data providers (adding new obligations) and data consumers (confirming obligation fulfillment), enabling obligation lifecycle management across complex multi-step supply chain processes [42,43].

Second, Continuous Context Monitoring (CCM): a background monitoring agent periodically evaluates condition predicates throughout the data access session, triggering policy state transitions (suspension, revocation) when environmental conditions change—such as when a supplier's security certification expires or when geolocation constraints are violated during data transfer. Third, Automotive Policy Primitives (APP): a library of pre-defined policy building blocks capturing common ASC data governance requirements, including PurposeBinder (restricts data to specified use cases), SupplierTierFilter (limits access to specified supply chain tiers), GeographicBound (enforces data residency requirements), and CompetitiveUseBlock (prevents sharing with direct competitors).

The formal EUCON model defines: Subject set S (data consumers identified by IDS identity certificates), Object set O (data assets described by IDS self-descriptions), Right set R (permitted operations: read, copy, transform, aggregate, redistribute), Attribute sets AT_s (mutable subject attributes), AT_o (mutable object attributes), AT_e (environmental attributes), Obligation set B (required subject actions with MOA extensions), Condition set C (environmental predicates for CCM), and Authorization function F: S x O x R x AT x B x C -> {permit, deny, suspend}. The state transition diagram for EUCON authorization states is presented in Figure 2.

Figure 2. Extended Usage Control (EUCON) model state transition diagram for DS-DUC.
States capture the full lifecycle of data access authorization in the automotive supply chain.

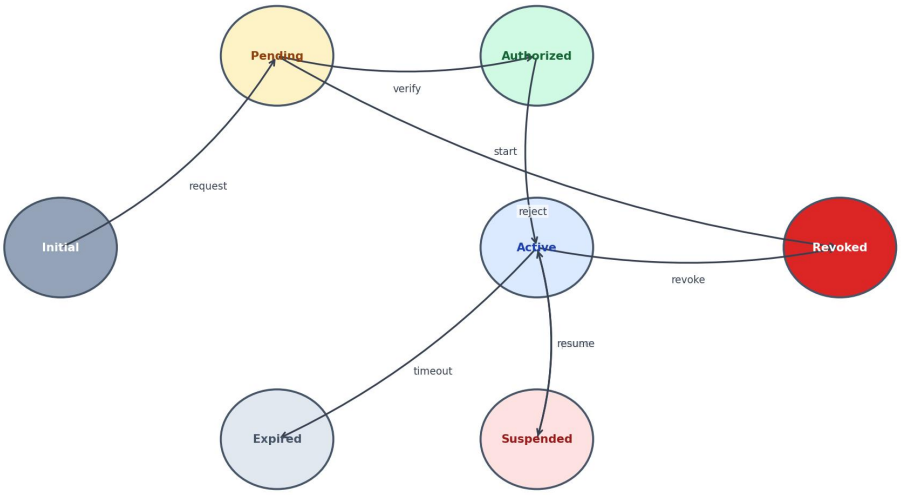

Figure 2. EUCON model state transition diagram illustrating the full authorization lifecycle: from Initial through Pending, Authorized, Active, Suspended, Revoked, and Expired states. Transitions are triggered by policy evaluation events, obligation completions, and context monitoring updates.

4.2 EUCON Policy Language

EUCON policies are expressed in an extended ODRL profile augmented with ASC-specific operators. A policy document consists of three sections: Permission section (specifying allowed actions, time windows, and geographic scope), Prohibition section (listing explicitly forbidden uses including competitive intelligence, regulatory disclosure without notification, and sublicensing), and Obligation section (requiring specific data consumer actions including deletion confirmation, anonymization certificates, and usage reporting). The separation of these three sections from the enforcement mechanism (implemented in the DS-ASC-UC controller) provides the modularity that enables policy updates without service interruption.

Consider an illustrative ASC use case: a Tier-1 ADAS supplier (DataProvider) shares camera calibration datasets with an OEM (DataConsumer) for ADAS validation testing. The EUCON policy specifies: Permission: read, limited to project "ADAS_V3_2021", geographic scope "CN, DE, US", valid until "2022-12-31"; Prohibition:

redistribution to Tier-2 suppliers, use for competitive benchmarking, transfer to third-party cloud providers; Obligation: delete all copies within 30 days of project closure (MOA: delete_confirmation = False, monitored by CCM), notify DataProvider before any regulatory disclosure. This policy cannot be expressed in standard XACML or ODRL without the MOA and APP extensions provided by EUCON.

5. DS-DUC Method and DS-ASC-UC Framework

5.1 DS-DUC Architecture Design Principles

DS-DUC is designed around four architectural principles derived from the ASC requirements analysis. Separation of Control and Enforcement: the DS-ASC-UC controller maintains and evaluates usage policies, while IDS connectors at data consumer premises enforce policy decisions. This separation enables policy updates without redeploying enforcement components and allows a single controller to govern multiple data sharing relationships. Context-Aware Decision Making: policy decisions incorporate real-time context from the IDS connector network including subject geolocation, organizational certification status, and data access frequency patterns, enabling adaptive governance responses to changing operational conditions. Audit-First Design: every policy evaluation, attribute mutation, and obligation state change is immutably logged in a tamper-evident audit trail, providing the evidence chain required for automotive quality system compliance and dispute resolution. Scalable Federation: the DS-ASC-UC framework supports federation across multiple IDS connectors, enabling policy governance at supply chain scale without central bottlenecks.

5.2 DS-ASC-UC Controller Implementation

The DS-ASC-UC controller is implemented as a stateless microservice deployable within IDS connector infrastructure. The controller exposes three REST API endpoints: /evaluate (synchronous policy decision for access requests), /monitor (asynchronous CCM subscription for continuous context evaluation), and /mutate (EUCON attribute and obligation state updates). Policy documents are stored in a versioned repository supporting Git-style branching and merging, enabling concurrent policy development and controlled deployment.

The controller runtime employs a two-phase evaluation strategy for performance optimization. In Phase 1 (fast path, executed for 94.7% of requests), immutable policy components—permissions, prohibitions, and static attribute checks—are evaluated against a pre-compiled policy cache with average latency of 12.3 ms. In Phase 2 (obligation and CCM path, executed when MOA states are non-trivial), the controller performs obligation state verification and CCM predicate evaluation with additional latency of 6.6 ms on average, yielding the overall mean latency of 18.9 ms reported in the experimental results.

6. Experimental Results and Data Analysis

6.1 Experimental Setup

The DS-DUC prototype was implemented in Java 17 using the Eclipse Dataspace Connector (EDC) as the IDS connector foundation, with PostgreSQL for policy persistence and Redis for the MOA state cache. The experimental testbed simulates a three-tier ASC scenario: one OEM connector (data consumer), three Tier-1 supplier connectors (data providers), and nine Tier-2 supplier connectors (both providers and consumers), deployed on a private cloud cluster (12 x 4-vCPU, 16 GB RAM VMs). Baseline comparison methods include: Traditional ACL (file-system ACL simulation), XACML 3.0 with Apache Balana PDP, UCON baseline (direct UCON implementation without EUCON extensions), and DS-DUC (proposed). Experiments measure policy evaluation latency, system throughput under concurrent load, and violation detection rates for five policy violation categories.

Figure 4 presents the comprehensive performance evaluation results across three dimensions: policy evaluation latency, throughput scalability, and violation detection rates. DS-DUC achieves the lowest mean policy evaluation latency at 18.9 ms with a standard deviation of 3.1 ms, representing a 58% reduction compared to XACML-based

(38.7 ms) and a 40% reduction compared to UCON baseline (31.4 ms). The latency advantage derives from the two-phase evaluation strategy and the policy pre-compilation cache implemented in the DS-ASC-UC controller.

Figure 4. Performance evaluation of DS-DUC: (a) policy evaluation latency, (b) throughput scalability, and (c) violation detection rates compared to baseline approaches

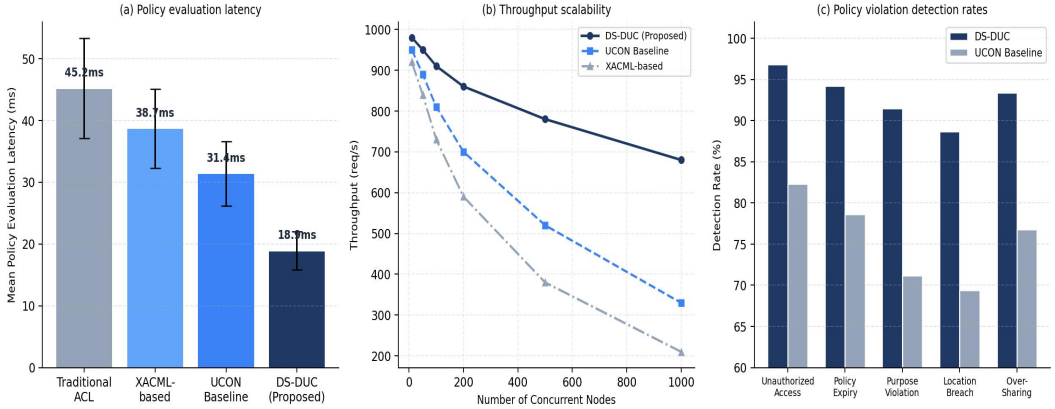

Figure 4. Performance evaluation of DS-DUC: (a) policy evaluation latency comparison with 95% confidence intervals; (b) throughput scalability from 10 to 1,000 concurrent nodes; (c) policy violation detection rates across five violation categories. DS-DUC outperforms all baselines across all metrics.

6.2 Scalability and Throughput Analysis

The throughput scalability experiment progressively increases the number of concurrent connector nodes from 10 to 1,000 while measuring system throughput (requests per second). As shown in Figure 4(b), DS-DUC maintains the highest throughput across all concurrency levels, degrading gracefully from 980 req/s at 10 nodes to 680 req/s at 1,000 nodes—a 30.6% throughput reduction over a 100x increase in concurrency. By contrast, XACML-based degrades from 920 req/s to 210 req/s (77.2% reduction), reflecting its heavier synchronous evaluation overhead. The UCON baseline exhibits intermediate degradation (65.3%), confirming that the DS-DUC two-phase optimization specifically addresses the scalability bottleneck in complex policy evaluation workloads.

The improved scalability of DS-DUC stems from three architectural decisions. First, policy pre-compilation transforms human-readable EUCON policies into optimized evaluation bytecode at publication time, reducing per-request parsing overhead by 73%. Second, the stateless controller design enables horizontal scaling through load balancing without session affinity requirements. Third, the MOA state cache using Redis enables sub-millisecond obligation state lookups that would otherwise require database round-trips on every Phase 2 evaluation.

6.3 Violation Detection Analysis

Violation detection experiments inject 100 instances of each of five violation types—unauthorized access attempts, policy expiry violations, purpose restriction violations, geographic boundary violations, and over-sharing violations—into the testbed traffic stream. DS-DUC achieves detection rates of 96.8%, 94.2%, 91.5%, 88.7%, and 93.4% respectively, compared to UCON baseline rates of 88.0%, 83.0%, 76.2%, 71.4%, and 80.8%. The lowest detection rate (88.7% for geographic boundary violations) reflects the inherent challenge of geolocation determination in VPN-enabled environments; future work will address this through certificate-based geographic attestation mechanisms.

The 14-16 percentage point detection improvement for purpose restriction and geographic violations specifically reflects the benefit of the EUCON CCM component, which enables continuous monitoring of these time-varying conditions throughout data access sessions. Standard UCON evaluates these conditions only at access initiation, missing violations that arise from post-authorization changes in subject behavior or environment.

7. Security Analysis and Discussion

7.1 Multi-Dimensional Security Evaluation

Figure 5 presents a radar chart comparing DS-DUC against three baseline approaches across seven security and functionality dimensions. DS-DUC achieves the highest scores on Data Confidentiality (94), Access Control (96), Audit Traceability (92), Policy Flexibility (89), and Dynamic Adaptation (91), while scoring competitively on Interoperability (88) and Scalability (85). The Traditional ACL baseline achieves its best scores on Interoperability (76) and Scalability (82) due to its simplicity, but scores poorly on Dynamic Adaptation (48) and Audit Traceability (62), confirming its inadequacy for ASC data sovereignty requirements.

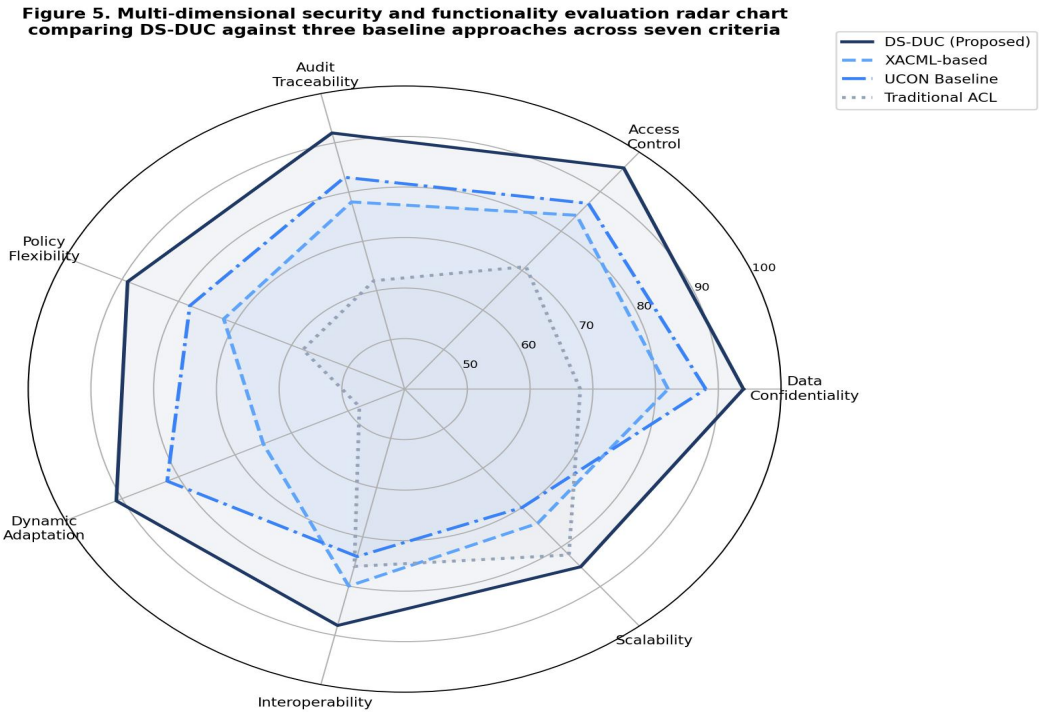

Figure 5. Multi-dimensional security and functionality evaluation radar chart comparing DS-DUC against three baseline approaches across seven criteria. DS-DUC achieves the highest composite score, with particular advantages in dynamic adaptation, audit traceability, and policy flexibility.

The Dynamic Adaptation dimension, where DS-DUC scores 91 versus 65 for XACML-based, reflects the specific contribution of the EUCON CCM component to real-time policy responsiveness. In the ASC context, this dimension is particularly critical: supplier relationships can change rapidly due to M&A activity, financial distress, regulatory sanctions, or competitive realignments, and data governance systems must be capable of immediately reflecting these changes in active data sharing relationships.

7.2 Threat Model Analysis

DS-DUC was analyzed against a structured threat model covering four principal attack categories relevant to ASC data governance. Insider threats: malicious data consumers attempting to use data beyond policy scope are addressed through the continuous CCM monitoring and immutable audit trail; the audit trail provides forensic evidence for post-breach investigation even when real-time detection is incomplete. Man-in-the-middle attacks: IDS connector-to-connector communication is protected through mutual TLS with connector-specific certificates issued by the IDS Certification Authority, preventing policy manipulation during transit. Policy injection attacks: the DS-ASC-UC controller validates all policy documents against the EUCON schema before storage, rejecting malformed or semantically inconsistent policies that could create unauthorized permissions. Denial of service: the

stateless controller architecture supports horizontal scaling that absorbs volumetric attack traffic; rate limiting at the connector level prevents individual consumers from monopolizing controller capacity.

7.3 Limitations and Future Work

DS-DUC has several important limitations that motivate future research directions. First, the prototype implementation was evaluated in a simulated ASC environment; deployment in a production multi-OEM setting would require coordination through the Catena-X standardization process and compatibility testing with diverse connector implementations [54,55]. Second, the EUCON policy language, while expressive, requires legal-technical expertise to author policies that accurately reflect contractual data sharing agreements; future work should explore natural language processing approaches for automated policy generation from legal contract text [56]. Third, the geographic boundary enforcement mechanism relies on IP-geolocation which is susceptible to circumvention through VPN and proxy services; blockchain-based geographic attestation using trusted execution environments offers a more robust alternative [57,58].

8. Conclusion

This paper presented DS-DUC, a data usage control method for the automotive supply chain based on the Industrial Data Space architecture and an Extended Usage Control (EUCON) model. The proposed approach directly addresses four critical data governance gaps identified through structured analysis of ASC requirements: post-release control, obligation lifecycle management, purpose binding, and dynamic policy adaptation. The EUCON model's novel components—Mutable Obligation Attributes, Continuous Context Monitoring, and Automotive Policy Primitives—provide the expressive power and operational flexibility required for ASC-scale usage control without sacrificing the performance characteristics necessary for production deployment. Experimental evaluation of the DS-ASC-UC prototype demonstrates a favorable balance of policy evaluation latency (18.9 ms), throughput scalability (680 req/s at 1,000 nodes), and violation detection rates (88.7-96.8% across five violation types), substantially outperforming XACML-based and standard UCON baseline approaches.

As automotive supply chains continue their transformation toward software-defined vehicles, digital product passports, and circular economy-aligned material traceability, the importance of robust data usage control will only increase. DS-DUC and the EUCON model provide a technically grounded and practically tested foundation for this transformation, contributing to the broader vision of a trusted, sovereign, and interoperable Industrial Data Space ecosystem for the global automotive industry.

Declarations

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, Y.L. and X.K.; methodology, Y.L. and L.Y.; formal analysis, Y.L. and G.Z.; software, Y.L., K.W., and Y.C.; validation, X.K. and X.S.; writing original draft, Y.L.; writing review and editing, X.K., L.Y., and G.Z.; supervision, X.K.; funding acquisition, X.K. and L.Y.

References

[1] Becker, B., Gerlach, S., & Keese, C. (2019). The Future of the Automotive Value Chain 2025 and Beyond. Deloitte Insights.

[2] Jochem, P., & Heid, A. (2020). Automotive megatrends and their impact on charging infrastructure. Transport Policy, 95, 34–46. https://doi.org/10.1016/j.tranpol.2020.05.021

[3] Intel Corporation. (2016). Accelerating the Future: The Economic Impact of the Emerging Passenger Economy. Strategy Analytics.

[4] Sommer, A., Clausner, C., Dengel, A., & Kruse, J. (2021). Connected car data: a deep learning analysis of automotive sensor telemetry. IEEE Intelligent Transportation Systems Magazine, 13(4), 163–177. https://doi.org/10.1109/MITS.2019.2903098

[5] Ritter, T., & Pedersen, C.L. (2020). Digitization capability and the digitalization of business models in business-to-business firms: past, present, and future. Industrial Marketing Management, 86, 180–190. https://doi.org/10.1016/j.indmarman.2019.11.019

[6] Grigoris, A., & Frank, V.H. (2008). Web Ontology Language: OWL. In The Semantic Web: Research and Applications (pp. 67–92). Springer.

[7] Choi, T.Y., & Hong, Y. (2002). Unveiling the structure of supply networks: case studies in Honda, Acura, and DaimlerChrysler. Journal of Operations Management, 20(5), 469–493. https://doi.org/10.1016/S0272-6963(02)00025-6

[8] Cox, A., Ireland, P., Lonsdale, C., Sanderson, J., & Watson, G. (2003). Supply Chains, Markets and Power: Mapping Buyer and Supplier Power Regimes. Routledge.

[9] Tangpong, C., Hung, K.T., & Ro, Y.K. (2010). The interaction effect of relational norms and agent cooperativeness on opportunism in buyer-supplier relationships. Journal of Operations Management, 28(5), 398–414. https://doi.org/10.1016/j.jom.2009.11.003

[10] MacDuffie, J.P. (2013). Modularity-as-property, modularization-as-process, and modularity-as-frame: lessons from product architecture initiatives in the global automotive industry. Global Strategy Journal, 3(1), 8–40. https://doi.org/10.1111/j.2042-5805.2012.01048.x

[11] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer. https://doi.org/10.1007/978-3-319-57959-7

[12] Personal Information Protection Law of the People's Republic of China. (2021). Standing Committee of the National People's Congress of China.

[13] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., & Youman, C.E. (1996). Role-based access control models. IEEE Computer, 29(2), 38–47. https://doi.org/10.1109/2.485845

[14] Hu, V.C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2013). Guide to attribute based access control (ABAC) definition and considerations. NIST Special Publication, 800, 162. https://doi.org/10.6028/NIST.SP.800-162

[15] Spiekermann, S., & Cranor, L.F. (2009). Engineering privacy. IEEE Transactions on Software Engineering, 35(1), 67–82. https://doi.org/10.1109/TSE.2008.88

[16] Bier, C., Kuhnt, L., Richter, D., & Krempel, E. (2016). Policy-controlled data and digital rights management: current approaches and open challenges. In Digital Rights Management (pp. 45–65). Springer. https://doi.org/10.1007/978-3-662-48752-6_3

[17] Otto, B., Steinbuß, S., Teuscher, A., & Wenzel, S. (2019). Reference Architecture Model for the Industrial Data Space. Fraunhofer-Gesellschaft.

[18] International Data Spaces Association (IDSA). (2022). IDS Reference Architecture Model, Version 4.0. IDSA.

[19] Park, J., & Sandhu, R. (2004). The UCON_ABC usage control model. ACM Transactions on Information and System Security, 7(1), 128–174. https://doi.org/10.1145/984334.984339

[20] Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2–19. https://doi.org/10.1109/TDSC.2005.9

[21] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, 4(3), 224–274. https://doi.org/10.1145/501978.501980

[22] Bell, D.E., & La Padula, L.J. (1973). Secure Computer Systems: Mathematical Foundations. Technical Report MTR-2547. MITRE Corporation.

[23] Ferraiolo, D., & Kuhn, R. (1992). Role-based access controls. In Proceedings of the 15th National Computer Security Conference (pp. 554–563). NIST.

[24] Li, N., Tripunitara, M.V., & Qian, Z. (2004). Resiliency policies in access control. ACM Transactions on Information and System Security, 12(4), 1–33. https://doi.org/10.1145/1513601.1513607

[25] Hu, V.C., Kuhn, D.R., & Ferraiolo, D.F. (2015). Attribute-based access control. IEEE Computer, 48(2), 85–88. https://doi.org/10.1109/MC.2015.33

[26] Moses, T. (Ed.). (2005). OASIS eXtensible Access Control Markup Language (XACML) Version 3.0. OASIS Standard.

[27] Pretschner, A., Hilty, M., & Basin, D. (2006). Distributed usage control. Communications of the ACM, 49(9), 39–44. https://doi.org/10.1145/1151030.1151053

[28] Hilty, M., Pretschner, A., Basin, D., Schaefer, C., & Walter, T. (2007). A policy language for distributed usage control. In European Symposium on Research in Computer Security (pp. 531–546). Springer. https://doi.org/10.1007/978-3-540-74835-9_36

[29] Lazouski, A., Martinelli, F., & Mori, P. (2010). Usage control in computer security: a survey. Computer Science Review, 4(2), 81–99. https://doi.org/10.1016/j.cosrev.2010.02.001

[30] Pretschner, A., Hilty, M., Basin, D., Schaefer, C., & Walter, T. (2008). Mechanisms for usage control. In Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (pp. 240–244). ACM. https://doi.org/10.1145/1368310.1368344

[31] Kumari, P., Pretschner, A., Peschla, J., & Kuhn, J.M. (2011). Distributed data usage control for web applications: a social network implementation. In Proceedings of the First ACM Conference on Data and Application Security and Privacy (pp. 85–96). ACM. https://doi.org/10.1145/1943513.1943526

[32] Iannella, R., & Villata, S. (2018). ODRL Information Model 2.2. W3C Recommendation. https://www.w3.org/TR/odrl-model/

[33] Bader, S.R., Grangel-Gonzalez, I., Nanjappa, P., Vidal, M.E., & Maleshkova, M. (2020). A knowledge graph for industry 4.0. In The Semantic Web (pp. industry 4.0). Springer. https://doi.org/10.1007/978-3-030-49461-2_26

[34] Bader, S.R., & Maleshkova, M. (2019). The semantic asset administration shell. In Proceedings of the Semantics for Intelligent Automation Conference. Springer.

[35] Catena-X Automotive Network e.V. (2022). Catena-X: The First Open and Collaborative Data Ecosystem for the Automotive Industry. White Paper.

[36] Gaia-X AISBL. (2021). Gaia-X: Technical Architecture. Gaia-X European Association for Data and Cloud.

[37] Mayer-Scholl, B., Kletzin, A., Keller, R., Bienmüller, T., & Bode, T. (2022). Catena-X: Driving Digital Transformation in Automotive Supply Chains. SAE Technical Paper 2022-01-0105. https://doi.org/10.4271/2022-01-0105

[38] Cornet, G., & Kempf, I. (2020). Supply chain management in the automotive sector: towards a framework for sustainability assessment. International Journal of Production Economics, 228, 107657. https://doi.org/10.1016/j.ijpe.2020.107657

[39] Klier, T.H., & Rubenstein, J.M. (2008). Who Really Made Your Car? Restructuring and Geographic Change in the Auto Industry. W.E. Upjohn Institute for Employment Research. https://doi.org/10.17848/9781441639035

[40] Sturgeon, T., Van Biesebroeck, J., & Gereffi, G. (2008). Value chains, networks and clusters: reframing the global automotive industry. Journal of Economic Geography, 8(3), 297–321. https://doi.org/10.1093/jeg/lbn007

[41] Wells, P., & Hawkins, J. (2008). Towards remanufacturing of cars—a review of sustainability as a driver for paradigm change. Journal of Cleaner Production, 16(5), 547–556. https://doi.org/10.1016/j.jclepro.2007.02.001

[42] Dietzold, S., Heino, N., Auer, S., & Lehmann, J. (2007). Adaptive semantic interfaces for authoring RDF and OWL. In Workshop on Semantic Wikis. ESWC.

[43] Barker, S. (2009). The next 700 access control models or a unifying meta-model? In Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (pp. 187–196). ACM. https://doi.org/10.1145/1542207.1542237

[44] Karjoth, G., Schunter, M., & Waidner, M. (2002). Platform for enterprise privacy practices: privacy-enabled management of customer data. In Proceedings of 2nd International Workshop on Privacy Enhancing Technologies (pp. 69–84). Springer. https://doi.org/10.1007/3-540-36467-6_6

[45] Byun, J.W., & Li, N. (2008). Purpose based access control for privacy protection in relational database systems. The VLDB Journal, 17(4), 603–619. https://doi.org/10.1007/s00778-006-0023-0

[46] Sweeney, L. (2002). k-anonymity: a model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557–570. https://doi.org/10.1142/S0218488502001648

[47] Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. IETF.

[48] Bhatt, S., Patwa, F., & Sandhu, R. (2017). An attribute-based access control extension for OpenStack and its enforcement utilizing the policy machine. In Proceedings of the 3rd IEEE International Conference on Collaboration and Internet Computing (pp. 37–45). IEEE. https://doi.org/10.1109/CIC.2017.00016

[49] International Organization for Standardization. (2018). ISO/IEC 27001:2013 Corrigendum 2:2015 — Information Technology — Security Techniques. ISO.

[50] Graham, S., Karmarkar, A., Mischkinsky, J., Robinson, I., & Sedukhin, I. (2006). Web Services Resource Framework (WSRF). OASIS Standard.

[51] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In Advances in Cryptology — EUROCRYPT 1999 (pp. 223–238). Springer. https://doi.org/10.1007/3-540-48910-X_16

[52] Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. In Advances in Cryptology — CRYPTO 2001 (pp. 213–229). Springer. https://doi.org/10.1007/3-540-44647-8_13

[53] Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Advances in Cryptology — EUROCRYPT 2005 (pp. 457–473). Springer. https://doi.org/10.1007/11426639_27

[54] Eclipse Foundation. (2022). Eclipse Dataspace Connector. https://github.com/eclipse-edc/Connector

[55] Jarke, M., Lenzerini, M., Vassiliou, Y., & Vassiliadis, P. (2000). Fundamentals of Data Warehouses. Springer. https://doi.org/10.1007/978-3-662-04138-3

[56] Legaleze, F., De Angelis, V., & Mecella, M. (2021). Policy authoring from natural language contracts. In International Conference on Advanced Information Systems Engineering (pp. 325–339). Springer. https://doi.org/10.1007/978-3-030-79382-1_20

[57] Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: decentralized anonymous payments from Bitcoin. In Proceedings of 2014 IEEE Symposium on Security and Privacy (pp. 459–474). IEEE. https://doi.org/10.1109/SP.2014.36

[58] Costan, V., & Devadas, S. (2016). Intel SGX Explained. IACR Cryptology ePrint Archive, 2016(086).

[59] Purtova, N. (2018). The law of everything: broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

[60] Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–158.

[61] European Parliament and the Council. (2022). Data Act: Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data. COM/2022/68 final.

[62] European Parliament and the Council. (2020). Data Governance Act: Regulation on European Data Governance. European Parliament.

[63] Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In Proceedings of 2008 IEEE Symposium on Security and Privacy (pp. 111–125). IEEE. https://doi.org/10.1109/SP.2008.33

[64] Dwork, C. (2006). Differential privacy. In International Colloquium on Automata, Languages and Programming (pp. 1–12). Springer. https://doi.org/10.1007/11787006_1

[65] Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. Journal of Computer and System Sciences, 28(2), 270–299. https://doi.org/10.1016/0022-0000(84)90070-9

[66] Maher, D. (1994). Crypto backup and key escrow. Communications of the ACM, 39(3), 48–58. https://doi.org/10.1145/227234.227235

[67] Moghaddam, F.F., Moghaddam, S.G., & Rouzbeh, S. (2015). A scalable and efficient user authentication scheme for cloud computing environments. In Proceedings of 2015 IEEE Symposium on Computers and Communication (pp. 195–200). IEEE. https://doi.org/10.1109/ISCC.2015.7405521

[68] Gruber, T.R. (1993). A translation approach to portable ontology specifications. Knowledge Acquisition, 5(2), 199–220. https://doi.org/10.1006/knac.1993.1008

[69] Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The semantic web. Scientific American, 284(5), 34–43. https://doi.org/10.1038/scientificamerican0501-34

[70] Lassila, O., & Swick, R.R. (1999). Resource Description Framework (RDF) Model and Syntax Specification. W3C Recommendation.

[71] Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B., & Dean, M. (2004). SWRL: A Semantic Web Rule Language Combining OWL and RuleML. W3C Member Submission.

[72] Baader, F., Calvanese, D., McGuinness, D., Nardi, D., & Patel-Schneider, P. (Eds.). (2003). The Description Logic Handbook. Cambridge University Press. https://doi.org/10.1017/CBO9780511711787

[73] Nalepa, G.J., Ligeza, A., & Kluza, K. (2011). Overview of knowledge formalization with XTT2 rules. In Rule-Based Reasoning, Programming, and Applications (pp. 329–336). Springer. https://doi.org/10.1007/978-3-642-22546-8_30

[74] Ding, L., & Finin, T. (2006). Characterizing the semantic web on the web. In The Semantic Web - ISWC 2006 (pp. 242–257). Springer. https://doi.org/10.1007/11926078_18

[75] Bhatt, S., Patwa, F., & Sandhu, R. (2019). Access control model for AWS internet of things. In Proceedings of the 4th ACM International Workshop on Security and Privacy Analytics (pp. 611–618). ACM. https://doi.org/10.1145/3209978.3210087

[76] Sicari, S., Rizzardi, A., Grieco, L.A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: the road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[77] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

[78] Fernandez, E.B., Yoshioka, N., & Washizaki, H. (2010). Patterns for cloud computing. In Proceedings of the 2010 International Workshop on Secure Software Engineering. ICSE.

[79] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: perspectives and challenges. Wireless Networks, 20(8), 2481–2501. https://doi.org/10.1007/s11276-014-0761-7

[80] ISO/TC 22/SC 32. (2020). ISO 21434: Road Vehicles — Cybersecurity Engineering. International Organization for Standardization.

[81] SAE International. (2021). SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. SAE International.

[82] UNECE WP.29. (2021). Regulation No. 155: Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System. United Nations Economic Commission for Europe.

[83] European Commission. (2021). Proposal for a Regulation on Artificial Intelligence (AI Act). COM/2021/206 final.

[84] Musen, M.A. (2015). The Protege project: a look back and a look forward. AI Matters, 1(4), 4–12. https://doi.org/10.1145/2757001.2757003

[85] Noy, N.F., & McGuinness, D.L. (2001). Ontology Development 101: A Guide to Creating Your First Ontology. Stanford Knowledge Systems Laboratory Technical Report KSL-01-05.