Forbes

The Promise and Peril of AI in the Energy Sector

ByAriel Cohen, Contributor.

Ariel Cohen is a D.C.-based contributor who covers energy and security

Jun 29, 2023, 09:00am EDT

Artificial Intelligence (AI) is revolutionizing the energy industry, driving digitalization and predictive capabilities. While boosting efficiency, it also exposes vulnerabilities that require careful management. Cyberattacks, which will increasingly leverage AI, experienced a significant surge of 2000% between 2018 and 2019, but the frequency has since stabilized.

On the positive side, AI and machine learning advancements are revolutionizing the energy sector. Through powerful algorithms, data can be processed to predict high-stress, peak demand periods, identify equipment failures, and optimize production, supply chains, and delivery systems. While grappling with climate challenges, the energy sector is evolving into a decentralized and diverse landscape, with AI emerging as a vital tool to navigate this new frontier.

In the green energy sector, algorithms have immense potential to optimize storage, predict and direct the output of renewable energy sources like solar panels and wind turbines. This empowers producers and consumers to participate in an optimized pricing system while effectively managing challenges arising from increased volatility. The transition toward new management methods in the energy industry is driven by the proliferation of connection points due to the rapid growth of smaller-scale energy sources. Stakeholders can leverage advanced algorithms to enhance efficiency and maximize the benefits of renewable energy.

A successful neural network developed by Vistra and McKinsey at the Martin Lake Power Plant in Texas achieved efficiency gains of around 2 percent after just 3 months of operations resulting in an added value of $4.5M reducing Co2 emissions equivalent of taking 66,000 cars off the road. Following a successful pilot, Vistra has since scaled the technology across its power plants to achieve significant gains which are expected to increase further in the future.

Unfortunately, the energy industry faces several challenges hindering its endorsement of rapid digitalization. The energy sector's software architecture is much older than that of other sectors such as finance. Additionally, the energy industry needs to ensure that any change is compatible with on-the-ground infrastructure located across great distances. This makes the implementation of modern technology more costly and difficult, especially for smaller companies. Combined with the complexity of training models and limitations in accessing adequate computational power, the cost-benefit analysis of energy AI requires further investigation.

Digitalization and increased connectivity also expand potential points of attack making the energy sector vulnerable to cyber threats. Aging and unprotected points in the grid can be exploited to gain access to the entire ecosystem. A study by MIT has found the energy sector to be especially vulnerable, with each average 2020 attack costing about $6.4M in damages, double the global average. Compromised critical infrastructure goes beyond hurting the bottom line and has a profound impact on safety.

Beyond their increase in frequency, attacks have become more sophisticated and effective. Groups carrying out operations against critical infrastructure have seen a shift away from small and financially driven to skilled state-sponsored operations. Consequently, the implementation of new technologies in the energy sector raises significant national security implications, leading to a growing concern among government officials.

Companies can protect these vulnerabilities in several ways. One important part of navigating the threat landscape is to develop new technology with security as the foundation and invest in advanced protection software. Companies such as Duke Energy are partnering with tech giant Amazon Web Services to develop smart grid solutions for consumer protection and seamless clean energy transition. AI-based models and services can monitor the vast and intricate energy infrastructure and identify subtle abnormalities which can remain dormant for extended periods under traditional methods. Systems can self-correct or alert professionals about potential threats. Despite the global AI energy market being worth $5.9B in 2022, only 18% of firms use emerging technology for cyber security with most investment focused on support services.

Industry experts and government officials advocate for increased cooperation and partnerships within the highly-targeted industry. Information sharing and discussion between firms about potential vulnerabilities can reduce their overall effectiveness. The New York Power Authority (NYPA) has partnered with Siemens Energy to form the Center of Excellence, a centralized security effort between 53 utilities. Pooled efforts greatly reduce costs of personnel and technology while providing algorithms and NYPA with aggregated data.

Prioritizing an adequate overhaul of safety systems is imperative, integrating them throughout the transformation process before pursuing efficiency gains. Moreover, government agencies, especially the Departments of Energy and the Department of Homeland Security can play a vital role in ensuring the security of such systems. The Federal Smart Grid Task Force is critical to this mission and should closely monitor the exposure and protection capabilities of companies operating critical infrastructure. An inter-agency effort is also required to increase investment in sensitive information-sharing capabilities, forge international cooperation with allies, develop a skilled workforce to defend against AI-assisted cyber-attacks and establish robust and comprehensive regulatory frameworks. These measures are crucial for ensuring national security and facilitating a seamless energy transition.

Follow me on Twitter or LinkedIn. Check out my website or some of my other work.

With acknowledgement to Gabor Swistak