Clareus Scientific Science and Engineering
Volume 2 Issue 7 September 2025
DOI: 10.70012/CSSE.02.044
ISSN: 3065-1182

Clareus Scientific

Adaptive AI Frameworks to Secure and Manage Distributed Energy Networks in Smart Urban Environments

Citation: Jovita Nsoh. "Adaptive AI Frameworks to Secure and Manage Distributed Energy Networks in Smart Urban Environments". Clareus Scientific Science and Engineering 2.7 (2025): 16-52.

Article Type: Research Article

Received: August 19, 2025

Published: September 06, 2025

Jovita Nsoh*

Department of Information Science Technology, Cullen College of Engineering, University of Houston, Houston, TX, USA

***Corresponding Author:** Jovita Nsoh, Department of Information Science Technology, Cullen College of Engineering, University of Houston, Houston, TX, USA.

Abstract

The rapid growth of smart cities requires the implementation of advanced technologies to effectively manage and secure distributed energy systems. As energy forms become increasingly interconnected due to urbanization, the systems in place become more complex, raising concerns about security and functionality. This research aims to address these challenges by proposing adaptive AI architectures specifically designed to protect and enhance distributed energy systems in smart urban environments. The main concern is the vulnerability of energy networks to cyberthreats and challenges, which consequently poses a threat to the reliability of energy delivery as well as the stability of urban infrastructures. This study focuses on developing innovative artificial intelligence (AI)-based techniques to mitigate these risks and enhance energy networks. Our approach involves analyzing current energy network management processes and designing new architectural models that incorporate adaptive AI features. The proposed framework, which leverages real-time data, anomaly detection, and predictive maintenance, aims to strengthen both security and operational efficiency. To ensure the framework's stability and alignment with best practices in addressing cyberthreats, it is modeled after the Cyber Assessment Framework provided by the United States National Cyber Security Centre. Future research will focus on refining these AI frameworks through simulations and pilot programs, tailoring them to different cities and ensuring compliance with evolving security protocols. Additionally, ongoing efforts aim to create a viable and flexible strategy for managing and safeguarding distributed energy systems (DERs) in smart cities.

Keywords: Smart Grid; Distributed Energy Network (DENs); Cyber Security and Privacy; Consequence-driven Cyber-Informed Engineering (CCE); Adaptive AI frameworks

Introduction

Background on Distributed Energy Networks

The transformation of urban energy systems into smart grids marks a substantial advancement in energy management and utilization within cities [1]. Microgrids, which are distributed energy systems incorporating renewable sources such as solar PV and wind power, alongside energy storage and electric vehicles, are gradually being deployed in urban areas. These networks are touted for their ability to enhance energy performance, availability, and sustainability by improving the generation, distribution, and consumption of energy [2-3]. However, the advancement of these technologies introduces a new set of challenges, particularly in the areas of security and privacy.

Additionally, Distributed Energy Networks (DENs) are defined as systems where energy is produced locally rather than solely by large power plants [4]. Technological advancements in renewable energy, energy storage, and digital communication are key drivers of this shift. These networks differ significantly from traditional centralized power grids due to their unique components and operational structure [5-6]. They rely on sophisticated control mechanisms to regulate electricity flow, integrate various power sources, and ensure grid efficiency [5]. However, merging these diverse elements into a cohesive system necessitates robust communication and control frameworks. Current smart grids utilize Advanced Metering Infrastructure (AMI), demand response systems, and other technologies that facilitate real-time adjustments, improve the integration of renewable energy sources and optimizing energy usage [6-7]. Despite these advancements, the complexity and interconnectedness of such systems present significant challenges, as they create multiple access points for cyberthreats through various system interfaces.

Furthermore, security remains a critical concern in urban smart environments. Integrating Distributed Energy Resources (DER) and utilizing digital communication networks to manage and control them opens multiple avenues for cyberthreats [7-8]. Unlike traditional electricity networks, which were not linked to digital systems and were less vulnerable to cyberattacks, smart grids are continuously connected to information technology systems, making them more susceptible to cyberthreats [9]. Another significant challenge in smart grid cybersecurity is balancing the need for strong security measures while maintaining optimal system performance. These systems must be resilient to cyberattacks while also adapting to fluctuations in energy supply and demand [10-11]. Traditional static security approaches are insufficient for smart grids, as they require dynamic security solutions capable of addressing emerging threats over time.

Recent cyber incidents highlight the urgency of addressing these vulnerabilities. For instance, the American power grid has been targeted by multiple cyberattacks, exposing numerous system weaknesses. In 2015 and 2016, the Ukrainian power grid was successfully compromised by cybercriminals, leading to widespread blackouts across the country [11]. These events underscored the potential devastation of such attacks, raising awareness and driving the need for enhanced security measures. Several cyberattacks on the U.S. power grid have also occurred, revealing the infrastructure's vulnerabilities. In 2020, the U.S. government reported that advanced persistent threats, including state-sponsored actors, had been gathering intelligence and probing critical energy infrastructure [12]. These incidents were part of broader cyber-espionage and sabotage efforts targeting key systems.

The 2021 attack on Colonial Pipeline, though affecting a different sector, demonstrated how ransomware attacks could paralyze business operations and cause significant economic damage [12-13]. While distinct from a power grid attack, it highlighted the risks to critical infrastructure. One of the most concerning trends in cyberthreats is Industroyer V2, a new malware designed to target Industrial Control Systems (ICS) in critical infrastructure. Industroyer V2 is an upgraded version of the malware used in the 2016 attack on Ukraine's power grid [14]. This malware not only disrupts industrial control systems but also poses a severe threat to smart grids and other essential infrastructure. The growing sophistication of Industroyer V2 illustrates the continuous evolution of threats, emphasizing the need for new layers of protection [14]. Its ability to directly communicate with industrial control systems enables it to cause tangible damage, such as physical destruction and operational disruptions, rather than merely compromising data or systems. This underscores the critical need for dynamic security architecture that can detect and counter such threats in real time.

In response to increasing threats, novel approaches like Consequence-driven Cyber-Informed Engineering (CCE) have been developed by the Idaho National Laboratory to enhance critical infrastructure security. CCE focuses on understanding the impact of cyber-threats on system operations. This approach involves assessing the consequences of potential vulnerabilities and designing systems that can minimize the effects of an attack [15-16]. Additionally, CCE emphasizes integrating cybersecurity considerations into the fundamental engineering and design of infrastructure. The goal of CCE is to strengthen the security of digitized systems such as smart grids and other Industrial Control Systems (ICS) by accounting for the potential impacts of cyberthreats and embedding protective measures into these systems' design [16].

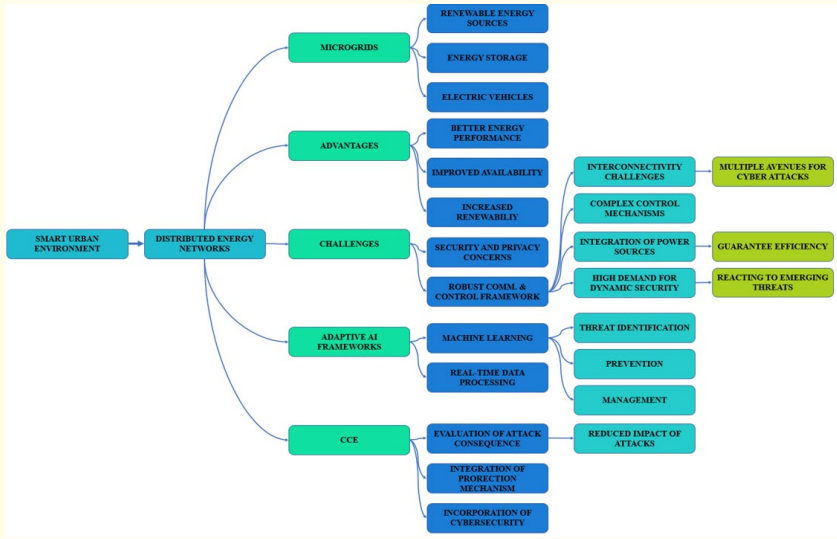

Figure 1: Structure of the Distributed Energy Networks in Smart Urban Environment regarding Adaptive AI framework and CCE.

As urban environments develop increasingly complex smart grid systems and cyberthreats continue to evolve, it becomes essential to design and implement enhanced security measures, as illustrated in Figure 1. The proposed application of adaptive AI structures for distributed energy systems presents a significant opportunity to improve the security and control of these systems. By leveraging AI technologies—particularly those based on machine learning and real-time data processing—adaptive and effective security solutions can be developed to safeguard smart grids from emerging threats [16]. Furthermore, this research aims to investigate how adaptive AI frameworks can address security challenges facing smart grids in urban settings [17]. By analyzing AI's potential to identify, prevent, and manage threats, this study seeks to lay the groundwork for improving the security of energy networks. Additionally, the research will explore the application of various frameworks, including Consequence-driven Cyber-Informed Engineering (CCE), to adaptive AI and assess how integrating these methodologies can enhance the overall security posture [18].

Therefore, while the development of distributed energy networks and smart grids offers significant digital transformational benefits such as predictive analytics, productivity and environmental sustainability, it also introduces new risks that demand novel security measures. This study emphasizes the importance of incorporating adaptive AI frameworks and methodologies like CCE to enhance the cyber-resilience of smart urban grids. Ultimately, the goal of this research is to contribute valuable insights and solutions to the construction, management and operations of distributed energy networks in the face of evolving threats.

Importance of Protection and Management in Smart Urban Environments

The shift toward smart cities has significantly transformed energy production, distribution, and consumption. Central to this transformation is the smart grid, which integrates information technology and communication networks with traditional electrical grids [18-19]. These networks have the potential to enhance flexibility, reliability, and efficiency of energy delivery. However, increased reliance on and integration of smart grids also introduces substantial cybersecurity risks. Therefore, this paper aims to propose frameworks for safeguarding and managing smart grid systems as cities continue to adopt this technology. Specifically, this paper explores the importance of designing adaptive AI frameworks to enhance the security of smart urban environments, with a particular focus on distributed energy systems.

Smart Grids Complexity and Interconnection

- ***Advanced Technology Integration***: Smart grids comprise various technologies, including sensors, control systems, and communication networks [19]. The integration of these technologies results in intricate and interconnected systems, which significantly heightens their vulnerability to cyber threats.
- ***Dynamic Nature of Operations***: Smart grids are designed to be adaptive systems that can respond in real time to fluctuations in energy demand and supply. While this flexibility offers significant advantages, it complicates security efforts, as protective measures must also be able to adapt to emerging threats in real time.

Threats Posed by Cyber-Space to Smart Grids

- ***Targeted Attacks***: As critical infrastructure, smart grids are increasingly targeted by cybercriminals and state-sponsored hackers. These attacks can disrupt electricity supply, damage infrastructure, and result in significant economic losses.
- ***Ransomware and Malware***: Another major threat to smart grids is ransomware and malware, which can cripple system operations and compromise sensitive information. Given the critical nature of these services, such attacks can have devastating consequences, especially when essential services are impacted [21].
- ***Insider Threats***: Employees or contractors who manage smart grid systems may pose insider threats, either through explicit or implicit malicious actions. Because insider threats originate within an organization, they are particularly difficult to detect and mitigate.

Protection and Management Relevance

- ***Operational Continuity***: Ensuring the security of smart grids is essential to maintaining the stability of energy supplies. Any disruption could lead to widespread outages, affecting homes, businesses, and critical facilities.
- ***Economic Implications***: Cyberattacks that compromise or disrupt energy systems result in significant economic costs, both from direct damage and the expenses associated with restoration and future prevention.
- ***Public Safety***: Smart grids control vital infrastructure, and any interference could pose risks to public safety. Protecting against potential hazards, such as voltage spikes or power failures, is crucial where electrical energy is used.
- ***Regulatory Compliance***: Governments, regulatory bodies, and managers of critical infrastructure have established stringent security standards. Adhering to these standards is essential to avoid legal repercussions and to maintain public trust.

AI Frameworks in Organizations

- ***Real-time Threat Detection***: Adaptive AI architectures can process vast amounts of data from smart grid systems in real time, identifying abnormal patterns or indicators of cyber threats [21]. This enables swift responses and, if necessary, immediate threat mitigation.
- ***Predictive Analytics***: By analyzing historical data and utilizing machine learning, predictive analytics can anticipate potential vulnerabilities and future threats. This approach enhances the ability to build proactive defenses against emerging risks.

- ***Automated Response***: AI-driven systems can autonomously respond to threats they detect by isolating affected components, adjusting security settings, or initiating countermeasures. This reduces reliance on human intervention and significantly improves response times.
- ***Adaptive Learning***: AI frameworks continuously evolve as they encounter new threats or attack types. This capability allows security measures to dynamically adjust and adapt to the specific threats faced, ensuring ongoing protection.

Implementation Strategies

- ***Integration with Existing Systems***: Adaptive AI frameworks should be seamlessly integrated into existing smart grid systems without compatibility issues [22]. They must be able to work with the current hardware and software while causing minimal disruption to the organization's operations.
- ***Scalable Solutions***: Given the wide distribution and diversity of smart grids, AI security solutions must be highly scalable. They should accommodate increasing data volumes, a growing number of devices, and expanding network parameters.
- ***Collaborative Approach***: Effective security management requires a multidisciplinary effort, involving utility companies, technology providers, and government agencies. AI frameworks should promote information sharing and foster collaborative defense strategies.
- ***Continuous Monitoring and Evaluation***: AI-driven security systems must undergo regular reviews and assessments to maintain their effectiveness. This includes updating algorithms, enhancing threat detection models, and addressing any vulnerabilities that arise.

Challenges and Considerations

- ***Data Privacy***: The use of AI frameworks entails the use of major data, which is a contentious issue regarding data privacy and confidentiality. To address these issues, one has to ensure the use of efficient measures to protect data.
- ***Resource Requirements***: Sophisticated AI structures demand substantial computing power and programming knowledge. Therefore, it is important for smart grid operators to have access to the enabling infrastructure and skills to make the project a success.
- ***Ethical and Legal Issues***: It is therefore essential that the application of AI in security management is subjected to specific legal frameworks and ethical norms. This helps to promote the use of AI to enhance security while at the same time observing the regulations set down.

Thus, the issue of smart grid security becomes even more critical as more and more urban frameworks transform into smart cities. This is because the emergence of adaptive AI frameworks is one of the potential solutions to the diverse and dynamic nature of cyber-threats confronting dispersed energy systems. AI frameworks in smart grids improve the safety and security of these infrastructures, their operation, the overall economy and people's safety by applying real time threat identification, predictive analysis and response automation. However, some factors must be taken into consideration when implementing such a system among those are integration, scalability, collaboration, and ethical issues. With the threat actors not ceasing to invent new ways of attacking smart urban environments, such constant development will be critical in ensuring the security of smart urban environments of the future.

Recent Attacks on US Power Grids

The digitalization and integration of smart technologies in managing urban energy systems have transformed how electricity is delivered and consumed [12]. However, this shift has also introduced significant risks, as the interconnected nature of power grids makes them attractive targets for cybercriminals. Recent incidents have highlighted the urgent need to strengthen security measures for these critical infrastructures. This paper examines several notable cyberattacks on U.S. electric power grids, focusing on key events and their implications for the security of smart grids.

Persistent Breach Attempts on U. S. Electric Power Facilities

Overview of Recent Cyberattacks

- ***Increase in Frequency and Complexity***: Over recent years, there has been a noticeable rise in both the frequency and sophistication of cyberattacks targeting U.S. electric grids [12]. These attacks are no longer isolated incidents but part of a growing trend aimed at disrupting critical infrastructure.
- ***Intent and Consequences***: Cyberattacks on power grids are often designed to cause service outages, steal sensitive data, or even inflict physical damage, posing serious risks to national security and public safety. The consequences can be devastating, leading to widespread blackouts, compromised personal and organizational data, and damage to vital infrastructure.
- ***Exploiting System Vulnerabilities***: These attacks typically exploit vulnerabilities in outdated grid structures, insufficiently secured systems, and inadequate monitoring processes. For instance, the 2015 and 2016 cyberattacks on Ukraine's power grid, which caused significant blackouts, served as a wake-up call for many countries. In 2020, U.S. grid operators were targeted by cyberattacks believed to be linked to state-sponsored actors, exposing weaknesses in the infrastructure's security systems. Similarly, the Colonial Pipeline ransomware attack in 2021, although not directly targeting the power grid, highlighted the potential for ransomware to disrupt essential services and emphasized the need for improved security measures in critical infrastructure. These incidents demonstrate how attackers can exploit outdated technology, poor security protocols, and lack of real-time monitoring to cause widespread disruption.

INDUSTROYER V2

- ***Description***: INDUSTROYER V2, also known as CRASHOVERRIDE, is a highly advanced malware specifically designed to target Industrial Control Systems (ICS) and disable power grids. It has been identified by experts as a highly specialized ICS malware aimed at disrupting the operations of critical infrastructure [14].
- ***Incident Overview***: The original INDUSTROYER malware was responsible for a large-scale blackout in Ukraine in December 2016, which targeted the electric power sector. The newer, more sophisticated version, INDUSTROYER V2, has been identified as even more capable of interfering with power grid network functions, posing an even greater threat [14].
- ***Capabilities***: INDUSTROYER V2 can compromise various components of the power grid, including circuit breakers and transformers, causing widespread disruption to the electricity supply and even inflicting physical damage on critical infrastructure.
- ***Impact***: The malware's potential to create large-scale blackouts and cause physical destruction to key infrastructure demonstrates the significant risk it poses to the reliability and safety of power grids.

Case Study: Colonial Pipeline Cyberattack 2021

- ***Incident Overview***: In May 2021, the DarkSide group executed a now-infamous ransomware attack on the Colonial Pipeline, a critical fuel supply line in the United States [13].
- ***Attack Mechanism***: The attackers deployed ransomware to encrypt the pipeline's data, demanding a ransom for the decryption key, which brought operations to a standstill.
- ***Impact on Power Grids***: While the direct impact on electric grids was not immediately apparent, the attack underscored broader concerns about the vulnerability of critical infrastructure. It highlighted the susceptibility of essential facilities, like power grids, to ransomware attacks and demonstrated how such disruptions could have far-reaching consequences.
- ***Response and Lessons Learned***: The attack prompted swift action from the government and various industries to improve cybersecurity standards. It underscored the need for stronger response strategies, particularly for power grids and other critical infrastructures, to mitigate the risks posed by similar threats in the future.

Case Study: The Supply Chain Attack of 2023

- ***Incident Overview***: The SolarWinds attack, first detected in December 2020 and active until 2023, occurred via a supply chain attack on SolarWinds' Orion software, which is widely used by both government agencies and private companies [20].

- ***Attack Mechanism***: The attackers inserted malicious code into software updates, granting unauthorized access to numerous networks and server systems, compromising the security of critical infrastructure.
- ***Impact on Power Grids***: The attack highlighted the vulnerabilities posed by supply chain risks, particularly their potential impact on infrastructure and critical sectors such as power networks. It demonstrated that interconnected systems, when linked through a single network, can be exploited as entry points to other vital infrastructures.
- ***Response and Lessons Learned***: Key lessons from this incident include the insufficiency of security measures in supply chains and the lack of thorough checks on software integrity. It also emphasized the importance of collaboration between public and private entities to address complex cyber threats and strengthen collective defense mechanisms.

Cyber Warfare - Attack on North Carolina's Electrical Power System

- ***Incident Overview***: In December 2022, North Carolina experienced a series of cyberattacks targeting its electric grid infrastructure, resulting in power outages across several regions [21].
- ***Attack Mechanism***: The attacks involved both physical sabotage and cyber intrusions, with components of the electrical grid, including substations, being vandalized, while the potential for cyber intrusions further endangered the system's integrity.
- ***Impact***: These disruptions affected tens of thousands of people and revealed critical weaknesses in both the physical security and cybersecurity of the grid networks.
- ***Response and Lessons Learned***: The incident prompted a reassessment of security measures and heightened concerns over the protection of both physical assets and digital information. It emphasized the need for a comprehensive security strategy that addresses both traditional and emerging threats.

Recent cyberattacks on several U.S. electric power grids underscore the urgent need for robust protection systems. Notable incidents such as the INDUSTROYER V2 malware in OT environments, the 2021 Colonial Pipeline ransomware attack, the 2023 SolarWinds supply chain breach, and the attacks on North Carolina's electric grid highlight the critical importance of adopting dynamic security architectures. To achieve high levels of smart grid security in urban settings, it is essential to deploy adaptive AI models capable of proactively detecting emerging threats. These frameworks should integrate features such as real-time monitoring, anomaly detection, and feedback mechanisms to effectively combat cyber threats. Enhanced utilization of advanced technologies and stronger collaboration among stakeholders will significantly improve the security of smart grid systems, ensuring that urban energy networks are better protected against the rising challenges posed by cyberattacks.

Contributions of the Study

By implementing adaptive AI frameworks and applying the principles of Consequence-driven Cyber-Informed Engineering (CCE), this study aims to enhance the security and resilience of smart grids in urban environments, protecting distributed energy networks from both current and future cyber threats. The key contributions of this study are outlined below:

i. ***Increased Complexity of Urban Smart Grids***: Urban smart grids consist of numerous distributed energy resources, sensors, and communication systems, making the overall system highly complex. This complexity introduces risks that conventional security solutions struggle to address effectively. Dynamic AI frameworks offer the ability to assess and counter emerging threats, providing robust defense mechanisms against even the most sophisticated cyberattacks that exploit these system dynamics.
ii. ***Proliferation of Cyberthreats***: As urban smart grids become more interconnected, their vulnerability to a wide range of cyber threats, from ransomware to advanced persistent threats, increases. Adaptive AI, with its capacity to learn and identify new threat patterns, offers a more secure approach, defending systems in real time. This capability is particularly useful for preventing incidents related to the ever-evolving nature of cyber threats.
iii. ***Real-time Threat Detection and Response***: Given the constant evolution of smart grids in urban areas, threats must be detected and mitigated in real time. Adaptive AI frameworks, leveraging machine learning and data analytics, can quickly identify and respond to anomalies, thereby minimizing the impact of cyber threats. These frameworks also need to function in real time to

ensure the stability and resilience of distributed energy systems.

iv. ***Enhanced Risk Management through CCE***: Cyber-Informed Consequence-driven Engineering (CCE) focuses on identifying and analyzing the consequences of cyber threats on specific infrastructures. By integrating CCE principles into adaptive AI frameworks, it becomes possible to concentrate resources on the area's most vulnerable to damage, thereby protecting critical zones more effectively and prioritizing risks based on their potential impact.

v. ***Scalability and Flexibility***: Urban smart grids are continuously evolving, with new components and technologies being added. Scalable security management solutions are essential to align with the expanding and increasingly complex grid. These scalable solutions ensure that security practices grow alongside the grid, maintaining effective protection as new technologies are integrated.

vi. ***Integration with Existing Infrastructure***: Adaptive AI can be seamlessly incorporated into existing smart grid infrastructures in urban areas, enhancing security without the need for drastic overhauls. This approach allows for incremental improvements in security, building on current systems and architectures while introducing new AI-driven security layers that can operate in real time.

Objectives of the Study

The following are the objectives of the study:

i. ***Dynamic Threat Detection and Response***: The adaptive AI frameworks are designed to keep learning about the new threats and anomalies within the network. In this case, these frameworks are effective in the identification and real time learning of new threats through the use of machine learning algorithms. This helps ensure that the smart grid in urban areas is ready to address complex attacks and threats and respond to them effectively improving the resilience of the system as a whole in the process.

ii. ***Context-Aware Security Measures***: Adaptive AI incorporates security measures that consider the surrounding environment in which a smart grid operates. This involves analyzing the data collected from various sources to reveal the network's and its different components' behavior. In this way, the AI can better differentiate between normal behaviors and suspicious activities and minimize false positives in threat analysis.

iii. ***Proactive Vulnerability Management***: Thus, adaptive AI frameworks assist in monitoring and predicting possible flaws in the smart grid infrastructure. By pinpointing the areas that can be targeted and are in some way exposed, these frameworks help initiate action to counter threats, thereby strengthening the grid against threats and further reducing the consequences of possible invasions.

iv. ***Adaptive Risk Assessment and Mitigation***: Applying Consequence-driven Cyber-Informed Engineering (CCE), the AI frameworks used are adaptive and evaluate cyberthreats in accordance with their consequences rather than their probability. This approach enables prioritization of risks to be managed by identifying the potential impacts that are most likely to occur and then devising special measures to curb these risks, as seen from CCE analysis.

v. ***Enhanced Incident Response and Recovery***: In the case of a cyberattack, adaptive AI frameworks help in fast identification, analysis, and containment of the attack. They also help in easy recovery by directing what to do next based on past and current performance data. This helps in quick recovery from such incidences, ensuring that normal functioning is not disrupted for long.

vi. ***Scalable Security Solutions***: With the development of more smart grids in urban areas and the connection of more distributed energy resources into the grid, AI-based security architectures provide a more elastic security solution that can grow in tandem with the smart grid. Thus, through the use of modular AI components and distributed learning schemes, these frameworks can cope with elevated levels of complexity and scale while preserving their security when the smart grid develops.

Manuscript Structure

The structure of the manuscript is as follows: Chapter 2 presents the literature review, forming the foundation for the subsequent work. Chapters 3 and 4 delve into cyber threats and vulnerability analysis, alongside a discussion on Cyber-Physical Systems (CCE) and their relationship with adaptive AI frameworks. Chapter 5 outlines the identified challenges and opportunities, and introduces a novel

framework. Chapter 6 details the architectural modeling of this framework and offers insights on how it can be integrated into current energy management systems. In Chapter 7, the author elaborates on the implications, applications, strengths, and weaknesses of the proposed framework. Finally, Chapter 8 provides the concluding remarks and suggests directions for future research. This structure offers systematic progression from the theoretical background to practical applications of the research findings.

Literature Review

Overview of Distributed Energy Networks

Dynamic AI systems have been developed to address the limitations of traditional security methods by incorporating capabilities for adaptive learning and decision-making. For example, these systems can be trained to identify abnormal traffic patterns or unusual operations that may signal a cyberattack. As highlighted by [6], adaptive systems play a crucial role in detecting threats and determining their severity before initiating a response. Their research demonstrates that AI-enhanced security features can significantly reduce response times and improve threat detection capabilities.

Another key factor in smart grid security is the control of distributed energy systems (DERs). These networks are decentralized, which presents both advantages and challenges from a security perspective. The integration of DERs introduces additional complexity, as each component must be securely managed to prevent potential threats. This concern is emphasized by [8], who highlight the need for special attention to both operational and cybersecurity aspects when managing these resources. Their work underscores the importance of developing a comprehensive security plan that addresses the unique challenges posed by distributed energy systems.

In addition to threat detection, AI can optimize the management and allocation of resources within distributed energy networks. AI applications in these systems enhance efficiency and reliability by predicting energy demand, distributing resources, and identifying vulnerabilities. For instance, [9] explores how learning-based models can predict energy demand and control DERs to improve both security and performance.

However, several challenges remain in developing AI-based security frameworks. One major concern is the need for high-quality, labeled data to properly train AI models. The effectiveness of AI systems is directly tied to the quality of the data used for training; insufficient labeled data can compromise their accuracy. As noted by [11], ongoing research aims to improve data collection and labeling techniques to enhance AI models for smart grid security.

Additionally, the use of AI-based security solutions raises ethical and privacy concerns. Data protection and the issue of user consent are critical in the context of AI-powered smart grids. A study by [17] stresses the importance of addressing these concerns to promote the responsible and ethical use of AI technologies in smart grid security.

In conclusion, adaptive AI frameworks present a promising solution for improving smart grid security in urban environments and enhancing decision-making in the management of distributed energy. AI offers significant advancements over traditional security methods due to its ability to analyze vast amounts of data and adapt to new threats. However, the full potential of these technologies can only be realized if challenges related to data quality, ethical issues, and system integration are resolved. Further research and development in these areas are essential to ensuring that AI can effectively protect future smart urban grids.

Current Protection and Management Strategies

In recent years, the growth of intelligent grids, particularly in urban areas, has brought increased focus on security to address existing and emerging cyber threats. Microgrids, which integrate distributed energy management systems and advanced communication technologies, have become essential components of modern urban systems. While this integration has significantly improved the grid's efficiency and reliability, it has also introduced new security challenges. Previous and current efforts in smart grid protection and management reveal a combination of traditional security measures and innovative technologies to combat cyber threats.

Traditional security measures remain the first line of defense for smart grids. Key components of these security architectures include firewalls and intrusion detection systems (IDS). Firewalls act as boundary controls, managing traffic between internal networks and untrusted external networks through defined protocols. IDS, on the other hand, monitor network traffic for suspicious activities that may indicate a security breach. These systems are effective in detecting and tracking known threats in real time. However, as the sophistication of cyber threats has increased, traditional security measures alone are no longer sufficient.

To address the limitations of traditional approaches, there has been a shift toward more flexible and advanced methods. For instance, machine learning (ML) algorithms are widely used to enhance smart grid security by detecting anomalies and conducting predictive analytics to identify potential threats before they escalate [18]. These algorithms process large amounts of data from the grid, identifying irregularities and alerting operators to potential cyber threats. Another emerging approach involves the use of Artificial Intelligence (AI) in adaptive security models. AI systems continuously learn from new data, allowing them to improve security measures over time. This capability is particularly valuable in the context of smart grids, where threats are constantly evolving. AI-based systems can adapt security protocols in response to changing threat landscapes, providing a more dynamic defense than traditional methods [19].

Blockchain technology has also been applied to smart grids to enhance security. As a decentralized and tamper-resistant system, blockchain improves data integrity and transparency, making it difficult for malicious actors to manipulate system data. Research by [22] and [23] demonstrates how blockchain can secure smart grids by ensuring that only authorized personnel can modify records. Additionally, smart contracts within blockchain frameworks automatically enforce security policies, reducing the likelihood of human error. Cyber-Physical Systems (CPS) security solutions have also become critical in safeguarding the integration of smart grids, combining computational elements with physical processes. Adaptive encryption techniques and secure communication protocols protect data as it moves through the grid, while physical security measures prevent attacks on infrastructure.

A notable trend is the development of hybrid security models that combine various technologies and strategies. Some studies propose enhanced IDS architectures that integrate traditional IDS with AI-based anomaly detection and blockchain verification processes [24]. These integrated models leverage multiple technologies to offer more comprehensive security solutions. Furthermore, policy and regulation are critical aspects of smart grid security. Recent literature emphasizes the need for robust policies and regulations to guide cybersecurity and data protection efforts. Regulatory agencies are increasingly focused on formulating guidelines that address the unique security challenges posed by smart grids.

In conclusion, the protection and management of urban smart grids have evolved beyond traditional methods, incorporating adaptive and advanced technologies. While firewalls and IDS remain essential, the use of machine learning, AI, blockchain, and hybrid security models has opened new possibilities for enhancing grid security. Strong policy and regulatory frameworks also play a vital role in establishing security standards. As urban smart grids continue to develop, ongoing research and innovation will be crucial to maintaining the security and reliability of these systems in the face of future threats.

AI and Machine Learning in Energy Systems

The application of Artificial Intelligence (AI) and Machine Learning (ML) in energy systems has transitioned from theoretical research and experimentation to practical implementation, significantly influencing the design and operation of energy infrastructures. Recent literature has thoroughly analyzed this shift, particularly in the context of smart grids, where these technologies are being increasingly integrated.

AI and ML algorithms offer powerful tools for enhancing various aspects of energy management. These technologies facilitate predictive maintenance, load forecasting, and dynamic energy management, ultimately improving system efficiency and reducing operational costs. For instance, a study by [22] demonstrated how an ML-based model could predict energy consumption rates with high accuracy, which is crucial for balancing supply and demand in real time. Neural networks and ensemble methods have also been employed to forecast energy loads and generation patterns, aiding in better planning and operational adjustments for smart grids.

Additionally, AI improves the integration of renewable energy sources. Renewable energies like solar and wind are subject to significant fluctuations, making effective forecasting algorithms essential for managing this variability. A 2024 study by Johnson and Lee explored the use of reinforcement learning for dispatching renewable energy resources to meet grid demand at the lowest operating cost. These advancements not only enhance grid stability but also contribute to more efficient energy distribution.

AI also plays a critical role in the management of Distributed Energy Resources (DERs). As more households install rooftop solar systems, home batteries, and other distributed energy assets, tracking and managing these systems becomes increasingly complex. AI platforms help by aggregating data from diverse sources, improving the effectiveness of energy distribution. A study by [23] detailed how AI systems are used to control and operate DERs, leveraging grid information to minimize energy losses

Challenges and Limitations

While AI and ML offer many advantages in energy systems, they also present challenges and limitations. One primary concern is the security of AI-driven systems. As these technologies become central to managing energy systems, they also introduce new cyber vulnerabilities. For example, reviews by [24] and [25] highlighted security concerns in smart grids, including vulnerabilities that could disrupt energy supplies or result in data breaches due to advanced AI applications. These findings stress the need for robust security measures to mitigate such risks.

Another limitation is the significant demand for high-quality, labeled data. AI and ML models require vast amounts of data for training, and in the energy sector, collecting and processing this data can be labor-intensive and time-consuming. Inadequate data or biased datasets can lead to inaccurate predictions and ineffective business decisions. [26] also pointed to data quality and availability challenges in AI applications for energy management, emphasizing the need for standardized data collection and processing guidelines to improve AI model accuracy.

Additionally, there is the challenge of explainability in AI models. Although AI systems can produce highly accurate forecasts, the reasoning behind their predictions is often opaque, creating a “black box” problem. This lack of transparency prevents operators from fully trusting AI outputs when making critical decisions. Research is ongoing to develop more interpretable AI models, but progress in this area is still in its early stages.

Conclusion

AI and ML have made significant strides in improving energy management, from enhancing forecasting accuracy to better integrating and coordinating distributed energy resources. However, challenges remain, particularly in terms of security, data quality, and model interpretability. While progress in research and development has been substantial, overcoming these challenges is essential for ensuring that AI technologies can be fully effective and reliable in managing future energy systems.

Previous Work on AI Frameworks for Smart Grids

The incorporation of Artificial Intelligence (AI) and Machine Learning (ML) in energy systems has garnered significant attention in recent years, primarily due to the potential of these technologies to enhance the operational efficiency, resilience, and security of energy infrastructures. With the transition from centralized energy systems to more distributed networks, and the growing integration of renewable energy sources, such as smart grids and Distributed Energy Resources (DERs), AI and ML have become essential tools for addressing the challenges that arise from this evolution.

Recent studies highlight several key applications of AI and ML in energy systems. In energy management, AI technologies have been applied to improve energy efficiency, grid stability, and the integration of renewable energy. For instance, [27] explored the use of deep reinforcement learning algorithms in demand response (DR), demonstrating how AI techniques can optimize demand response to stabilize the grid while simultaneously reducing costs. This work emphasizes the role of AI in facilitating dynamic energy management that responds effectively to fluctuations in energy demand and supply.

AI-based predictive maintenance has also emerged as a critical field within the energy sector. Machine learning algorithms that focus on predictive analytics have been utilized to forecast equipment failures and schedule maintenance accordingly. In a recent study by [27], the authors applied ensemble learning techniques to predict the failure of wind turbines, achieving improved accuracy in failure prediction and reducing maintenance costs. This demonstrates how AI can enhance the reliability of energy systems by minimizing downtime and improving the effectiveness of infrastructure management.

AI has also played a crucial role in the integration of renewable energy systems. Methods such as supervised learning and neural networks have been used to predict solar and wind energy generation, reducing the inaccuracies associated with renewable energy production. For example, [28] introduced a hybrid model combining a convolutional neural network (CNN) and a long short-term memory (LSTM) network for solar power forecasting. The simulated results showed that this approach outperformed traditional ARIMA models, which could significantly aid grid balancing and energy storage management.

Despite the many advancements in integrating AI and ML into energy systems, there are still several challenges and limitations. One major issue is the quality and availability of data. AI and ML algorithms require vast amounts of high-quality data to function effectively. However, energy systems data are often noisy, incomplete, or sparse, which can negatively impact AI models. In their work, [29] discussed the impact of data quality on the efficiency of machine learning in grid management, stressing the need for improved data collection and preparation techniques to enhance the reliability of AI results.

Another significant challenge is the interpretability—or explainability—of AI models. Many AI techniques, particularly deep learning models, are often referred to as "black boxes" due to their lack of transparency. This opacity is problematic in energy systems, where it is crucial to understand how decisions are made to foster trust and ensure compliance. [30] addressed this issue by proposing methods to improve the interpretability of AI models used in energy forecasting. They emphasized that greater model transparency would aid stakeholders in making informed decisions.

Additionally, cybersecurity concerns must be addressed as more energy systems rely on AI and are increasingly connected to digital networks. The use of AI introduces new risks, as AI systems can themselves become targets for cyberattacks. In a recent study, [31] examined the security challenges associated with AI in smart grids, identifying risks such as adversarial attacks on machine learning models and data poisoning. Mitigating these threats requires the development of robust security measures and continuous monitoring to detect potential dangers.

In conclusion, the integration of AI and ML in energy systems offers several advantages, including improved energy management, enhanced predictive maintenance, and better incorporation of renewable energy. However, there are significant challenges related to data quality, model explainability, and cybersecurity. Further research and innovation are needed to overcome these barriers and fully harness the potential of AI in building more efficient and resilient power networks. Future efforts should focus on improving data management, increasing AI model transparency, and enhancing information security to ensure the successful integration of AI technologies into energy systems.

Cyber Threat and Vulnerability Analysis of the US Electric Sector

Overview of Cyber Threat Framework

The U.S. electric sector, which is crucial to the nation's infrastructure, is facing increasingly sophisticated cyberthreats that pose significant risks to its operations and security [4]. With the growing use of smart grid technology to manage and deliver energy in urban areas, the sector has become more vulnerable to cyberattacks. While modern technology introduces greater flexibility and improved methods for managing distributed energy resources and integrating them into the grid, it also creates new opportunities for attackers [5].

Threats facing the electric sector stem from foreign nation state actors, cybercriminals, and individual hackers. Nation-state actors, driven by geopolitical motives, have shown an increased intent to target critical infrastructure like the electric grid. These highly so-

phisticated actors utilize advanced persistent threats (APTs) and other complex methods to infiltrate systems, disrupt operations, or steal sensitive information [6-7]. Well-funded and technologically advanced, these attackers can bypass traditional security measures, posing a serious threat to grid stability and national security. On the other hand, financially motivated individuals exploit system vulnerabilities to demand ransoms or commit theft. In recent years, ransomware attacks have become more prevalent, where attackers seize control of critical data or operational technology (OT) systems and demand payment for their release. Such attacks can paralyze grid operations, leading to significant economic disruptions [8]. The increased use of interconnected networks and the expansion of smart grids into digital platforms provide potential entry points for these attackers.

Additionally, inherent vulnerabilities exist within the electric sector due to a combination of legacy systems and newer technologies that comprise smart grids. Unfortunately, many electric utilities still rely on outdated infrastructure that was not designed to defend against modern cyberthreats. These systems lack the necessary security measures to withstand contemporary attack strategies, making them prime targets for cyberattacks [9]. Moreover, while new smart grid technologies are designed to optimize the distribution and management of distributed energy resources, they also introduce new vulnerabilities. For example, the increased interconnectivity and data sharing between various parts of the smart grid can be exploited if not adequately protected.

Adaptive AI frameworks offer a viable solution to improving the security of smart grids in urban environments. These frameworks leverage artificial intelligence to monitor and counter threats in real time, transitioning the defense system from a reactive to a proactive approach [10]. AI systems can analyze vast amounts of data to identify patterns or anomalies that may indicate a cyberattack. As a result, these systems can become more preventive and self-correcting, effectively mitigating threats as they evolve and learning from new data inputs.

In addition to enhancing threat detection, AI frameworks can improve incident response and management. Traditional security mechanisms rely on predefined rules and signatures, which may be ineffective against new, complex threats [11]. In contrast, AI-based systems continuously learn about emerging threats and threat actors, offering recommendations on how to prevent further damage. For instance, if a file is accessed inappropriately, an AI system can automatically block the traffic, alert the relevant personnel, and suggest appropriate actions.

Strengthening cybersecurity in the electric sector requires a comprehensive approach that includes policies, training, and collaboration, in addition to technical measures. Managers must ensure that security protocols are up to date, conduct regular vulnerability assessments, and educate employees on the risks and necessary precautions [12]. Both public and private organizations must collaborate in sharing intelligence about threats and coordinating responses to cybersecurity incidents.

The threat landscape targeting the U.S. electric sector is complex and constantly evolving, making smart grid protection a significant challenge. Adaptive AI frameworks offer innovative solutions for identifying, combating, and recovering from cyberattacks. However, security also depends on a holistic approach that includes physical security measures, sound policies, regular training, and sector-wide coordination. As the electric sector continues to advance and invest in smart grid technologies, a dynamic and adaptable security framework will be essential to safeguarding the nation's critical infrastructure.

Vulnerability Assessment Techniques

In the age of smart grids, urban energy systems are becoming more advanced and interconnected. While this complexity offers opportunities for increased efficiency, it also creates vulnerabilities that can be exploited by cyberthreats. To effectively address these challenges, a comprehensive approach to vulnerability assessment is necessary. This approach typically includes threat modeling, risk assessment frameworks, and innovative techniques such as Consequence-driven Cyber-Informed Engineering (CCE). Figure 2 provides an overview of these methods and their critical role in enhancing the security of urban smart grids:

Threat Modeling

i. ***Definition and Purpose***: Threat modeling is a structured method for identifying and assessing potential threats and vulnerabilities within a system. Its primary objective is to anticipate and understand the different ways a system could be targeted, enabling the implementation of proactive security measures.

ii. ***Key Components***
- ***Asset Identification***: Identify critical components of the smart grid, including communication networks, control systems, and energy management elements.
- ***Threat Identification***: Recognize potential threats, such as malicious actors, insider risks, and natural disasters.
- ***Vulnerability Identification***: Evaluate system weaknesses that could be exploited by the identified threats.
- ***Attack Vectors***: Examine how threats could leverage vulnerabilities to compromise system integrity.

iii. ***Techniques***
- ***STRIDE***: A framework that focuses on six key threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
- ***PASTA***: The Process for Attack Simulation and Threat Analysis, which emphasizes simulating attacks to assess their potential impact on the system.
- ***OCTAVE***: The Operationally Critical Threat, Asset, and Vulnerability Evaluation method, designed to prioritize risks by considering the specific context of the organization.

Risk Assessment Frameworks

i. ***Definition of Purpose***: Risk assessment frameworks provide a structured approach to evaluating risks within a system by considering the likelihood of threats and the potential impact of vulnerabilities. This helps prioritize security measures based on risk levels.

ii. ***Key Components***
- ***Risk Identification***: Identify risks associated with each vulnerability, including potential impact and likelihood.
- ***Risk Analysis***: Evaluate the severity of each risk, considering both the probability of occurrence and the potential consequences.
- ***Risk Prioritization***: Rank risks based on their potential impact and likelihood to focus resources on the most critical threats.

iii. ***Common Frameworks***
- ***NIST Risk Management Framework (RMF):*** A comprehensive framework provided by the National Institute of Standards and Technology (NIST) for managing risk through asset categorization, control selection, and continuous monitoring to ensure security and compliance.
- ***ISO/IEC 27005:*** An international standard from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that provides a systematic approach to managing information security risks, covering risk assessment, treatment, and communication.
- ***Factor Analysis of Information Risk (FAIR):*** A methodology that focuses on quantifying information risk to provide clearer insight into potential impacts and prioritization, enabling organizations to make more informed decisions about risk management.

Consequence-driven Cyber-Informed Engineering (CCE)

i. ***Definition and Purpose***: CCE is a methodology designed to incorporate cyber-attack's potential consequences into the engineering process. The aim is to enhance resilience by understanding how attacks could impact system functionality and performance [15].

ii. ***Key Components***
- ***Consequences Assessment***: Evaluate how different cyber-attack types could affect system operations, safety, and security.

- ***Design Adaptations***: Modify system design and engineering practices to mitigate the potential consequences of identified threats.
- ***Resilience Building***: Implement measures to enhance system resilience against attacks, including redundancy, fail-safes, and robust incident response protocols.

iii. ***Application in Smart Grids***

- ***Scenario Analysis***: Use CCE to model various attack scenarios and their potential impact on smart grid operations, such as power outages or data breaches.
- ***Engineering Controls***: Integrate CCE findings into the design of smart grid components to ensure they can withstand and recover from cyberthreats.
- ***Continuous Improvement***: Use insights from CCE to continuously refine and update security measures and engineering practices.

Integrating Techniques for Enhanced Security

i. ***Holistic Approach***

- ***Combining Threat Modeling and Risk Assessment***: Use threat modeling to identify potential attack vectors and risk assessment frameworks to evaluate the impact and likelihood of these threats. This integration allows for a comprehensive understanding of vulnerabilities and risks.
- ***Incorporating CCE***: Apply CCE to ensure that the smart grid's engineering design accounts for potential consequences of cyberthreats, leading to more resilient systems.

ii. ***Adaptive AI Frameworks***

- ***AI-Driven Threat Detection***: Utilize machine learning algorithms to continuously monitor and analyze network traffic for unusual patterns indicative of cyberthreats.
- ***Predictive Analytics***: Implement AI tools to predict potential vulnerabilities based on historical data and emerging threat trends.
- ***Automated Response***: Deploy AI-based systems for real-time threat mitigation, enabling quick responses to detected threats and minimizing potential damage.

iii. ***Continuous Monitoring and Improvement***

- ***Feedback Loops***: Establish mechanisms for ongoing evaluation and updating of security measures based on new threats and vulnerabilities.
- ***Collaboration***: Foster collaboration between engineers, cybersecurity experts, and AI developers to ensure that security measures are both technically sound and practical for real-world applications.

In conclusion, enhancing urban smart grid security requires a robust and adaptive approach to vulnerability assessment. Resilient and secure distributed energy networks can be built by integrating threat modeling, risk assessment frameworks, and CCE and leveraging advanced AI techniques. This comprehensive strategy not only addresses current vulnerabilities but also prepares the system to effectively manage and mitigate future cyberthreats.

Security and Privacy in Smart Grid

Smart grid technologies have become a common feature in many urban environments such that the energy networks have become more complex and interconnected. With the incorporation of digital communication and control systems into the conventional power networks known as smart grids there is hope for more efficiency, reliability and sustainability. However, this integration also poses a lot of security risks and privacy issues that are a great concern. This post describes smart grids' security and privacy challenges and discusses how AI-based adaptive frameworks and data protection can help.

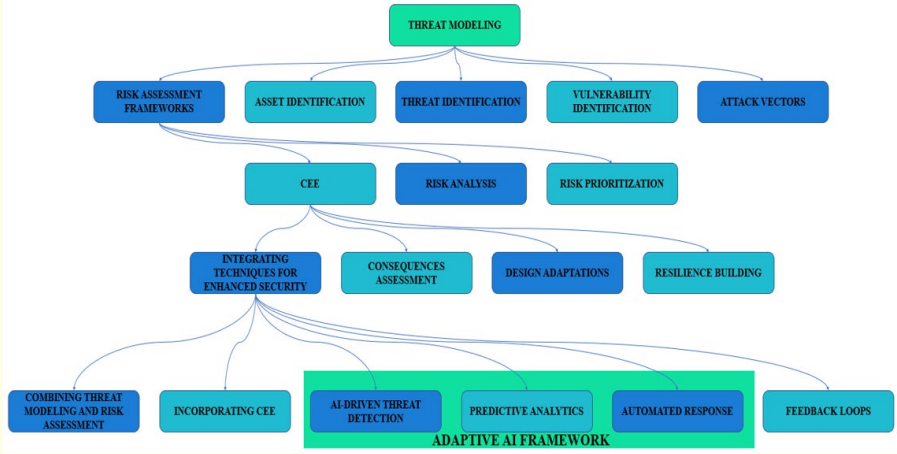

Figure 2: Framework for Vulnerability Assessment Techniques in Smart Grids.

Security Challenges in Smart Grids

i. ***Network Complexity and Interconnectivity***
   - ***Description***: Other sub-elements of the smart grid are smart meters, sensors and communications systems that enable the exchange of information between these entities in real time and provide control.
   - ***Challenge***: The complex interconnectivity increases the exposure to cyberthreats, making it difficult to protect the whole network from threats.

ii. ***Vulnerability to Cyber Attacks***
   - ***Description***: Smart grids are very vulnerable to different cyber risks including hacking, malware, and even Distributed Denial of Service (DDoS) attack.
   - ***Challenge***: In the current world, attacks can cut off power supplies, expose confidential information, and result in significant losses in terms of money and operations.

iii. ***Data Integrity and authentication Issues***
   - ***Description***: It is very important to guarantee that parameters exchanged between the grid components are accurate and genuine.
   - ***Challenge***: In other cases, attackers may alter the data used to control grid operations, which may cause inefficiencies or create dangerous situations.

iv. ***Insufficient Security Protocols***
   - ***Description***: Significant percentage of smart grid systems utilize counterproductive or insufficient security measures.
   - ***Challenge***: And finally, weak security features can make the system vulnerable to complex and unauthorized penetration.

Smart Grids Privacy Concerns

i. ***Acquisition and Transmission of Personal Data***
   - ***Description***: Smart meters and sensors gather the utilization of individual homes and companies.
   - ***Concern***: This data might contain information about personal habits and behaviors, thus touching on privacy and cases of data misuse.

ii. ***Data Aggregation and Analysis***
- ***Description***: Cumulative data is applied for grid control and the general organization of the functioning process.
- ***Concern***: However, individual data can be re-identified, or the information contained therein can be inferred, hence leading to a breach of privacy even by analyzing aggregated data.

iii. ***Third-Party Access***
- ***Description***: The data collected in smart grids is usually conveyed to third-party service providers for analysis and management.
- ***Concern***: When data is in the hands of third parties, either through abuse or otherwize, it is vulnerable to piracy and loss of privacy.

Countermeasures to Security and Privacy Threats

i. ***Adaptive AI Frameworks***
- ***Description***: Adaptive AI frameworks apply machine learning approaches to learn unknown threats while in operational environments.
- Benefits:
- ***Threat Detection***: AI systems can easily identify any possible threat through the patterns and behaviors identified, which will improve attack prevention.
- ***Automated Response***: These advantages of using Artificial Intelligence in cybersecurity. It can automatically introduce countermeasures and thus decrease the time taken to respond to incidents.
- ***Continuous Learning***: It learns about new threats and thus makes changes to enable it to handle new attack strategies better than previous ones.

ii. ***Security Controls for Protecting Data Confidentiality***
- ***Description***: Encryption makes it possible to send data securely across the smart grid without the information passing being understandable to anyone with ill intentions.
- ***Benefits***:
- ***Data Confidentiality***: Encryption ensures that data transmitted in a communication channel is not easily intercepted and/or modified.
- ***Integrity Checks***: Encryption methods were adopted to guarantee the integrity of the content both in transit and at the storage facility.

iii. ***Access Control and Authentication***
- ***Description***: Incorporation of proper authentication procedures and access authorization controls reduce the chances of access by unauthorized persons.
- ***Benefits***:
- ***User Verification***: Two-factor authentication improves security because the user is expected to provide more than one verification code.
- ***Access Management***: This type of information security constrains data and system accessibility and only allows access to authorized people according to their job description.

iv. ***Privacy-Preserving Technologies***
- ***Description***: Data masking and Differential Privacy are used to balance the privacy of data and its usability, that is, the ability to analyze the data.
- ***Benefits***:
- ***Anonymization***: Evaluating datasets is done to make sure that no personally identifiable information of a person is included.
- ***Differential Privacy***: The most important reason is to ensure that the contribution of individual data does not skew the result of data analysis in a way that compromises individual privacy.

v. ***Annual Security Assessment and Revision***
- ***Description***: Security audits and updates of software and security protocols assist in checking for gaps that may be exploited or outdated security systems.
- ***Benefits***:
- Vulnerability Assessment also assists in identifying poorly implemented areas in the system that may be vulnerable to attackers.
- ***Patch Management***: This way, the updates can address known weaknesses and improve system security in general.

Integrating Security and Privacy Solutions

i. ***Holistic Security Approach***
- ***Description***: Increasing the protection level by applying AI-based frameworks, encryption, access control, and privacy-preserving mechanisms.
- ***Benefits***:
- ***Enhanced Protection***: Layers of security are very effective at combating multiple threats simultaneously.
- ***Unified Management***: Error-excluding security solutions enhance the security management and response operations.

ii. ***Collaboration and Information Sharing***
- ***Description***: Communicating with partners in the industry and other government agencies so that threats emerging in the market are identified and effective new practices are well understood.
- ***Benefits***:
- ***Threat Intelligence***: The exchange of threat intelligence provides a better capability to anticipate new threats.
- ***Industry Standards***: Best practices promote collaboration, which leads to the setting and implementation of standards and regulations.

Enhancing the security and privacy of urban smart grids is crucial for realizing their full potential while protecting against cyber threats and safeguarding individual privacy. The following challenges can be effectively mitigated with adaptive AI frameworks, robust data protection measures, and privacy-preserving technologies. The integration of these solutions, combined with an interdisciplinary approach, will strengthen the resilience of smart grids against emerging threats and support the development of a sustainable and secure urban energy network.

Regulatory and Compliance Issues

Several regulatory and compliance questions emerge as urban smart grids actively incorporate adaptive AI frameworks to oversee and safeguard distributed energy networks. These questions are important to enhance the security of these systems and assess them against current laws.

i. ***Data Privacy and Protection***
- ***Regulatory Framework***: Using smart grids with AI entails dealing with vast amounts of data, some of which could be considered data sensitive, such as personal data and energy consumption data. In the US, the principal legislation that applies to data privacy is the California Consumer Privacy Act (CCPA) for specific regions and the General Data Protection Regulation (GDPR) for organizations operating internationally.
- ***Compliance Challenges***: Implementing and following these regulations calls for stringent data protection elements, including encryption and access control. Organizations must also address data handling policies and user consent.

ii. ***Cybersecurity Standards***
- ***Regulatory Framework***: To this end, the two regulatory bodies of the U.S., the U.S. Department of Energy (DOE) and the Federal Energy Regulatory Commission (FERC), have developed standards and guidelines to strengthen cybersecurity in the electric grid. Several important requirements are, for instance, the North American Electric Reliability Corporation's (NERC)

Critical Infrastructure Protection (CIP) standards.

- ***Compliance Challenges***: Smart grid systems should follow these standards and must constantly be updated and reevaluated due to the existing cyber threats. Adapting AI also guarantees that such systems are secure from high-tech attacks and compatible with existing cybersecurity rules.

iii. ***Interoperability and Standardization***

- ***Regulatory Framework***: The National Institute of Standards and Technology (NIST) in the USA proposes two major frameworks to define the measures of interoperability and standardization in smart grids: the NIST Cybersecurity Framework and Smart Grid Interoperability Standards [25].
- ***Compliance Challenges***: The application of adaptive AI frameworks requires the following standards for them to work compatibly with the current grid infrastructure and other systems. This encompasses the following standards for sharing information and communication between the various technologies.

iv. ***Operational Transparency and Accountability***

- ***Regulatory Framework***: Some authorities, like FERC in the United States and the DOE, support public disclosure of grid management and operational information and require a plan in place in case of a security incident or a system failure [25-26].
- ***Compliance Challenges***: AI systems should have an incorporated means of tracking incidents besides having a transparent reporting system where the AI system is accountable for disruptions or breaches. These regulatory requirements call for routine audits and assessments.

v. ***Risk Management and Incident Response***

- ***Regulatory Framework***: The National Institute of Standards and Technology (NIST) defines risk management and incident handling in its Cybersecurity Framework, which is essential for managing and controlling risks in smart grid platforms.
- ***Compliance Challenges***: Adaptive AI frameworks, risk management strategies, and incident response plans must be updated and tested periodically. Compliance is about developing complex response plans, maintaining auditable documentation, and quick disaster recovery.

vi. ***Cross-Jurisdictional Compliance***

- ***Regulatory Framework***: Since smart grids are interrelated, they must meet both federal and state legal requirements. Notably, state standards may also be relevant from time to time, depending on the state's public utility commissions.
- ***Compliance Challenges***: It is necessary to understand the federal and state laws that apply to a particular case. This comprises standardizing AI frameworks to the levels of compliance required by different states and equalizing the level of compliance across states.

vii. ***Current Regulation of the US Electric Grid Sector***

- In the US, the regulatory framework for electric grid security is characterized by several key frameworks and bodies:
- ***North American Electric Reliability Corporation (NERC):*** The NERC CIP standards are foundational for protecting electric grid against cyberthreats and mitigating risks [25, 27]. These standards define measures that must be implemented for safeguarding key infrastructure by defining assets to be safeguarded, access controls to be implemented, and response mechanisms to be followed in the event of an attack.
- ***Federal Energy Regulatory Commission (FERC):*** FERC is another organization responsible for establishing standards and their enforcement within the grid sector. FERC monitors the compliance processes enacted by NERC. Some of the tasks assigned to FERC are to approve standards and ensuring that utilities are in compliance with the regulations.
- ***Department of Energy (DOE):*** The DOE sets and funds efforts related to goals focused on the grid's overall security and its ability to withstand attacks. It also supports research and development in the areas of cyber security and smart grid.
- ***National Institute of Standards and Technology (NIST):*** The Cybersecurity Framework (CSF) and the Smart Grid Interoperability Standards (SGIS) developed by NIST provide strategies for addressing risks and achieving interoperability in smart grid systems.

These regulatory frameworks outline strategies for safeguarding smart grids in urban environments, emphasizing the need for robust security measures, adherence to standards, and continuous adaptation in response to evolving threats.

Consequences-driven Cyber-Informed Engineering

CCE and its Relevance to Adaptive AI Framework for DEN

Cyber Consequence-Driven Cyber-Informed Engineering (CCE) is a critical approach in modern engineering, particularly for enhancing cybersecurity in smart grids. It emphasizes understanding the potential consequences of cyber threats and system failures to better manage these risks. This method is especially relevant for adaptive AI frameworks within distributed energy systems in smart cities, due to the complexity of the technologies and the decentralized nature of these systems.

Analyzing outcomes oriented Cyber-Informed Engineering

i. ***Definition and Objective***
   - ***Definition***: CCE is an IT strategic direction that considers future impacts of cyberthreats and system malfunctions.
   - ***Objective***: The objective is to bring the engineering processes closer to the probable consequences of cyber incidents, improving the security regimes.

ii. ***Significance in Present-Day Engineering***
   - ***Evolution of Threats***: The current threats do not allow for the use of engineering techniques only focused on the risks and their identification.
   - ***Focus Shift***: CCE eliminates the emphasis on risks and instead aims at the impacts of cyberthreats in the short term and in the long run.

Importance of CCE to Adaptive AI systems in Smart Integrated Cities Energy Management

i. ***Integrated Energy Systems in Smart Cities***
   - ***Characteristics***: Smart grids, and distributed energy networks including AI, IoT, and renewable energy resources.
   - ***Requirements***: These systems require information in real-time for the system to function and to be controlled as required.

ii. ***Adaptive AI Frameworks: A Brief Discussion and Its Function***
   - ***Role of AI***: Developmental AI architectures self-learn and apply changes in the network risks and situations in real-time.
   - ***Improvement***: These frameworks improve the decision-making process and the system by accommodating new information and threats.

iii. ***Implementation of CCE with Adaptive AI.***
   - ***Integration***: CCE can be easily integrated into the AI systems as it gives a structure and a way of categorizing consequences.
   - ***Proactive Planning***: The integration enables adaptive AI frameworks to be more suitable for proactive planning and responding to cyberthreats.

CCE Phases in the Perspective of Smart Grid Security

i. ***Consequences Prioritization***
   - ***Definition***: Categorizing the impact of cyber threats based on their likelihood and potential severity.
   - Application to Smart Grids: This approach helps identify the most critical subsystems, whose failure would have the greatest impact on overall grid stability.
   - ***Example***: Protecting control centers and communication networks is essential to maintaining grid stability and ensuring uninterrupted operations.

ii. ***System Analysis***
   - ***Definition***: Analyzing the relationships and interconnections between system components.
   - ***Application to Smart Grids***: Understanding these interactions helps predict how a problem or cyberattack could propagate

through the system.

- ***Example***: Evaluating the connections between energy supply sources, supply infrastructure, and end-user devices to assess potential risks.

iii. ***Consequence-Based Targeting***

- ***Definition***: Concentrating on the threats and risks that may result in the worst-case scenario makes it possible to provide proper protection.
- ***Application to Smart Grids***: The protection of essential aspects such as SCADA systems and energy control systems so as to sustain energy delivery and steady supply of electrical power to the grids.
- ***Example***: Establish sound protective measures for critical sectors to avoid significant breaks.

iv. ***Mitigation and Protection Strategies***

- ***Definition***: Measures to counter the identified risks and protect and safeguard people both in and out of work.
- ***Application to Smart Grids***: Includes the approach to using intrusion detection systems, increasing encryption, and elaborating on the approach to incident response.
- ***Example***: Applying artificial intelligence for deviation detection in order to identify the appearing suspicious actions and using backup in communication lines to decrease the malicious impact.

Implementation of CCE in Adaptive AI frameworks

i. ***Integrated into Artificial Intelligence***

- ***Incorporation***: Integrating CCE principles into AI algorithms to interpret the consequences of cyberthreats and to act upon it.
- ***Example***: Train the AI systems to detect important alarms and use reasonable time to address threats affecting the stability of the grid.

ii. ***Enhancing Resilience***

- ***Role***: Applying CCE principles to AI frameworks in smart grids allows to mitigate cyber impacts before they turn into critical.
- ***Example***: Measures of different kinds of attacks in order to evaluate the effectiveness of protective measures.

iii. ***Continuous Improvement***

- ***Updates***: AI frameworks must constantly be adjusted to reflect new threat intelligence and previous attacks.
- ***Example***: Regular supplementation of threat data and post incident analysis to enhance the deployed systems' efficiency and reliability.

Challenges and Considerations

i. ***Smart Grids Complexity***

- ***Issue***: CCE principles are difficult to implement in smart grids due to their numerous integrated elements.
- ***Need***: Complex scenarios are used in order to model and simulate the likely outcomes of any action.

ii. ***Evolving Threat Framework***

- ***Issue***: A cyber threat is not static, so CCE and AI should be as flexible as well.
- ***Need***: Therefore, we must remain vigilant and even update the frameworks to counter emerging threats.

iii. ***Resource Allocation***

- ***Issue***: Resource management is essential when it comes to considering consequences and aiming at defense.
- ***Need***: Safeguarding the important regions without overloading the entire system.

iv. ***Risk Management and Compliance***

- ***Issue***: CCE and adaptive AI solutions must meet the regulatory norms and the cybersecurity necessities.
- ***Need***: There is also the need to adhere to and conform to current regulations and data protection requirements.

Consequently, CCE enhances the security and reliability of smart grids and other distributed energy networks by prioritizing the potential consequences of cyberattacks and system failures. By aligning engineering practices with current cyber threats, CCE strengthens the defense against system disruptions. When integrated with adaptive AI frameworks, CCE further boosts the security of smart urban energy networks, offering improved control and protection of critical infrastructures.

Proposed Adaptive AI Frameworks

Framework Overview

Changes in urban energy management have led to the embrace of distributed energy networks comprising renewable energy, energy storage systems, and smart grid technologies. Nevertheless, such developments bring new and sophisticated security issues, especially in protecting against cyberthreats and risks. To overcome these challenges, new adaptive AI frameworks have been developed as prerequisites for improving the stability and safety of smart grids.

Understanding Adaptive AI Frameworks

Adaptive AI frameworks describe a high-level procedural approach to addressing distributed energy networks' control and protection problems using artificial intelligence capable of changing its performance in reaction to current circumstances [31-32]. Unlike previous approaches, adaptive systems adjust the model and the strategies used in the system with new data, changes in the environment, and the presence of new threats. This dynamic capability is essential to enabling efficient safeguarding and control of contemporary smart grids, which are more complicated and vulnerable to cyber risks because of their decentralized structure.

Key Components of Adaptive AI frameworks

i. ***Real-Time Data Analytics***: Self-learning AI solutions use big data analysis to track and evaluate the efficiency and safety of dispersed power systems [33]. These frameworks can also analyze data from smart meters, sensors, and control systems and thereby recognize patterns and irregularities and even anticipate threats. This means that the organization can make pre-emptive adjustments before such vulnerabilities can compromise it.

ii. ***Machine Learning Algorithms***: Leveraging deep learning techniques as the core of adaptive AI frameworks, detecting new types of cyberthreats is possible. These algorithms analyze previous data to learn its standard fluctuations and then distinguish signs of a security threat. They also improve their accuracy and efficiency as they are trained with new data, making the network more secure from new threats.

iii. ***Automated Response Mechanisms***: This is one of the significant value propositions of adaptive AI frameworks, namely the capability to incorporate response mechanisms. In case of identification of a potential threat, the framework can initiate the predetermined response actions, including isolation of the network segments, activation of the countermeasures, or alerting the human operators. This automation also minimizes the time taken to respond to the threat while at the same time eliminating the possible errors human beings are capable of making in cases of high security threats.

iv. ***Adaptive Defense Strategies***: Adaptive AI frameworks employ adaptive defense strategies that continuously evolve based on the changing threat landscape. Instead of relying on static security measures, these frameworks dynamically adjust their defense protocols to counter new and emerging threats. This adaptability ensures the network remains protected even as attackers develop more sophisticated techniques.

v. ***Integration with Existing Systems***: Adaptive AI frameworks must seamlessly integrate with existing energy management and security systems to be effective. This integration allows for aggregating data from various sources and ensures that AI-driven insights are incorporated into the broader security strategy. The ability to interface with legacy systems while enhancing their capabilities is a key strength of adaptive AI frameworks.

Significance in Managing and Protecting Distributed Energy Networks

It is therefore important to establish how adaptive AI frameworks are crucial in governing and securing distributed energy systems. These frameworks address several critical aspects of smart grid security:

i. ***Enhanced Threat Detection and Prevention***: Because they use real-time data and machine learning, adaptive AI frameworks provide sophisticated threat detection and countermeasures. They can better understand the early symptoms of cyberthreats that conventional security tools may not be able to detect, which would enable them to apply better prevention and control measures [34-35].
ii. ***Improved Resilience***: Hence, adaptive AI frameworks provide an overall reinforcement of distributed energy networks. The capability to operate in real time and adapt and modify defense mechanisms means that the network is not compromised despite complex attacks.
iii. ***Efficient Resource Management***: Besides security, adaptive AI frameworks enhance the efficiency of resource utilization in smart grids. Using such frameworks, operation data can be analyzed to optimize energy distribution, increase grid stability, and minimize costs [36].
iv. ***Futureproofing***: The nature of threats in cyberspace changes continuously, meaning that an organization requires a robust approach to security in the future. Adaptive AI frameworks may work as a scalable solution because, with new challenges arising and new technologies coming up, the solutions can be modified and adapted to include the new aspects, which will provide the long-term protection of distributed energy networks.
v. ***Minimized Downtime and Disruptions***: Swift and technical approaches to security incidents reduce the time that services are out of order, which is important for the reliability of energy services in cities. This capability is significant in critical infrastructure since energy has to be supplied continually.

Therefore, adaptive AI frameworks represent a revolutionary paradigm of the interacting energy networks and their security. To this end, the following frameworks have incorporated real-time data analytics, machine learning, automation, and learning defense mechanisms to solve the problems existing in smart grids. Because of the features that allow them to increase threat awareness, increase resistance, and optimize the use of resources, they are an indispensable part of the continuous struggle to defend urban energy systems from cyberthreats and risks. Based on the further adoption of smart grid technologies in cities, it is crucial to have adaptive AI to provide security and effectiveness of such systems.

Mathematical Modelling

AI Algorithms for Anomaly Detection

Adaptive artificial intelligence frameworks are used to improve the security of smart grids in urban areas. These frameworks use algorithms and mathematical models to protect distributed energy networks against cyberthreats and risks. In this study, I provide an overview of the main components, algorithms, and mathematical models used in these frameworks.

Components of Adaptive AI Framework

Adaptive AI frameworks have the following components.

i. ***Data Collection and Preprocessing***
   - ***Sensors and IoT Devices***: Capture data on the go from devices such as smart meters, grid sensors, and network devices.
   - ***Data Preprocessing***: Sub-processes involve cleaning, normalizing, and transforming data to make it suitable for analysis.
ii. ***Feature Extraction***
   - ***Feature Engineering***: Conveys raw data and selects features that help to define anomalies and possible threats.
   - ***Dimensionality Reduction***: Some of them include Principal Component Analysis (PCA) or t-Distributed Stochastic Neighbor Embedding (t-SNE) which serve to decrease the number of features but retain important data.

iii. ***AI Algorithms***

- ***Supervised Learning***: Other methods, such as Support Vector Machines (SVM), Random Forests, and Neural Networks, are used to develop models that differentiate normal behaviors from anomalous ones based on labelled data.
- ***Unsupervised Learning***: Clustering algorithms, such as k-Means, DBSCAN, and autoencoders, are used to detect anomalies without even knowing that the data set was labeled.
- ***Semi-Supervised Learning***: Combining a little strongly labeled data with many weakly labeled data to better detect anomalies.

iv. ***Anomaly Detection Models***

- ***Statistical Models***: Utilize statistical analysis of data to identify deviations from normal behavior.
- ***Machine Learning Models***: Apply trained algorithms to detect or predict anomalies in the data.

v. ***Decision-Making and Response***

- ***Alerts and Notifications***: Issue real-time alarms whenever an anomaly or threat has been identified.
- ***Automated Responses***: Some of the security measures that should be employed include Quarantine, which is achieved by isolating the nodes or systems that have been affected.

vi. ***Feedback and Adaptation***

- ***Model Updating***: This means that models should also be updated continually according to the new data to more accurately meet the current threat.
- ***Performance Evaluation***: It is imperative to monitor the functioning of the AI framework to determine its effectiveness periodically.

AI Algorithms and Their Functionality

i. ***Support Vector Machines (SVM)***

- ***Functionality***: SVM is used on data where categorizing some data into certain classes is necessary. It determines the best hyperplane that effectively divides data between normal and anomalous classes with the greatest margin possible.
- ***Mathematical Model***:

$$minimize = \frac{1}{2}\|w\|^2 y_i(w.x_i + b) \geq 1, \forall i \qquad (1)$$

w: Weight vector.

x_i: Feature vector.

y_i: Class label (+1 or -1).

b: Bias term.

ii. ***Random Forests***

- ***Functionality***: A technique that uses several decision trees to arrive at the final decision on classification. Every tree is learned on a randomly selected subset of data and its features.
- ***Mathematical Model***: The forest output is the aggregated vote of all the decision trees in the forest.

iii. ***Autoencoders***

- ***Functionality***: Neural networks used for the purpose of unsupervised anomaly detection task. They transform the input information into a latent space and reconstruct it back, learning to detect distortions from normal patterns.
- ***Mathematical Model***: minimize $\|x - \hat{x}\|^2$ (2)

x: Original Input.

$\hat{x}$: Reconstructed Input.

Mathematical Model for Anomaly Detection

i. ***Statistical Anomaly Detection***
- ***Model***: Gaussian Mixture Model (GMM)
- ***Equations***:

$$p(x) = \sum_{i=1}^{k} \pi_i N\ (x \mid \mu_i, \Sigma_i) \qquad (3)$$

$p(x)$: probability Density Function.
π_i: Weight of the i-th component.
μ_i: Mean of the i-th component.
Σ_i: Covariance matrix of the i-th component.
$\sum_{i=1}^{k} \pi_i N\ (x \mid \mu_i, \Sigma_i)$: Gaussian Distribution.

ii. ***Isolation Forest***
- ***Model***: Constructs isolation trees to isolate the anomalies in an ensemble form.
- ***Equations***:

Path Length= number of edges in the path from root to the node where the sample is isolated

$$Anomaly\ Score = 2^{-\frac{E(x)}{c(n)}} \qquad (4)$$

$E(x)$: Average path length.
$c(n)$: Normalizing constant based on the number of samples *n.*

Computational Methods

i. ***Training and Testing***
- ***Cross-Validation***: In order to determine the accuracy and transferability of models.
- ***Hyperparameter Tuning***: Tunes or adjusts any parameters of a trained model to improve its performance.

ii. ***Real-Time Processing***
- *Streaming Data Analysis*: Uses sliding windows and online learning methods to deal with streaming data.

iii. ***Scalability and Efficiency***
- ***Distributed Computing***: Cloud based and parallel processing based for processing large data set.

Thus, adaptive AI frameworks for improving city smart grid security based on big data use data preprocessing, sophisticated AI algorithms, anomaly detection models, and feedback [37]. Mathematical models like Gaussian Mixture Models and Isolation Forests, which are used for anomaly detection, are fundamental tools that help identify threats in distributed energy networks and respond to them accordingly.

Predictive Maintenance Models

PdM models are crucial in improving the reliability and effectiveness of smart grids in the urban environment by identifying possible equipment failures before they happen. This is especially important in smart grids where DERs and multiple interfacing have been incorporated, making the system more complicated and prone to attacks.

Predictive Maintenance Models

i. ***Predictive Maintenance Overview***

This maintenance approach involves using data analytical methods to anticipate possible equipment breakdowns. These models use historical and real-time data from sensors and other sources to guide the operators in scheduling maintenance activities just

before they become due, hence improving the efficiency and reliability of the smart grid.

ii. ***Mathematical Formulation and Methods***

The following mathematical models and techniques are used in predictive maintenance; Some can be classified under statistical models, machine learning and time series analysis. It is now time to describe these methods, emphasizing their use in urban smart grids.

Statistical Models

Regression Analysis: One of the simplest approaches employed to forecast equipment's remaining useful life from its historical data. For instance, if x represents the time or usage of the equipment and y represents the failure rate, the linear regression model can be expressed as:

$$y = \beta_0 + \beta_1 x + \in \qquad (5)$$

Where:

β_0, is the Intercept,
β_1, is the slope,
$\in$, is the error term.

Survival Analysis: Most of the time is used to represent the time until a failure. The Weibull distribution has two parameters: the shape parameter (β) and the scale parameter (η). The probability density function (PDF) is:

$$f(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} e^{-(t/\eta)^{\beta}} \qquad (6)$$

Where t is the time until failure.

Machine Learning Algorithms

- ***Decision Trees***: These models make predictions using simple decision rules derived from the data features. They can handle nominal and ordinal data and can aid in establishing which factors could lead to equipment failures [38].
- Random Forests are a strategy that involves using an integrated decision tree to increase the chances of making a correct and reliable decision. In contrast to a single decision tree, this strategy minimizes overfitting.
- ***Feedforward Neural Networks***: These networks are formed of layers of nodes (neurons) for which information passes from the input to the output layer. It is possible that the network can develop complex patterns in the data which are effective in predicting failures [39].
- ***Recurrent Neural Networks (RNN) and Long-Short-Term Memory Networks (LSTM):*** Suitably applicable to time-based data, these networks can incorporate temporal relationships and predict future failures based on the past record of the data.

Time-Series Analysis

- ***Autoregressive Integrated Moving Average:*** The most related type of models to time series data is the ARIMA models used in analyzing and forecasting the data. The model is represented as:

$$Y_t = \propto + \emptyset_1 Y_{t-1} + \emptyset_p Y_{t-p} + \theta_1 \in_{t-1} + \theta_q \in_{t-q} + \in_t \qquad (7)$$

Where:

Y_t is the time series value at time t,
$\emptyset_i$ are the autoregressive parameters,

θ_i are the moving average parameters,
ϵ_t is the white noise error term.

Exponential Smoothing State Space Model (ETS): ETS models are used for the data with trend and seasonal patterns. The model smooths past observations to predict future values:

$$Y_t = \propto + \beta_t + \epsilon_t + \gamma S_{t-m} + \epsilon_t \qquad (8)$$

Where:

$\propto$ is the level component.
β, is the new trend component.
γ, is the seasonal component.
S_{t-m}, is the seasonal factor at time t.
ϵ_t, is the error term.

Application in Smart Grid Security

In the context of urban smart grids, predictive maintenance models not only help in anticipating equipment failures but also in identifying potential security threats. For instance, abnormal patterns in equipment performance could indicate a cyber-attack or system breach.

i. ***Adaptive AI Frameworks***
   - ***Anomaly Detection Algorithms***: These can be integrated with predictive maintenance models to identify unusual patterns or deviations in the system that might indicate a cyber threat. Techniques such as Isolation Forests or One-Class SVM (Support Vector Machine) are commonly used.
   - ***Threat Intelligence Integration***: Combining PdM data with threat intelligence can enhance the ability to predict and mitigate security risks. For example, if an equipment anomaly coincides with known attack patterns, it can trigger preemptive security measures.

ii. ***Resilience Enhancement***
   - ***Automated Response Systems***: Predictive maintenance can be coupled with automated response systems to quickly address potential issues, whether equipment-related or security threats. This ensures a robust and adaptive grid that can handle both operational and cyber challenges.

In summary, predictive maintenance models use a combination of statistical, machine learning, and time-series techniques to forecast equipment failures. These models enhance operational reliability and security by integrating anomaly detection and adaptive AI frameworks when applied to urban smart grids. This integrated approach ensures a proactive stance in managing and protecting distributed energy networks.

Real-Time Data Processing and Decision Making

Real-time data processing and decision making are significant in improving smart grid security in urban areas to counteract cyber-threats and vulnerabilities in managing distributed energy networks. Smart grids use interconnected sensors, actuators and communication technologies to monitor and manage electric power distribution in the smart grid networks. These data need to be transformed and analyzed in real-time to maintain effective and stable functioning of the grid. Here's how real-time data processing and decision-making play a role, along with the mathematical techniques used:

i. ***Real-Time Data Processing***
   - ***Data Acquisition***: Smart meters and sensors dispersed throughout the grid gather information on consumption, grid stabil-

ity, and climatic conditions. This data is then sent to another system or directly to edge devices for processing.

- ***Data Integration***: The current state of the grid is analyzed by accumulating data from various sources, such as power generation, consumption, and weather conditions.
- ***Data Filtering and Cleaning***: Each data type collected can be regarded as raw data; however, raw data is frequently filled with noise and gaps. Data pre-processing, which includes filtering and cleaning, is done to get rid of undesirable characteristics.
- ***Real-Time Analytics***: Advanced mathematics and computing are then applied to the collected data to identify potential threats, determine demand levels in real time, and so on. This entails monitoring the systems for patterns that may result from a cyber attack or failed equipment.
- ***Decision Support***: Real-time insights help decision-making processes including load distribution, fault identification and maintenance prevention.

ii. ***Decision-Making***

- ***Anomaly Detection***: Machine learning finds outliers in behavior and/or anything that causes a system to act differently from what is expected. Methods include statistics, machine learning, and pattern recognition.
- ***Predictive Analytics***: Predictive models describe future conditions using past and present information. This facilitates demand forecasting or failure prediction in the system in the case of congestion.
- ***Automated Response***: The findings suggest that automated systems can control the grid, compartmentalize, or raise the alarm for the human operator.
- ***Adaptive Control***: The system constantly learns from new data inputs and the autonomously changing environment to perform its tasks and protect data efficiently.

Mathematical Techniques for Real-Time Data Analysis

i. ***Statistical Methods***

- ***Time-Series Analysis***: This is to predict loads and trends over time which is highly important in detecting anomalies in the system.
- ***Regression Analysis***: Facilitate the development of graphical representations of relations between a set of variables, such as power consumption and environmental factors.

ii. ***Machine Learning***

- ***Supervised Learning***: Classification algorithms include decision trees, Support Vector Machines (SVM), and neural networks, which are useful for processes like identifying patterns that characterize threats.
- ***Unsupervised Learning***: Pattern recognition algorithms (for instance, k-means clustering and hierarchical clustering) aim to group similar data points, which can be a feature for identifying anomalies.
- ***Reinforcement Learning***: In adaptive control approaches, the system acquires the best course of action from the environment's response.

iii. ***Optimization Techniques***

- ***Linear and Non-Linear Programming***: Stabilize grid operations such as, for example reducing energy loss or matching supply and demand.
- ***Dynamic Programming***: Used in decision-making contexts where decisions have to be made to improve them over time, such as when assigning maintenance periods.

iv. ***Graph Theory***

- ***Network Analysis***: Generally used to represent the grid in the form of a graph where the nodes can be any component such as generator, transformer or the edges can represent the connections. This is of assistance in evaluating the consequences of failure and weaknesses.

v. ***Bayesian Methods***
   - ***Probabilistic Inference***: This approach offers a mechanism for adjusting the prior about the state of the grid in light of the evidence, which is particularly helpful when making stochastic choices.

Mathematical Model

A mathematical model for real-time data processing in the context of smart grid security might involve the following components:

i. ***State Variables***: Model current condition of the grid (e. g., voltage levels, power flows).
ii. ***Observation Model***: Explain how state variables are associated with sensor data. For instance, if $x(t)$ represents the grid state at time t, and $z(t)$ is the observed data, the observation model might be $z(t) = Hx(t) + \epsilon(t)z(t)$, where H is a matrix relating state to observations, and $\epsilon(t)$ represents noise.
iii. ***State Transition Model***: This model explains how the grid state looks at different points in time. It might be modeled as $x(t + 1) = Fx(t) + w(t)$, where F is the state transition matrix and $w(t)$ is process noise.
iv. ***Decision Rule***: Based on the observed data and state model, a decision rule $u(t)$ might be applied to control actions, such as adjusting power flows or isolating affected grid segments. This could be derived from using optimization techniques to minimize a cost function, such as $min_u J(x(t), u(t))$, where J is the cost function represents operational and security objectives.

Thus, adapting these mathematical techniques into AI systems can improve the security of smart grids deployed in urban areas to ensure the proper generation and distribution of energy.

Model Architecture for Adaptive AI Frameworks

The proposed model architecture for the adaptive AI frameworks and their integration with the existing system.The integration of adaptive AI frameworks into electric grids follows a comprehensive process that involves advancements in both technology and cybersecurity, in line with the NCSC Cyber Assessment Framework (CAF). The first step in this integration process is the assessment and planning phase. This phase begins with an evaluation of the existing infrastructure, which involves creating an inventory of the electric grid components, including generation sources, transmission lines, substations, and distribution points. As shown in Figure 3, the following model illustrates the architecture for integrating adaptive AI frameworks with the electric grid:

Evaluate Existing Infrastructure

- ***Identify Components***: The first step involves identifying the current state of the electric grid and Distributed Energy Networks (DENs). This includes cataloging generation sources such as solar panels, wind turbines, conventional power plants, transmission lines, substations, and distribution points. Understanding these components helps in planning and identifying gaps in the current structure.
- ***Assess Capabilities***: The next step is to assess the existing control systems, data acquisition methods, and communication interfaces. This involves evaluating the grid management software, sensor networks, and data acquisition systems currently in use. Key aspects to consider include the frequency of data collection, real-time monitoring capabilities, and how communication occurs, all of which should be analyzed to determine how they can integrate with AI technologies.

Data Integration

i. ***Data Collection***
   - ***Gather Historical Data***: Collect data on the grid's past performance, energy usage profiles, and climatic conditions. This historical data is essential for training AI models and provides valuable insights into past trends. Analyzing this data helps identify patterns and anomalies that may influence current and future operations.
   - ***Real-Time Data***: Ensure that real-time data from sensors, smart meters, and other sources is consistently received and available. A critical requirement for AI systems is real-time data input, allowing them to make immediate decisions and pre-

dictions. This data should include operational metrics, energy usage parameters, and environmental conditions.

ii. ***Data Infrastructure***

- ***Gather Historical Data***: Collect data on the grid's past performance, energy usage profiles, and climatic conditions. This historical data is essential for training AI models and provides valuable insights into past trends. Analyzing this data helps identify patterns and anomalies that may influence current and future operations.
- ***Real-Time Data***: Ensure that real-time data from sensors, smart meters, and other sources is consistently received and available. A critical requirement for AI systems is real-time data input, allowing them to make immediate decisions and predictions. This data should include operational metrics, energy usage parameters, and environmental conditions.

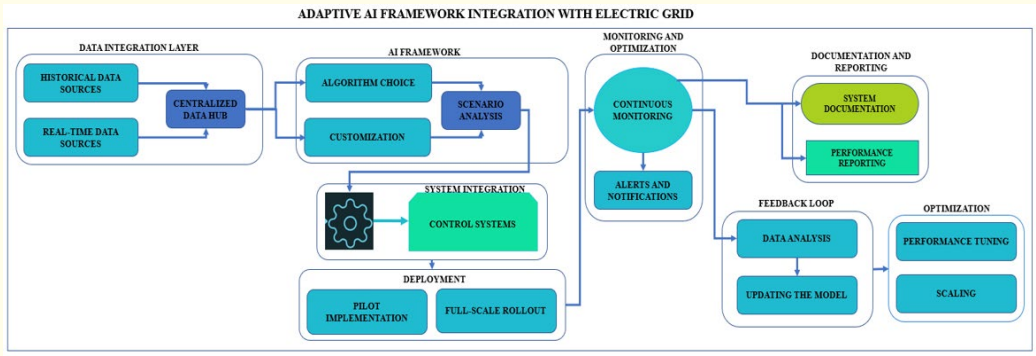

Figure 3: Architecture Model for Adaptive AI framework in Smart Grid.

AI Framework Development

i. ***Model Selection***

- ***Algorithm Choice***: When choosing AI algorithms, one must consider the goals and constraints that are expected from the program. For example, load forecasting can be solved by machine learning algorithms, whereas predictive maintenance can be carried out by employing neural networks. Thus, the choice of algorithms should correspond to the complexity of the tasks and the type of data at hand.
- ***Customization***: Modify the above selected models in such a way that they can be applied appropriately in the electric grid and DENs. Flexibility is the process of tuning the algorithm to incorporate any specific qualities of the grid, for example geographical location, energy mix and load demands. This is important in making sure that the AI models are made to fit the operation environment.

ii. ***Training and Validation***

- ***Training***: Perform AI modeling using data samples collected from historical and real-time data retrieval. The process of training therefore involves presenting the models with data so as make them develop patterns and relationships. It can therefore be seen that the quality of training data can greatly affect the performance of the AI models.
- ***Validation***: Finally, test the trained models on another set of test data in order to confirm the effectiveness and robustness of the developed model. Validation assists in comparing the effectiveness of the models in the actual environment and in establishing the weaknesses. This is an important step to make certain that the models are efficient and reliable.

Simulation

- ***Scenario Analysis***: Perform scenario-based studies to evaluate how AI models operate in different situations, including maximum loads, equipment breakdowns, or shifts in energy availability. They are used in the testing and validation of the models through examination of their behavior in other scenarios and to discover flaws that would arise in the model before it goes to the field.

System Integration

i. ***Interface Development***
   - ***API Integration***: Create interfaces that integrate the AI frameworks with the existing grid management systems such as APIs (Application Programming Interfaces). APIs allows the data communication and interactivity between the components of software so that the AI models can easily accommodate with the target systems.
   - ***User Interface***: Design interfaces with which operators will be able to communicate with AI systems and obtain information. It should be possible to use the interface and have an understanding of what the information is telling, in an easy and clear manner. Operators should be able to retrieve given AI recommendations and to supervise the system's performance.

ii. ***Control System Adaptation***
   - ***Integration Points***: Determine in which cases AI models would interact with control systems, for instance, with the dispatching system or load balancing system. Integration points are necessary so that the information derived from the use of AI can be put into practice within operation matters.
   - ***Automation***: Promote use of automated decision making where appropriate. For instance, it can be used to proactively shift loads according to the real-time information minimizing the time spent on manual operations. Automation can enhance speed of operation and even response time.

Deployment

i. ***Pilot Implementation***
   - ***Test Deployment***: Use AI frameworks in a scaled- down manner to ensure that the framework functions as required and meets the intended performance benchmarks. The pilot implementation helps in determining any possible problems or constraints encountered with the implementation venture before a widespread implementation. This phase should be more of testing and validation of the various solutions and models that have been developed.
   - ***Performance Monitoring***: Implement the performance of the AI frameworks in the pilot phase and obtain feedback from the operators. Performance monitoring assists in determining the efficiency of the AI models and making the required changes. Users' feedback is useful when it comes to fine-tuning the system.

ii. ***Full-Scale Rollout***
   - ***Gradual Expansion***: Transition AI frameworks to other sections of the grid depending on the outcomes of the pilot study. This approach helps in scaling the solution gradually and fixes all the problems that may be seen during the pilot phase.
   - ***Training and Support***: It is important to involve operators and offer training and support as the change to the new system occurs. Training is very essential so that the users can be in a position to work with the AI tools in the right way. There should also be follow-up to attend to any complications which may arise during the process of implementation.

Monitoring and Optimization

i. ***Performance Monitoring***
   - ***Continuous Monitoring***: Establish methods for continuous evaluation of AI performance as well as grid performance. Supervisory monitoring enables one to identify or detect when something is wrong, check on the performance indicator, and also check whether the AI models are performing as required.

- ***Alerts and Notifications***: If you need to monitor key web pages for specific events like anomalies or performance problems then create alerts for it. Informant can be used to alert a person to possible problems so that corrections can be made as soon as possible. Notifications should be set in a manner that they give the operators the right information at the right time.

ii. ***Feedback Loop***

- ***Data Analysis***: It is important to constantly review performance data in order to discover potential opportunities for growth. Evaluation assists in knowing the performance of the created AI models and possible changes to be made. This feedback loop is very important so that there can be some improvement made in the future.
- ***Model Updates***: Refine current AI models and algorithms as per new data and or feedback. The effectiveness of the models used can be compromised as the grid environment changes over time and will require some changes in its application. The models can get outdated, and that makes it crucial that they are updated periodically.

iii. ***Optimization***

- ***Performance Tuning***: Fine-tune AI models and control strategies for better performance. The tuning of the performance is the optimization of the algorithms, the data and the decisions to be made to obtain superior outcomes.
- ***Scaling***: Scalability - It must be possible to scale the solutions as a function of data volumes or complexity of the scenarios. When these grid and DENs increase the AI systems should be capable of accommodating the increased complexity and data in the system.

Reporting

i. ***Reporting***

- ***Performance Reports***: Generate performance reports detailing the effectiveness of the AI system and the overall efficiency of the grid. These reports should include recommendations on the degree to which the AI models have met their objectives, as well as improvements achieved. Performance reports play a key role in evaluating the impact of AI integration.
- ***Stakeholder Communication***: Effectively communicate progress, outcomes, and system enhancements to stakeholders and regulatory authorities. Clear communication demonstrates the value of AI integration, especially when addressing any concerns raised by stakeholders.

Given the complexity of the issue, this paper outlines a detailed, step-by-step method for integrating adaptive AI frameworks into electric grids and Distributed Energy Networks (DENs). Each step, from the initial assessment phase to subsequent optimization, is designed to ensure an efficient integration process. In combination with the NCSC Cyber Assessment Framework (CAF), this approach allows for the successful incorporation of adaptive AI frameworks into electric grids, fostering technological innovation while maintaining robust cybersecurity and productivity measures.

Discussion

The rapid development of smart cities necessitates the use of advanced technologies to manage and secure distributed power systems. This evolution has increased the interconnection of cities with various energy resources, leading to the creation of complex networks that present challenges in terms of security and efficiency. This discussion examines proposed adaptive AI frameworks designed to protect and enhance distributed energy networks, focusing on their architectural models and compatibility with the NCSC Cyber Assessment Framework (CAF).

The integration of smart grids and Distributed Energy Resources (DERs) represents a significant shift in energy management systems in urban environments. Smart grids enhance the reliability, efficiency, and sustainability of power systems by incorporating technologies like the Internet of Things (IoT), big data, and advanced analytics. However, this technological advancement also introduces new risks, such as cyberattacks, which pose serious threats to grid stability.

Adaptive AI frameworks offer a promising solution to these challenges by leveraging machine learning and artificial intelligence to respond dynamically to emerging risks and system changes. By continuously learning from operational data and cyberthreat patterns,

AI solutions can detect risks in real time, respond quickly, and minimize threats to the reliability and performance of distributed energy networks.

Elements which constitute the Adaptive AI Frameworks

Adaptive AI frameworks for energy networks typically comprise several key components:

- ***Data Collection and Preprocessing***: AI systems rely on input from various sources, such as sensors, meters, and control systems. The collected data is then cleaned and processed to ensure its relevance and quality. Data preprocessing includes tasks like noise elimination, data normalization, and information integration, all of which improve the system's understanding of the network environment.
- ***Machine Learning Models***: At the core of adaptive AI frameworks are machine learning models, which analyze the gathered data. These models are trained on normal operational parameters and learn to identify unusual events that could indicate problems. For instance, anomaly detection algorithms are employed to spot deviations that may signal cyberattacks or system failures
- ***Real-Time Monitoring and Analysis***: Dynamic AI systems continuously evaluate network conditions and analyze data in real time. This real-time analysis allows for the rapid identification of irregularities and threats. Advanced AI models are also used for predictive analytics, enabling the system to anticipate future issues.
- ***Automated Response Mechanisms***: When an anomaly or threat is detected, adaptive AI frameworks can trigger autonomous response mechanisms. These responses may include isolating affected components, reconfiguring power flow routes, or taking measures to protect the system from further damage.
- ***Feedback Loops and Learning***: A critical aspect of adaptive AI is its ability to learn from past interactions. Feedback loops enable the system to refine its models based on new data and the outcomes of previous interventions. This continuous learning process enhances the system's ability to counter emerging threats and adapt to operational changes.

Architecture Model of Adaptive AI Framework for Integration in Electric Grid

Adaptive AI frameworks are integrated into electric grids through a carefully designed architecture that ensures a seamless interface between AI and the grid systems. This architecture typically includes the following key components:

- ***Data Acquisition Layer***: Once the data has been collected, it is transferred to the data processing and analytics layer, where AI models analyze the information to generate actionable insights. This layer includes several critical modules, such as data preprocessing, feature engineering, and model prediction. Data preprocessing involves cleaning, normalizing, and integrating the collected data to remove noise and make it suitable for analysis. Feature engineering identifies key variables that influence grid performance and security, and model prediction applies advanced machine learning techniques to forecast future conditions, detect anomalies, and predict potential threats. This layer serves as the brain of the AI framework, providing a deep understanding of grid behavior through advanced analytical tools.
- ***Data Processing and Analytics Layer***: In this layer, AI models analyze data that has been collected to provide useful insights. This layer contains several modules such as data preprocessing, feature engineering as well as model prediction. Advanced Analytical Tools are used in the form of Machine Learning to make predictions.
- ***Decision-Making Layer***: The decision-making layer interacts with the outputs from the analytics layer to formulate appropriate responses. It consists of decision support systems and automated response systems that determine the best course of action based on AI-driven recommendations. For example, if an anomaly is detected in the data, this layer will assess its severity and make decisions, such as adjusting power flow, isolating a part of the grid, or escalating the issue for human intervention. This layer is crucial for translating AI insights into tangible actions that ensure the grid's stability and security
- ***Control and Actuation Layer***: The control and actuation layer is responsible for implementing the decisions made by the AI system. It communicates directly with grid control systems to execute commands, such as adjusting power flows, triggering security mechanisms, or reconfiguring network elements. This layer acts as the operational arm of the AI framework, taking the neces-

sary actions to mitigate risks or optimize performance. In the event of a cyberattack or system failure, the control layer might disconnect compromised components, reroute power to maintain supply, or activate emergency protocols to safeguard the grid.

- ***User Interface and Reporting Layer***: he user interface and reporting layer facilitates interaction between human operators and the AI system. This layer includes dashboards, visualization tools, and reporting features that present real-time data and insights about the grid's status and security. It enables operators to monitor system performance, review AI-driven decisions, and gain an overview of security measures in place. Additionally, the reporting features generate performance summaries and incident reports, helping stakeholders understand the impact of the AI system and its role in enhancing grid security and efficiency. This layer is crucial for ensuring transparency, allowing operators to stay informed and intervene when necessary.

Conformity to the needs of the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF)

The NCSC's Cyber Assessment Framework (CAF) provides a structured approach for evaluating an organization's cybersecurity posture and guiding continuous improvement. When integrating adaptive AI frameworks into distributed energy networks, adhering to the CAF is essential to ensuring robust and secure systems. The key components of the CAF in relation to adaptive AI implementation are as follows:

- ***Security Governance***: The CAF emphasizes that security governance is a fundamental aspect of cybersecurity. In the context of adaptive AI, this means establishing clear roles and responsibilities for managing AI systems, ensuring compliance with cybersecurity standards, and maintaining control over AI decision-making processes. Effective governance ensures that AI-driven decisions align with broader organizational security policies and that oversight mechanisms are in place to monitor AI actions.
- ***Risk Management***: The CAF outlines a systematic approach to risk management, involving risk identification, analysis, and mitigation. Adaptive AI frameworks play a critical role in this process by providing real-time threat detection and response capabilities. However, to remain effective, AI models must be continuously evaluated and updated to address emerging threats. This ensures that risk management strategies evolve in line with the dynamic nature of cyber risks, keeping the distributed energy networks secure against new vulnerabilities.
- ***Security Controls***: The CAF underscores the importance of implementing strong security controls to safeguard data and systems. For adaptive AI frameworks, this includes the deployment of encryption, access controls, and authentication mechanisms to protect sensitive information and prevent unauthorized access. These controls ensure that data integrity is maintained and that the AI systems operate within a secure environment, minimizing the risk of corruption or breaches.
- ***Incident Response***: A key component of the CAF is the development of comprehensive incident response plans. Adaptive AI frameworks can significantly enhance incident response by providing immediate alerts and automated responses to detected threats. However, it is crucial to coordinate these automated responses with human decision-makers to ensure that incidents are managed effectively. By combining AI-driven actions with human oversight, organizations can mitigate the impact of security incidents more efficiently.
- ***Continuous Improvement***: The CAF advocates for a closed-loop improvement process in addressing cybersecurity challenges. Adaptive AI frameworks naturally align with this approach, as they are designed to learn from new data and evolving threat landscapes. To maintain their effectiveness, AI models and security protocols must be regularly updated to address changing risks. Continuous improvement ensures that the security measures remain adaptive and potent over time, enabling organizations to stay ahead of emerging threats.

Challenges and Considerations

While adaptive AI frameworks offer substantial advantages, their implementation and integration with electric grids also present several challenges:

- ***Data Privacy and Security***: The use of adaptive AI frameworks involves processing vast amounts of data, which raises concerns about data privacy and security. It is essential to ensure that privacy-sensitive information is adequately protected and that AI

systems comply with relevant data protection regulations, such as the General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA). Safeguarding this data is critical, as any breach could lead to severe legal and reputational consequences.

- ***Model Accuracy and Reliability***: The effectiveness of adaptive AI systems heavily depends on the accuracy and reliability of their models. Ensuring that these models produce reliable outputs is crucial for their success in managing and securing electric grids. Regular validation, testing, and updates are necessary to minimize the risk of false positives or false negatives, which could result in incorrect decisions. Maintaining high model performance requires continuous monitoring and fine-tuning, especially as new data and evolving threats are introduced.
- ***Integration Complexity***: Integrating AI frameworks into existing grid infrastructure can be complex and challenging. Issues such as compatibility between different systems, legacy technologies, and communication protocols can pose significant barriers during implementation. Additionally, the expertise required to manage and operate AI-based systems within a grid environment may be limited, leading to potential delays and inefficiencies in integration efforts. Overcoming these challenges requires careful planning, collaboration between AI experts and grid operators, and potentially upgrading existing systems to support AI integration.
- ***Ethical and Governance Issues***: The deployment of AI in critical infrastructure, such as electric grids, raises important ethical and governance concerns. One challenge is ensuring transparency and explainability, meaning it must be clear how AI systems make decisions. Accountability is another key issue—determining responsibility for decisions made by AI systems can be difficult, especially in the case of errors or failures. Additionally, AI models may exhibit bias, leading to unfair or discriminatory outcomes. Addressing these ethical concerns requires developing governance frameworks that ensure fairness, accountability, and transparency in AI operations.

While the implementation of adaptive AI frameworks offers significant potential benefits for organizations and enterprises, several key factors must be considered to ensure success. These include addressing challenges related to data privacy, ensuring model accuracy, and managing the complexity of system integration. By effectively overcoming these challenges and continually improving AI models, smart grids can achieve enhanced security and performance. This lays the foundation for a more reliable, resilient, and environmentally friendly urban electric system.

Conclusion and Future Work

Several areas warrant further research to improve and refine the proposed adaptive AI frameworks for distributed energy networks. First, there is a pressing need to enhance the current algorithms and models used in energy distribution to better reflect the complexities and variability inherent in distributed energy systems. This includes the development of new machine learning methods and improving the accuracy and efficiency of predictive models. As energy networks become more dynamic and diverse, advanced algorithms that can adapt to fluctuations in supply and demand will be critical.

Second, additional research should focus on integrating AI frameworks with emerging technologies such as blockchain for enhanced data security and smart contracts for more effective grid management. The convergence of AI and blockchain could offer new opportunities to safeguard data integrity and automate transactions within the grid, ensuring more secure and transparent operations. This combination could potentially lead to groundbreaking improvements in grid stability and overall functionality.

Third, there is a need for expanded research into the ethical and societal implications of using AI in energy networks. Understanding how AI impacts workers' roles, personal data privacy, and public perception is essential for addressing potential concerns and fostering greater acceptance of AI technologies in energy management. Exploring these societal aspects will help mitigate resistance and build trust, ensuring that AI implementation aligns with broader social values.

Lastly, it is crucial to continue fostering collaboration between academia, industry professionals, and regulatory bodies to ensure that AI guidelines evolve in line with current trends and norms. This means involving key stakeholders in the integration process to ad-

dress challenges, share knowledge, and generate new ideas for improving AI deployment. Continuous dialogue between these groups will support the development of adaptive AI frameworks that are both effective and compliant with evolving legislative standards.

In conclusion, further development of adaptive AI frameworks for distributed energy networks presents significant opportunities to improve grid management in smart urban environments. By adhering to best practices, pursuing constant innovation, and addressing key challenges such as data security, ethical concerns, and stakeholder collaboration, AI in energy management can lead to more resilient, reliable, and secure energy systems. The continued advancement of these technologies will be critical to the future of sustainable energy management.

Availability of data and material: All the necessary datasets and results generated and analyzed during the current study are available are available within the manuscript. Code snippets are available from the corresponding author on reasonable request.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of Interest: The author declares no conflict of interest.

Acknowledgments: Not applicable.

References

1. Zheng Z., et al. A systematic review towards integrative energy management of smart grids and urban energy systems. Renewable and Sustainable Energy Reviews 189 (2024): 114023.
2. Kinga Stecuła, Wolniak R and Wieslaw Grebski. AI-Driven Urban Energy Solutions—From Individuals to Society: A Review. Energies 16.24 (2023): 7988-7988.
3. Mishra P and Singh G. Energy Management Systems in Sustainable Smart Cities Based on the Internet of Energy: A Technical Review. Energies 16.19 (2023): 6903.
4. Morteza SaberiKamarposhti., et al. A comprehensive review of AI-enhanced smart grid integration for hydrogen energy: Advances, challenges, and future prospects. International Journal of Hydrogen Energy (2024).
5. Selvaraj R, Kuthadi VM and Baskar S. Smart building energy management and monitoring system based on artificial intelligence in smart city. Sustainable Energy Technologies and Assessments 56 (2023): 103090.
6. Xu B., et al. ProcSAGE: an efficient host threat detection method based on graph representation learning. Cybersecurity 7.1 (2024).
7. Sulaiman A., et al. Artificial Intelligence-Based Secured Power Grid Protocol for Smart City. Sensors 23.19 (2023): 8016.
8. Krause T., et al. Cybersecurity in Power Grids: Challenges and Opportunities. Sensors 21.18 (2021): 6225.
9. Vetrivel Subramaniam Rajkumar., et al. Cyberattacks on Power Grids: Causes and Propagation of Cascading Failures. IEEE Access 11 (2023): 103154-103176.
10. Suciu G., et al. SealedGRID: Secure and Interoperable Platform for Smart GRID Applications. Sensors 21.16 (2021): 5448-5448.
11. Imai S., et al. Unexpected Consequences: Global Blackout Experiences and Preventive Solutions. IEEE Power and Energy Magazine 21.3 (2023): 16-29.
12. Cardenas AA. Keynote: A Tale of Two Industroyers: It was the Season of Darkness (2024).
13. INSURICA. Cyber Case Study: Colonial Pipeline Ransomware Attack. INSURICA (2024). https://insurica.com/blog/colonial-pipeline-ransomware-attack/
14. Mandiant. INDUSTROYER.V2: Old Malware Learns New Tricks | Mandiant. Google Cloud Blog; Google Cloud (2022). https://cloud.google.com/blog/topics/threat-intelligence/industroyer-v2-old-malware-new-tricks/
15. Consequence-driven Cyber-informed Engineering (CCE). (2016). Idaho National Laboratory. https://inl.gov/national-security/cce/
16. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector Mission Support Center Analysis Report (2016).
17. Sulaiman A., et al. Artificial Intelligence-Based Secured Power Grid Protocol for Smart City. Sensors 23.19 (2023): 8016.

18. Márquez-Sánchez S., et al. Enhancing Building Energy Management: Adaptive Edge Computing for Optimized Efficiency and Inhabitant Comfort. Electronics 12.19 (2023): 4179-4179.
19. Khan IA., et al. A privacy-conserving framework-based intrusion detection method for detecting and recognizing malicious behaviors in cyber-physical power networks. Applied Intelligence (2021).
20. Oladimeji S and Kerner SM. SolarWinds hack explained: Everything you need to know. WhatIs.com; Techtarget (2023). https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
21. North Carolina power outage: Moore County attacks underscore power grid vulnerabilities - CBS News (2022). Www.cbsnews.com. https://www.cbsnews.com/news/north-carolina-power-grid-attack-vulnerable/
22. Jiao Y, Kang H and Sun H. An intelligent landscaping framework for net-zero energy smart cities: A green infrastructure approach. Sustainable Energy Technologies and Assessments 64 (2024): 103665-103665.
23. Fadhel MA., et al. Comprehensive Systematic Review of Information Fusion Methods in Smart Cities and Urban Environments. Information Fusion (2024): 102317-102317.
24. Vassilis Demiroglou., et al. Adaptive Multi-Protocol Communication in Smart City Networks. IEEE Internet of Things Journal 11.11 (2024): 20499-20513.
25. Minkoff Y. Substation attacks prompt national review of U.S. electric grid. Seeking Alpha; Seeking Alpha (2022). https://seekingalpha.com/news/3917905-substation-attacks-prompt-national-review-of-us-electric-grid
26. Wu J, Wang H and Yao J. Computer-aided urban energy systems cyber attach detection and mitigation: Intelligence hybrid machine learning technique for security enhancement of smart cities. Sustainable Cities and Society (2024): 105384-105384.
27. Zhao X and Zhang Y. Integrated management of urban resources toward Net-Zero smart cities considering renewable energies uncertainty and modeling in Digital Twin. Sustainable Energy Technologies and Assessments 64 (2024): 103656-103656.
28. Ordouei M., et al. Optimization of energy consumption in smart city using reinforcement learning algorithm. Int. J. Nonlinear Anal. Appl. In Press (2022): 2008-6822.
29. Lal Verda Cakir., et al. AI in Energy Digital Twining: A Reinforcement Learning-Based Adaptive Digital Twin Model for Green Cities 47 (2024): 4767-4772.
30. Amir Meydani., et al. Comprehensive Review of Artificial Intelligence Applications in Smart Grid Operations (2024): 1-13.
31. Ahmad Anwar Zainuddin., et al. Artificial Intelligence: A New Paradigm for Distributed Sensor Networks on the Internet of Things: A Review. International Journal on Perceptive and Cognitive Computing 10.1 (2024): 16-28.
32. Abiodun E Onile., et al. "Smartgrid-based hybrid digital twins framework for demand side recommendation service provision in distributed power systems". Future Generation Computer Systems 156 (2024): 142-156.
33. CISA Releases 2023 Year in Review Showcasing Efforts to Protect Critical Infrastructure | CISA (2024). Www.cisa.gov. https://www.cisa.gov/news-events/news/cisa-releases-2023-year-review-showcasing-efforts-protect-critical-infrastructure
34. Jia-Hao Syu, Jerry Chun-Wei Lin and Srivastava G. Distributed Learning Mechanisms for Anomaly Detection in Privacy-Aware Energy Grid Management Systems. ACM Transactions on Sensor Networks (2024).
35. Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid (2022).
36. Camacho J de J., et al. Leveraging Artificial Intelligence to Bolster the Energy Sector in Smart Cities: A Literature Review. Energies17.2 (2024): 353.
37. Boutin, C. NIST Releases Version 2.0 of Landmark Cybersecurity Framework. NIST (2024). https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
38. Alaa Awad Abdellatif, Shaban, K., and Massoud, A. SDCL: A Framework for Secure, Distributed, and Collaborative Learning in Smart Grids. IEEE Internet of Things Magazine 7.3 (2024): 84-90.
39. Onile AE., et al. Smartgrid-based hybrid digital twins' framework for demand side recommendation service provision in distributed power systems. Future Generation Computer Systems 156 (2024): 142-156.