Panic Room AI Agent

Aygün Varol[†], Johanna Virkki[†], Mirka Leino[††], and Naser Hossein Motlagh[‡]
[†] Department of Computing Sciences, Tampere University, Finland
[††]Faculty of Technology, Satakunta University of Applied Sciences, Finland
[‡]Department of Computer Science, University of Helsinki, Finland

***Abstract*—Smart spaces seamlessly IoT devices with artificial intelligence (AI) agents to enhance adaptability and user convenience. These environments rely heavily on internet connectivity to leverage AI capabilities and maintain continuous operation. However, this dependency exposes them to significant vulnerabilities, such as cyber-attacks and network disruptions, which can compromise critical functions. This paper introduces the Panic Room AI Agent, an edge-based AI system designed for emergency scenarios in smart spaces. The proposed system leverages environmental sensors to monitor key parameters, including air quality, temperature, humidity, and CO2 levels. It incorporates an Large Language Models (LLMs) based AI agent, ensuring robust and reliable performance even during network isolation. Key functionalities include managing tasks like lighting control and real-time data processing, enabling the system to operate independently of external networks. This study proposes edge-based AI systems in improving the resilience, functionality, and security of smart spaces, particularly in critical scenarios where uninterrupted operation is essential.**

***Index Terms*—AI agents, smart spaces, edge computing, IoT security, environmental monitoring, large language models**

I. Introduction

The Internet of Things (IoT) devices can enable us to utilize Artificial Intelligence (AI) in smart spaces to transform them into proactive indoor environments. These spaces are equipped with interconnected sensors and devices that interact with users and adapt to their needs. Local devices can be equipped with AI agents to manage resources, personalize settings, and monitor environmental conditions [1], [2]. However, these agents consume energy and requires computational power. IoT systems of have limited computational resources, scalability issues, and exposure to cyberattacks [3], [4].

Addressing these challenges involves developing systems that function effectively under constrained conditions. Cloud-based solutions improve computational capacity and data management but depend on stable network connectivity [5]. This reliance can limit their reliability in situations where networks are unavailable or compromised. Edge computing provides an alternative by enabling local data processing, reducing latency, and minimizing external dependencies [6].

Recent work has explored combining AI with security-focused techniques at the edge to detect and respond to threats autonomously [7]. Still, many solutions struggle to maintain essential operations when external connections are disrupted or unavailable.

This paper presents the Panic Room AI Agent, an AI-driven system operating on edge devices for smart spaces. It integrates Large Language Models (LLMs), such as Llama 3.2-1B-Instruct, based AI agent that has access to environmental sensors and historical data of the environment. This approach supports independent operation during network outages or cyber-attacks. For instance, users can query the system about the current temperature and receive immediate responses based on sensor data.

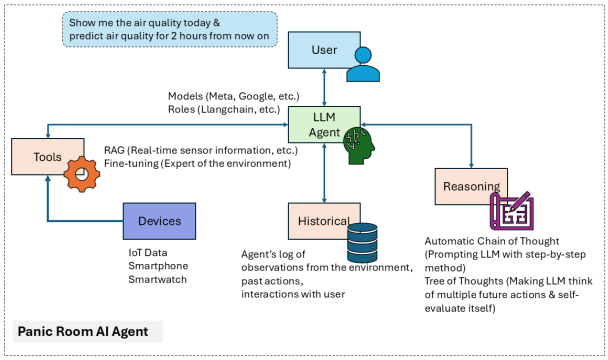

Fig. 1. Framework of AI Agent

II. Applications - Justifications

Locally deployed AI agents ensure reliable, and secure operations in scenarios involving network disruptions or privacy concerns. Privacy concerns are significant in environments where sensitive data, such as health metrics, location information, or personal preferences, are being collected and processed. Cloud-based systems can expose this data to risks like unauthorized access, data breaches, or misuse by third parties. Localized AI agents keep data within the local environment, reducing exposure to external threats and improving user trust.

A. Human Activity Recognition (HAR)

Using sensor data, such as gyroscope readings, the Sensor-LLM framework aligns large language models with motion sensors to detect and classify human activities [8]. Localized AI agents process data directly from sensors, minimizing latency and reducing privacy risks associated with cloud-based HAR systems.

B. Environmental Monitoring and Control

[5].

C. Emergency Response Management

[7].

D. Security Threat Detection

[6].

E. Personalized User Interaction

Localized AI systems adapt to user preferences, such as lighting and climate settings. This ensures high-quality user experiences without exposing sensitive user data to external systems [4].

F. Latency Reduction

Local data processing minimizes delays, which is crucial for real-time applications [3].

Leveraging LLMs at the network edge facilitates the development of autonomous systems capable of understanding and executing complex tasks locally. This decentralization reduces reliance on cloud services, thereby decreasing latency and improving reliability in critical applications [9].

Implementing AI models on edge devices supports applications like connected vehicles and smart cities, where immediate data processing is crucial. Edge AI enables devices to operate with greater autonomy, making instantaneous decisions without the delays associated with cloud communication [10].

G. Enhanced Privacy

By avoiding cloud-based data processing, sensitive information remains secure within the local environment. Deploying LLMs on edge devices, like smartphones and IoT devices, enables real-time language processing while preserving user privacy. However, the limited computational resources of these devices pose challenges. Techniques such as model quantization and efficient neural architecture search are employed to optimize LLMs for edge deployment [11].

H. Operational Resilience

Localized AI agents maintain functionality during network disruptions, a key requirement for emergency scenarios.

I. Energy Efficiency

Edge computing reduces energy costs associated with data transmission and cloud processing [7].

III. Related Work

This section reviews IoT security, localized AI systems, and their application in smart spaces.

A. IoT Security in Smart Spaces

IoT systems are vulnerable to security threats due to their distributed nature and reliance on network connectivity. Traditional cloud-based security solutions, while robust, suffer from latency issues and dependency on stable network connections. These limitations have driven interest in localized AI approaches for enhancing IoT security.

Deep et al. [3] provided a layered perspective on IoT security, highlighting the challenges of securing data transmission and device authentication in heterogeneous networks. They emphasized the need for context-aware security solutions that can adapt to dynamic environments. Similarly, Shen et al. [6] explored the integration of machine learning with key agreement protocols, demonstrating how localized data processing can mitigate risks associated with centralized systems. These studies underscore the importance of real-time threat detection and autonomous response mechanisms in IoT ecosystems.

B. Localized AI Systems

The transition from cloud-centric to edge-centric AI models has been a pivotal development in addressing the computational and privacy challenges of IoT systems. Localized AI systems leverage edge computing to process data closer to the source, thereby reducing latency and enhancing operational resilience.

Qu et al. [11] conducted a comprehensive survey on the deployment of large language models (LLMs) in mobile edge environments. Their work highlighted the potential of techniques such as model quantization and neural architecture search to optimize LLMs for resource-constrained devices. Similarly, Li et al. [8] introduced the Sensor-LLM framework, which aligns motion sensors with LLMs for human activity recognition, demonstrating the feasibility of deploying complex AI models on edge devices.

In the context of smart spaces, Zou et al. [10] discussed the role of wireless multi-agent AI systems in enabling collective intelligence. Their study emphasized the importance of decentralized decision-making and collaborative learning in dynamic environments. These findings align with the goals of the Panic Room AI Agent, which seeks to enhance the autonomy and reliability of smart spaces through localized processing.

C. Applications of AI in Smart Spaces

Localized AI systems have been successfully applied to various domains within smart spaces, including environmental monitoring, emergency management, and personalized user interaction. Lim et al. [5] explored the integration of edge computing with AI for IoT applications, highlighting opportunities for energy efficiency and latency reduction. Al-Doghman et al. [7] examined AI-enabled secure microservices, proposing architectures that combine machine learning with edge-based security protocols to safeguard IoT devices.

The Panic Room AI Agent builds on these advancements by integrating environmental sensors with LLMs to support autonomous decision-making and enhance user experience. By addressing the limitations of existing solutions, such as dependency on cloud connectivity and high energy demands, this system represents a significant step forward in the development of resilient and efficient smart spaces.

IV. System Design and Architecture

V. Experimental Setup

VI. Results and Discussion

VII. Conclusion

Acknowledgment

References

[1] A. Varol, N. H. Motlagh, M. Leino, S. Tarkoma, and J. Virkki, "Creation of ai-driven smart spaces for enhanced indoor environments–a survey,"

arXiv preprint arXiv:2412.14708, 2024.

[2] A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in internet of things," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 4, pp. 208–218, 2018.

[3] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the internet of things from the layered context," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, p. e3935, 2022.

[4] X. Guo, Z. Shen, Y. Zhang, and T. Wu, "Review on the application of artificial intelligence in smart homes," *Smart Cities*, vol. 2, no. 3, pp. 402–420, 2019.

[5] E. H. Lim, T. Y. Chai, M. ap Muniandy, T. F. Yong, B. Y. Ooi, and J.-M. Lin, "Edge computing and ai for iot: Opportunities and challenges," in *2023 International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan)*. IEEE, 2023, pp. 357–358.

[6] T. Shen, L. Ding, J. Sun, C. Jing, F. Guo, and C. Wu, "Edge computing for iot security: integrating machine learning with key agreement," in *2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*. IEEE, 2023, pp. 474–483.

[7] F. Al-Doghman, N. Moustafa, I. Khalil, N. Sohrabi, Z. Tari, and A. Y. Zomaya, "Ai-enabled secure microservices in edge computing: Opportunities and challenges," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 1485–1504, 2022.

[8] Z. Li, S. Deldari, L. Chen, H. Xue, and F. D. Salim, "Sensorllm: Aligning large language models with motion sensors for human activity recognition," *arXiv preprint arXiv:2410.10624*, 2024.

[9] Y. Shen, J. Shao, X. Zhang, Z. Lin, H. Pan, D. Li, J. Zhang, and K. B. Letaief, "Large language models empowered autonomous edge ai for connected intelligence," *IEEE Communications Magazine*, 2024.

[10] H. Zou, Q. Zhao, L. Bariah, M. Bennis, and M. Debbah, "Wireless multi-agent generative ai: From connected intelligence to collective intelligence," *arXiv preprint arXiv:2307.02757*, 2023.

[11] G. Qu, Q. Chen, W. Wei, Z. Lin, X. Chen, and K. Huang, "Mobile edge intelligence for large language models: A contemporary survey," *IEEE Communications Surveys & Tutorials*, 2025.