Objective- and Utility-Based Negotiation for Access Control [a]

Aditya Sissodiya[b], Ulf Bodin[c] and Olov Schelén[d]
Luleå University of Technology, Luleå, Sweden
{aditya.sissodiya, ulf.bodin, olov.schelen}@ltu.se

Keywords: Negotiation, Access Control, Automation, Digital Ecosystems, Stakeholder Collaboration, Interoperability.

Abstract: Access control in modern digital ecosystems presents significant challenges due to the dynamic nature of digital resources and the involvement of diverse stakeholders. Traditional access control mechanisms often fail to adapt properly to these complexities, leading to inefficient and inequitable data access. This paper proposes a novel access control policy negotiation algorithm that automates the negotiation process using objective optimization and utility-based approaches. The algorithm allows stakeholders to jointly select the best access control policy according to their respective preferences, provided that at least one such policy exist. To enable this, we introduce robust criteria for negotiation that guide the algorithm in evaluating predefined access control policies. A mathematical formulation of the algorithm is presented, detailing how stakeholder preferences are quantified through utility functions and how objective optimization is used to reach consensus. The algorithm's time and space complexity is analyzed, showing multilinear scalability, and a comparative analysis with existing frameworks highlights significant improvements in automation, complexity handling, and scalability. An evaluation tool has been developed to facilitate the application and testing of the algorithm, providing practical insights into its performance. Our approach enhances operational efficiency and trust within digital ecosystems by streamlining access control negotiations and ensuring equitable data access.

1 INTRODUCTION

The evolution of access control mechanisms is pivotal in the landscape of digital ecosystems for enabling circular economies, especially with emerging technologies like Digital Product Passports (DPPs) (King et al., 2023; Jansen et al., 2023). As these ecosystems become increasingly intricate with the involvement of multiple stakeholders, the limitations of traditional access control models become more apparent (Servos and Osborn, 2017; Zhang et al., 2015; Morisset et al., 2019). By using negotiation to address and reconcile differences in security policies, stakeholders can achieve a higher level of interoperability (Gligor et al., 2002; Martins and Guerreiro, 2019). This approach enables them to work together more effectively, leveraging their respective systems and security measures to ensure collective protection (Bouchami et al., 2015).

Negotiation facilitates the integration of diverse security policies without the need for each entity to overhaul their systems (Gligor et al., 2002). This integration is crucial in maintaining security while enabling collaboration among various organizations (Subramaniam et al., 2019; Shojaiemehr et al., 2018). For example, in dynamic cross-enterprise collaborations, a negotiation framework can help reconcile different access control rules by inferring relationships between disparate attributes, thereby facilitating smoother and secure interactions (Preuveneers et al., 2018; Sussan and Acs, 2017; Martins and Guerreiro, 2019). Hence, the need for an advanced access control negotiation algorithm that can address dynamic access control and the specific challenges of complex digital environments is justified.

One perspective on these conflicts of interest is to frame them as an objective optimization problem inspired by cooperative game theory, where stakeholders collaboratively pursue a shared goal while accounting for their individual interests. This offers a structured approach to model the interactions and

[a]The work presented in this paper was supported by the European Regional Development Fund, Region Norrbotten, Skellefteå Municipality, Luleå University of Technology, and industrial companies. The work has also been funded by Digitala Stambanan IndTech, a Swedish collaborative project between the Vinnova strategic innovation programs PiiA and Produktion 2030.

[b] https://orcid.org/0009-0009-9695-2308
[c] https://orcid.org/0000-0001-5194-4421
[d] https://orcid.org/0000-0002-4031-2872

conflicts among stakeholders, identifying strategies that facilitate consensus and balance the rational self-interests of all parties involved (Moura et al., 2019).

Objective optimization techniques complement this by enabling the formulation of access control policies that balance competing objectives (Marden and Shamma, 2018; Shamma, 2020; Medvet et al., 2015) like usability, accessibility etc. optimizing them within a coherent framework. Incorporating objective optimization into access control negotiation offers a robust framework for developing equitable and efficient access control policies (Zhang and He, 2015; Wang et al., 2019; Ma, 2015; Zhao et al., 2008).

In this paper, we facilitate automation of access control negotiation by proposing an algorithm based on objective optimization that addresses the above-mentioned critical needs in modern digital ecosystems. In such systems the complexity of interactions, the diversity of stakeholders and the dynamic nature of digital resources demand a flexible, context-aware, and secure approach to access control, which due to lack of a negotiation framework a standalone access control system cannot achieve (Bharadwaj and Baras, 2003b; Bharadwaj and Baras, 2003a).

By leveraging the strengths of access control in conjunction with objective optimization, stakeholders can develop access control policies that are not only secure and privacy-preserving but also adaptable and reflective of the diverse interests inherent in digital ecosystems (Moura et al., 2019; Zhang et al., 2016; Vamvoudakis and Hespanha, 2018).

The main contributions of the paper are as follows:

- We identify the primary challenges regarding access control in complex digital ecosystems (Section 2) and introduce robust criteria, aligned with IDSA standards, to guide the negotiation algorithm (Section 3).
- We provide a mathematical definition of our proposed access control negotiation algorithm (Section 4).
- We evaluate the algorithm illustrating its key features through simulations (Section 5), and provide a time and space complexity analysis, demonstrating its multilinear scalability (Section 6) along with a comparative analysis to existing negotiation frameworks (Section 7).

Additionally, we developed a tool to evaluate the algorithm's performance (GitHub) (Sissodiya, 2024) and also presented some related work (Section 8).

2 Challenges in Access Control

The evolution of digital ecosystems into more complex, interconnected environments has necessitated a reevaluation of traditional access control mechanisms (Subramaniam et al., 2019). The proposed access control negotiation algorithm emerges as a critical innovation in this landscape, aiming to address several pressing needs exacerbated by the advent of collaborative digital platforms. This section delves into the specific motivations behind the development of this algorithm, highlighting the gaps it seeks to fill in the current access control systems.

- **Dynamic Access Control Requirements and Automation:** Digital ecosystems are characterized by rapidly changing access control requirements due to the dynamic nature of digital resources, user roles, and operational contexts (Subramaniam et al., 2019). Traditional access control mechanisms often fail to adapt quickly enough to these changes (Servos and Osborn, 2017; Zhang et al., 2015). Existing Negotiation-Based Access Control (NAC) frameworks typically rely on manual negotiation processes where stakeholders must negotiate through predefined communication protocols, which can be inefficient especially as the number of stakeholders increases. By automating the negotiation process through mathematical optimization, our algorithm transforms a time-consuming process into an efficient and fair system capable of adapting to the dynamic nature of modern digital ecosystems.
- **Complexity and Scalability in Multi-Stakeholder Environments:** The presence of multiple stakeholders, each with distinct interests and requirements regarding resource access and sharing compounds the complexity of a digital ecosystem (Shojaiemehr et al., 2018). This necessitates a new approach that can handle complexity by aggregating utilities centrally and resolving conflicts through objective optimization, rather than direct negotiations between each pair of stakeholders. Such an approach would reduce communication complexity from quadratic to linear growth, enhancing scalability and allowing the system to manage a larger number of stakeholders and policies efficiently.
- **Equitable Access and Efficient Negotiation:** A foundational principle of access control in digital ecosystems should be the assurance of equitable access to resources (Subramaniam et al., 2019; Steinbuss et al., 2021). This principle demands a system that ensures all parties have fair opportunities to benefit from digital resources, ir-

respective of their size, influence, or geographic location. However, existing frameworks, including blockchain-based access control methods like FairAccess (Ouaddah et al., 2016) and Policychain (Chen et al., 2021), often focus on enforcing immutable policies, which can be problematic when policies need to be adjusted dynamically in response to changing stakeholder needs. Thus, a need for a negotiation mechanism that facilitates transparent processes, allowing stakeholders to voice their needs and preferences, and providing mechanisms for compromise and consensus-building without introducing excessive latency like its decentralized counterparts is justified.

- **Regulatory Compliance and Adaptability:** With the proliferation of data protection regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), organizations are under significant pressure to ensure that their access control policies comply with legal requirements (Dasgupta et al., 2019; Otto et al., 2021). By allowing stakeholders to continually negotiate policies in line with current regulations, the algorithm ensures compliance and helps organizations avoid legal penalties and reputation damage.

3 Criteria for Negotiation

The success of our negotiation algorithm relies heavily on the criteria we use to evaluate access control policies. To ensure these criteria are comprehensive and robust we've based them on established principles, particularly from International Data Spaces Association (IDSA).

The IDSA standards offer key advantages, they provide a solid technical foundation, ensuring secure and reliable data exchange (Otto et al., 2021). In sectors like manufacturing, where data sovereignty is vital, our criteria address the varied needs of stakeholders, drawing on relevant research (Larrinaga, 2022). By aligning our approach with proven frameworks, we aim to improve access and usage control, as previous work on usage control frameworks has shown (Steinbuss et al., 2021). We also ensure taking into account the importance of legal compliance that iterates through initiatives like IDSA and GAIA-X, reducing the risk of non-compliance while maintaining secure data practices (Otto et al., 2021; Huber et al., 2022).

3.1 Criteria:

1. **Applicability**: Reflects the practical benefits and functionality that the policy provides to stakeholders. This includes how well the policy supports the operational goals and needs of each stakeholder.
2. **Usability**: Evaluates how user-friendly and accessible the policy is for end-users. A policy with high usability facilitates smoother interactions and reduces the likelihood of errors or misuse.
3. **Accessibility**: Determines the ease with which stakeholders can access the resources they need. This criterion ensures that policies do not unduly restrict legitimate access or create barriers to collaboration.
4. **Compliance**: Ensures that the policy adheres to relevant legal and regulatory standards, minimizing legal risks and promoting trust among stakeholders.

These criteria ensure that negotiations remain relevant and user-friendly despite changing operational contexts and user roles, all while reducing the complexity inherent in multi-stakeholder negotiations. By explicitly considering these boundary conditions, the algorithm ensures that the negotiated access control policies are feasible and sustainable within the given constraints.

3.2 Policy Evaluation Guidance

To ensure consistency when stakeholders rate the criteria, we propose a structured scoring framework for each criterion. Stakeholders rate each policy on a standardized scale from 1 to 10, with detailed guidelines provided to interpret each score level. This approach acknowledges that each stakeholder may value certain criteria differently based on their unique context. Subjective ratings empower stakeholders to express their preferences and concerns accurately, leading to a more representative and satisfactory negotiation outcome.

1. **Applicability:**
   - **1-3** *(Low Applicability)*: The policy offers minimal or no benefits to the stakeholder's needs.
   - **4-6** *(Moderate Applicability)*: The policy is somewhat relevant but may not fully support the stakeholder's needs.
   - **7-8** *(High Applicability)*: The policy aligns well with the stakeholder's needs, providing significant benefits.

- **9-10** *(Very High Applicability)*: The policy is essential to the stakeholder's needs, offering maximal benefit and alignment.

2. **Usability:**
   - **1-3** *(Low Usability)*: The policy is complex and difficult to use, likely causing user frustration or errors.
   - **4-6** *(Moderate Usability)*: The policy is usable but may have some complexities that hinder user experience.
   - **7-8** *(High Usability)*: The policy is user-friendly, with clear instructions and minimal complexity.
   - **9-10** *(Very High Usability)*: The policy is highly intuitive and streamlined, significantly enhancing user experience.
3. **Accessibility:**
   - **1-3** *(Low Accessibility)*: The policy severely restricts access, impeding the stakeholder's ability to perform tasks.
   - **4-6** *(Moderate Accessibility)*: The policy allows access but with limitations that may hinder the stakeholder's ability to perform tasks.
   - **7-8** *(High Accessibility)*: The policy provides adequate access, enabling stakeholders to perform tasks effectively.
   - **9-10** *(Very High Accessibility)*: The policy offers seamless access, fully supporting the stakeholder's ability to perform tasks without barriers.
4. **Compliance:**
   - **1-3** *(Low Compliance)*: The policy fails to meet key regulatory requirements, posing legal risks.
   - **4-6** *(Moderate Compliance)*: The policy complies with some regulations but may lack in certain areas.
   - **7-8** *(High Compliance)*: The policy meets all standard compliance requirements relevant to the stakeholder.
   - **9-10** *(Very High Compliance)*: The policy not only meets but exceeds compliance standards, incorporating best practices and anticipating regulatory changes.

4 Access Control Negotiation Algorithm

This section represents the negotiation algorithm incorporating objective optimization and stakeholder preferences through utility functions mathematically:

- Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the set of stakeholders involved in the negotiation.
- Let $P = \{P_1, P_2, \ldots, P_m\}$ represent the set of potential policies up for negotiation.

4.1 Algorithm Steps

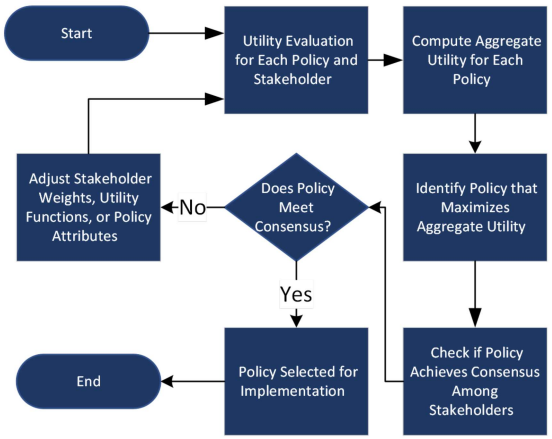

Figure 1: Algorithm for Negotiation.

- **Utility Evaluation:** Calculate the utility $U_{a_i}(P_j)$ for each policy P_j from the perspective of each stakeholder a_i.
- **Aggregate Utility Calculation:** Compute the aggregate utility $U_{agg}(P_j)$ for each policy.
- **Optimization:** Identify the policy P^* that maximizes $U_{agg}(P_j)$.
- **Consensus Check:** Verify whether P^* achieves consensus among stakeholders.
- **Policy Selection:** If P^* meets the consensus criterion, it is selected for implementation. Otherwise, adjust stakeholder weights, utility functions, or reconsider policy attributes, followed by a repetition of the steps until a satisfactory policy is identified.

4.1.1 Aggregate Utility Function

For a generalized mathematical representation focusing solely on the utility functions, we abstract the stakeholders and their preferences towards a set of policies.

Each stakeholder $a_i \in A$ has a utility function $U_{a_i} : P \to \mathbb{R}$, which maps each policy P_j to a real number representing the stakeholder's preference for that policy. The utility functions are defined as follows:

$$U_{a_i}(P_j) = w_{a_i,1} \cdot f_1(P_j) + w_{a_i,2} \cdot f_2(P_j) + \cdots + w_{a_i,k} \cdot f_k(P_j)$$

- $f_1(P_j), f_2(P_j), \ldots, f_k(P_j)$ are functions that evaluate policy P_j based on criteria important to stakeholder a_i. These criteria might include aspects

such as the policy's security level, its impact on usability, or compliance with regulations.

- $w_{a_i,1}, w_{a_i,2}, \ldots, w_{a_i,k}$ are weights chosen by stakeholder a_i that reflect the importance of each criterion in their utility function.

The utility function for each stakeholder is a weighted sum of evaluations based on multiple criteria, allowing for a nuanced expression of preference that takes into account various aspects of each policy.

In a more generalized form, the utility function for a stakeholder a_i regarding a policy P_j can be represented as:

$$U_{a_i}(P_j) = \sum_{l=1}^{k} w_{a_i,l} \cdot f_l(P_j)$$

where k is the number of criteria considered, $w_{a_i,l}$ is the weight assigned to criterion l by stakeholder a_i, and $f_l(P_j)$ is the evaluation of policy P_j based on criterion l.

By abstracting away from specific applications and focusing on the utility function, this formulation provides a flexible foundation that can be adapted to various contexts where stakeholders with differing priorities need to negotiate over a set of options, each with multiple attributes influencing the stakeholder preferences.

4.1.2 Objectives Optimization

The optimization step within the algorithm focuses on identifying the policy, denoted as P^*, that maximizes the aggregate utility, $U_{agg}(P_j)$, across all considered policies. Mathematically, this process aims to find the policy that yields the highest level of collective satisfaction or preference among all stakeholders based on the predefined utility functions and their associated weights (Enkhbat et al., 2015; Allahviranloo and Axhausen, 2018). Here's how this optimization process is formulated and executed mathematically:

- A set of potential policies $P = \{P_1, P_2, \ldots, P_m\}$,
- The aggregate utility function for a policy P_j, $U_{agg}(P_j)$, which combines the preferences of all stakeholders for policy P_j,

The objective of the optimization step is to find the policy P^* where that maximizes $U_{agg}(P_j)$:

$$P^* = \arg\max_{P_j \in P} U_{agg}(P_j)$$

4.1.3 Evaluate Aggregate Utility for Each Policy

For every policy P_j in the set P, calculate the aggregate utility $U_{agg}(P_j)$ as previously defined:

$$U_{agg}(P_j) = \sum_{i=1}^{n} \alpha_i \cdot U_{a_i}(P_j)$$

where α_i is the weight reflecting the importance of stakeholder a_i and $U_{a_i}(P_j)$ is the utility of policy P_j according to stakeholder a_i.

4.1.4 Maximization

The process then involves evaluating $U_{agg}(P_j)$ for all $P_j \in P$ and identifying the policy that yields the highest aggregate utility. Mathematically, this involves comparing the aggregate utility values across all policies and selecting the one with the maximum value.

4.1.5 Selection of Optimal Policy

The policy P^* with the highest aggregate utility is selected as the optimal policy. Formally, this selection process can be represented as:

$$P^* = \arg\max_{P_j \in P} \left(\sum_{i=1}^{n} \alpha_i \cdot U_{a_i}(P_j) \right)$$

A policy P_j is selected if it satisfies the following criteria:

- ***Maximizing Aggregate Utility***: It has the highest aggregate utility among all policies.
- ***Consensus Achievement***: It meets or exceeds a predetermined utility threshold for consensus among stakeholders, which can be formalized as:

$$Consensus(P_j) = \begin{cases} True & \text{if } U_{a_i}(P_j) \geq \theta,\ \forall a_i \in A \\ False & \text{otherwise} \end{cases}$$

where θ is the consensus threshold.

4.2 Interpretation

- The aggregate utility $U_{agg}(P_j)$ quantifies the overall satisfaction or preference of the stakeholder group for the policy P_j. A higher $U_{agg}(P_j)$ indicates a higher collective preference for P_j.
- By computing $U_{agg}(P_j)$ for each policy in the set P, the algorithm can compare these aggregate utilities to identify which policy is most favoured by the stakeholders as a whole.
- The policy with the highest aggregate utility is considered the optimal choice under the assumption that it best satisfies the combined preferences and priorities of all stakeholders involved in the negotiation.

This approach to calculating aggregate utility facilitates a rational and systematic method for policy selection within the access control framework, ensuring that the selected policy maximizes overall stakeholder satisfaction according to their defined preferences and the weights assigned to them.

4.3 Algorithm Evaluation Tool

We developed an Algorithm Evaluation Tool to assist in evaluating and optimizing various access control policies by considering the influence of different stakeholders and the weights they assign to various policy attributes (Sissodiya, 2024).

This tool, which is available on GitHub under the MIT licence, empowers users to add policies and stakeholders, assign and update weights, and calculate the optimal policy based on the aggregate utility, all while ensuring that stakeholder consensus is considered. We developed this tool using Flask and PostgreSQL for the backend, combined with simple HTML/CSS/JavaScript for the frontend, to ensure a user-friendly interface. The application is containerized using Docker for easy deployment.

- **Features:**
  - Add Policies: Users can add new policies with specific attributes such as security, applicability, privacy, and accessibility scores.
  - Add Stakeholders: Users can add stakeholders and set their influence levels.
  - Assign Weights: Assign weights to different policy attributes from each stakeholder's perspective.
  - Calculate Optimal Policy: Determine which policy has the highest aggregate utility based on weights assigned by all stakeholders.
  - Check Consensus: Verify if the optimal policy reaches a consensus among stakeholders based on a defined utility threshold.

(Implementation of the algorithm along with the tool and quantitative analysis is available at this GitHub repository.)

5 Real-World Scenario Evaluation

To illustrate how our negotiation algorithm works in practice, let's consider a connected car ecosystem where multiple stakeholders need to agree on access control policies for shared data. This data includes sensitive information such as vehicle telemetry, maintenance records, and user data. The stakeholders involved are:

- **Car Owner (O)**: Prioritizes privacy and wants control over who can access their vehicle's data.
- **Car Manufacturer (M)**: Seeks access to vehicle performance data to improve car designs and address manufacturing defects.
- **Insurance Company (I)**: Desires driving patterns and maintenance records for risk assessment and setting insurance rates.
- **Car Workshop (W)**: Needs access to vehicle diagnostics and maintenance history to provide better service.

The goal is to reach a consensus on an access control policy that balances the preferences and priorities of all stakeholders.

Three potential proposed policies are:

- **Policy** P_1: Open access without explicit consent from the car owner.
- **Policy** P_2: Limited access based on predefined roles, with personal data requiring the car owner's consent.
- **Policy** P_3: Restricted access requiring explicit approval from the car owner for each data access request.

Each stakeholder evaluates the policies based on the criteria defined earlier: Applicability **(A)**, Usability **(U)**, Accessibility **(Ac)**, and Compliance **(C)**. The importance of each criterion to a stakeholder is represented by weights, which sum to 1 for each stakeholder.

5.1 Algorithm Steps

5.1.1 Step 1: Define Priorities and Weights

- **O**: Places a high priority on Compliance and Usability due to privacy concerns and the need for ease in managing permissions. $w_{O,A} = 0.1$, $w_{O,U} = 0.3$, $w_{O,Ac} = 0.1$, $w_{O,C} = 0.5$.
- **M**: High priority on Applicability and Accessibility to access data for improvements. $w_{M,A} = 0.4$, $w_{M,U} = 0.1$, $w_{M,Ac} = 0.4$, $w_{M,C} = 0.1$.
- **I**: Prioritizes Applicability and Compliance. $w_{I,A} = 0.5$, $w_{I,U} = 0.1$, $w_{I,Ac} = 0.3$, $w_{I,C} = 0.1$.
- **W**: Places a high priority on Applicability and Accessibility, with a moderate emphasis on Usability $w_{W,A} = 0.4$, $w_{W,U} = 0.2$, $w_{W,Ac} = 0.3$, $w_{W,C} = 0.1$.

5.1.2 Step 2: Stakeholder Ratings for Policies

Each stakeholder rates each policy on a scale from 1 to 10 for each criterion, as shown in Table 1.

Table 1: Stakeholder ratings for Policies P_1, P_2, and P_3

Stakeholder	Applicability (A)	Usability (U)	Accessibility (Ac)	Compliance (C)
Policy P_1: Open Access Without Consent				
Car Owner (O)	2 (Low benefit)	2 (Poor usability)	8 (High for others)	1 (Fails privacy)
Car Manufacturer (M)	9 (High benefit)	8 (Easy access)	9 (Very high)	3 (Regulatory issues)
Insurance Company (I)	9 (High benefit)	7 (Easy integration)	9 (Very high)	3 (Privacy concerns)
Car Workshop (W)	9 (High benefit)	8 (Easy diagnostics)	9 (Very high)	3 (Compliance issues)
Policy P_2: Role-Based Access with Owner Consent				
Car Owner (O)	7 (Moderate benefit)	6 (Complex management)	6 (Acceptable)	8 (Aligns with regulations)
Car Manufacturer (M)	7 (Good access)	6 (Some restrictions)	7 (Acceptable)	7 (Better compliance)
Insurance Company (I)	6 (Some access)	6 (Moderate complexity)	6 (Restricted)	7 (Improved compliance)
Car Workshop (W)	7 (Adequate access)	7 (User-friendly)	7 (Acceptable)	7 (Good compliance)
Policy P_3: Owner Approval for Each Request				
Car Owner (O)	9 (Full control)	5 (Burdensome approval)	5 (Impedes services)	9 (Highly compliant)
Car Manufacturer (M)	4 (Limited access)	5 (Complicated process)	4 (Low accessibility)	8 (Compliant)
Insurance Company (I)	3 (Difficult data access)	5 (Cumbersome)	3 (Low accessibility)	8 (Compliant)
Car Workshop (W)	5 (Access delays)	6 (User-friendly)	5 (Moderate access)	8 (Compliant)

5.1.3 Step 3: Calculate Individual Utilities

For each stakeholder and policy, calculate the utility using the formula:

$$U_{a_i}(P_j) = \sum_{l=1}^{k} w_{a_i,l} \times f_l(P_j)$$

Where:

- $w_{a_i,l}$ = weight of criterion l for stakeholder a_i
- $f_l(P_j)$ = rating of policy P_j on criterion l by stakeholder a_i

$U_O(P_1) = (0.1 \times 2) + (0.3 \times 2) + (0.1 \times 8) + (0.5 \times 1) = 2.1$

Similarly, we calculate the individual utilities for each stakeholder and get the following values, as shown in Table 2.

Table 2: Utility Values for Each Stakeholder and Policy

Stakeholder	$U_{a_i}(P_1)$	$U_{a_i}(P_2)$	$U_{a_i}(P_3)$
Car Owner (O)	2.1	7.1	7.4
Car Manufacturer (M)	8.3	6.9	4.5
Insurance Company (I)	8.2	6.1	3.7
Car Workshop (W)	8.2	7.0	5.5

5.1.4 Step 4: Compute $U_{agg}(P_j)$ for Each Policy

Assuming equal importance for all stakeholders, we set the weights $\alpha_i = 1$ for all i.

$$U_{agg}(P_j) = \sum_{i=1}^{n} U_{a_i}(P_j)$$

- $U_{agg}(P_1) = U_O(P_1) + U_M(P_1) + U_I(P_1) + U_W(P_1) = 2.1 + 8.3 + 8.2 + 8.2 = 26.8$
- $U_{agg}(P_2) = U_O(P_2) + U_M(P_2) + U_I(P_2) + U_W(P_2) = 7.1 + 6.9 + 6.1 + 7.0 = 27.1$
- $U_{agg}(P_3) = U_O(P_3) + U_M(P_3) + U_I(P_3) + U_W(P_3) = 7.4 + 4.5 + 3.7 + 5.5 = 21.1$

5.1.5 Step 5: Identify the Optimal Policy P^*

$$P^* = \arg\max_{P_j} U_{agg}(P_j)$$

- $U_{agg}(P_1) = 26.8$
- $U_{agg}(P_2) = 27.1$ (Highest)
- $U_{agg}(P_3) = 21.1$

Therefore, the optimal policy is $P^* = P_2$.

5.1.6 Step 6: Consensus Check

We need to ensure that P^* meets a minimum acceptable utility θ for all stakeholders. Let's set $\theta = 5.0$.

Check $U_{a_i}(P_2)$ for each stakeholder:

- Car Owner (O): $U_O(P_2) = 7.1 \geq 5.0$ ✓
- Car Manufacturer (M): $U_M(P_2) = 6.9 \geq 5.0$ ✓
- Insurance Company (I): $U_I(P_2) = 6.1 \geq 5.0$ ✓
- Car Workshop (W): $U_W(P_2) = 7.0 \geq 5.0$ ✓

All stakeholders have a utility equal to or above the threshold θ. Therefore, consensus is achieved.

5.2 Insights and Interpretation

By systematically applying the negotiation algorithm, stakeholders were able to:

- *Quantify Preferences*: Stakeholders expressed their preferences numerically, allowing for objective comparisons.
- *Balance Priorities*: The algorithm balanced the diverse priorities, ensuring that no stakeholder's essential needs were ignored.

- *Ensure Compliance*: Policies that failed to meet regulatory requirements (like P_1) were effectively penalized in the utility calculations.
- *Achieve Consensus*: The consensus check ensured that the selected policy was acceptable to all parties, promoting cooperative decision-making.

This detailed walkthrough demonstrates how the negotiation algorithm facilitates collaborative policy selection in complex, multi-stakeholder environments, ensuring that the final decision is both optimal and equitable.

5.3 Quantitative Analysis

5.3.1 Utility Distribution Plot

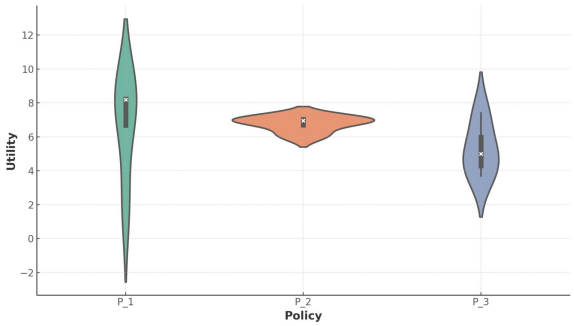

Figure 2: Utility Distribution Across Policies (Violin Plot)

- Policy P_2 has a more balanced distribution. The violin shape is somewhat even, and the white dot (median) is near the center. This suggests that the utility values for Policy P_2 are more concentrated around the middle and are not as spread out, indicating broad agreement among the stakeholders.
- Policy P_1 has a wider, more elongated shape at the top, indicating that the utility values are skewed towards higher values for most stakeholders, even though some stakeholders (like the car owner) have much lower utility scores.
- Policy P_3 shows more spread and lower values. The distribution is concentrated towards the bottom of the violin, meaning that most stakeholders rated it poorly, except for the car owner, who gave it a relatively higher utility.

5.3.2 Stakeholder Utility Heatmap

- The heatmap provides an immediate visual comparison of how each stakeholder rates each policy. Darker colors indicate higher satisfaction, while lighter colors show lower utility. This helps identify which policies are widely supported (e.g. Policy P_2) and which have polarizing effects (e.g.

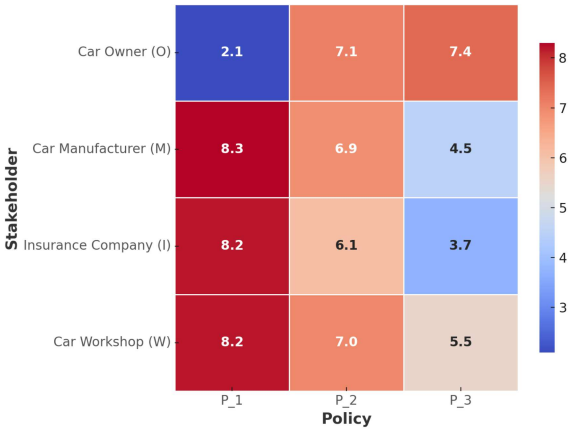

Figure 3: Stakeholder Utility Heatmap

Policy P_1, highly favored by manufacturers but disliked by the car owner).

- It also clearly highlights conflicts of interest, such as the sharp contrast between the Car Owner's low utility for Policy P_1 (due to privacy concerns) and the other stakeholders' high utility (due to ease of access). Conversely, Policy P_2 shows a more balanced distribution, indicating its potential for broad consensus among all stakeholders.
- Finally, it visually emphasizes how well each policy aligns with individual stakeholder priorities. For example, Policy P_3 scores high for the Car Owner (due to strong control over data), but performs poorly for the Car Manufacturer and others, showing that this policy prioritizes privacy at the cost of accessibility for other stakeholders.

6 Algorithm Complexity Analysis

6.1 Time Complexity

- *Utility Calculation*: $O(c)$, where c is the number of criteria.
- *Aggregate Utility Calculation*: $O(p \times s \times O(c))$, where p is the number of policies and s is the number of stakeholders and $O(c)$ is called for each policy.
- *Optimal Policy Evaluation*: $O(p)$, as it needs to iterate through the aggregate utilities of all policies once to find the maximum.
- *Consensus*: $O(p)$, as it checks the Aggregate Utility value for each policy against the set threshold.

The overall time complexity of the algorithm is the sum of the complexities of its parts, primarily dominated by Aggregate Utility Calculation: $O(p \times s \times O(c)) + O(p) + O(s)$. Since $O(p \times s \times O(c))$ is

the most significant term, we can simplify the overall complexity to $O(p \times s \times O(c))$. Therefore the complexity would be considered multilinear rather than strictly linear. The computational cost increases linearly with an increase in any one of p, s, or c while keeping the others constant, but increases polynomially as all increase proportionally.

6.2 Space Complexity

- *Aggregate Utilities*: $O(p)$ since there is one entry per policy and a dictionary is where the key is the policy name and the value is its aggregate utility score is stored.
- *Utility Calculations*: Uses a temporary variable to store the utility score $O(1)$.
- *Consensus Check*: The maximum space required is proportional to the number of stakeholders, $O(s)$.

When considering the space required for input data and computational storage together, the overall space complexity of the algorithm can be represented as: $O(p)+O(s) = O(p+s)$ this means the space complexity is linearly proportional to the sum of the number of policies and the number of stakeholders.

7 Comparative Analysis

Several Negotiation-Based Access Control (NAC) frameworks have been developed, particularly for distributed systems and cloud environments, where entities must negotiate access rights in real-time. For instance, (Gligor et al., 2002) proposed a negotiation protocol for resolving access conflicts between dynamic coalitions in large-scale systems.

- **Automation:** Traditional NAC frameworks often rely on semi-automated or manual negotiation processes, where stakeholders must negotiate through predefined communication protocols. In contrast, the proposed algorithm automates the entire negotiation process by calculating and optimizing stakeholder utilities. Assuming the negotiation time T_{manual} increases linearly with the number of stakeholders n. So,

  $$T_{\text{manual}} = k_1 \cdot n$$

  where k_1 is a proportionality constant depending on the complexity of the manual process.

  If the proposed method automates this process and optimizes utility, the time could be modeled as logarithmic or a small constant time:

  $$T_{\text{auto}} = k_2 \log n \quad \text{or} \quad T_{\text{auto}} = k_3$$

  with k_2 and k_3 representing efficiencies of the system.

- **Complexity:** Existing NAC frameworks struggle with complex multi-stakeholder environments, as they require direct communication between entities. The proposed model handles this complexity by aggregating utilities and resolving conflicts through objective optimization, rather than direct negotiations between each pair of stakeholders.

  In traditional NAC, each stakeholder must communicate with others. The number of communication links grows as the square of the stakeholders:

  $$C_{\text{NAC}} = \frac{n(n-1)}{2}$$

  This is a quadratic growth, leading to a bottleneck in large systems.

  The proposed algorithm aggregates utilities centrally, so the number of interactions grows linearly.

- **Scalability:** The proposed algorithm offers better scalability, as it can manage a larger number of stakeholders and policies by utilizing a centralized utility aggregation process. Traditional NAC frameworks often face performance bottlenecks in large-scale environments due to the overhead of individual negotiations.

The performance degradation in NAC frameworks could be modeled as the inverse of the number of stakeholders handled, leading to slower processing as the number of stakeholders grow. In contrast, the proposed algorithm, using a centralized model, could maintain a constant or near-constant efficiency even as n increases.

Blockchain-Based Access Control (BAC) frameworks such as FairAccess (Ouaddah et al., 2016) and Policychain (Chen et al., 2021) use blockchain's decentralized ledger to manage access control policies. These systems aim to provide transparency, auditability, and decentralization, which can be beneficial for security and privacy.

- Blockchain-based methods typically decentralized, whereas the proposed algorithm operates in a centralized or semi-centralized fashion, allowing for more efficient negotiation. Blockchain solutions can introduce latency and complexity, especially when managing access control policies across large networks.

  Latency in decentralized systems tends to increase as the network grows due to the need for consensus and verification steps:

  $$L_{\text{BAC}} = k_6 \cdot \log n$$

where L_{BAC} is the latency.

In the centralized or semi-centralized model, the negotiation process avoids such latency issues and can be modeled as constant.

- Blockchain-based methods focus more on enforcing immutable policies, which can be an issue when policies need to be adjusted dynamically in response to changing stakeholder needs. The proposed model excels in environments that require real-time negotiation and flexibility.
- While blockchain methods are robust in terms of auditability, they can be less adaptable to rapidly changing regulatory landscapes. The proposed algorithm ensures compliance by allowing stakeholders to continually negotiate policies in line with current regulations.

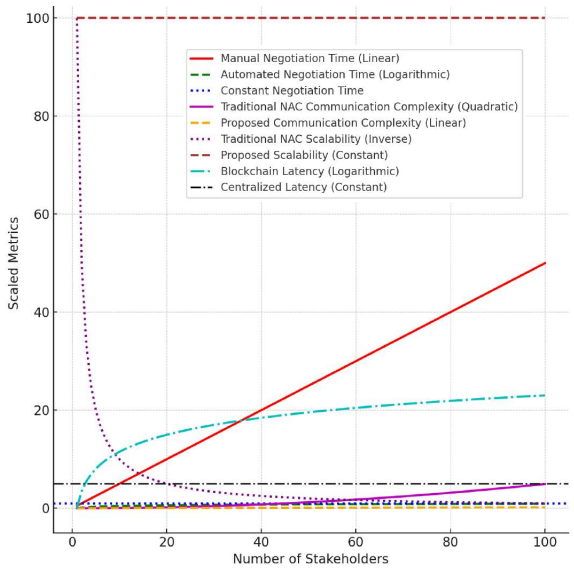

Figure 4: Comparitive Analysis Graph.

- ***Figure 4*** compares the performance, complexity, and latency of various access control frameworks as the number of stakeholders increases.
  - The red line (manual negotiation) grows steadily with more stakeholders, while the green dashed line (automated negotiation) shows faster, logarithmic growth. The blue dashed line reflects systems with constant negotiation time.
  - The magenta line shows rapid growth in traditional frameworks, while the orange dashed line (proposed algorithm) scales more efficiently due to centralized aggregation.
  - Traditional frameworks (purple line) degrade as stakeholders increase, but the proposed algorithm (brown dashed line) maintains constant performance.
  - Blockchain-based systems (cyan dashed line) experience rising latency with more stakeholders, while the proposed system (black dashed line) maintains steady latency.

8 Related Work

The literature on negotiation and management reflects a growing recognition of the need for dynamic, secure, and collaborative approaches to policy management in digital ecosystems. From relationship-based access control to blockchain-enabled frameworks, these algorithms represent key innovations in facilitating consensus on access control policies among stakeholders, ensuring confidentiality, and enabling flexible access control mechanisms in complex digital environments.

Negotiation is a critical aspect of managing access control and privacy settings in various digital and distributed systems, including cloud services, digital ecosystems, and multi-agent systems (Mehregan and Fong, 2016; Subramaniam et al., 2019; Sussan and Acs, 2017). With the advancement of complex digital platforms and the increasing need for fine-grained access control, traditional policy management approaches have evolved to incorporate dynamic policy negotiation algorithms. These algorithms enable stakeholders to agree on access control policies that satisfy multiple constraints and preferences.

Research in the field of negotiation, especially within the context of Relationship Based Access Control (ReBAC), offers a range of advancements and methodologies to address the complexities and challenges of access control in digital and collaborative environments. An approach allowing co-owners with conflicting privacy preferences to collaboratively formulate an access control policy has been outlined (Mehregan and Fong, 2016). This methodology leverages SAT solvers for efficient verification of policy satisfiability, addressing the challenge of multiple ownership in digital content management.

The emergence of negotiation within access control policies, including practical examples and processes for dynamic coalitions and large-scale Internet access control, is thoroughly explored in (Gligor et al., 2002). The development of software agents that can autonomously negotiate access control policies between domains with minimal human intervention, along with a proposed mathematical framework for expressing negotiation problems, is detailed in (Bharadwaj and Baras, 2003b). The strategic implications of digital ecosystems for businesses, em-

phasizing the need for adaptive negotiation mechanisms to manage rapidly changing interdependencies among participants, are discussed in (Subramaniam et al., 2019). This work highlights the importance of flexible frameworks to support new sources of value and growth avenues in digital ecosystems.

Blockchain-Based access control presents a novel approach to access control management using blockchain technology. By leveraging the immutable and transparent nature of blockchain, the approach enables the decentralized management and enforcement of access control policies, ensuring auditability and trust among parties. The main security concern within Internet of Things based industrial collaboration systems (IoT-ICS) is that these systems share data-processing tasks and IoT-based access to services and resources. The "Policychain" (Chen et al., 2021) framework aims to address this by delegating the responsibility of ABAC policy administration and decision-making to blockchain nodes. This ensures policies are highly available, autonomous, and traceable. FairAccess (Ouaddah et al., 2016) leverages blockchain technology to decentralize access control management. This approach eliminates the need for a central authority to manage access permissions, thereby enhancing security and privacy. The AuthPrivacyChain (Yang et al., 2020) framework utilizes the unique account addresses of blockchain nodes as identities for access control, redefining how access permissions to data stored in the cloud are encrypted and maintained on the blockchain. The framework includes processes for access control, authorization, and revocation of authorization, providing a comprehensive solution for managing access to cloud resources.

The literature on negotiation and management reflects a growing recognition of the need for dynamic, secure, and collaborative approaches to policy management in digital ecosystems. From relationship-based access control to blockchain-enabled frameworks, these algorithms represent key innovations in facilitating consensus on access control policies among stakeholders, ensuring confidentiality, and enabling flexible access control mechanisms in complex digital environments.

Our proposed algorithm fills a crucial gap and automates the negotiation of access control policies. Unlike traditional approaches that often require significant manual intervention, our algorithm allows for dynamic, context-aware, and equitable negotiation. It ensures that the negotiated policies are reflective of the diverse interests of all stakeholders involved, by incorporating standardization from the IDSA, our approach enhances interoperability and security, addressing the critical needs of digital ecosystems.

9 Conclusion

This paper identifies challenges for access control negotiation in multi-party ecosystems and defines a model including criteria and an algorithm for such negotiations. The development and implementation of the proposed negotiation algorithm offers a noteworthy improvement in access control systems, especially within complex and dynamic digital environments.

Traditional access control methods often fail to address the multifaceted nature of modern digital ecosystems, where the needs of various stakeholders require a more detailed approach. The proposed negotiation algorithm meets these challenges effectively, providing a solid framework that balances security, confidentiality, and usability.

Utilizing objective optimization, the algorithm introduces a structured way for stakeholders to negotiate access control policies that are fair and considerate of the diverse interests in digital ecosystems. This approach ensures that all parties can participate in the policy formulation process, fostering trust and cooperation in managing digital resources.

Additionally, the algorithm uses standardized policy specifications from the International Data Spaces Association, ensuring that negotiation is technically sound, enforceable, and adaptable to various stakeholder needs. Its ability to adapt dynamically to changing conditions further highlights its relevance in today's evolving digital landscape.

The implications of this research extend beyond immediate improvements in access control negotiation. It encourages a reevaluation of existing negotiation frameworks, promoting ongoing innovation in digital ecosystem management.

REFERENCES

Allahviranloo, M. and Axhausen, K. (2018). An optimization model to measure utility of joint and solo activities. *Transportation Research Part B: Methodological*, 108:172–187.

Bharadwaj, V. G. and Baras, J. S. (2003a). A framework for automated negotiation of access control policies. In *DARPA Information Survivability Conference and Exposition,*, volume 3, pages 216–216. IEEE Computer Society.

Bharadwaj, V. G. and Baras, J. S. (2003b). Towards automated negotiation of access control policies. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, pages 111–119. IEEE.

Bouchami, A., Goettelmann, E., Perrin, O., and Godart, C. (2015). Enhancing access-control with risk-metrics for collaboration on social cloud-platforms. *2015 IEEE Trustcom/BigDataSE/ISPA*, 1:864–871.

Chen, E., Zhu, Y., Zhou, Z., Lee, S.-Y., Wong, W. E., and Chu, W. C.-C. (2021). Policychain: a decentralized authorization service with script-driven policy on blockchain for internet of things. *IEEE Internet of Things Journal*, 9(7):5391–5409.

Dasgupta, A., Gill, A., and Hussain, F. (2019). A conceptual framework for data governance in iot-enabled digital is ecosystems. In *8th International Conference on Data Science, Technology and Applications*. SCITEPRESS–Science and Technology Publications.

Enkhbat, R., Enkhbayar, J., and Griewank, A. (2015). Global optimization approach to utility maximization problem. *International Journal of Pure and Applied Mathematics*, 103(3):485–497.

Gligor, V. D., Khurana, H., Koleva, R. K., Bharadwaj, V. G., and Baras, J. S. (2002). On the negotiation of access control policies. In *Security Protocols: 9th International Workshop Cambridge, UK, April 25–27, 2001 Revised Papers 9*, pages 188–201. Springer.

Huber, M., Wessel, S., Brost, G. S., and Menz, N. (2022). Building trust in data spaces.

Jansen, M., Meisen, T., Plociennik, C., Berg, H., Pomp, A., and Windholz, W. (2023). Stop guessing in the dark: Identified requirements for digital product passport systems. *Systems*, 11(3):123.

King, M. R., Timms, P. D., and Mountney, S. (2023). A proposed universal definition of a digital product passport ecosystem (dppe): Worldviews, discrete capabilities, stakeholder requirements and concerns. *Journal of Cleaner Production*, 384:135538.

Larrinaga, F. (2022). Data sovereignty-requirements analysis of manufacturing use cases.

Ma, S. (2015). Dynamic game access control based on trust. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1369–1373. IEEE.

Marden, J. R. and Shamma, J. S. (2018). Game theory and control. *Annual Review of Control, Robotics, and Autonomous Systems*, 1:105–134.

Martins, H. and Guerreiro, S. (2019). Access control challenges in enterprise ecosystems. *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government*.

Medvet, E., Bartoli, A., Carminati, B., and Ferrari, E. (2015). Evolutionary inference of attribute-based access control policies. In *Evolutionary Multi-Criterion Optimization: 8th International Conference, EMO 2015, Guimarães, Portugal, March 29–April 1, 2015. Proceedings, Part I 8*, pages 351–365. Springer.

Mehregan, P. and Fong, P. W. (2016). Policy negotiation for co-owned resources in relationship-based access control. In *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies*, pages 125–136.

Morisset, C., Willemse, T. A., and Zannone, N. (2019). A framework for the extended evaluation of abac policies. *Cybersecurity*, 2(1):6.

Moura, J., Marinheiro, R. N., and Silva, J. C. (2019). Game theory for cooperation in multi-access edge computing. In *Paving the Way for 5G Through the Convergence of Wireless Systems*, pages 100–149. IGI Global.

Otto, B., Rubina, A., Eitel, A., Teuscher, A., Schleimer, A. M., Lange, C., Stingl, D., Loukipoudis, E., Brost, G., Boege, G., et al. (2021). Gaia-x and ids.

Ouaddah, A., Abou Elkalam, A., and Ait Ouahman, A. (2016). Fairaccess: a new blockchain-based access control framework for the internet of things. *Security and communication networks*, 9(18):5943–5964.

Preuveneers, D., Joosen, W., and Zudor, E. (2018). Policy reconciliation for access control in dynamic cross-enterprise collaborations. *Enterprise Information Systems*, 12:279 – 299.

Servos, D. and Osborn, S. L. (2017). Current research and open problems in attribute-based access control. *ACM Computing Surveys (CSUR)*, 49(4):1–45.

Shamma, J. S. (2020). Game theory, learning, and control systems. *National Science Review*, 7(7):1118–1119.

Shojaiemehr, B., Rahmani, A. M., and Qader, N. N. (2018). Cloud computing service negotiation: a systematic review. *Computer Standards & Interfaces*, 55:196–206.

Sissodiya, A. (2024). Access policy negotiation algorithm. https://github.com/adityasissodiya/AccessControlPolicyNegotiationAlgorithm.

Steinbuss, S. et al. (2021). Usage control in the international data spaces.

Subramaniam, M., Iyer, B., and Venkatraman, V. (2019). Competing in digital ecosystems. *Business Horizons*, 62(1):83–94.

Sussan, F. and Acs, Z. J. (2017). The digital entrepreneurial ecosystem. *Small Business Economics*, 49:55–73.

Vamvoudakis, K. G. and Hespanha, J. P. (2018). Game-theory-based consensus learning of double-integrator agents in the presence of worst-case adversaries. *Journal of Optimization Theory and Applications*, 177:222–253.

Wang, Y., Tian, L., and Chen, Z. (2019). Game analysis of access control based on user behavior trust. *Information*, 10(4):132.

Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., and Yu, K. (2020). Authprivacychain: A blockchain-based access control framework with privacy protection in cloud. *IEEE Access*, 8:70604–70615.

Zhang, Y. and He, J. (2015). A proactive access control model based on stochastic game. In *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, volume 1, pages 1008–1011. IEEE.

Zhang, Y., He, J., Zhao, B., Huang, Z., and Liu, R. (2015). Towards more pro-active access control in computer systems and networks. *Computers & Security*, 49:132–146.

Zhang, Y., He, J., Zhao, B., and Liu, R. (2016). Application of game theory for dynamic access control in security systems. *International Journal of High Performance Computing and Networking*, 9(5-6):451–461.

Zhao, M., Ren, J., Sun, H., Li, S., and Chen, Z. (2008). A game theoretic approach based access control mechanism. In *2008 The 9th International Conference for Young Computer Scientists*, pages 1464–1469. IEEE.