Privacy-Patterns for IoT Application Developers

Nada Alhirabi[1,3], Stephanie Beaumont[2], Omer Rana[1], Charith Perera[1]

[1]Cardiff University   [2]My Data Fix Ltd   [3]King Saud University

1 Motivation

- IoT apps typically collect and analyse personal data categorised as sensitive which may be subject to a higher degree of protection under data privacy laws.
- Privacy concerns for app design or implementation are rarely discussed by developers.
- There are limited tools to assist developers' privacy learning.
- **PARROT**, an interactive IoT application design tool, is supplemented with different techniques to help increase developers' privacy awareness.
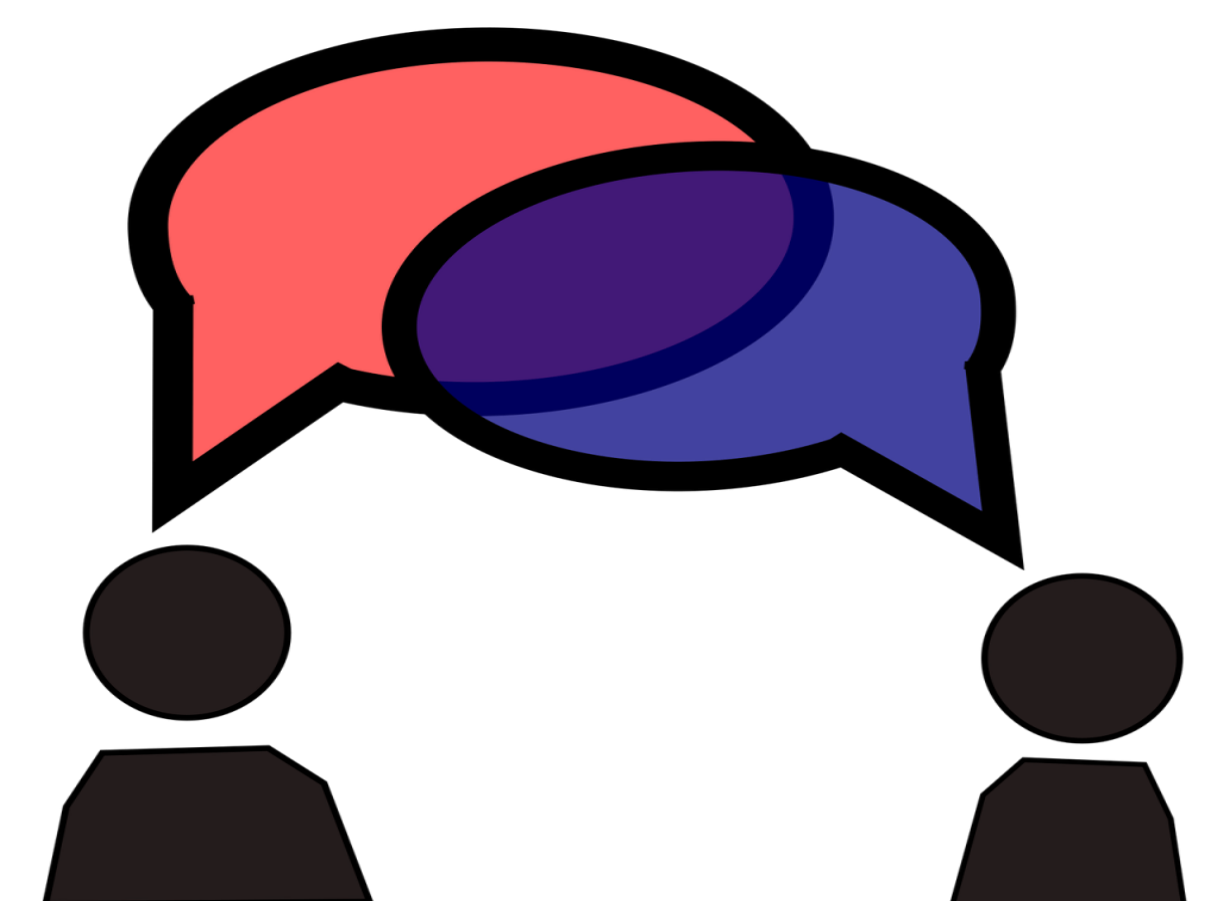
2 Methodology

Qualitative user research:

1. 12 semi-structured interviews.

2. 6 IoT application design tasks.
3. Discussion session with participants to explore how they integrate privacy and how PARROT could help.
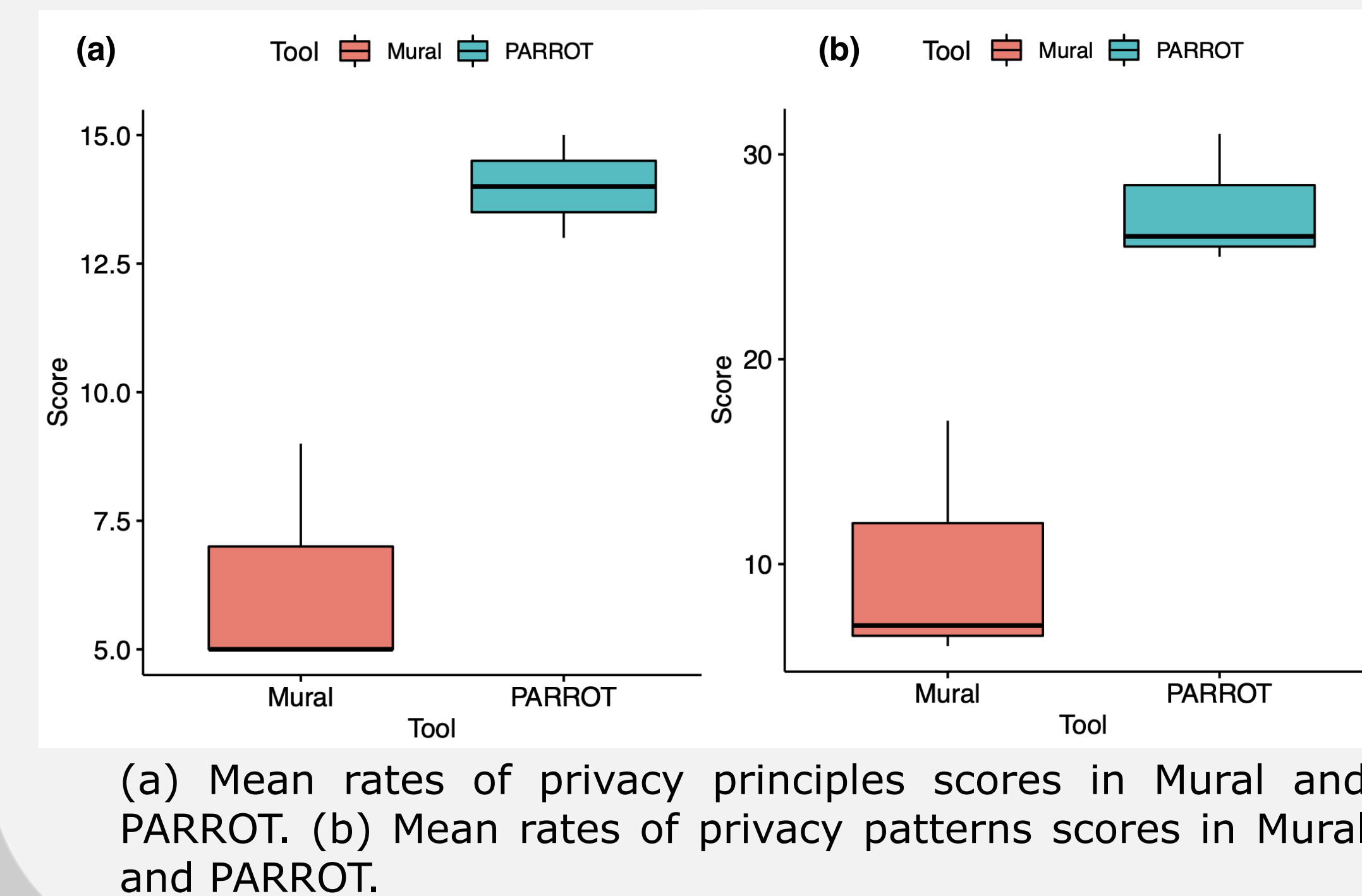
3 Design tasks

- Between-subjects study.

Privacy measures:

- **6** privacy by design principles.
- **20** privacy patterns.

1. Use of dummies
2. Location granularity.
3. Minimal information asymmetry.
4. Asynchronous notice
5. Privacy policy display
6. Outsourcing [with consent]
7. ~~~~
8. Anonymity set
9. Pseudonymous identity
10. Privacy icons
11. Data breach notification
12. Privacy dashboard
13. Added-noise obfuscation
14. Increasing aggregation awareness
15. Privacy awareness panel
16. Obtaining explicit consent
17. ~~~~
18. Who's listening
19. Sticky policies
20. Lawful consent

4 Results

(a) Mean rates of privacy principles scores in Mural and PARROT. (b) Mean rates of privacy patterns scores in Mural and PARROT.

PARROT design:

Circular shape reflects privacy-by-design requirement

Triangular shape represents best practices that not part of privacy by design.

Privacy configuration area: The questions are a combination of direct and indirect ones to make sure developers read and understand their choices.

Design area: It shows connected nodes while the data transfer between them.

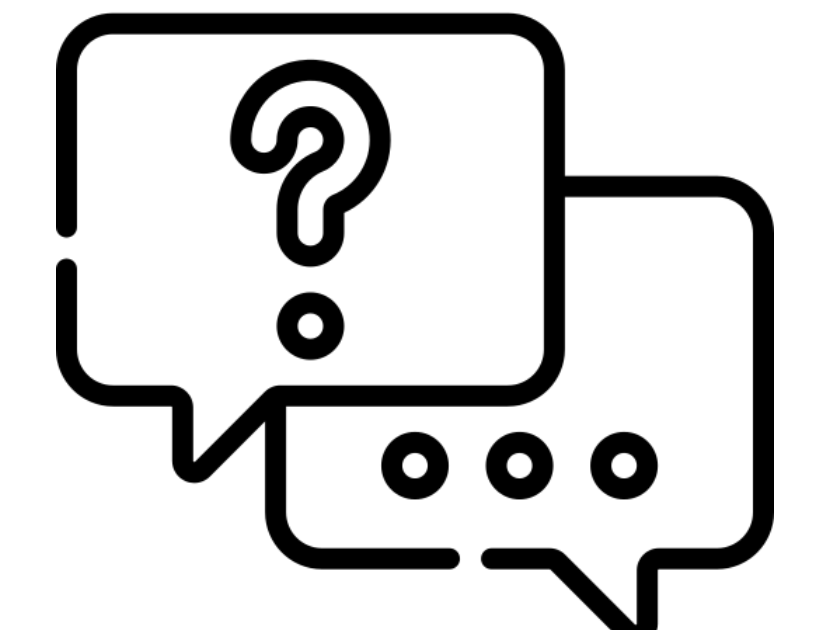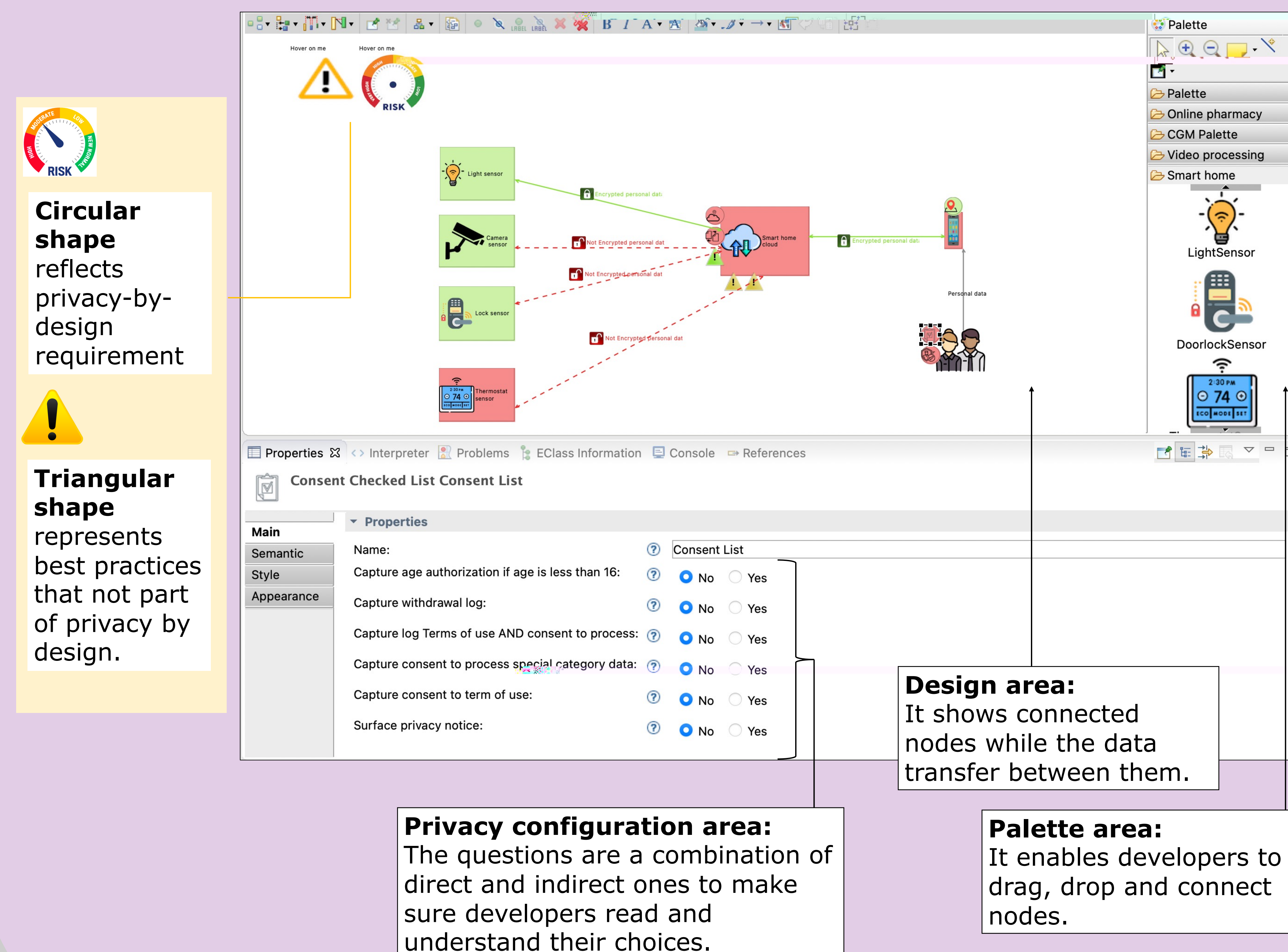**Palette area:** It enables developers to drag, drop and connect nodes.

5 What do you expect from PARROT?

"I definitely struggle to understand and apply privacy and privacy patterns because there are many different documents, laws and IoT devices... PARROT will tell you already what privacy needs to be fulfilled for that node which is super useful, in my opinion...you don't have to start researching about it" (Pair 4).

6 What is the legal perspective?

PARROT is able to include privacy-specific design components into the IoT application "from the beginning rather than retrospectively" (lawyer).

7 What does PARROT offer to you?

- "The questions help me to think more about the data subject perspective, not the problem owner only" (Pair 5).
- "The generated colours are helpful to flag any privacy issue immediately... I think it helps to rethink the question again" (Pair 2).

8 Conclusion

The participants demonstrated how an assistant tool helps to embed privacy principles and increases their awareness of privacy patterns.

Contact: alhirabin@cardiff.ac.uk