Tampere University

Augmentative Technology

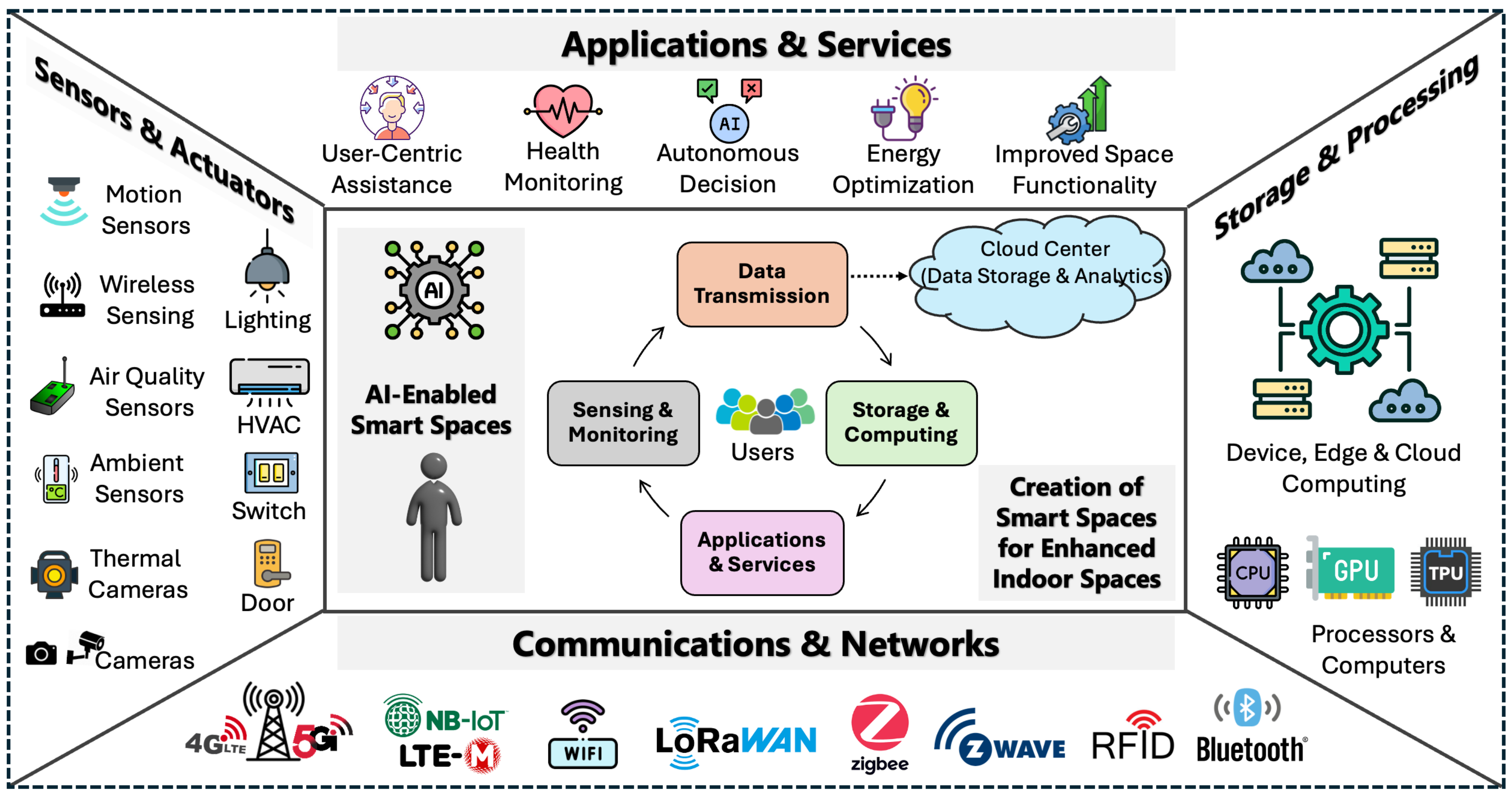
AI-Driven Smart Environments for Secure, Personalized, Sustainable Indoors

Aygün Varol
Faculty of Information Technology and Communication Sciences, Tampere University, Finland
aygun.varol@tuni.fi

Research Gaps

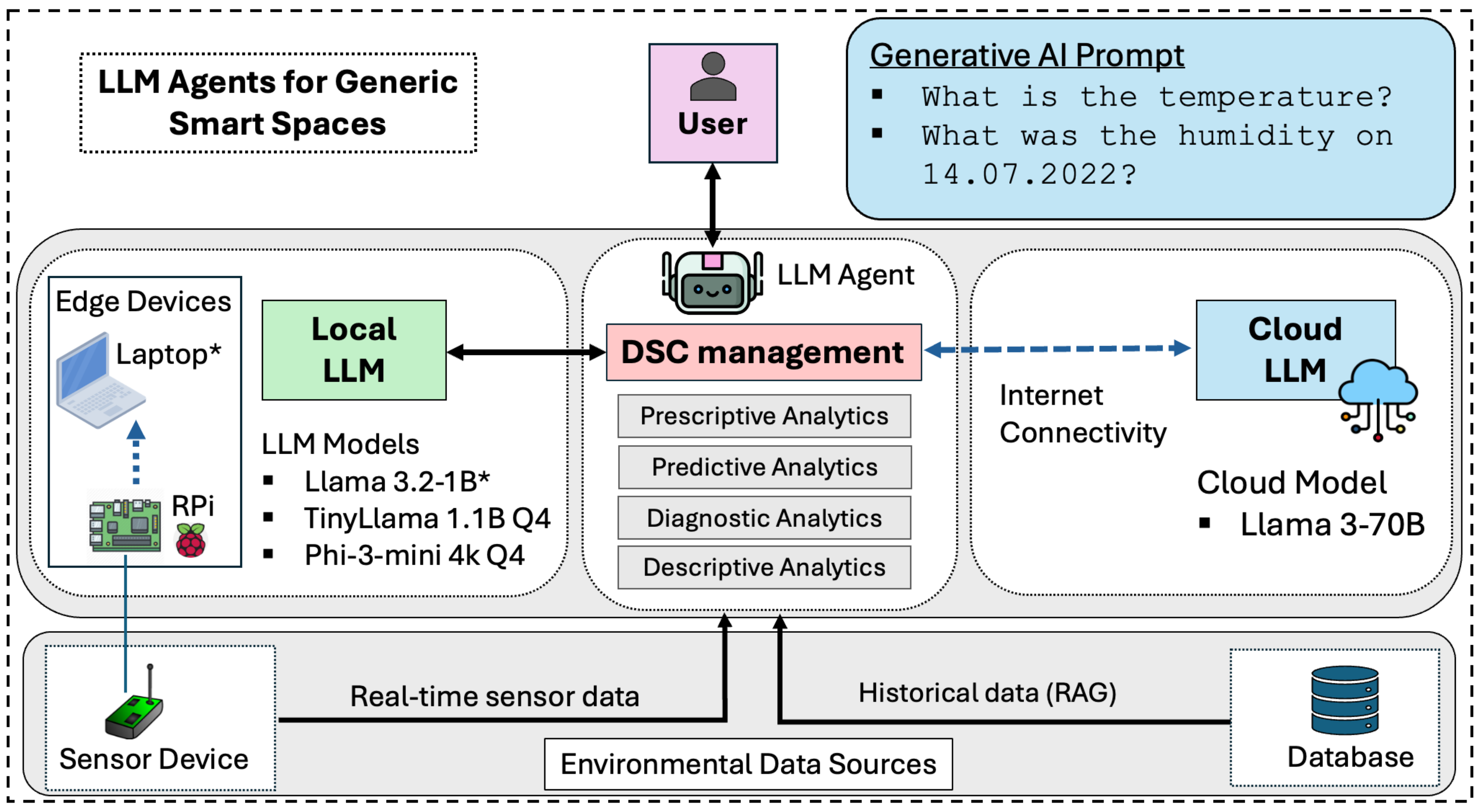
Smart environments are indoor environments equipped with Internet of Things (IoT) devices, that collect data such as temperature, pressure, humidity. This data is then used to provide services to the residents. These services include activity recognition, fall detection, air quality monitoring.

Large language model (LLM) agents can turn ordinary rooms into responsive smart environments able to reason over multi-modal sensor streams and inform the occupants. They enable enhanced services thanks to their ability to understand natural language.



Research Questions

1. What is the optimal integration of IoT-based sensor networks to smart environments for creating sustainable living environments?
2. What are the most effective AI models for processing and inferring knowledge from heterogeneous sensor data?
3. What are the potential risks and unintended consequences of AI deployment in smart environments, and how can they be mitigated?



Methodology

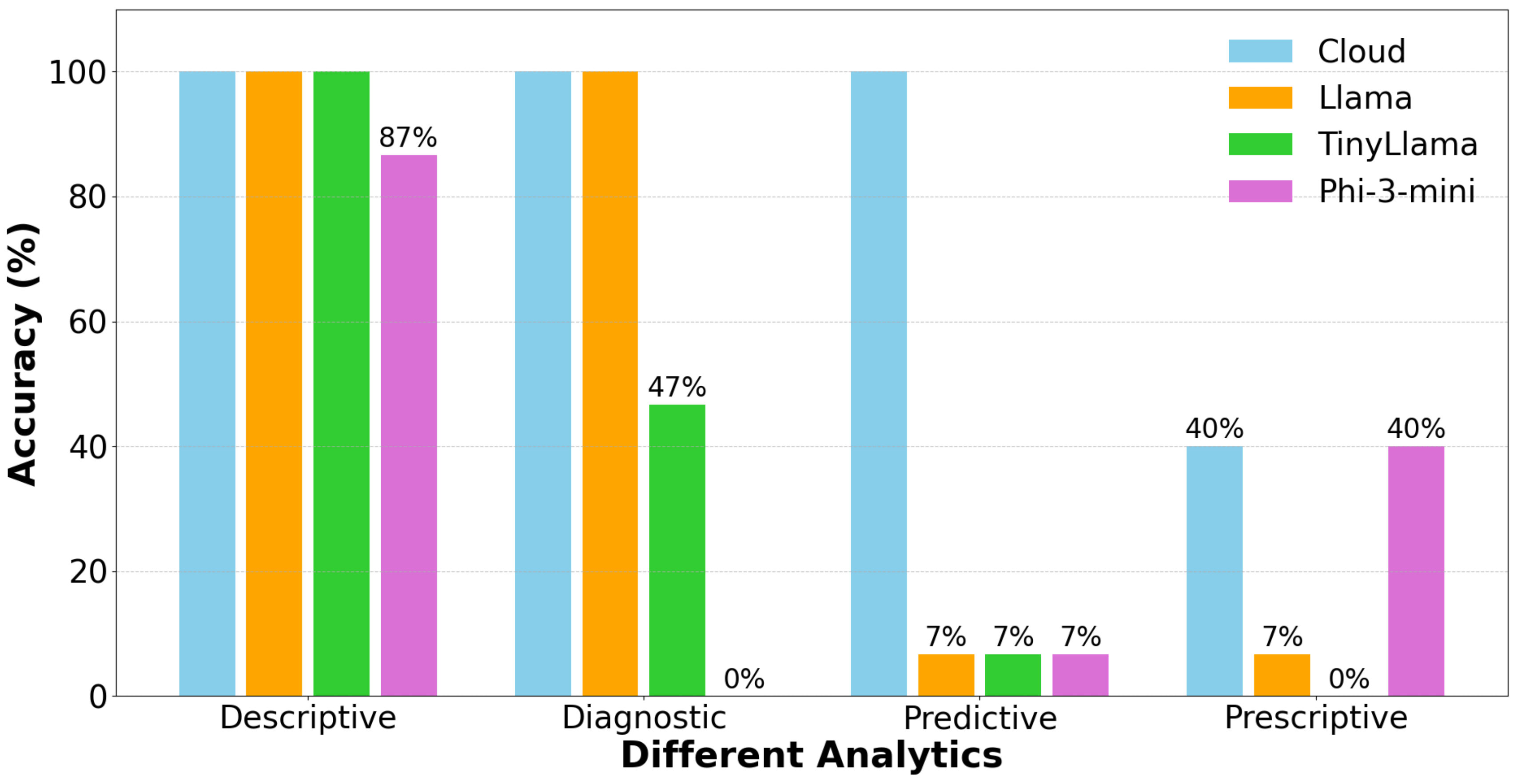
1. **Survey:** To support RQ1, a comprehensive survey identified key components for AI-driven smart spaces, covering sensor technologies, communication protocols, network management, data collection, and analytics.
2. **Hybrid Framework:** Addressing RQ2, this study develops a hybrid LLM-based AI architecture to process multimodal sensor data (e.g., air quality, temperature, CO_2) for indoor air quality analytics.
3. **On-Device LLMs:** Also, for RQ2, we build an edge sensor-driven AI framework to collect and analyze indoor data in real-time using local LLMs, detect patterns, and adapt smart environments for improved decision making in these spaces.
4. **Evil AI Benchmark:** In response to RQ3, EVIL-AI, a benchmark for LLM-powered agents in smart environments that assigns quantitative security scores via executable attacks, prompt injection, persuasion, man-in-the-middle, data leaks, and unsafe action requests, providing a toolkit to assess LLM security.

Key Challanges

❑ **Latency vs. privacy trade-off:** Cloud inference is fast-but-remote, while edge devices are slow-but-local.
❑ **Resource constraints:** IoT devices often have small computational capability
❑ **Safety and "evil" behavior:** LLM agents remain vulnerable to prompt-injection, data-poisoning and persuasive misuse.
❑ **Privacy:** real-time monitoring, activity logs rasies ethical concerns. Explainable AI needed to maintain trust. Personal data needs to be stored locally.

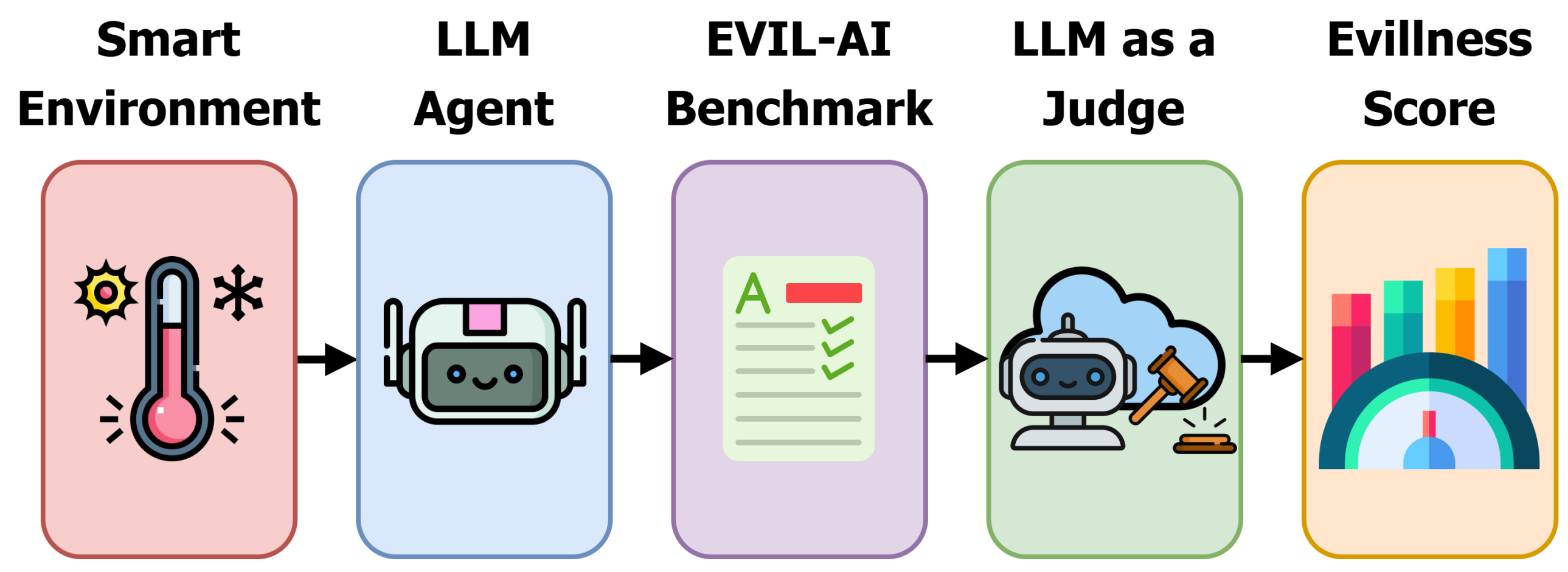
Preliminary Results

❑ Cloud LLMs deliver 100% accuracy with 496–528 ms mean latency on descriptive & predictive queries
❑ Edge LLMs also deliver 100% accuracy at 663 ms mean latency, best offline substitute
❑ On-device LLMs can reach 100% accuracy with latency tradeoffs.



Impact

1. **Technical Impact:** Establishes a real-time, edge-enabled framework that integrates environmental sensing with AI analytics, enabling accurate and low-latency decision-making in smart indoor environments.
2. **Scientific Impact:** Advances resilient, secure AI in IoT ecosystems by combining data preprocessing methodologies for edge-driven AI, hybrid computing framework methodologies to enhance system accuracy.
3. **Societal Impact:** Promotes safe and ethical AI deployment by addressing security risks and unintended behaviors, supporting the development of privacy-preserving, autonomous smart environments.



References

1. Varol, A., Motlagh, N. H., Leino, M., Tarkoma, S., & Virkki, J. (2024). Creation of AI-driven Smart Spaces for Enhanced Indoor Environments--A Survey. arXiv preprint arXiv:2412.14708.
2. Varol, A., Motlagh, N. H., Leino, M., & Virkki, J. (2025, June). Performance of Large Language Models Across Edge and Cloud Platforms in Smart Spaces. In 2025 10th International Conference on Smart and Sustainable Technologies (SpliTech) (pp. 1-6). IEEE.
3. King, E., Yu, H., Lee, S., & Julien, C. (2024). Sasha: creative goal-oriented reasoning in smart homes with large language models. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 8(1), 1-38.
4. Zhang, M., Shen, X., Cao, J., Cui, Z., & Jiang, S. (2024). Edgeshard: Efficient llm inference via collaborative edge computing. IEEE Internet of Things Journal.