AI for Energy-Efficient Buildings: Innovations, Challenges, and the Path Forward

by Tiina Kasuk - Monday, 11 November 2024, 10:02 PM
Number of replies: 0

Authors: Vladimir Rostok, Ivan Sukhanov, Tiina Kasuk

Introduction

The rapid pace of urbanization, industrial growth, and rising living standards have led to a substantial increase in energy consumption within buildings. Currently, buildings account for nearly 40% of global annual energy consumption and a similar proportion of CO_2 emissions [1]. As we grapple with the pressing challenges of climate change, integrating Artificial Intelligence (AI) into building management systems emerges as a promising solution. This blog post delves into the application of AI in building energy management, assessing its technological readiness, and critically analyzing its strengths and weaknesses through the lens of innovation challenges in legacy sectors and responsible research and innovation.

AI in Building Management

Approximately half of the energy consumed in commercial buildings comes from heating, ventilation, and air conditioning (HVAC) systems [2], which are essential for maintaining indoor comfort. Traditional HVAC operations often lack the adaptability to respond to fluctuating occupancy patterns and external environmental conditions, leading to energy inefficiencies. Proactive operations based on modeling can prepare systems to reduce energy consumption during peak hours without compromising comfort. However, implementing such strategies requires aligning technical parameters, safety regulations, and the visions of building owners or managers.

AI-based software solutions with remote control capabilities have been developed to address these complexities. By processing real-time data related to building dynamics, these solutions enable smart computing

and control of HVAC systems, achieving the required comfort levels at minimal costs. In essence, AI acts as the brain of the building, optimizing energy usage while ensuring occupant comfort.

Technological Readiness and Implementation Process

In modern multifunctional buildings, the automation infrastructure comprises diverse elements, for example:

- Building Management Systems (BMS): Integrate air handling units, heating and cooling plants.
- KNX Systems: Used for room-level control, leveraging widely adopted communication protocols in smart homes.
- Air Quality and Temperature Sensors: Strategically placed with separate APIs for detailed environmental monitoring.

To optimize synergy among these components, a cloud-based data-driven solution works as a bridge. It synchronizes critical components like cooling/heating plants, ventilation units, rooms, and sensors. This integration enhances individual performance while fostering a unified and responsive building automation ecosystem. Data acquisition is commonly accomplished through BMS in facilities, with methods for data reading and writing supported by API connections. Remote connections via APIs vary depending on the deployed BMS software, often requiring custom solutions for reliable data communication. Data transmission is secured through encrypted VPN tunnels [3].

We estimate the technology readiness level to use AI for energy efficiency in buildings to be six (6). The technology is demonstrated in an appropriate environment (important for critical enabling technologies industrially) [4]. The legal readiness level is six (6) and has a detailed description in the EU, USA, and China of the required or recommended changes in relevant laws, regulations, or organizational rules to ensure full compliance with the proposed solution [5].

Benefits of AI Optimization Solutions in the Building Sector:

1. Fault Detection Algorithms and Analytics: AI can predict and identify faults within HVAC systems, enabling preemptive maintenance and reducing downtime.
2. Software Cloud Solutions Without New Hardware: Implementing AI does not always necessitate new hardware investments, as existing systems could be enhanced through software upgrades.

3. Smart Demand-Based Control: AI adjusts HVAC operations based on real-time occupancy, electricity price, and weather data, aligning energy usage with real building needs.
4. Consumption Reduction: By optimizing operations, AI helps significantly reduce energy consumption and operational costs.
5. Enhanced Building Management Quality: AI provides detailed analytics and insights, improving decision-making processes for the local Technical Teams.
6. Increased Equipment Lifespan: Optimized operations reduce strain on equipment, prolonging its operational life.

Strengths of AI Integration in Building Management

The use of AI in building management enables cost savings and energy efficiency. By utilizing AI, could be adjusted the energy requirements in buildings (for electricity, heating, and cooling) based on real-time data and behavioral patterns. For example, since spring 2022, Ülemiste City has incorporated AI in managing its building systems. On average, this AI implementation has resulted in annual savings of €750,000 and reduced carbon dioxide emissions by 1,200 tons—equivalent to the emissions of a small manufacturing facility. The described AI solution already manages 2.5% of Estonia's electricity consumption and achieved over 20% energy savings, preventing 2,000 tons of CO_2 emissions for the entire quarter by 2023 [6].

AI-powered building management systems can monitor resident needs and environmental conditions to ensure an optimal indoor climate. That way building management can contribute to higher resident occupant satisfaction. In commercial buildings, it can also enhance productivity. AI-enhanced building management provides detailed analysis and forecasting options for building managers. A data-driven approach simplifies building management.

AI solutions can be scaled across multiple buildings or facilities, adapting to various architectural designs and occupancy patterns. This flexibility makes AI a viable solution for both new constructions and retrofitting existing buildings and helps address complex, property-specific challenges.

Challenges and Weaknesses

We face multiple challenges and constraints when solving the problem of building energy efficiency with AI. Problems can be the following: technical, legal, economic, and cybersecurity-related constraints.

Challenges that are connected to cybersecurity risks are described further in a later text. A large amount of High-quality data is essential to train a properly working AI model to solve the problem. The required dataset must include data on building energy consumption, indoor climate, and other similar parameters. However, the quality and reliability of the data often need to be improved to determine the accuracy and subsequent reliability of the AI model. An AI-based solution relying on unreliable data is unlikely to be effective in improving the energy efficiency of a building [7].

Additionally, Legacy Infrastructure Limitations, implementing AI solutions requires additional investments in both infrastructure and equipment to process large amounts of data and to respond dynamically to energy demand. Older buildings may not have the necessary sensors and automation, which leads to additional investments to address these deficiencies. Older buildings may have limitations in equipment controllability, making it challenging to integrate AI solutions without significant hardware upgrades. This can increase implementation costs and complexity. Thus, introducing AI in older buildings is economically costly, especially for smaller buildings [7]. Adopting new technologies in the Building is challenging because of the complexity and established "legacy" of the sectors that often face significant hurdles due to entrenched systems and practices. Several construction companies are involved in constructing one new building, all interested in balancing cost and efficiency. Innovation in the construction industry can come from the side of the suppliers [9].

Farbegue [5] highlights that deploying AI solutions is also prompted by legal and other regulatory constraints, which governments may impose. For example, in the European Union, the Artificial Intelligence Act has been adopted, regulating the use of AI in various sectors, including in the context of Smart Homes or Smart Cities. Together with the General Data Protection Regulation (GDPR), the regulations strictly govern data collection procedures, privacy, and security. Implementers of AI-based solutions are responsible for addressing data security and privacy issues.

It is also important to address ethical questions when using AI to improve building energy efficiency, where all processes must ensure fairness, privacy, and transparency. Otherwise, users may become distrustful, reducing end-user readiness to adopt AI solutions [5].

AI-based systems require constant monitoring and updating, as the energy needs of buildings and technological solutions are constantly evolving. With ongoing maintenance, these systems may become efficient, losing the initial goal of improving energy efficiency [7].

Implementing and maintaining AI systems requires a higher level of technical expertise among facility management staff. There may be a learning curve and a need for ongoing training to ensure staff can effectively collaborate with AI systems.

Cybersecurity Risks

The integration of AI and IoT devices increases the potential attack surface for cyber threats. Secure data transmission and robust cybersecurity protocols are essential to protect sensitive building data and prevent unauthorized access to control systems. Cloud AI solutions should be utilized only for non-critical infrastructure. As the connection to the cloud can be lost at any moment if the global network goes down, the critical infrastructure must have a physical connection over the local network to sustain in conditions of a global network connection loss, the system must be able to work autonomously to ensure there will be no downtime or unexpected behavior in the system.

Implementation of smart systems and risks

AI should be integrated into smart systems responsibly, the use of AI solutions and additional software imposes a significant risk to systems, such as software infrastructure, physical network devices, hardware, and related equipment. The impact of cyber attacks, data leaks, and flaws in system security undermines the potential for technology application in smart building management systems. In case if left unseen it might impose a significant risk to residents and the surrounding area.

Potential for cyber attack focused on the equipment

Any component of the cyber system can be subject to attack. Attacks might focus on user devices, core components of the system such as servers and databases, personal data stored across the network devices, data collection modules, and network infrastructure to infect people’s devices through the local network connection. If the smart system is given enough power to manipulate physical processes in the infrastructure a successful attack can take real-world equipment down

leaving people with no heating/cooling/lifts/locks or other critical systems functioning properly. If there is AI-based heavy energy equipment e.g., boilers, heaters, generators, and pumps with no extra security means applied to protect it from working in a faulty mode, then expensive equipment can be damaged and pose a real threat to lives.

In case there is a centralized access system for the entire building area, a sudden system takedown with a complete erase of data will render people unable to access their property as every smart lock will be down and the entire building will be technically paralyzed. Things can go much worse if the house is connected to the digitally controlled energy grid system and has AI control over the local energy flow as interruptions and spikes in the energy flow can damage electronic components and energy overflow might end up in fire.

Real incidents

A good example is the cyber attack that happened in 2016, in Finland, it caused a heating system outage during the winter for residents of two living blocks [8]. The attack involved two apartment buildings in Lappeenranta, a city with a population of around 60,000 people in eastern Finland. This time the attack targeted systems that control the central heating and hot water circulation in the buildings effectively cutting off the central heating distribution to residents during the freezing temperatures below -5 outside. The system was forced to enter an endless rebooting loop and it was unable to operate, thankfully once the smart home systems affected were disconnected from the internet the heating resumed normal function.

Potential for cyber attack focused on personal data

If the entire activity in the house is managed by the centralized system, a potential data leak and unauthorized access can be used to leak all the personal data from the system to spy on the residents, control people’s behavior, and perform manipulations over the affected people using the personal/behavioral data extracted from the system.

if the house is equipped with a complete set of AI systems like computer-vision systems that rely on surveillance e.g., in parking lots, hallways, and private living areas to control the lighting and heating, this might lead to audio and visual data leaks from the residential living areas as well, this is highly sensitive data and once the data is leaked it

can be used to blackmail victims for an unlimited time rendering victims completely helpless to future attacks and blackmailing.

The danger of sensor data poisoning

Smart systems are capable of adapting to changes in activity behaviors and continual learning algorithms in AI can be turned against the system itself. AI can track human behavior to keep office buildings warm during the daytime and spend less energy at night when the office is empty, but if the continual learning model is fed enough poisoned data then it will do what it was never intended to do and cause massive energy losses. The massive flow of synthetic poisoned traffic over the network will cause disruptions across all related adjustable systems, resulting in massive resource, energy, and financial losses for residents and owners of the affected buildings.

Figure 1 represents a proposed system architecture for data poisoning attacks. The main idea of this proposed system is to blend actual measurements generated by sensors with injected data and feed it to the system over the network connection. Not only the actual measurements collection can have injected data, but the training and test datasets can be replaced as well leading to changes in the future machine learning module behavior. If hackers disrupt the cooling and heating rhythms they will potentially cause buildings to use excessive power and cause more emissions as a result. The damage caused by the attack might have the potential to even outweigh the benefits that the smart building system provided during its functioning time.

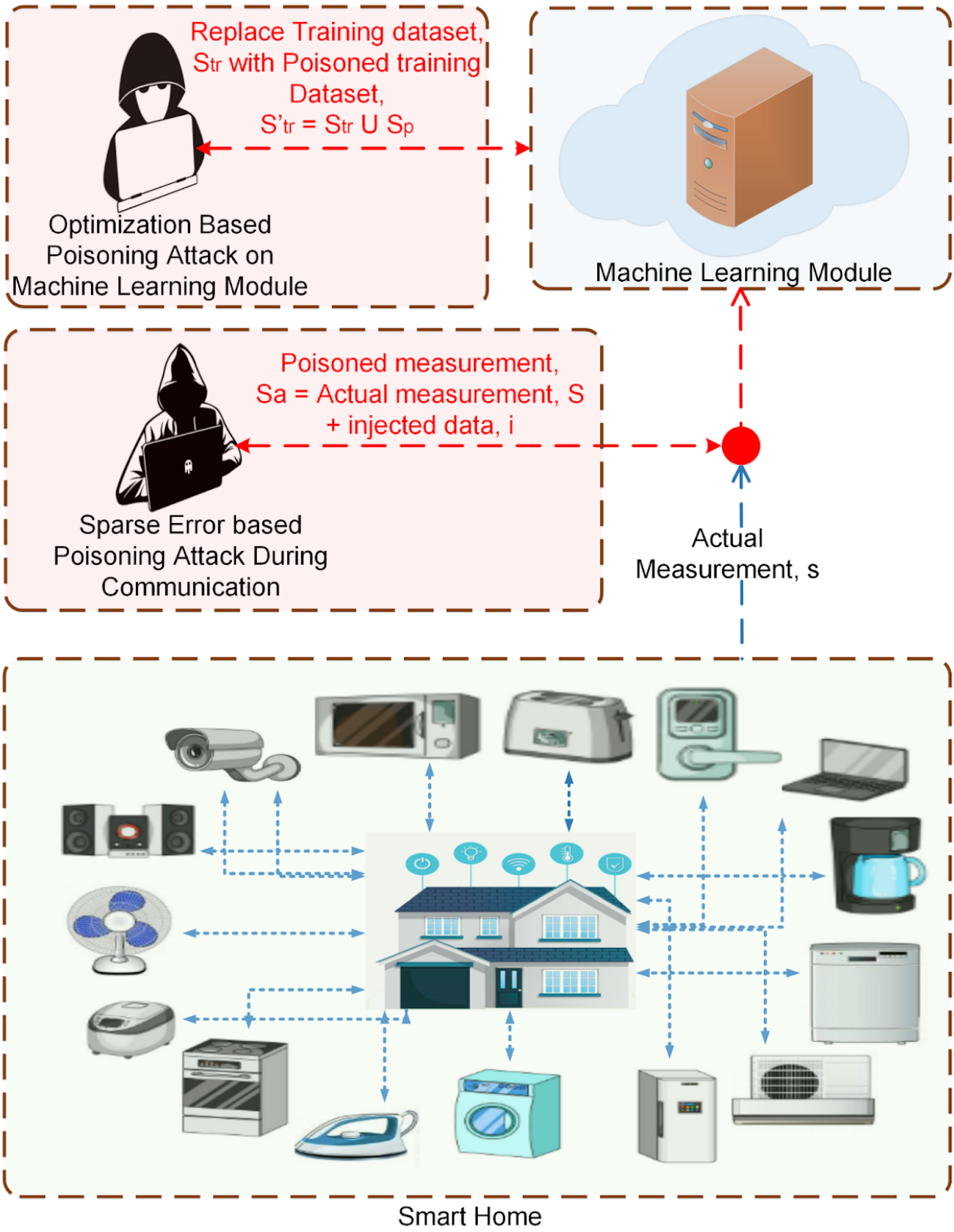

Figure 1. Proposed system architecture [9]

Risk of accidental data loss caused by hardware failure

In theory, there are multiple ways to attack the cyber system and some of the attacks might result in complete data/system loss and damage the equipment but there is always a probability that hard drive disks or flash memory will fail and the system will be unable to function due to the memory corruption error rendering its completely dysfunctional. If critical systems such as heating systems and water pumps shut down during the winter under conditions of temperatures below freezing, the damage can make it unsuitable for living. If water pumps stop and the heating system turns off during the winter, the frozen water might cause major damage to the water pipes, and the pipes used by heating and cooling systems as well. The defrosting process in a house can take a very long time, especially if frozen water has already damaged the pipes and there are cracks in them, the house cannot be occupied until all the pipes are replaced, including those hidden in the walls.

Cyber incident investigation

Investigation of cyber incidents is a very difficult and knowledge-intensive process. It requires a huge competence among all the bodies, authorities, and police, to obtain all the necessary data for the investigation, but in order to obtain the data, you first need to know what data to request and in what time period, and you also need to collect convincing evidence. If the system had security problems and was hacked, this means that the system was used in an unexpected way, because it is very likely that the standard functions of the system were not able to track the attack and somehow record everything that happened in the history log, as well as somehow mark the beginning of the attack, if it was possible at all, hackers can overwrite the event log in the system and potentially substitute other residents, indicate other addresses, other people, other users, and there will be no original history of the incident anywhere, as well as convincing evidence.

Risk prevention

Given that a system breach is not a typical use case, additional practices and failover strategies are needed to mitigate risks and provide options to recover it quickly after the attack. Connections between systems must be encrypted, secure VPN connections can help secure traffic, and additional measures must be in place to scan network activity and warn of data anomalies and unusual network activity. If a backdoor is used to breach a system, it is necessary to have full backups of the system and all data. The system must be able to disable all access to the external network to put the whole system into a secure isolated mode of operation in which no external access

will be possible. There always must be a way to restore the backup copy of the entire system and its data to bring the system back to the functioning state as it was when launched before the system began generating data and learning from it (an unmodified reference state).

Responsible Innovation and Stakeholder Engagement

Using AI for Energy-Efficient Buildings can also create Resistance to Change. Stakeholders who are used to traditional building management practices may resist changes, i.n., the adoption of AI. Convincing building owners and managers of the long-term benefits of AI requires demonstrating tangible results and return on investment.

Human-Technology Collaboration

To mitigate technical and communication issues, comprehensive training for technical staff is essential. Training should elucidate the workflow and emphasize that AI tools are designed to enhance, not replace, the technical team. This strategy aims to boost operational efficiency and minimize user complaints [3].

Transparent Communication Practices

Implementing transparent communication is vital for stakeholder buy-in. Regular reports detailing energy savings and indoor climate results should be communicated to clients and tenants. Additionally, displaying real-time consumption data and CO_2 levels on information panels within the building can foster a culture of energy awareness among occupants.

User-Friendly Interfaces

Transitioning from traditional technological processes to transparent analytical tools can be facilitated through user-friendly interfaces. A transparent web platform can serve as a bridge between complex BMS and end-users, eliminating the need for deep technical knowledge. This inclusive approach promotes a better understanding and acceptance of AI-driven building management.

Responsible Research and Innovation Framework

The Responsible Research and Innovation (RRI) framework by Owen et al. (2013) provides a foundation for ensuring sustainable and ethical

innovation in using AI to improve building energy efficiency. It establishes a basis where innovation is not merely the result of individual thinking but also directs community and public collaboration to understand impacts better, address issues, and see the broader picture [11]. The RRI framework comprises the following components:

- Anticipatory – assists in describing and analyzing potential economic, social, environmental, and other impacts associated with the use of AI. Using proposed methods, it outlines potential applications of AI in achieving building energy efficiency. These companies encourage researchers and innovators to think forward, developing new and more effective solutions for using AI for energy efficiency. It provides a starting point for considering potential issues and impacts that may arise from applying AI for this purpose.

- Reflective – reflects on the fundamental goals, motivations, and potential impacts of AI in building management, including both known and unknown aspects. It allows for identifying weaknesses and risks and acknowledging limitations associated with AI and building management that may stem from legislation, ethics, or other governmental regulations.

- Deliberative – supports the engagement of public sectors and other stakeholders through debates and discussions to identify visions, goals, and pressing questions related to implementing AI in building energy management.

- Responsive – supports the collective process of reflexivity to influence the direction, trajectory, and speed of innovation. For AI to be effectively used in enhancing building energy efficiency, this component must operate continuously.

Digitalization in Real Estate

The real estate industry is embracing digitalization and advanced technology. Adopting data-driven technology has become standard in modern properties, simplifying efficient building management. Data-driven solutions offer real estate owners effective tools for proficient building management, energy cost reduction, carbon emission mitigation, and numerous other benefits. This approach signifies a path

toward energy-efficient building operations and represents a forward-looking blueprint for the industry's journey into the digital era.

Schot and Kanger (2018) discuss the concept of "deep transitions," where multiple innovations converge to create systemic changes across fields [12]. The implementation of AI in building management systems can be seen as part of such a transition, leading to effective shifts in how we design, operate, and interact with built environments.

Conclusion

Integrating AI into building management systems presents a significant opportunity to address climate change-related challenges by reducing energy consumption and carbon emissions. While there are risks and challenges associated with technological readiness, cybersecurity, and stakeholder acceptance, these can be resolved through responsible innovation practices, comprehensive training, and transparent communication with all parties.

The success stories, such as that of Ülemiste City, prove that AI could be a game-changer in the real estate field. As technology keeps advancing and we perfect our methods of implementation, AI is set to transform building management, making a huge impact on global sustainability goals.

References

[1] M. Santamouris and K. Vasilakopoulou, "Present and future energy consumption of buildings: Challenges and opportunities towards decarbonization," E-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 1, p. 100002, 2021. https://doi.org/10.1016/j.prime.2021.100002

[2] L. Pérez-Lombard, J. Ortiz, and C. Pout, "A review on buildings energy consumption information," Energy and Buildings, vol. 40, no. 3, pp. 394–398, 2008.

[3] Sukhanov, I., Volkova, A., Kose, A., Hani, A., & Petlenkov, E. (2024). "Challenges, benefits, and open questions in Data-Driven Commercial Building Cooling Optimization." In E3S Web of Conferences (Vol. 562, p. 06003). EDP Sciences.

[4] I. Bruno et al., ‘Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services’, in Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, in ICEGOV ’20. New York, NY, USA: Association for Computing Machinery, Oct. 2020, pp. 369–380. doi: 10.1145/3428502.3428552.

[5] B. Fabregue, ‘Artificial intelligence governance in smart cities: A European regulatory perspective’, Journal of Autonomous Intelligence, vol. 7, no. 2, 2024, doi: 10.32629/jai.v7i2.672.

[6] R8 Technologies, "Artificial Intelligence takes over the management of Ülemiste City," https://r8tech.io/news/artificial-intelligence-takes-over-the-management-of-ulemiste-city/

[7] G. Halhoul Merabet et al., ‘Intelligent building control systems for thermal comfort and energy-efficiency: A systematic review of artificial intelligence-assisted techniques’, Renewable and Sustainable Energy Reviews, vol. 144, p. 110969, Jul. 2021, doi: 10.1016/j.rser.2021.110969.

[8] Ashok, I. (2016) Hackers leave Finnish residents cold after DDoS attack knocks out heating systems, IBTimes. Available at: https://www.ibtimes.co.uk/hackers-leave-finnish-residents-cold-after-ddos-attack-knocks-out-heating-systems-1590639 (Accessed: 08 November 2024).

[9] Billah, M.; Anwar, A.; Rahman, Z.; Galib, S.M. Bi-Level Poisoning Attack Model and Countermeasure for Appliance Consumption Data of Smart Homes. Energies 2021, 14, 3887. https://doi.org/10.3390/en14133887

[10] Weiss, C., & Bonvillian, W. B. (2011). "Complex, Established ‘Legacy’ Sectors: The Technology Revolutions That Do Not Happen." Innovations: Technology, Governance, Globalization, 6(2), 157-187.

[11] R. Owen, J. Stilgoe, P. Macnaghten, M. Gorman, E. Fisher, and D. Guston, ‘A Framework for Responsible Innovation’, in Responsible Innovation, John Wiley & Sons, Ltd, 2013, pp. 27–50. doi: 10.1002/9781118551424.ch2.

[12] Schot, J., & Kanger, L. (2018). "Deep transitions: Emergence, acceleration, stabilization and directionality." Research Policy, 47(6), 1045-1059.

Declaring AI Use:
AI tools were used to generate a document structure concept, search relevant articles (Scopus AI). We used AI tools (Grammarly and ChatGPT) to improve text quality (proofing, spelling errors, rephrasing, restructuring, clarification of definitions).