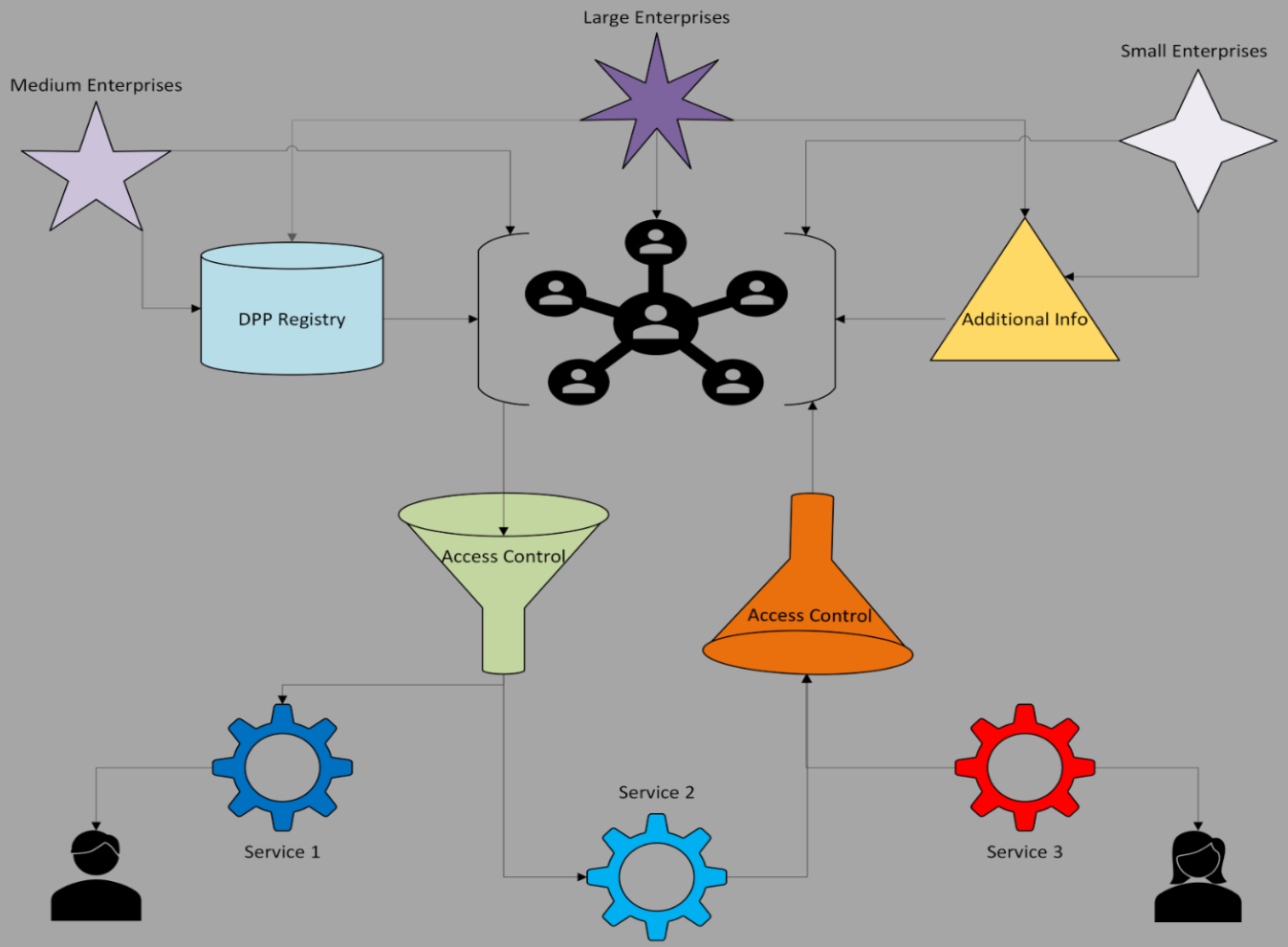
Objective- and Utility-Based Negotiation for Access Control

Aditya Sissodiya, Ulf Bodin, Olov Schelén
Luleå University of Technology, Sweden

Agenda

- Problem Statement & Challenges
- Proposed Negotiation Criteria and Algorithm
- Key Assumptions & Methodology
- Evaluation & Results
- Conclusion & Future Work
- Q&A

The Problem with Dynamic Access Control



- Growing need for data sharing and collaboration among multiple stakeholders, where these complex policies evolve over time.
- This can lead to conflicts, reduced usability, and inflexibility in dynamic environments.
- Emerging scenarios: Digital Product Passports, IoT, collaborative supply chains.
- Regulatory Pressures: GDPR, CCPA, and industry-specific policies (e.g., IDSA, GAIA-X).

Why Negotiation?

- Different stakeholders have diverse and sometimes conflicting requirements (privacy, compliance, usability, etc.)
- Manual negotiation is inefficient and error-prone
- **Key Insight:**

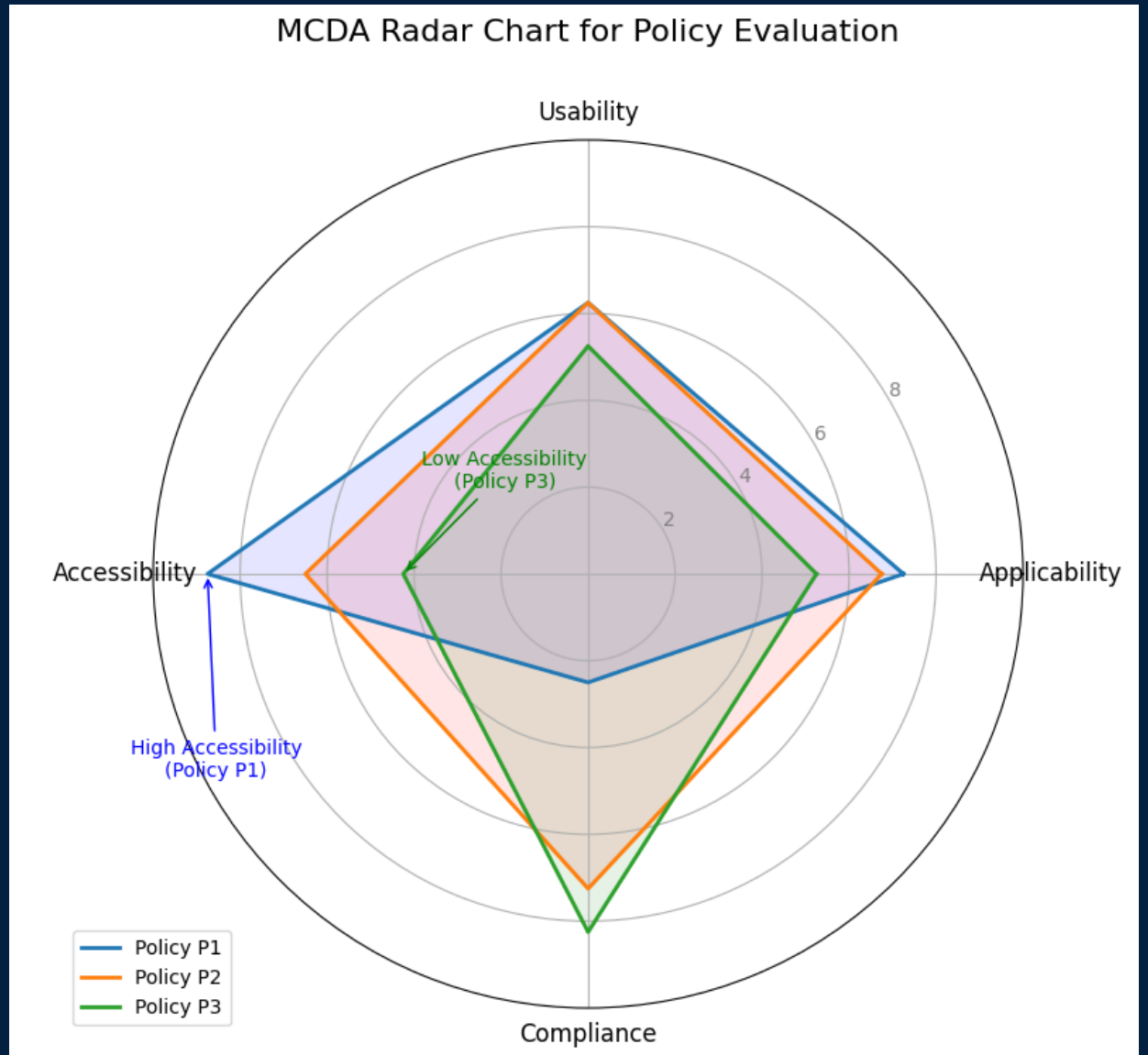
We propose that access control policies should be negotiable.

Negotiability here means choosing the most suitable policy among a set of pre-defined policies.

- **Clarification:**

We do not build new policies during negotiation.

The current focus is on selecting the best option based on stakeholder preferences.



Negotiation addresses conflicting stakeholder requirements by selecting the policy that best balances diverse ratings (e.g., bridging the gap between high and low Accessibility).

Where Do the Negotiation Criteria Come From?

	Data spaces design principles			
Data space architecture requirements	**Data soverei-gnty**	**Level palying field**	**Descentralised soft infraestructure**	**Public-private governance**
Data-sharing empowerment	●	○	○	●
Data-sharing trustworthiness	●	●	●	●
Data-sharing publication	●	○	○	○
Data-sharing economy	●	●	●	○
Data-sharing interoperability	○	●	●	○
Data space engineering flexibility	○	●	●	○
Data space community	○	●	●	○

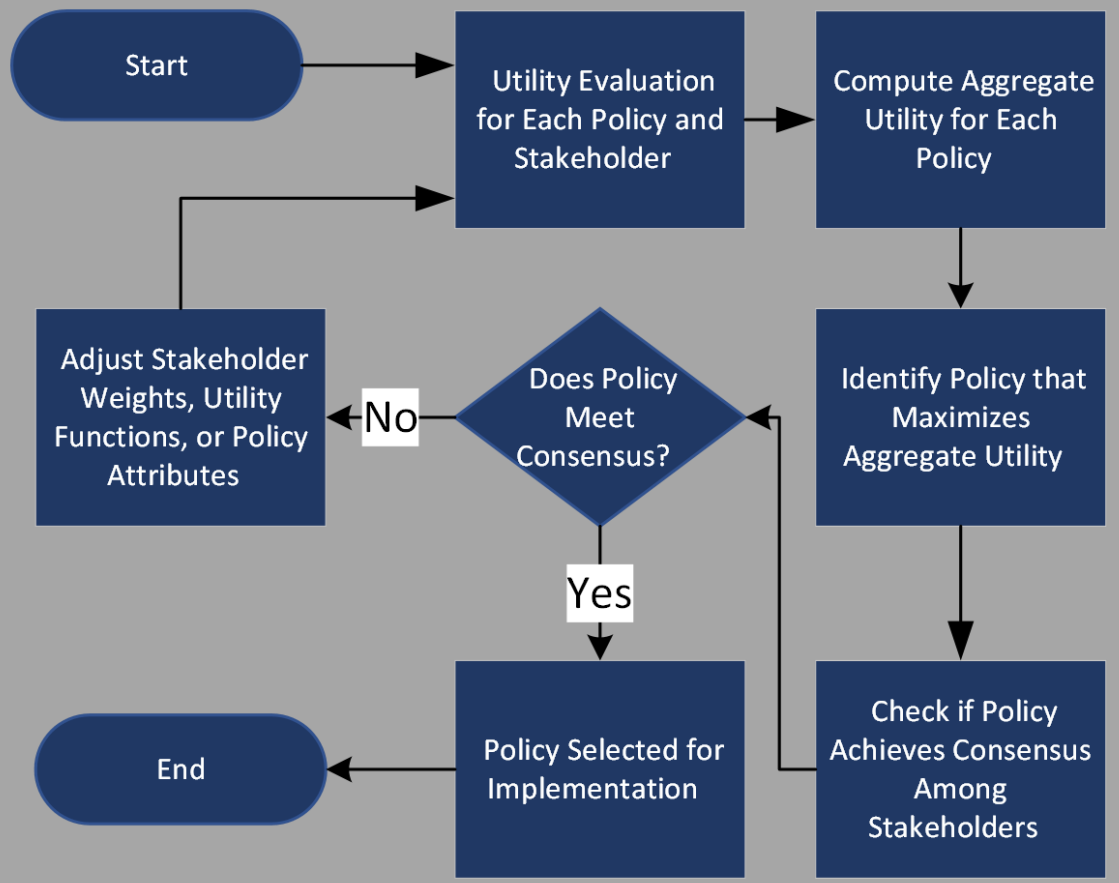
Criteria are derived from stakeholder needs and established standards (IDSA).

Typical criteria include:

- Applicability: How well does the policy serve operational needs?
- Usability: Is the policy user-friendly?
- Accessibility: Does it allow sufficient access?
- Compliance: How well does it meet regulatory requirements?

Assumption: Unlike conventional views, we assume that even strict policies can be negotiated based on these diverse criteria.

Our Negotiation Approach



- Define a set of candidate access control policies.
- Stakeholders assign weights to each criterion.
- Evaluate each policy using utility functions.
- Aggregate utilities to select the optimal policy.
- Check consensus to ensure stakeholder satisfaction.

Example Scenario

- Scenario: Connected Car Ecosystem
- Stakeholders:

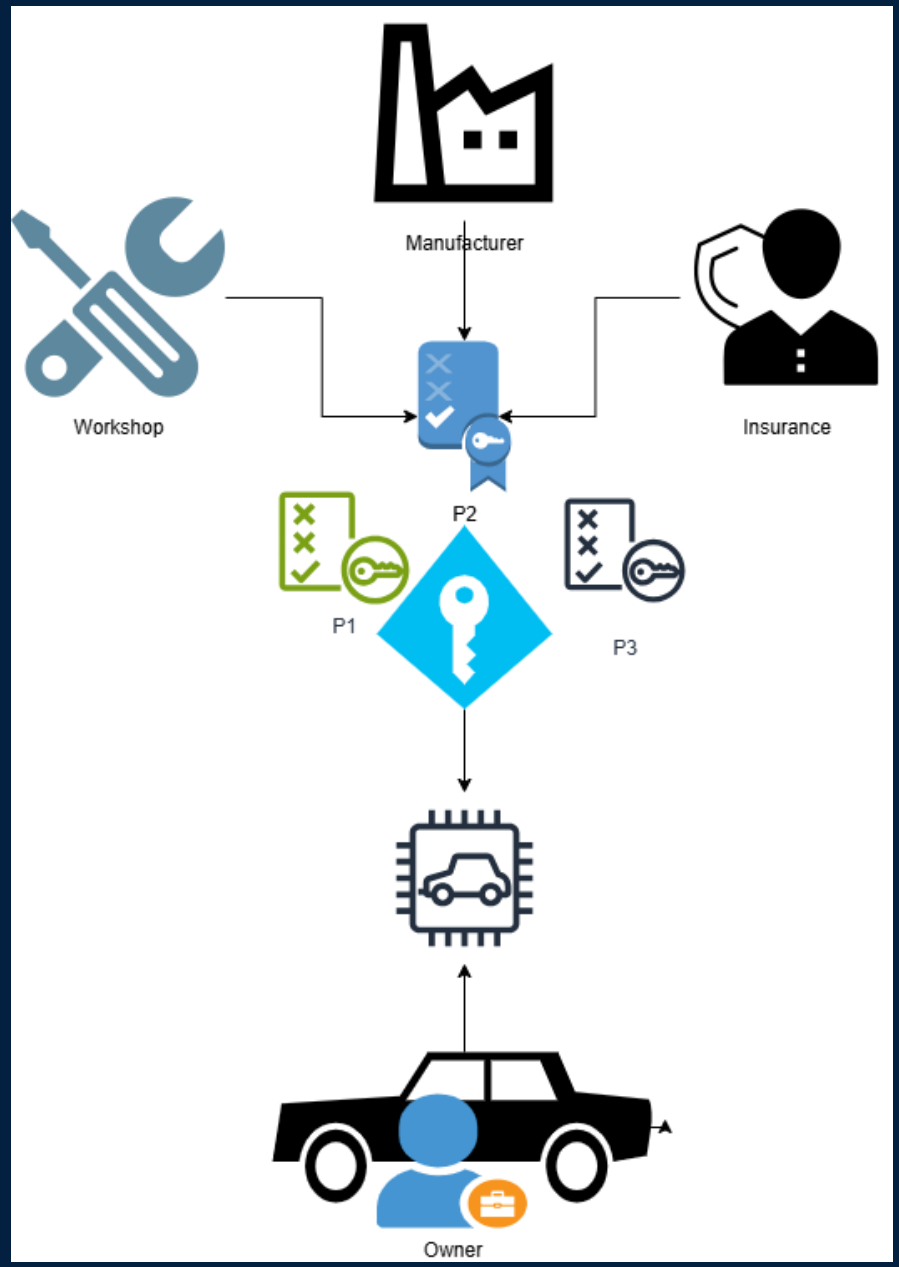
a. Car Owner

b. Manufacturer

c. Insurance

d. Workshop

- Candidate Policies: e.g., Open Access, Role-Based Access, Owner Approval.



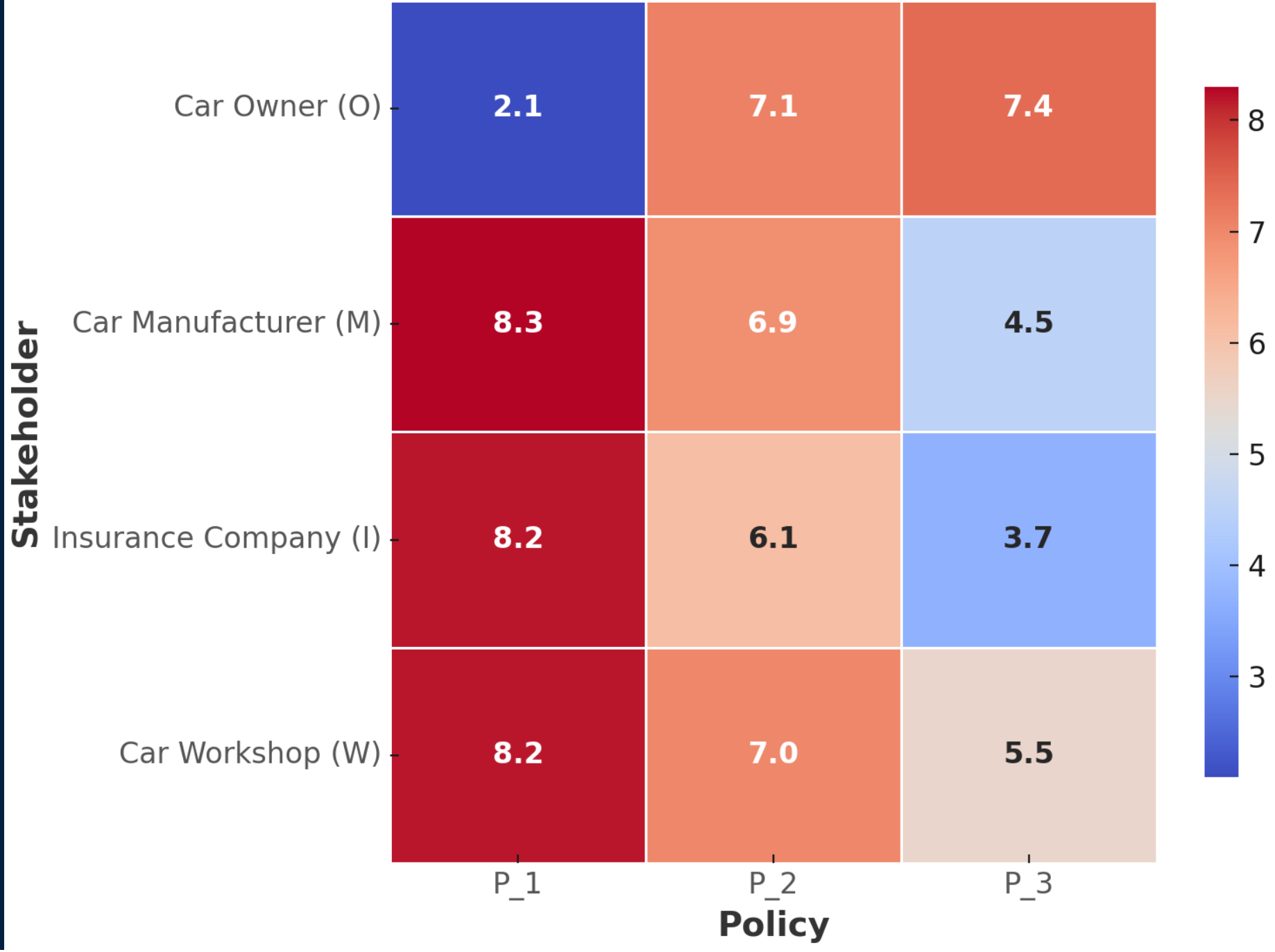
Stakeholder	Applicability (A)	Usability (U)	Accessibility (Ac)	Compliance (C)
Policy P_1: Open Access Without Consent				
Car Owner (O)	2 (Low benefit)	2 (Poor usability)	8 (High for others)	1 (Fails privacy)
Car Manufacturer (M)	9 (High benefit)	8 (Easy access)	9 (Very high)	3 (Regulatory issues)
Insurance 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)

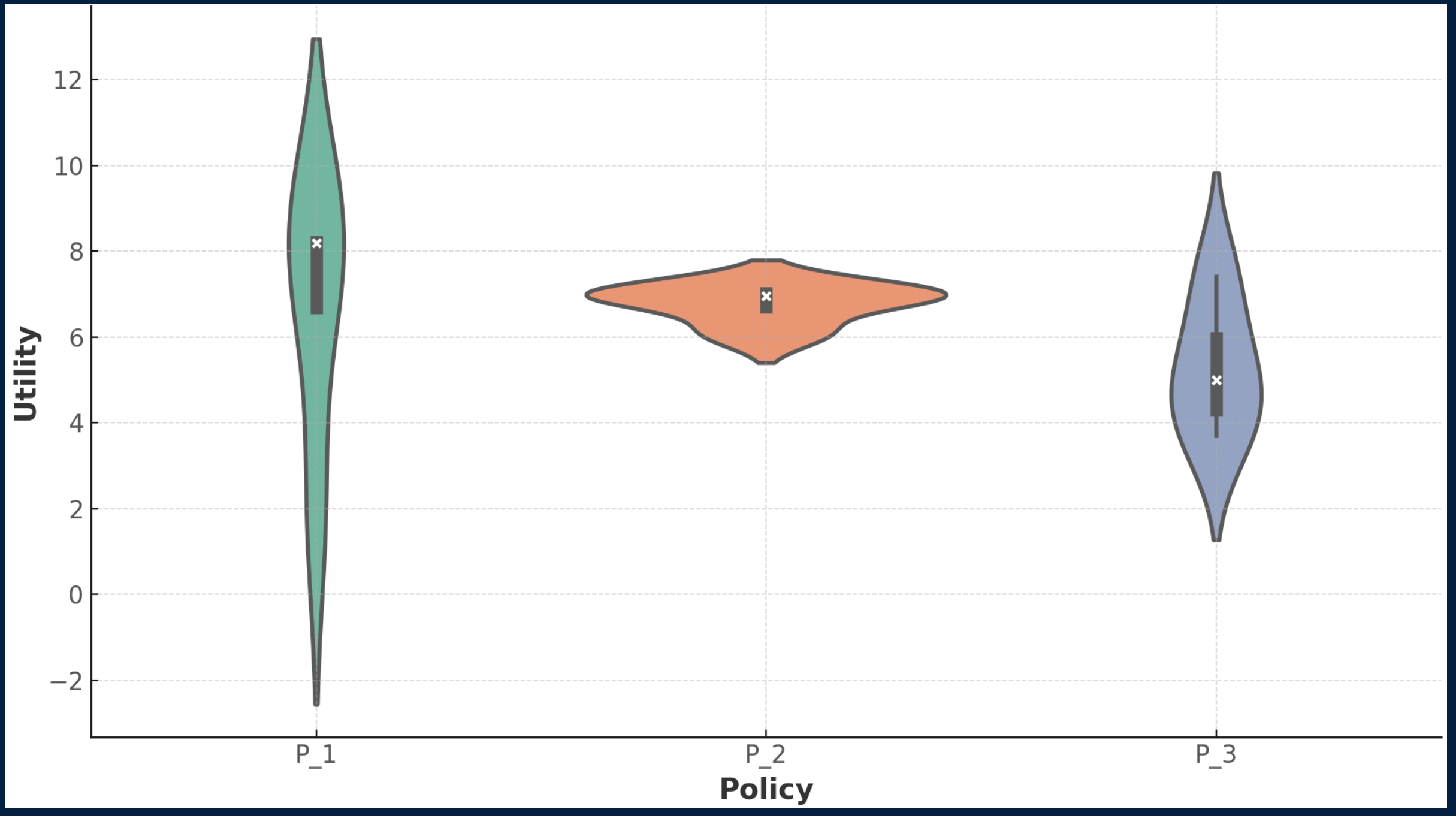
1. Utility Evaluation: $U_{a_i}(P_j) = \sum_{l=1}^{k} w_{a_i,l} \cdot f_l(P_j)$

2. Aggregate Utility: $U_{\text{agg}}(P_j) = \sum_{i=1}^{n} \alpha_i \cdot U_{a_i}(P_j)$

3. Optimization: $P = \arg\max_{P_j \in P} U_{\text{agg}}(P_j)$

4. Consensus Check: $\forall i : U_{a_i}(P^{)} \geq \theta$


Car Owner (O)
Car Manufacturer (M)
Insurance Company (I)
Car Workshop (W)
Stakeholder
2.1
7.1
7.4
8.3
6.9
4.5
8.2
6.1
3.7
8.2
7.0
5.5
P_1
P_2
P_3
Policy
8
7
6
5
4
3


12
10
8
6
4
2
0
−2
Utility
P_1
P_2
P_3
Policy

Policy Evaluation Tool

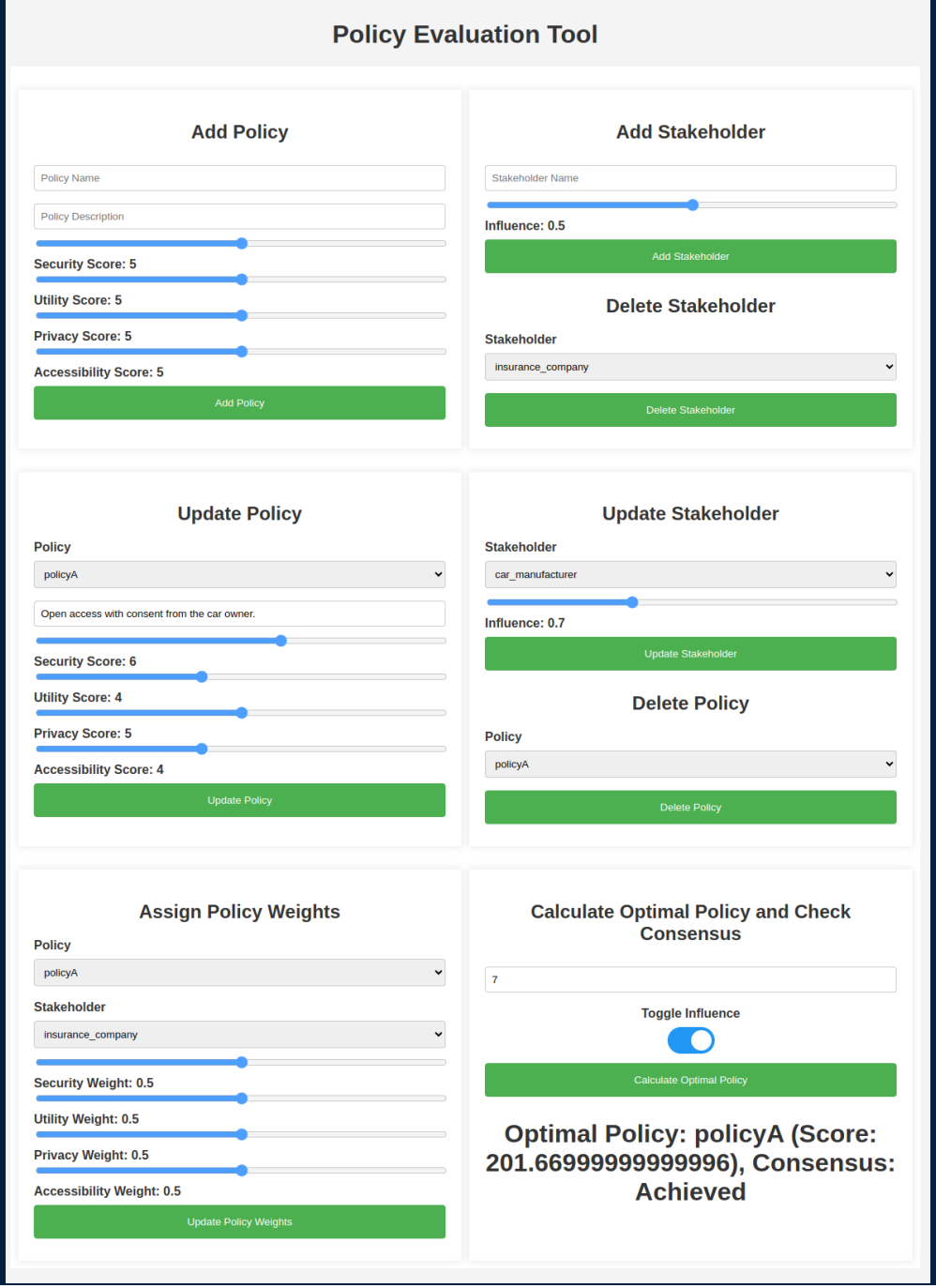
Tool Features:

Web-based interface (Flask, PostgreSQL, Docker).

Allows users to add policies, define stakeholder weights, and compute optimal policies.

Purpose:

Demonstrates the viability of the approach in a user-friendly environment.

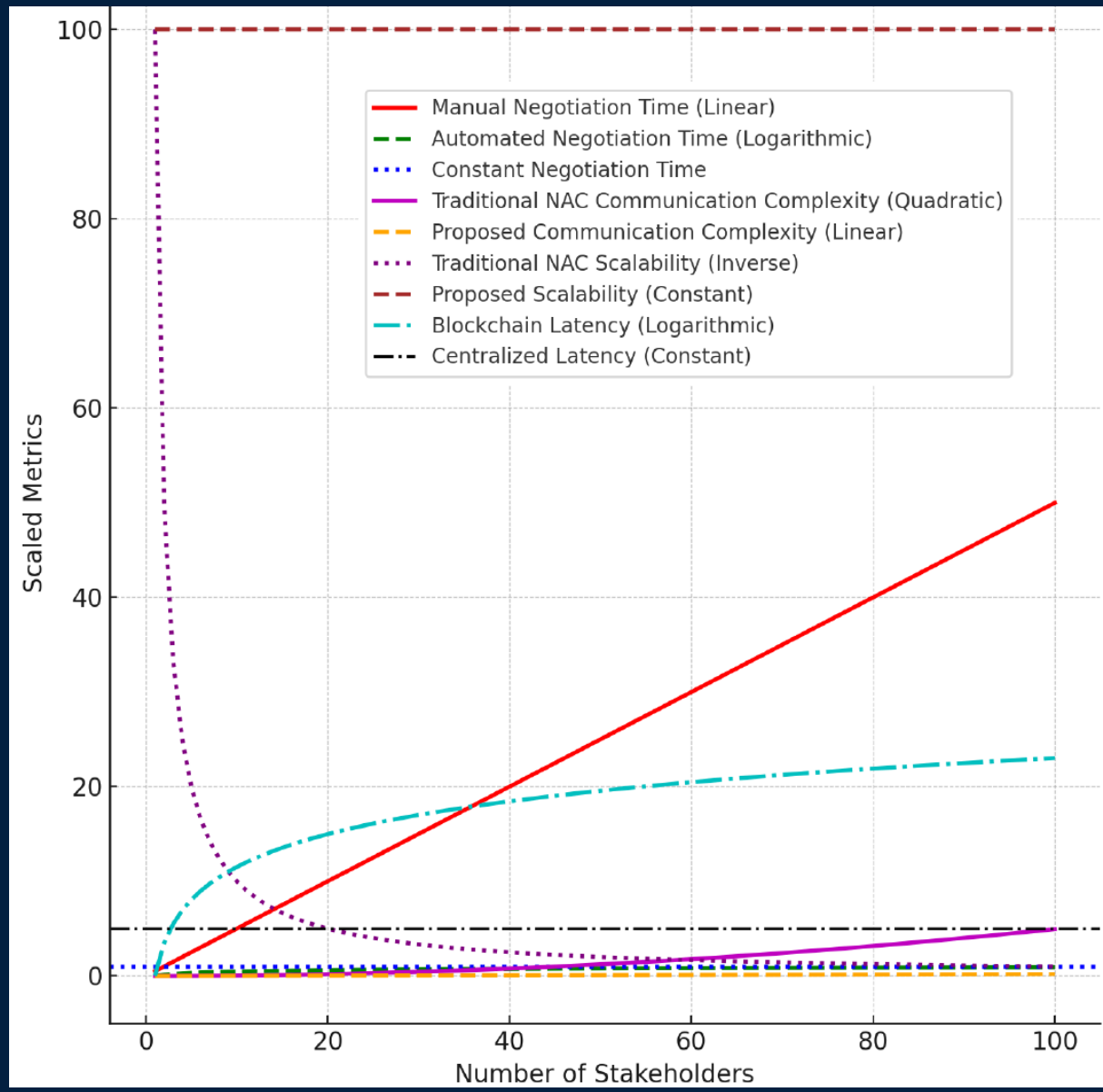


Comparative Analysis

- **Negotiation Time.**
- **Complexity.**
- **Scalability.**
- **Decentralization:**

  Systems like FairAccess use **distributed ledgers** for transparency and auditability.

  However, consensus mechanisms introduce **latency and complexity**.



Results & Discussion

- Key Takeaways:

The approach attempts to enhances flexibility and stakeholder satisfaction in dynamic environments.

Side note: Negotiability in access control here means selecting the best existing policy, not inventing a new one.

Future Work:

- Extending the framework to synthesize new policies.
- Integrating more advanced negotiation techniques and criteria.


LULEÅ
UNIVERSITY
OF TECHNOLOGY