Chapter 8
Cybersecurity Challenges in AI-Driven Energy Systems:
Current and Future Prospects Concerning Ethical and Legal Provisions

Kanchan Tolani
https://orcid.org/0000-0003-2788-0987
Ramdeobaba University, Nagpur, India

A. Vijayalakshmi
Chaitanya Bharathi Institute of Technology, Hyderabad, India

Pritam Lanjewar
https://orcid.org/0000-0001-7166-884X
Datta Meghe Institute of Management Studies, Nagpur, India

Monali G. Dhote
Yeshwantrao Chavan College of Engineering, Nagpur, India

Saurabh Chandra
https://orcid.org/0000-0003-4172-9968
Bennett University, Greater Noida, India

Saquib Ahmed
https://orcid.org/0009-0008-1891-6910
Sharda University, India

Bhupinder Singh
https://orcid.org/0009-0006-4779-2553
Sharda University, India

ABSTRACT

Artificial intelligence in energy systems has brought a significant improvement of efficiency, management and optimization making them dependable, there are also big concerns in the cybersecurity domain. A major worry is the risk of AI algorithms being influenced by data poisoning which is when bad actors introduce corrupted data to cause malfunctions on a system. AI-powered energy systems frequently connect thousands of IoT devices and every one of these represents a potential gateway to a system breach if not correctly protected. In addition, threats such as ransomware, phishing and Distributed Denial of Service (DDoS) attacks can compromise the integrity of energy management systems. Security of AI models and data, strong encryption protocols to ensure that these infra are secure from the cyber threat elites of today because of which we must build a real-time monitoring system too. Energy industry can prevent catastrophe by prioritizing cybersecurity.

DOI: 10.4018/979-8-3373-0045-0.ch008

1. INTRODUCTION

The application of artificial intelligence (AI) in energy systems is revolutionizing the way we produce, distribute and consume energy. AI is central to how we will address the challenges of both optimizing renewable sources such as solar and wind, as well increasing the efficiency of our power grids. AI in the modern energy ecosystem plays a vital role across many functions, including predictive maintenance, demand forecasting and grid optimization to even balancing volatile supply with shifts in real-time consumption (Salleh et al., 2020). It will boost the potential of these AI applications to drive a low-carbon economy, lower costs and increase system resiliency against disruptions. This growth parallels a greater need for robust cybersecurity to protect the critical infrastructure that AI increasingly powers. This convergence of AI and energy infrastructure is a double-edged sword, promising unique operational efficiencies alongside emergent opportunities for cyber attackers

The fact is, AI-powered systems function with a cross-layer of data-driven algorithms and devices connected to an ecosystem that implies various cybersecurity risks. Not only do cyber-attacks on critical infrastructure, like power grids, come at a high price. They can also have devastating impacts on public safety; national security and financial stability. Specifically, the AI dependency also means that such attacks can manipulate these systems to render grid instability by causing unintended changes in energy flows as well as unauthorized access seeking sensitive information that leads into massive power outages (Singh, 2023). Unlike conventional threats to cybersecurity AI-specific cyber-threats such as adversarial attacks, data poisoning and model inversion are also unique where the capability of these type of attacks can be quite advanced making them more difficult for detection or possible mitigation. As such, the need to secure AI-driven energy infrastructure has reached near-celebrified status as major actors across state and industry recognize that cybersecurity is a critical issue for anyone with stake in providing reliable and resilient electricity.

The purpose of this chapter is to identify cybersecurity issues and discuss the rising demand for effective application solutions due to the increased dependence on AI in energy systems. The focus will be on the threats and vulnerabilities present in a cyber physical context, ethical and legal considerations around cybersecurity related to AI-based energy systems landscape today as well as areas of future concerns along with best practices for designing secure system (Bujang et al., 2016). The programme of research, which comprises the key developments as:

-Mapping out the ethical aspects concerning data privacy and AI applications on accountability/ fairness roles in energy system.

-Assessing how legal and regulatory play a role as an enabler for safe ecosystem energies. The paper also provides economic, social and security implications of cyber risks in AI-energy systems could provide hints on the design for secure solutions to balance advantages of AI against rigid cybersecurity requirements.

- Applications of AI-driven energy systems cover the spectrum from generation, transmission and distribution to consumption. Renewable energies are optimized by AI, such as the prediction of weather patterns and thus output control to stable and efficient energy feeds. AI algorithms in grid management enable monitoring and balancing of the load on a dynamic basis so that grids can match aggregate demand with supply at most responsive levels.