AI-Enabled Cyber-Physical Power Systems: Review of Smart Grid Security, Optimization, and Decision Support

Syed Nurul Islam[1]*, Anik Biswas[2], Ashok Kumar Chowdhury[3]

Abstract

The integration of Artificial Intelligence (AI) into cyber-physical power systems in the United States has been increasingly explored to enhance the efficiency, security, and sustainability of energy infrastructures. Innovative grid technologies have been brought to life through AI, enabling two-way energy flow, real-time monitoring, predictive analytics, and autonomous decision-making. The facilitation of renewable energy integration and the optimization of energy storage systems have been achieved through advanced algorithms. AI-driven intrusion detection systems, anomaly recognition, and reinforcement learning techniques have strengthened cybersecurity measures. Acknowledgment of risks posed by legacy infrastructure, adversarial attacks, and resource constraints has led to the development of mitigation strategies. Predictive models, data analytics, and AI-powered optimization have supported decision-making processes, ensuring grid stability and reliability. Challenges related to governance and transparency of AI "black box" operations have been addressed by implementing federated and distributed learning approaches. Best practices have been informed through the analysis of lessons learned from case studies and pilot implementations, emphasizing the importance of stakeholder engagement, regulatory compliance, and socio-economic considerations. Future research directions have been identified, highlighting the need for hybrid optimization methods, adaptive control strategies, and quantum-resistant cybersecurity solutions. Overall, a vision has been created for the U.S. power grid to be transformed into a resilient, intelligent, and sustainable infrastructure, where AI is leveraged to manage operational complexity, anticipate disruptions, and integrate renewable energy sources effectively. It is recognized that strategic investments, regulatory oversight, and interdisciplinary collaboration are crucial to ensure that AI-enabled power systems are efficiently for long-term energy security.

Keywords: Artificial Intelligence, Cyber-Physical Systems, Smart Grids, Renewable Energy Integration, Cybersecurity

Significance | The significance of AI in cyber-physical power systems lies in enhancing security, efficiency, renewable integration, predictive decision-making, and operational resilience.

*Correspondence. Syed Nurul Islam, School of Information Technology Washington University of science and technology, VA, 22314, USA.
E-mail: snislam.student@wust.edu

Editor Binbin Cui, Ph.D., C.P.A., And accepted by the Editorial Board August 12, 2023 (received for review May 29, 2023)

1. Introduction

Artificial Intelligence (AI) is revolutionizing the way we manage our electric grids, making them smarter and more efficient. As the world's energy needs continue to grow, and as we push more towards renewable sources like wind and solar, these AI-enabled systems are becoming crucial for handling the complexities of energy distribution (Alexy et al.,2017). They help us allocate

Author Affiliation.
[1]School of Information Technology Washington University of science and technology, VA, 22314, USA.
[2]Department of College of Graduate and Professional Studies, Trine University, Detroit, Michigan, United States.
[3]Department of Electrical and Electronics Engineering, Bangladesh Institute of Technology, Dhaka, Bangladesh.

Please cite this article.
Islam, S. N., Biswas, A., Chowdhury, A. K. (2023). "AI-Enabled Cyber-Physical Power Systems: Review of Smart Grid Security, Optimization, and Decision Support", Applied IT & Engineering, 1(1),1-9,10396

resources effectively while ensuring that the power stays on, even when supplies fluctuate or face disruptions. In the United States, the need for these innovations is particularly urgent. The U.S. electric grid is massive and intricate, stretching over 600,000 miles and serving more than 150 million people. With ongoing efforts to reduce carbon emissions, like the Department of Energy's Grid Modernization Strategy AI is stepping in as a key player. It assists in integrating more renewable energy sources into our overall energy landscape. These advanced technologies not only improve how efficiently we operate the grid but also help keep it stable during extreme weather events, which have become more frequent, such as hurricanes and wildfires threatening our power infrastructure (Alkasasbeh et al.,2014). AI plays a dual role in this context: it helps optimize performance with advanced analysis tools and strengthens security against rising cyber threats. Smart grids use AI for real-time monitoring, detecting anomalies, and providing automated decision support. However, this digital shift also introduces significant cybersecurity risks, as these smart grids can become attractive targets for hackers. A notable example is the 2015 cyberattack on Ukraine's power grid, which highlighted the vulnerabilities in our energy systems. The U.S. has also faced its share of challenges, with the Colonial Pipeline ransomware incident in 2021 showing how critical our energy infrastructure is to national security. In response, the U.S. is increasing investments in AI-driven cybersecurity measures, backed by agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE) (Al-Sartawi et al.,2020). Nonetheless, while AI offers impressive benefits in optimizing energy management and enhancing security, implementing it isn't without its obstacles many smaller utilities in the U.S. struggle with limited resources to adopt these advanced AI solutions. There are also concerns about the safety of AI models from adversarial attacks and privacy issues regarding consumer energy data. In a landscape where trust and transparency are key, these issues can be significant barriers. Plus, integrating new technologies into our aging infrastructure can create operational and financial challenges, making careful planning and collaboration essential. As we continue to develop AI in power systems, we need to keep in mind governance, transparency, and ethical standards to build trust among all those involved and maintain the reliability of our energy systems. Current U.S. policy efforts, including initiatives by the Federal Energy Regulatory Commission (FERC) and various DOE-sponsored research programs, are starting to focus on resilience, accountability, and the responsible use of new technologies (Bohme et al.,2010). Looking ahead, AI and smart grid technologies are set to redefine how we manage energy, both in the U.S. and around the globe. As we advance, the emphasis will be on creating systems that can operate autonomously, adapt in real-time, and strengthen our safeguards against both cyber and physical threats. For the country, this journey aligns with broader goals of achieving net-zero emissions by 2050, enhancing energy independence, and fostering a sustainable and secure energy future. The shift from traditional grids to smart grids is fundamentally changing how we handle electricity, making it more responsive to our needs and the challenges of integrating renewable energy sources. With federal investments, like those from the Infrastructure Investment and Jobs Act of 2021, we are rapidly moving toward modernized grids that leverage AI for better analysis, renewable energy integration, and resilience against climate-related disruptions.

2. Smart Grids in the United States

Smart grids are transforming the way we think about electricity distribution, moving away from the old, one-way systems to dynamic networks that can communicate back and forth in real-time. This shift is all about smarter technology that allows everyone involved, utilities, consumers, and even renewable energy sources, to work together more effectively (Bose et al.,2014). Unlike traditional grids, smart grids support two-way energy flow, offering opportunities for consumers to engage in energy production and contribute to a more resilient energy system. At the core of this evolution in the U.S. is the use of advanced technologies like artificial intelligence, cloud computing, and fast communication networks. These innovations help devices function more autonomously, predict maintenance needs, and optimize energy usage on the fly. Utilities across the country are rolling out smart meters and sensors that gather vast amounts of data. AI processes this information to forecast energy demands, spot faults before they become problems, and automate essential decisions. This is especially critical for managing renewable energy sources—like wind and solar—that can be unpredictable based on the weather. The U.S. is focusing heavily on renewable energy, and smart grids play a crucial role in that transition, using advanced algorithms to anticipate changes in energy supply and adjust distribution accordingly to ensure reliable electricity flow (Brody et al.,2018). States like California and Texas, which have prominent renewable energy initiatives, depend on innovative grid technologies to maintain stability during peak demand or low energy generation periods. This adaptability not only helps improve efficiency but also eases the pressure on older infrastructure. However, as beneficial as smart grids are, they also introduce new cybersecurity challenges (Figure 1). Recent events, like the Colonial Pipeline ransomware attack, have shown that our vital energy systems can be vulnerable to cyber threats (Chen et al.,2017). Therefore, protecting these grids is now crucial not just for operational efficiency but for national security and economic stability. To combat these risks, U.S. utilities and federal agencies are investing in AI-based cybersecurity solutions that can detect unusual activities in real-time and respond quickly. This includes implementing security from the ground up

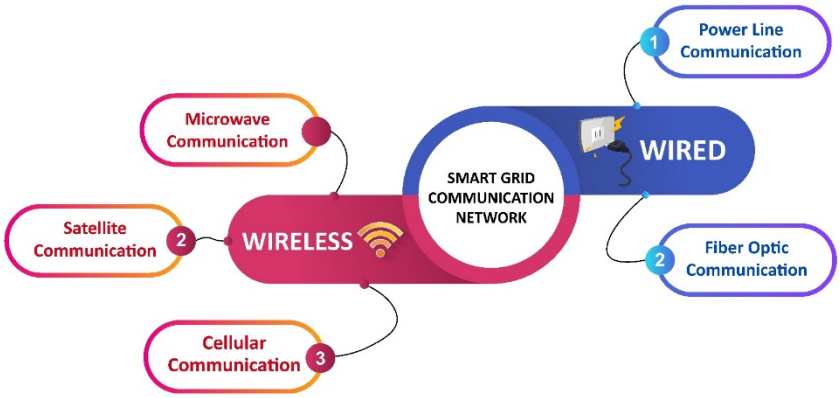

Figure 1. Smart grid cyber-physical systems.

during modernization efforts, using machine learning for constant monitoring, and simulating attacks to bolster defenses. Agencies like the Department of Energy and the Cybersecurity and Infrastructure Security Agency are leading collaborative efforts to strengthen the resilience of our nation's energy networks. Looking ahead, the U.S. smart grid is aimed at becoming even smarter and more autonomous. AI is increasingly moving beyond handling tasks in isolation to providing overall intelligence for the grid. Future grids will incorporate features like self-healing processes that automatically reroute power during outages, isolate faults to prevent widespread failures, and enable decentralized decision-making to enhance resilience against natural disasters and cyber threats (Cobanoglu et al.,2013). One of the most exciting aspects of AI in these smart grids is its role in decision-making. By analyzing extensive data from smart meters, weather reports, and distributed energy resources, AI can provide immediate insights on system performance. This will make it possible to automate load forecasting, streamline maintenance, and accelerate recovery during disruptions. As we integrate more renewable energy, having efficient AI systems in place will be key to balancing energy supply and demand while reducing waste. Overall, the vision for U.S. smart grids extends well beyond just upgrading technology they represent a crucial step towards achieving national goals like reducing carbon emissions, building resilience, and achieving energy independence. By investing in AI-driven optimization and robust cybersecurity, the U.S. is setting the stage for an energy system that is not only efficient but also secure, adaptable, and equipped to face the challenges of climate change and other future threats.

3. Security and Sustainability in AI-Enabled Cyber-Physical Power Systems

The integration of artificial intelligence into the U.S. power grid represents a significant shift in how we innovate and address vulnerabilities. On one hand, AI holds the promise of enhanced efficiency, better predictive control, and a smoother transition to renewable energy. On the other hand, it also brings new challenges in cybersecurity and reliability that we must handle carefully to protect our essential infrastructure (Table 1). Today's American power grid has increasingly become a digital entity, relying on smart meters, sensors, and AI-driven tools to manage energy demand and distribution. This interconnectedness, while beneficial, also opens the door to new cyber threats. U.S. utilities are now facing a growing array of attacks—not just from individual hackers but also from state-sponsored groups using sophisticated AI strategies (Coltman et al.,2015). These cyberattacks aim not just at stealing data but at undermining the stability of the grid itself, posing risks of blackouts that could disrupt daily life in cities, hospitals, and industries. One of the unique challenges we face is rooted in the age of our energy infrastructure. Much of it is quite old, built long before digital security became a consideration. This outdated foundation, combined with newer technologies, creates a complex environment that is challenging to secure. Moreover, the grid is susceptible to insider threats and physical sabotage, highlighting the necessity for comprehensive defense strategies. Interestingly, while AI brings risks, it also offers robust solutions for defending against them. Researchers and industry leaders are piloting AI-based intrusion detection systems that can identify potential threats in real time. These systems are capable of recognizing subtle signs of trouble before they escalate, thanks to

Table 1. Challenges in AI-Enabled Cyber-Physical Power Systems

Challenge Category	Specific Challenges	Description
Cybersecurity	Attacks on Legacy Infrastructure	Power systems with older, less secure components are highly vulnerable to cyberattacks.
	Adversarial Attacks & Malware	The increasing complexity of cyberattacks, including malware like Trojans and spyware, can disrupt the system. Attacks on power grids date back to the last century.
	False Data Injection Attacks (FDIA)	Attackers can inject false data, such as incorrect readings or pricing, to manipulate the smart grid's control system.
	Denial-of-Service (DoS) Attacks	These attacks aim to overload the network, blocking or delaying communication between system components and potentially causing power outages.
	IT/OT Integration Risks	The integration of Information Technology (IT) and Operational Technology (OT) systems creates new cybersecurity risks that malicious actors can exploit to disrupt grid operations.
System & Operational Issues	Resource Constraints	Insufficient resources can hinder the implementation of robust security measures.
	Real-Time Data Handling	Managing the vast amount of data generated by the smart grid and ensuring its integrity and confidentiality is a significant challenge.
	Grid Intermittency	The integration of fluctuating renewable energy sources like solar and wind can destabilize the energy infrastructure.
	Aging Infrastructure	Traditional grids rely on manual processes and limited automation, which are not sufficient to manage the complexities of modern energy systems.

their ability to learn from vast amounts of data across the grid. Advanced models are being tested to tackle specific threats, like denial-of-service attacks, and deep learning systems are helping utilities differentiate between normal fluctuations in the grid and deliberate interference (D'Arcy et al.,2020). As we look to the future, utilities are incorporating encryption methods that can withstand the challenges posed by quantum computing, crucial for safeguarding the electric grid as a prime target in global cyber warfare. AI's contribution to power systems extends beyond just security; it also plays a pivotal role in the transition to sustainable energy. While renewable energy sources like solar and wind can be unpredictable, AI helps smooth out these variations. By forecasting supply changes and balancing them with demand, AI ensures that renewable energy can be integrated into the grid without causing instability. This is especially important in states such as California and Texas, which are spearheading large-scale clean energy initiatives while also grappling with reliability issues. AI is also enhancing energy storage solutions, particularly within smart battery networks that can store surplus renewable energy and dispatch it when demand surges. This capability is particularly valuable during extreme weather events, which are becoming more frequent due to climate change, as it alleviates pressure on the grid. However, the successful integration of AI in American power systems isn't purely a technological matter; it also hinges on good governance (DeGroote et al.,2013). Policymakers, regulators, and utility companies need to work together to establish standards that ensure AI applications are transparent, accountable, and maintain public trust. The challenge of "black box" AI where decisions are made without clear explanations, is a significant concern, especially when those decisions can impact millions of people. Promising approaches like distributed and federated learning allow utilities across the U.S. to collaborate on AI training without compromising sensitive data, thereby also reducing the environmental impact of massive AI models. Ultimately, integrating AI into our power systems is a double-edged sword. When done correctly, it can enhance grid security, facilitate renewable energy adoption, and bolster our resilience against both cyber and climate threats. However, if mismanaged, it could expose one of the nation's most critical infrastructures to unprecedented risks. Moving forward will require ongoing investment, foresight in regulation, and collaboration among government, academia, and industry.

4. Case Studies in AI-Enabled Cyber-Physical Power Systems

Case studies showcasing the use of AI in cyber-physical power systems throughout the United States reveal a wealth of practical insights into how these technologies can be applied effectively, along with the operational hurdles that come along with them. They illustrate how AI can bolster security, streamline energy management, and assist in decision-making within smart grids. At the same time, these examples also point out the limitations that

need to be tackled for future resilience. AI has become a cornerstone in enhancing cybersecurity measures to protect the U.S. energy infrastructure. Through testbeds and pilot programs, utilities have been developing sophisticated anomaly detection systems that can monitor substations and distributed energy resources in real-time (Fink et al.,2009). Events like the 2015 Ukraine power grid attack stand as reminders of the vulnerabilities posed by advanced malware and cyber intrusions, highlighting the urgent necessity for AI-driven security solutions. In the U.S., AI has been increasingly integrated into intrusion detection systems, enabling them to identify eavesdropping, denial-of-service attacks, and various threats while filtering out natural grid fluctuations from potentially harmful activities. Advanced techniques, such as reinforcement learning models and deep neural networks, are enhancing these capabilities, enabling a proactive stance in defending against and responding to new threats. To further bolster grid security against sophisticated adversaries, complementary methods like quantum-resistant encryption and solid data governance are also being prioritized. On a broader scale, AI is reshaping energy management and optimization within American smart grids. By utilizing AI algorithms, utilities can analyze consumption patterns for better real-time load balancing—an essential factor for integrating renewable energy sources like solar and wind, which can be quite variable. Predictive analytics and machine learning facilitate accurate demand forecasting, optimize battery storage solutions, and help manage distributed generation more effectively (Furnell et al.,2020). Advanced control strategies like Model Predictive Control, adaptive control, and hybrid systems work together to ensure grid stability, particularly during fluctuations due to peak loads or extreme weather events that are increasingly frequent in states like California, Texas, and Florida. AI also plays a crucial role in enhancing decision support. Real-time monitoring systems, predictive algorithms, and incident response frameworks provide utilities with the necessary tools to foresee failures, allocate resources more effectively, and respond swiftly to emergencies. The integration of AI promotes operational transparency and improves informed decision-making, especially in complex networks that blend older infrastructure with contemporary digital systems. Additionally, the exploration of distributed and federated learning methods aims to advance AI training while safeguarding sensitive data and minimizing energy consumption, aligning with broader national sustainability initiatives. However, despite these advancements, challenges remain. Smaller utility operators often face resource limitations that hinder the deployment of comprehensive AI solutions. Edge devices often lack the computational power needed for advanced security and optimization tasks, and scaling AI solutions across diverse energy sources and IoT networks poses its own set of challenges (Georg et al.,2017). AI models can also be susceptible to adversarial attacks, where even minor changes in input data can circumvent detection. Their "black box" nature can erode trust and accountability. Moreover, issues surrounding regulatory compliance, economic disparities, and data privacy add more layers of complexity, demanding that utilities juggle innovation with their societal and legal responsibilities. Looking ahead, the role of AI in U.S. cyber-physical power systems is on the brink of a transformative shift. We can anticipate a future where AI enables autonomous load management, real-time power rerouting, predictive maintenance, and adaptive responses to emerging threats. Optimization techniques that fuse traditional mathematical programming with machine learning and heuristic methods will enhance system resilience and facilitate the efficient integration of renewables (Ghasemaghaei et al.,2021). Establishing robust governance frameworks and safety protocols, along with transparent AI decision-making processes, will be key to ensuring that these technological innovations remain accountable and foster public trust. Ultimately, the future U.S. power grid promises to be smarter, more resilient, and sustainable, equipped to manage both cyber threats and climate-driven challenges while delivering reliable electricity to millions.

5. Discussion

The integration of artificial intelligence (AI) into cyber-physical power systems is a game-changer for our modern energy landscape. In the United States, the power grid is a vast and interconnected web, and AI has the potential to fundamentally change how we generate, distribute, monitor, and secure energy. By bringing AI together with innovative grid technologies, we unlock the ability to analyze data in real time, predict issues before they occur, optimize our use of renewable energy, and fortify our systems against both cyber and physical threats (Ilmudeen et al.,2020). However, this transformation isn't without its challenges. One of the biggest concerns is cybersecurity. Today's power grids rely heavily on digital components like smart meters, sensors, and communication networks, which, while beneficial, also make the system more vulnerable to attacks. Utilities in the U.S. face threats from not just individual hackers but also sophisticated nation-state actors using advanced AI tools. These intrusions can threaten not only data integrity but also the very stability of the grid, opening up the risk of widespread blackouts that could affect entire regions. On the bright side, AI offers robust defenses against these challenges. With the ability to sift through enormous amounts of operational data, AI-driven systems can detect unusual patterns that may indicate cyberattacks or system malfunctions. Techniques like deep reinforcement learning help systems adapt in real time to emerging threats, while deep neural networks can distinguish between normal fluctuations and suspicious activity (Jang et al.,2014). We also see the use of quantum-resistant encryption and strong data

governance protocols coming into play to secure communications across our energy networks, enhancing the overall reliability of our power infrastructure. Beyond security, AI is making strides in improving operational efficiency and energy management, especially as more renewable energy sources are incorporated into the grid. The variability of solar and wind energy presents new challenges, but AI algorithms help predict these fluctuations and ensure real-time adjustments in energy distribution. They play a key role in balancing loads, forecasting demand, and automating energy storage management, ensuring a steady power supply even during peak times or adverse weather. Optimization techniques are crucial here. Methods like mixed-integer linear programming provide precise solutions for energy management issues, while other approaches offer near-optimal solutions with less computational heft. With AI-enhanced optimization tools such as artificial neural networks (ANNs), we can refine our forecasting and resource allocation even further (Johnston et al.,2018). This means utilities can smoothly integrate distributed solar, wind, and storage systems, all while keeping the system stable and minimizing energy waste. Decision support systems (DSS) are at the heart of managing these complex cyber-physical power networks. In the U.S., these applications range from monitoring operations in real time to enabling long-term planning. They help utility operators make informed, data-driven choices by tracking grid performance, catching anomalies, and providing early alerts about potential failures. Predictive analytics allow for foresight in energy demand and maintenance needs, giving operators the chance to act before issues become serious. Incident response planning, backed by AI, is essential for utilities to react effectively to cyber threats, equipment malfunctions, or natural disasters. A comprehensive DSS pulls data from various sources, like sensors and historical usage patterns, to support accurate decision-making. Agencies like the U.S. Department of Energy stress the importance of trust in these systems, insisting on transparency, auditability, and accountability in AI-driven decisions (Kwon et al.,2018). Emerging methods such as distributed and federated learning, which enable collaborative AI training across utilities while keeping sensitive data private, offer promising ways to enhance intelligence without compromising security. Real-world examples in the U.S. showcase AI's tangible impacts on cyber-physical power systems. Pilot projects targeting anomaly detection in substations and distributed energy resources have led to quicker monitoring responses and better overall grid management. Additionally, AI-driven intrusion detection systems applied to intelligent battery networks and microgrids have proven effective in real-time cyberattack detection. These advancements underline how vital AI has become in fortifying our energy infrastructure for the future. AI is making waves in the world of energy management, especially in the U.S., where utility companies are tapping into machine learning to understand better how we consume energy. By analyzing usage patterns, these systems help balance loads and predict demand, which is particularly beneficial in areas that rely heavily on renewable energy sources (Mithas et al.,2006). Since solar and wind generation can be unpredictable, AI plays a crucial role in adjusting operations to maintain grid stability, ultimately reducing the risk of outages and improving efficiency. However, the journey is not without its challenges. Many smaller utility companies struggle with limited resources, which makes it hard for them to adopt comprehensive AI solutions. Additionally, the edge devices they use often lack the necessary processing power to handle advanced tasks like cybersecurity and optimization. Scaling these AI solutions across various infrastructures is another complex hurdle to overcome. Moreover, AI systems are susceptible to adversarial attacks, where minor changes in data can circumvent detection, and the opaque nature of many machine learning models raises trust and transparency concerns. Regulatory issues and data privacy also complicate the adoption of AI in the energy sector. Utilities must navigate federal and state regulations while safeguarding consumer information. This can create disparities in how AI benefits are distributed, with wealthier regions often reaping more rewards. To tackle these issues, there's a need for substantial investments in infrastructure, strong governance frameworks, and strategies that prioritize security and sustainability (Morimura et al.,2018). Looking ahead, the integration of AI into U.S. power systems holds incredible promise. We're likely to see a shift from AI simply supporting specific applications to enabling fully autonomous grid management. Advanced intelligent systems will take on responsibilities like load distribution, fault isolation, and real-time power rerouting, enhancing both reliability and resilience in our energy grid. The blending of traditional programming with AI could lead to better renewable energy integration, lower energy losses, and improved demand-side management. In addition, governance will be crucial in ensuring that AI deployment is transparent and trustworthy. Collaborative approaches like distributed learning and privacy-preserving strategies can help utilities train AI models without putting sensitive information at risk. Moreover, incorporating sustainability into AI development—such as finding ways to minimize the carbon footprint of algorithms—will align technological progress with our national climate goals. Ultimately, integrating AI into U.S. energy systems offers both exciting opportunities and essential responsibilities. While AI can significantly enhance our grid's cybersecurity, operational efficiency, and decision-making abilities, we must remain vigilant about vulnerabilities, regulatory issues, and resource limits (Nevo et al.,2011). By blending cutting-edge AI technology with thoughtful governance and strategic investment, we can create a power grid that is not only secure and sustainable but also capable of adapting to the evolving challenges of our energy landscape

Table 2. AI-Enabled Solutions in Cyber-Physical Power Systems

Solution Category	AI Application	How It Addresses Challenges
Cybersecurity	AI-Driven Intrusion Detection Systems	AI can identify unusual behavioral patterns that may indicate a cyber threat. These systems are designed to detect and mitigate attacks on various parts of the smart grid.
	Real-Time Response & Protection	AI can be used to develop strong firewalls, intrusion prevention systems, and advanced authentication software to defend against attacks.
	Predictive Analytics & Anomaly Detection	AI analyzes sensor data to predict and detect anomalies, helping operators take action before issues arise.
Optimization & Efficiency	Predictive Maintenance	AI-powered predictive maintenance can lower unexpected downtime by forecasting potential failures.
	Load Forecasting & Demand Management	AI improves the accuracy of energy demand forecasting, helping utilities manage supply and demand efficiently.
	Energy Storage Optimization	Advanced algorithms facilitate the optimization of energy storage systems.
Decision Support & Control	Real-Time Autonomous Control	AI-enabled systems can make real-time decisions and manage the grid intelligently, adapting quickly to new conditions.

(Table 2). The future of AI-enabled power systems is bright, promising a more reliable energy delivery system that makes the most of renewable resources while effectively mitigating cyber and climate-related risks.

6. Challenges and Future Directions

The potential of artificial intelligence (AI) to strengthen the resilience of U.S. cyber-physical power systems is exciting, but there are still critical challenges to tackle. Many smaller utility operators, which represent a significant part of the American energy landscape, often struggle with limited resources. This makes it hard for them to implement advanced AI-driven security and optimization technologies. Budget constraints and workforce shortages lead to uneven technology adoption across different regions, leaving some parts of the power grid more exposed to risk than others. Moreover, we face difficulties when trying to integrate these modern technologies into an aging infrastructure. Many components in the U.S. power grid were designed decades ago, before the complexities of cyber threats, digital demands, and renewable energy became a concern. We need to introduce advanced AI solutions carefully to avoid causing instability in these older systems (Park et al.,2020). To navigate these challenges, optimization techniques are becoming crucial for enhancing efficiency and stability. This is especially relevant in the U.S., where the rapid growth of renewable energy sources, such as solar and wind, introduces variability and unpredictability to the grid. Advanced control strategies are being tested on renewable generators and distributed energy resources, aiming to create steady outputs and reduce fluctuations. Techniques like model predictive control, adaptive control, and hybrid systems are being piloted in different states to improve stability and minimize downtime under changing conditions (Sabherwal et al.,2019) (Figure 2). Energy management systems also use a mix of precise and approximate optimization techniques to deal with the grid's complexities. In practice, mathematical models can solve problems exactly, while heuristic and meta-heuristic algorithms provide quicker, nearly optimal solutions that can adapt in real time. For U.S. utilities, especially during peak demand or extreme weather, these quicker methods are essential for making immediate operational decisions. As operators strive for greater adaptability, tools like backtracking search algorithms and Markov decision processes are gaining traction. AI plays a significant role in boosting these optimization efforts by enhancing predictive capabilities. Machine learning models can help forecast consumption trends, detect anomalies, and optimize load balancing, enabling utilities to allocate resources more efficiently (Saeidi et al.,2019). Techniques such as neural networks and swarm intelligence are being tested in pilot projects across states like California, Texas, and New York to support the integration of large-scale renewable energy and manage storage effectively. However, challenges remain. Energy storage is a significant hurdle in the U.S. transition to renewables, as current battery and storage systems are not yet fully capable of balancing the intermittent nature of wind and solar power. Additionally, connecting new renewable projects to the existing transmission infrastructure can be slow and complex, delaying timelines for deployment. Many areas still rely heavily on centralized fossil fuel generation, making the goal of complete decarbonization seem far off (Thompson et al.,2017). Looking ahead, overcoming these issues will require a mix of infrastructure investment, robust cybersecurity measures, and more adaptive systems that can evolve with the nation's changing energy demands. It's also crucial to establish governance frameworks that ensure AI systems are transparent, explainable, and accountable, especially when decisions impact the reliability of power and public safety. The future of AI-enabled

Figure 2. Hybrid microgrid System.

cyber-physical power systems in the U.S. hinges not just on technological advancements but also on the commitment of policymakers, regulators, utilities, and industry leaders to collaborate and invest in long-term resilience.

7. Conclusion

The integration of AI into U.S. cyber-physical power systems is regarded as a pivotal advancement in modern energy management. Enhanced cybersecurity, optimized energy distribution, support for renewable integration, and intelligent decision-making are enabled by AI, strengthening grid resilience and operational efficiency. However, challenges such as legacy infrastructure, resource limitations, cybersecurity threats, and the need for transparency and governance must be carefully addressed. Advanced optimization techniques, distributed learning models, and robust regulatory frameworks must be adopted. With strategic investment and cross-sector collaboration, the U.S. power grid can be transformed into a secure, sustainable, and adaptive infrastructure for the future.

Author contributions

S.N.I. conceptualized the study, developed the methodology, supervised the research, and reviewed and edited the manuscript. A.B. conducted the literature review, curated the data, and prepared the original draft. A.K.C. validated the findings, performed the formal analysis, and reviewed and edited the final version of the manuscript.

Acknowledgment

None declared.

Competing financial interests

The authors have no conflict of interest.

References

Alexy, O., West, J., Klapper, H., & Reitzig, M. (2017). Surrendering control to gain advantage: Reconciling openness and the resource-based view of the firm. Strategic Management Journal, 39(6), 1704–1727. https://doi.org/10.1002/smj.2706

Alkasasbeh, A. A. (2014). The Effect of Information Technology Capabilities in Implementing Information Security Management Systems. European Scientific Journal, 10(18), 377–385. https://eujournal.org/index.php/esj/article/view/3606

Al-Sartawi, A. M., & Razzaque, A. (2020). Cyber Security, IT Governance, and Performance: A Review of the Current Literature. In Albastaki, Y. A., & Awad, W. (Eds.), Implementing Computational Intelligence Techniques for Security Systems Design (pp. 275-288). IGI Global. https://doi.org/10.4018/978-1-7998-2418-3.ch014

Bohme, R., & Moore, T. (2010). The iterated weakest link. IEEE Security & Privacy Magazine, 8(1), 53–55. https://doi.org/10.1109/msp.2010.51

Bose, R., & Luo, X. R. (2014). Investigating security investment impact on firm performance. International Journal of Accounting & Information Management, 22(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: death and destruction. International Journal of Accounting & Information Management, 26(4), 527–540. https://doi.org/10.1108/ijaim-04-2018-0046

Chen, Y., Wang, Y., Nevo, S., Benitez, J., & Kou, G. (2017). Improving Strategic Flexibility with Information Technologies: Insights for Firm Performance in an Emerging

Economy. Journal of Information Technology, 32(1), 10–25. https://doi.org/10.1057/jit.2015.26

Cobanoglu, C., Ayoun, B., Connolly, D., & Nusair, K. (2013). The Effect of Information Technology Steering Committees on Perceived IT Management Sophistication in Hotels. International Journal of Hospitality & Tourism Administration, 14(1), 1-22. https://doi.org/10.1080/15256480.2013.753801

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT Alignment: Twenty-Five Years on. Journal of Information Technology, 30(2), 91–100. https://doi.org/10.1057/jit.2014.35

D'Arcy, J., Adjerid, I., Angst, C. M., & Glavas, A. (2020). Too Good to Be True: Firm Social Performance and the Risk of Data Breach. Information Systems Research, 31(4), 1200–1223. https://doi.org/10.1287/isre.2020.0939

DeGroote, S. E., & Marx, T. G. (2013). The impact of IT on supply chain agility and firm performance: An empirical investigation. International Journal of Information Management, 33(6), 909–916. https://doi.org/10.1016/j.ijinfomgt.2013.09.001

Fink, L., & Neumann, S. (2009). Exploring the perceived business value of the flexibility enabled by information technology infrastructure. Information & Management, 46(2), 90–99. https://doi.org/10.1016/j.im.2008.11.007

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. Computer Fraud & Security, 2020(12), 6–12. https://doi.org/10.1016/s1361-3723(20)30127-5

Georg, L. (2017). Information security governance: Pending legal responsibilities of non-executive boards. Journal of Management & Governance, 21(4), 793–814. https://doi.org/10.1007/s10997-016-9358-0

Ghasemaghaei, M. (2021). Understanding the impact of big data on firm performance: The necessity of conceptually differentiating among big data characteristics. International Journal of Information Management, 57(1). https://doi.org/10.1016/j.ijinfomgt.2019.102055

Ilmudeen, A., & Bao, Y. (2020). IT strategy and business strategy mediate the effect of managing IT on firm performance: empirical analysis. Journal of Enterprise Information Management, 33(6), 1357–1378. https://doi.org/10.1108/jeim-03-2019-0068

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Johnston, J. A., & Zhang, J. H. (2018). Information Technology Investment and the Timeliness of Financial Reports. Journal of Emerging Technologies in Accounting, 15(1), 77–101. https://doi.org/10.2308/jeta-52066

Jha, A.V., Appasani, B., Ghazali, A.N., 2021, Smart grid cyber-physical systems: communication technologies, standards and challenges. Wireless Netw 27, 2595–2613.

https://doi.org/10.1007/s11276-021-02579-1

Kwon, J., & Johnson, M. E. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? MIS Quarterly, 42(4), 1043–1067.

https://misq.umn.edu/meaningful-healthcare-security-does-meaningful-use-attestation-improve-information-security-performance.html

Mithas, S., Almirall, D., & Krishnan, M. S. (2006). Do CRM Systems Cause One-to-One Marketing Effectiveness? Statistical Science, 21(2). https://doi.org/10.1214/088342306000000213

Morimura, F., & Sakagawa, Y. (2018). Information technology use in retail chains: Impact on the standardisation of pricing and promotion strategies and performance. Journal of Retailing and Consumer Services, 45, 81–91. https://doi.org/10.1016/j.jretconser.2018.08.009

Nevo, S., & Wade, M. (2011). Firm-level benefits of IT-enabled resources: A conceptual extension and an empirical assessment. The Journal of Strategic Information Systems, 20(4), 403–418. https://doi.org/10.1016/j.jsis.2011.08.001

Park, Y., & Mithas, S. (2020). Organized Complexity of Digital Business Strategy: A Configurational Perspective. MIS Quarterly, 44(1), 85–127. https://doi.org/10.25300/misq/2020/14477

Sabherwal, R., Sabherwal, S., Havaknor, T., & Steelman, Z. (2019). How Does Strategic Alignment Affect Firm Performance? The Roles of Information Technology Investment and Environmental Uncertainty. MIS Quarterly, 43(2), 453–474. https://doi.org/10.25300/misq/2019/13626

Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. Computer Standards & Interfaces, 63, 67–82. https://doi.org/10.1016/j.csi.2018.11.009

Thompson, C. G., Kim, R. S., Aloe, A. M., & Becker, B. J. (2017). Extracting the Variance Inflation Factor and Other Multicollinearity Diagnostics from Typical Regression Results. Basic and Applied Social Psychology, 39(2), 81–90. https://doi.org/10.1080/01973533.2016.1277529

Xue, Y., Liang, H., & Boulton, W. (2008). Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context. MIS Quarterly, 32(1), 67–96. https://doi.org/10.2307/25148829