Objective- and Utility-Based Negotiation for Access Control*

Aditya Sissodiya[a], Ulf Bodin[b] and Olov Schelén[c]
Luleå University of Technology, Luleå, Sweden

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

Abstract: Access control in modern digital ecosystems is challenging due to dynamic resources and diverse stakeholders. Traditional mechanisms struggle to adapt, causing inefficiencies and inequities. We propose a novel algorithm that automates access control policy negotiation via objective optimization and utility-based methods. It enables stakeholders to jointly select policies aligned with their preferences, provided a suitable policy exists. Suggested criteria guide the evaluation of predefined policies, and a mathematical formulation quantifies stakeholder preferences with utility functions, using optimization to achieve consensus. The algorithm's multilinear scalability is demonstrated through time and space complexity analysis. An evaluation tool supports practical testing, and the approach enhances efficiency and trust by ensuring equitable data access within digital ecosystems.

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). 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.

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; 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.

Viewing these conflicts as objective optimization problems grounded in cooperative game theory offers structured strategies for consensus (Moura et al., 2019), balancing stakeholder interests. Objective optimization refines policies amid competing goals (Marden and Shamma, 2018; Shamma, 2020; Medvet et al., 2015), aiding usability, accessibility, and more (Zhang and He, 2015; Wang et al., 2019; Ma, 2015; Zhao et al., 2008).

We propose an automated access control negotiation algorithm using objective optimization to address modern ecosystem challenges. Its context-aware approach enables flexible, secure, and equitable policies unattainable by standalone systems (Bharadwaj and Baras, 2003b; Bharadwaj and Baras, 2003a). Leveraging optimization and access control creates policies that are secure, privacy-preserving, adaptable,

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

* 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.

Sissodiya, A., Bodin, U. and Schelén, O.
Objective- and Utility-Based Negotiation for Access Control.
DOI: 10.5220/0013130000003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 2*, pages 493-501
ISBN: 978-989-758-735-1; ISSN: 2184-4356

and representative of diverse interests (Moura et al., 2019; Zhang et al., 2016; Vamvoudakis and Hespanha, 2018).

Contributions:

- We identify key challenges in complex digital ecosystems (Section 2) and introduce IDSA-aligned criteria to guide negotiation (Section 3).
- We provide a mathematical definition of our negotiation algorithm (Section 4).
- We evaluate the algorithm through simulations (Section 5), analyze complexity (Section 6).

A tool for evaluating the algorithm's performance is available on (GitHub), and related work is discussed in Section 7.

2 CHALLENGES IN ACCESS CONTROL

As digital ecosystems grow more interconnected and complex, traditional access control mechanisms must be reevaluated (Subramaniam et al., 2019). Our negotiation algorithm addresses critical needs arising in collaborative digital platforms.

- **Dynamic Requirements and Automation:** Digital ecosystems change rapidly in resources, roles, and contexts (Subramaniam et al., 2019). Traditional methods struggle to adapt (Servos and Osborn, 2017; Zhang et al., 2015), and existing NAC frameworks rely on manual negotiation. By automating negotiation via mathematical optimization, our algorithm efficiently adapts to modern ecosystems.
- **Complexity and Scalability:** Multiple stakeholders with varied interests complicate access control (Shojaiemehr et al., 2018). Our approach centralizes utility aggregation and resolves conflicts objectively, reducing communication complexity from quadratic to linear and enabling scalable stakeholder and policy management.
- **Equitable Access and Efficient Negotiation:** Equitable resource access is essential (Subramaniam et al., 2019; Steinbuss et al., 2021), but existing frameworks, including blockchain-based ones like FairAccess (Ouaddah et al., 2016) and Policychain (Chen et al., 2021), often enforce immutable policies. Our negotiation mechanism allows transparent, compromise-driven policy adjustments without excessive latency.
- **Regulatory Compliance and Adaptability:** Regulations like GDPR and CCPA (Dasgupta et al., 2019; Otto et al., 2021) demand ongoing compliance. By continuously negotiating policies according to current laws, our algorithm helps avoid legal risks and protects organizational reputation.

3 CRITERIA FOR NEGOTIATION

Our negotiation algorithm's success depends on the criteria used to evaluate access control policies. To ensure these are comprehensive and robust, we base them on principles from the International Data Spaces Association (IDSA).

IDSA standards provide a technical foundation for secure, reliable data exchange (Otto et al., 2021). In manufacturing, where data sovereignty is crucial, these criteria meet diverse stakeholder needs (Larrinaga, 2022). By aligning with proven frameworks, we improve access and usage control (Steinbuss et al., 2021) while ensuring compliance aligned with IDSA and GAIA-X, thus reducing legal risks and maintaining secure practices (Otto et al., 2021; Huber et al., 2022). The criteria are as follows:

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:** Assesses how understandable and user-friendly the policy is for those who must apply it. A user-friendly policy reduces friction, enhances the overall user experience, and mitigates the risk of misinterpretation or accidental non-compliance.
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 keep negotiations relevant and user-friendly as contexts change, reducing complexity in multi-stakeholder scenarios.

3.1 Policy Evaluation Guidance

We propose a scoring framework (1-10) for each criterion, with guidelines for interpreting scores. Stake-

holders value criteria differently, and subjective ratings reflect their preferences, leading to satisfactory outcomes.

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, offering maximal benefit and alignment.
2. **Usability:**
   - **1-3** (Low Usability): Complex, difficult to implement, causing frustration/errors.
   - **4-6** (Moderate Usability): Requires multiple approvals/specialized knowledge.
   - **7-8** (High Usability): User-friendly, clear instructions, minimal complexity.
   - **9-10** (Very High Usability): Highly intuitive, streamlined, enhancing user experience.
3. **Accessibility:**
   - **1-3** (Low Accessibility): Severely restricts access, impeding tasks.
   - **4-6** (Moderate Accessibility): Allows access but with limiting constraints.
   - **7-8** (High Accessibility): Adequate access, enabling effective task performance.
   - **9-10** (Very High Accessibility): Seamless, barrier-free access.
4. **Compliance:**
   - **1-3** (Low Compliance): Fails key regulatory requirements, posing legal risks.
   - **4-6** (Moderate Compliance): Complies partially, lacking in some areas.
   - **7-8** (High Compliance): Meets all relevant compliance requirements.
   - **9-10** (Very High Compliance): Exceeds standards, 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

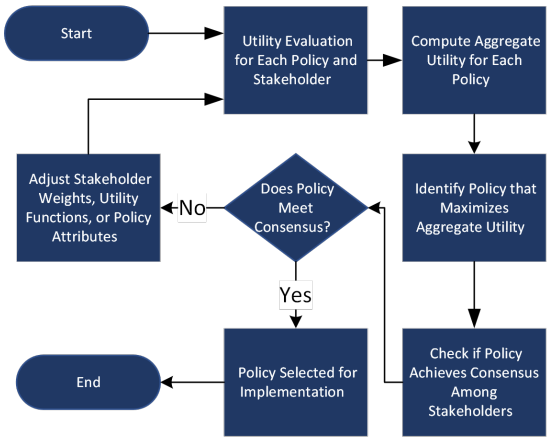

Figure 1: Algorithm for Negotiation.

- **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.

4.1.2 Objectives Optimization

The optimization step 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).

- 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 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 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. This tool, available on GitHub under the MIT license, empowers users to add policies and stakeholders, assign and update weights, and calculate the optimal policy based on the aggregate utility, ensuring that stakeholder consensus is considered. It uses Flask and PostgreSQL for the backend and HTML/CSS/JavaScript for the frontend, and is containerized with Docker for easy deployment.

- **Features:**
  - Add Policies: Introduce new policies with attributes like security, applicability, privacy, accessibility.
  - Add Stakeholders: Include stakeholders and define influence levels.
  - Assign Weights: Set weights for policy attributes per stakeholder perspective.
  - Calculate Optimal Policy: Identify the policy with highest aggregate utility.
  - Check Consensus: Confirm if the chosen policy meets the defined utility threshold across stakeholders.

(Implementation of the algorithm and the tool is available at this GitHub repository.)

5 REAL-WORLD SCENARIO EVALUATION

Consider a connected car ecosystem with multiple stakeholders sharing sensitive data like vehicle

telemetry, maintenance records, and user information:

- **Car Owner (O):** Values privacy and control over data access.
- **Car Manufacturer (M):** Needs performance data to improve designs.
- **Insurance Company (I):** Uses driving and maintenance data for risk assessment.
- **Car Workshop (W):** Requires diagnostics and history for better service.

They must agree on a policy that balances all interests. Three proposed policies are:

- **Policy P_1:** Open access without owner consent.
- **Policy P_2:** Role-based access, with personal data requiring owner consent.
- **Policy P_3:** Owner approval needed for every data request.

Each stakeholder rates these policies and assigns weights to each criterion (summing to 1).

5.1 Algorithm Steps

- **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 $w_{W,A} = 0.4$, $w_{W,U} = 0.2$, $w_{W,Ac} = 0.3$, $w_{W,C} = 0.1$.
- **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 2.
- **Step 3: Calculate Individual Utilities.** For each stakeholder and policy, calculate the utility using the formula:

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

  - $w_{a_i,l}$ = 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 1.

Table 1: 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

- **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.

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

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

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.

Table 2: 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)

5.2 Quantitative Analysis

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.

5.2.1 Utility Distribution Plot

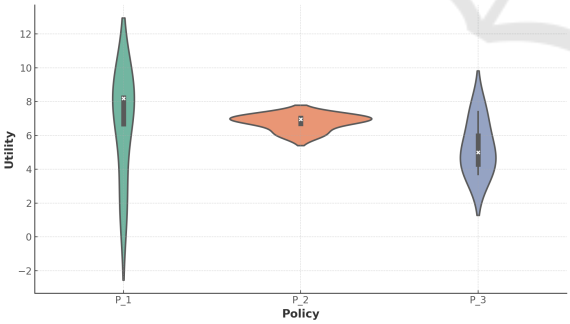

Figure 2: Utility Distribution Across Policies (Violin Plot).

- P_1: Higher values for most stakeholders, but the car owner's utility is much lower.
- P_2: Balanced distribution, values clustered around the median, indicating broad agreement.
- P_3: Lower overall values, except for the car owner, indicating varied stakeholder opinions.

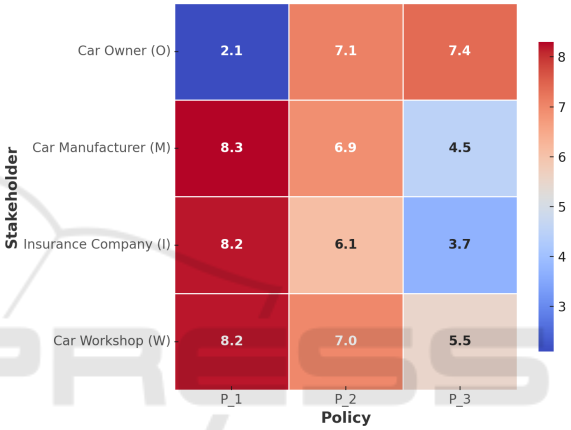

Figure 3: Stakeholder Utility Heatmap.

5.2.2 Stakeholder Utility Heatmap

- Darker colors mean higher satisfaction. P_2 shows balanced support, while P_1 pleases most but not the car owner.
- Clear conflicts appear (e.g. Car Owner vs. others on Policy P_1). P_2 is more acceptable to all.
- P_3 favors the Car Owner but not others, prioritizing privacy over accessibility.

6 ALGORITHM COMPLEXITY ANALYSIS

- 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.

- 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 RELATED WORK

Research increasingly recognizes the need for dynamic, secure, and collaborative policy management in digital ecosystems. Approaches range from relationship-based access control to blockchain-based frameworks, helping stakeholders reach consensus on policies, maintain confidentiality, and enable flexible mechanisms in complex environments.

Negotiation is critical for managing access control and privacy in digital systems, including cloud services, digital ecosystems, and multi-agent platforms (Mehregan and Fong, 2016; Subramaniam et al., 2019). Traditional methods now incorporate dynamic negotiation algorithms to handle fine-grained requirements, letting stakeholders set policies that reflect various constraints and preferences.

Work on Relationship Based Access Control (ReBAC) includes methods for resolving conflicting privacy needs among co-owners, using SAT solvers to verify policy satisfiability (Mehregan and Fong, 2016). Negotiation in large-scale and dynamic coalitions is explored in (Gligor et al., 2002), while autonomous agents and a mathematical negotiation framework are detailed in (Bharadwaj and Baras, 2003b). Adaptive negotiation to manage rapidly changing digital ecosystems is discussed in (Subramaniam et al., 2019).

Blockchain-based solutions support transparent, decentralized policy management, ensuring auditability and trust. Policychain (Chen et al., 2021) uses blockchain nodes for ABAC policy decisions, ensuring high availability and autonomy. FairAccess (Ouaddah et al., 2016) removes centralized authorities to enhance security and privacy. AuthPrivacyChain (Yang et al., 2020) employs blockchain node addresses as identities, providing secure encryption and management of cloud-stored data, including authorization and revocation processes.

Our algorithm addresses a gap by automating dynamic, context-aware, and equitable negotiations, reflecting all stakeholders' interests.

8 CONCLUSION

This paper identifies key challenges in multi-party access control negotiations and presents both criteria and an algorithm to address them. The proposed algorithm significantly improves access control in complex, dynamic digital ecosystems by balancing security, confidentiality, and usability.

While traditional methods struggle with the multifaceted needs of diverse stakeholders, our algorithm employs objective optimization to support fair, structured negotiations that accommodate various interests. This fosters trust and cooperation among stakeholders, enhancing the overall management of digital resources. By integrating standardized specifications from the International Data Spaces Association, the algorithm remains technically sound, enforceable, and adaptable. Its ability to respond dynamically to changing conditions underscores its relevance in today's evolving digital landscape.

Overall, this work not only advances immediate outcomes in access control negotiation but also encourages rethinking existing frameworks, driving ongoing innovation in the management of digital ecosystems.

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.

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.

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.

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.

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.